ISSN 2221-7975

ТРУДЫ

СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА СВЯЗИ И ИНФОРМАТИКИ

ЧАСТЬ I

РОСТОВ-НА-ДОНУ
2015

СЕВЕРО-КАВКАЗСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО
БЮДЖЕТНОГО УЧРЕЖДЕНИЯ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА
СВЯЗИ И ИНФОРМАТИКИ

Посвящается
120-летию со дня изобретения
радио Поповым А.С.

ТРУДЫ

СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА

МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

СВЯЗИ И ИНФОРМАТИКИ

ЧАСТЬ I

Подготовлены по результатам международной
молодежной научно-практической конференции СКФ МТУСИ
«ИНФОКОМ-2015»
20 – 25 апреля 2015 года

Ростов-на-Дону
2015

УДК 621.396.1

ББК 32
Т 81

Т 81 Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть I. - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2015, 552с.

Сборник зарегистрирован в международном центре ISSN (**ISSN 2221-7975)** и включен в перечень журналов РИНЦ

Сборник размещен в открытом бесплатном доступе на сайте www.skf-mtusi.ru

В настоящий сборник включены статьи, подготовленные по результатам работы VIII-ой Международной молодежной научно-практической конференции Северо-Кавказского филиала Московского технического университета связи и информатики «ИНФОКОМ-2015», которая проходила 20-25 апреля 2015 г. в СКФ МТУСИ. Сборник состоит из двух частей и объединяет статьи по актуальным научным направлениям создания, совершенствования, перспективного развития современных телекоммуникационных технологий связи и обработки информации, а также инфокоммуникационных технологий в образовании и в сфере экономики предприятий связи.

Первая часть сборника содержит материалы статей работы I и II секций конференции соответственно по направлениям:

- «Состояние и перспективы развития инфокоммуникаций»;
- «Информационная безопасность».

Вторая часть сборника содержит материалы статей работы III и IV секций конференции соответственно по направлениям:

- «Инфокоммуникационные технологии в образовании и в сфере экономики предприятий связи»;
- «State and prospects of infocommunications development».

Материалы IV секции по направлению «State and prospects of infocommunications development» представлены на английском и немецком языках.

Материалы статей представленных в сборнике даны в авторской редакции.

Сборник рассчитан на научных сотрудников, аспирантов, студентов и специалистов, работающих в области современных технологий связи, информационных технологий обработки информации, инфокоммуникационных технологий в образовании и в сфере экономики предприятий связи.

Составление, дизайн, редакционная верстка сборника: Суворов А.Б., Головенко М.В.

Подписано в печать 07.04.2015
Формат 60x84/8. Печать офсетная. Тираж 150 экз.
Полиграфический центр «Университет» СКФ МТУСИ,
Ростов-на-Дону, 344002, ул. Серафимовича, 62

СОДЕРЖАНИЕ

ЧАСТЬ I

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЧАСТЬ II

ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ И В СФЕРЕ ЭКОНОМИКИ ПРЕДПРИЯТИЙ СВЯЗИ

STATE AND PROSPECTS OF INFOCOMMUNICATIONS DEVELOPMENT

CONTENTS

PART 1

STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

INFORMATION SECURITY

PART II

INFOCOMMUNICATION TECHNOLOGIES IN EDUCATION AND ECONOMY OF TELECOMMUNICATIONS ENTERPRISES

STATE AND PROSPECTS OF INFOCOMMUNICATIONS DEVELOPMENT

О.С. Лабунько

АНТЕННЫ ПЕРСПЕКТИВНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Филиал федерального государственного унитарного предприятия
«Радиочастотный центр Центрального Федерального округа»
в Южном и Северо-Кавказскомфедеральных округах

Ключевые слова: цилиндр со звездным контуром, дифракция электромагнитной волны, параллельная и перпендикулярная поляризация электромагнитной волны, диаграмма рассеяния.

В докладе рассмотрены вопросы уменьшения уровня рассеянного поля несущими конструкциями антенных систем для улучшения электромагнитной совместимости с соседними радиоэлектронными системами для двух основных (продольной и поперечной) поляризаций электромагнитного поля. Для управления уровнем рассеянного поля предложено использовать цилиндрические конструкции со звездным контуром. Приведены результаты численных исследований, показывающие, что выбор геометрических параметров контура и электродинамических параметров покрытия позволяет изменять диаграмму рассеяния несущей конструкции в обратном направлении.

O.S. Labunko

ANTENNAS FOR PERSPECTIVE INFO- AND COMMUNICATION SYSTEMS

Branch of the Federal state unitary enterprise «Radio frequency center of the Central federal area» in the South and North Caucasian federal areas

Keywords: cylinder with a star circuit, diffraction of electromagnetic waves, parallel and perpendicular polarization of the electromagnetic wave, scatter pattern.

The report considers the issues of reducing the level of scattered fields bearing structures of the antenna systems to improve electromagnetic compatibility with neighboring electronic systems for two main (longitudinal and transverse) polarizations of the electromagnetic field. To control the level of the scattered field is proposed to use a cylindrical design with a star circuit. The results of numerical studies showing that the choice of the geometric parameters of the circuit and electrodynamics parameters of the coating allows you to change a scatterplot of the supporting structure in the opposite direction.

Одним из наиболее ярких примеров состояния и последующего развития инфокоммуникационных систем стало информационное обеспечение проведения в России XXII Олимпийских зимних игр и XIIПаралимпийских зимних игр. Естественно, что такое грандиозное мероприятие сопровождалось всесторонним освещением происходящих событий. Олимпийской вещательной службой за время проведения было произведено более 1300 часов прямого эфира международных программ, в том числе 456 часов выпусков новостей. Трансляция Олимпийских игр осуществлялась на 159 стран, что превышает количество стран в Ванкувере (120). Всего XXII зимние Олимпийские игры транслировали 464 канала, что почти вдвое превышает показатели предыдущей зимней олимпиады в Ванкувере. Хотя бы одну минуту телевизионных трансляций Олимпийских игр посмотрели около двух миллиардов человек, что на двести миллионов человек больше, чем в Ванкувере. Огромный поток передачи данных об олимпиаде в Сочи шёл через Интернет. Количество запросов о сочинской Олимпиаде превысило в два раза население Земли и достигло 13 млрд. Совокупный объём олимпийского интернет-трафика составил более 1 петабайта[1].

Обеспечение устойчивой работы такого количества радиоэлектронных средств (РЭС) потребовало серьезной подготовительной работы и, самое главное, слаженной работы различных

служб в течение всего срока проведения Олимпийских и Паралимпийских игр 2014 года. Другим немаловажным условием в таких случаях является и в дальнейшем приобретает все большую значимость улучшение электромагнитной совместимости (ЭМС) РЭС путем управления их характеристиками рассеяния. В первую очередь, это относится к антенным системам с высоким энергетическим потенциалом, устанавливаемым на несущих конструкциях, что обуславливает актуальность вопросов снижения рассеивающих свойств элементов несущих конструкций антенных систем.

Целью доклада является анализ одного из возможных технических решений по построению несущей конструкции, обеспечивающей снижение уровня рассеянного поля в обратном направлении для улучшения ЭМС с соседними РЭС.

Примером построения несущей конструкции антенны является мачта со звездным поперечным сечением (рисунок 1), поверхность которого покрыта слоем диэлектрика с параметрами ε и $\mu = 1$ [2-5].

Рисунок 1. Многослойная структура с диэлектрическим покрытием

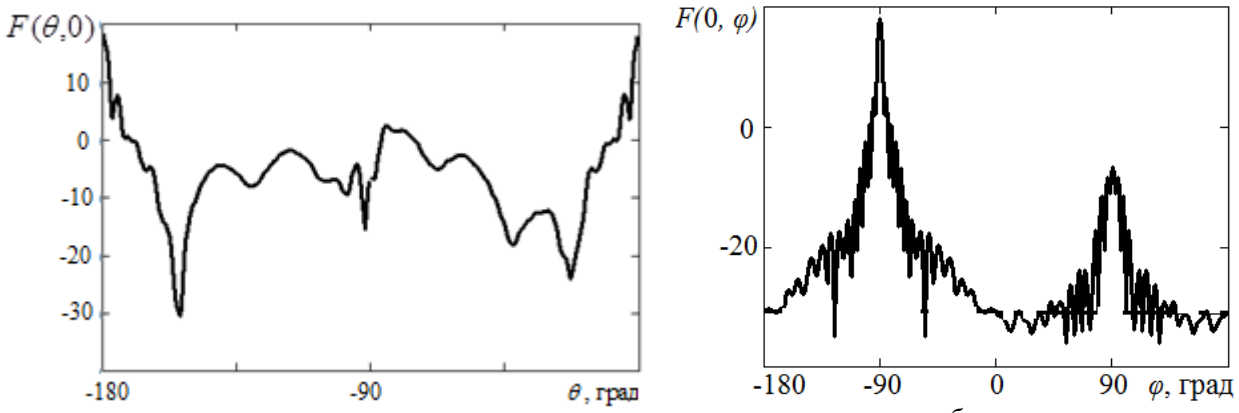
Решение задачи рассеяния для такой структуры может быть проведено с использованием метода интегральных уравнений [6]. В последующем получаемая система интегральных уравнений сводится к решению системы линейных алгебраических уравнений, которая решается одним из известных методов.

В статье рассматривается несущая конструкция в виде цилиндра, поперечное сечение которого описывается уравнением $\rho = \rho_0(1 + a \cdot \sin p\varphi)$ (металлическая поверхность - внутренний контур диэлектрического покрытия) и $\mathrm{P} = \mathrm{P}_0(1 + a \cdot \sin p\varphi)$ (внешний контур диэлектрического покрытия). При проведении исследований рассматривались следующие параметры цилиндра: $\rho_0 = 0{,}7\lambda$, $\mathrm{P}_0 = 0{,}8\lambda$, $a = 0{,}01\lambda$, $p = 9$.

Рассматривались два случая падения волны: в первом случае вектор напряженности электрического поля ориентирован перпендикулярно оси цилиндра (поперечная поляризация), во втором случае – вектор напряженности электрического поля ориентирован параллельно оси цилиндра (параллельная поляризация).

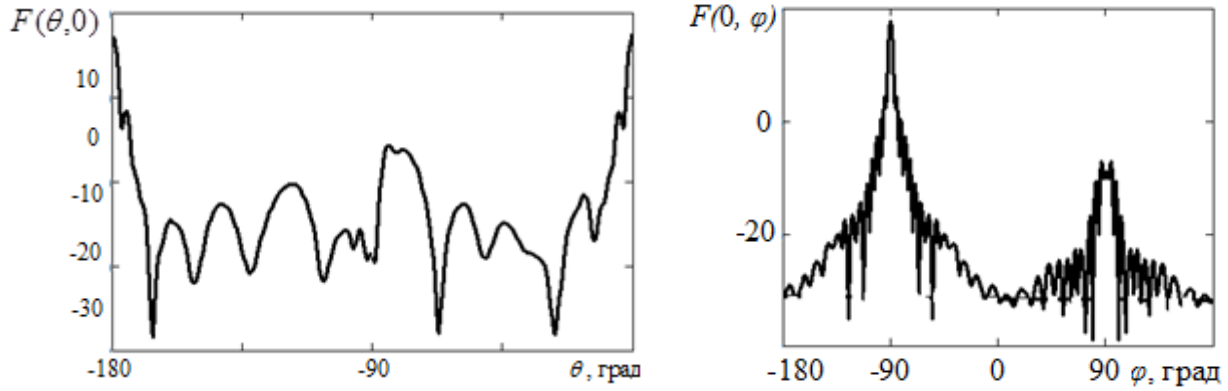
Полученные диаграммы рассеяния (ДР) $F(\theta, \varphi)$ приведены на рисунках 3, 4 для случая дифракции волны поперечной поляризации и на рисунках 5, 6 – для случая дифракции волны параллельной поляризации. При этом на рисунках с индексом «*а*» показаны сечения ДР плоскостью, проходящей через ось цилиндра и направление падения волны, на рисунках с индексом «*б*» – плоскостью, перпендикулярной оси цилиндра.

Приведенные результаты позволяют проследить основные закономерности, связанные с наличием диэлектрического покрытия на поверхности металлического цилиндра. Прежде всего, это проявляется в появлении волноведущих свойств такой поверхности. Однако указанные волноведущие свойства проявляются по разному для электромагнитных волн различной поляризации. Так для волн поперечной поляризации увеличение диэлектрической проницаемости покрытия обуславливает, как следует из сравнения графиков на рисунках 3, *а* и 4, *а*, значительное снижение уровня рассеянного поля (снижение составляет порядка минус 10 дБ). При этом в поперечной плоскости ДР практически не изменяется.



а *б*

Рисунок 3. Диаграмма рассеяния цилиндрической структуры при поперечной поляризации падающей волны ($\varepsilon = 0{,}5$)



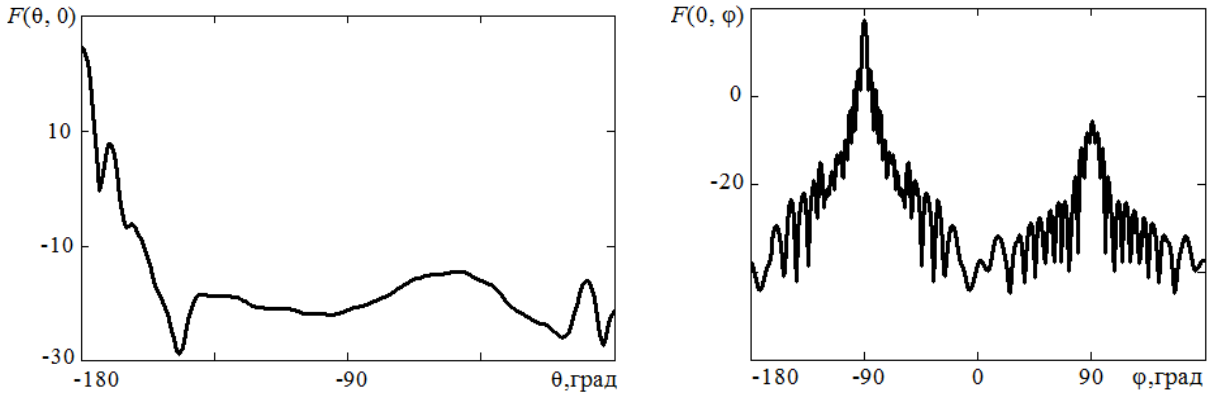
а *б*

Рисунок 4. Диаграмма рассеяния цилиндрической структуры при поперечной поляризации падающей волны ($\varepsilon = 4$)

В случае продольной поляризации, наоборот, увеличение диэлектрической проницаемости покрытия приводит к увеличению уровня рассеянного поля, как это следует из сравнения результатов, приведенных на рисунках 5, *а* и 6, *а*. Кроме этого, наблюдается снижение уровня ДР и в поперечной плоскости, что не происходит для случая поперечной поляризации.

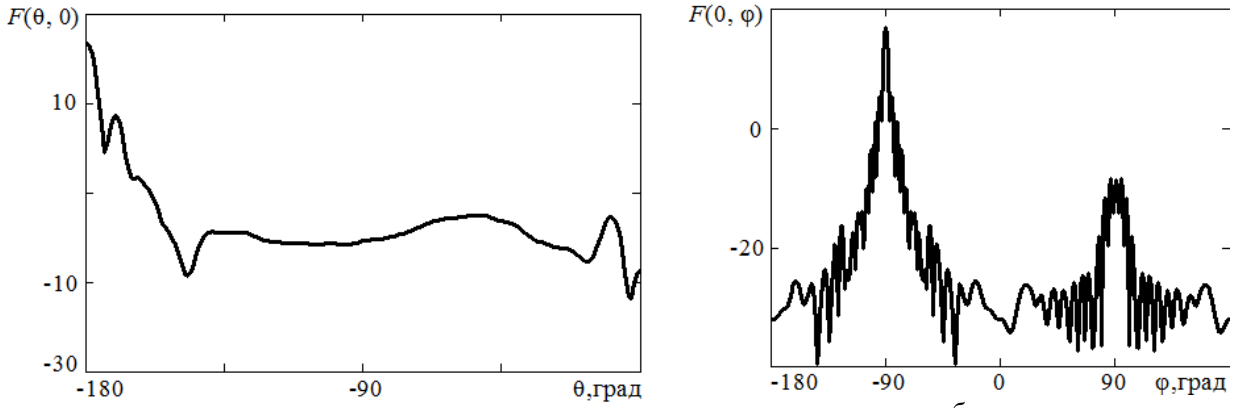
Таким образом, приведенные результаты показывают, что наличие диэлектрического покрытия приводит к появлению волноведущих свойств у цилиндрической структуры со звездным контуром. Увеличение диэлектрической проницаемости покрытия, наносимого на металлическую поверхность приводит к усилению данных свойств. Однако волноведущие свойства рассматриваемой структуры проявляются по-разному. В частности для волн поперечной поляризации наблюдается уменьшение уровня рассеянного поля, а для волн продольной поляризации – увеличение уровня рассеянного поля.

На основе полученных результатов можно указать, что рассматриваемые структуры могут использоваться в качестве несущих конструкций антенн для уменьшения уровня рассеянного поля и улучшения электромагнитной совместимости РЭС. При этом при выборе геометрических и электродинамических параметров конструкции и покрытия необходимо учитывать вид поляризации сигналов.



а *б*

Рисунок 5. Диаграмма рассеяния цилиндрической структуры при продольной поляризации падающей волны ($\varepsilon = 0{,}5$)



а *б*

Рисунок 6. Диаграмма рассеяния цилиндрической структуры при продольной поляризации падающей волны ($\varepsilon = 4$)

Таким образом, полученные результаты показывают принципиальную возможность изменения рассеивающих свойств цилиндрической поверхности с контуром сложного сечения, в частности со звездным контуром, при изменении параметров диэлектрического покрытия и учете поляризации падающей волны.

Литература:

1. Лабунько О.С. Опыт обеспечения использования радиочастотного спектра при проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр. //Технологии и средства связи. 2014 №4. С 38-41.

2. Звездина М.Ю., Лабунько О.С., Звездина Ю.А. Взаимосвязь геометрических параметров и поверхностного импеданса звездного контура. // Электромагнитные волны и электронные системы. 2008. Т. 13. № 5. С. 33-34.

3. Габриэльян Д.Д., Звездина М.Ю., Лабунько О.С., Безуглов Е.Д., Подзоров А.В.Особенности дифракции Е- и Н-поляризованных волн на цилиндрах со звездным контуром. // Электромагнитные волны и электронные системы. 2010. Т. 15. № 5. С. 19-21.

4. Габриэльян Д.Д., Звездина М.Ю., Лабунько О.С., Безуглов Е.Д. Распределение полей в ближней зоне цилиндра со звездным контуром при дифракции плоской волны. // Электромагнитные волны и электронные системы. 2011. Т. 16. № 5. С. 18-20.

5. Лабунько О.С.Особенности рассеяния электромагнитных волн многослойными структурами с метаматериалами. // Электромагнитные волны и электронные системы. 2011. Т. 16. № 5. С. 5-8.

6. Лабунько О.С.Строгий метод в задачах дифракции на цилиндрах с учетом свойств 2π - периодичности. // Электромагнитные волны и электронные системы. 2009. Т. 14. № 5. С. 18-20.

А.С. Агафонова, Ю.В. Заварыкина

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ «ОБЛАЧНЫХ» ТЕХНОЛОГИЙ

Уральский юридический институт МВД России, г. Екатеринбург, Россия

Ключевые слова: «облачные» технологии, «облачные» вычисления, частное «облако», публичное «облако», гибридное «облако».

В статье рассмотрены понятия «облачных» технологий, виды «облаков» (частные, публичные и гибридные), свойства «облачных» технологий. Сформулированы требования, предъявляемые к «облачным» технологиям. Представлены достоинства, недостатки, а также аспекты использования в различных областях. Анализируется практика применения рассматриваемых технологий в России и зарубежных странах. Обращено внимание на использование «облачных» технологий в финансовой сфере. Перечислены некоторые средства обеспечения информационной безопасности в «облаке».

A.S. Agafonova, Y.V. Zavarykina

POSSIBILITIES OF APPLICATION OF «CLOUDY» TECHNOLOGIES

Ural law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia

Keywords: «cloud» technology, cloud computing, privatecloud, publiccloud, hybridcloud

The article discusses the concept of «cloud» technologies, types of «clouds» (private, public, and hybrid), the properties of «cloud» technologies. The requirements to be met by «cloud» technologies. Presents the advantages, disadvantages, as well as aspects of the use in various fields. The practice of application of the considered technologies in Russia and abroad. Attention is paid to the use of «cloud» technologies in the financial sector. Are some of the means of information security in the «cloud».

С каждым годом тема «облачных» сервисов и технологий становится все более популярной. И это вполне закономерно, учитывая стремительный рост парка мобильных устройств – в первую очередь смартфонов и планшетных ПК. В отличие от настольных систем и полноценных ноутбуков, такие устройства обладают довольно ограниченной вычислительной мощностью и небольшим объемом встроенной памяти.

На сегодняшний день не существует эталонной, «облачной» инфраструктуры. Целый ряд различных программных и аппаратных решений может использоваться для построения «облачных» технологий. «Облачные» системы ориентированы, прежде всего, на предоставление сервисов со стороны информационных технологий. При этом для практической реализации требуется совместное использование множества технологий, в то время как каждая технология по отдельности не может служить полноценным решением для создания сервис-ориентированной инфраструктуры [1].

Различают три вида «облаков»: частные, публичные и гибридные.

Частное «облако» (privatecloud) – это ИТ-инфраструктура, контролируемая и эксплуатируемая в интересах одной единственной организации. Частное «облако» может находиться в собственности, управлении и эксплуатации у самой организации, либо у внешнего оператора, либо частично у заказчика и частично у оператора [2].

Публичное «облако» (publiccloud) – это ИТ-инфраструктура, предназначенная для свободного использования множеством компаний или частными лицами. Пользователи данных, размещенных в «облаке», получают только доступ к необходимым услугами, не имеют возможности управлять и обслуживать данное «облако», вся ответственность по этим вопросам возложена на его владельца.

Гибридное «облако» (hybridcloud) – это ИТ-инфраструктура, представляющая собой комбинацию частных и публичных «облаков», связанных между собой стандартизированными или собственными технологиями передачи данных и приложений.

«Облачные» технологии, вне зависимости от конкретной реализации, должны иметь некоторые свойства:

– эластичность – услуги могут быть предоставлены, расширены, сужены в любой момент времени, без дополнительных издержек на взаимодействие с поставщиком, как правило, в автоматическом режиме. Именно это свойство обеспечивает «облачным» системам ряд экономических преимуществ по сравнению с классическими информационными системами;
– отказоустойчивость – это обеспечение высокого уровня отказоустойчивости, требует избыточного количества ресурсов. В «облачных» системах возможно избавиться от этого за счет использования виртуализации. Однако для обеспечения аппаратной отказоустойчивости сохранение некой избыточности все-таки необходимо;
– обеспечение фиксированного качества сервиса – это не только обеспечение высокой доступности сервисов, но и другие, не менее важные характеристики: время реакции на действия пользователя, соответствие заявленной производительности универсальный доступ по сети и другие.

Преимущества «облачной» модели очевидны: все затраты на сохранность данных пользователя и функционирование программы ложатся на плечи компании-разработчика. Она же обеспечивает защиту и конфиденциальность информации, разрабатывает алгоритмы для ее шифрования, нанимает и обучает персонал для администрирования серверов, нет необходимости в тщательном изучении системных требований, покупке дорогих комплектующих и многоступенчатой установки программы. Нужно просто открыть браузер, зайти на определенный сайт и создать там учетную запись, следуя правилам предоставления услуги. После этого пользоваться профилем можно с любого устройства, не волнуясь о переносе информации с одного носителя на другой: она ведь хранится на сервере, для доступа к которому достаточно интернет-подключения, логина и пароля. И не важно, где находится пользователь: за офисным компьютером, дома за личным ноутбуком, или едет в транспорте, работая с программой через мобильное устройство, – все контакты, важные документы, статистика и другие необходимые данные доступны в любой момент.

Сегодня «облачные» технологии используются в любых сферах, от хранения документов простыми пользователями, до систем крупного бизнеса. Клиенту доступно множество «облачных» сервисов, в числе которых: почта, хостинг для корпоративного интернет-ресурса, ИТ-телефония, внутрикорпоративные системы, тестирование программного обеспечения, электронный документооборот. Это дает большую функциональную свободу, гибкость и позволяют быстро поднять бизнес на качественно более высокий уровень.

Хранение клиентской информации осуществляется на защищенных от несанкционированного доступа носителях высокой степени надежности. Специальным образом организуется резервное копирование важной информации для обеспечения возможности ее восстановления в случае ошибки пользователей.

Для глобального финансового рынка облачные технологии становятся все более привычными. Так, по данным исследования Information Week большое количество банков в мире активно использует «облачные» сервисы при ведении своего бизнеса (Рисунок 1).

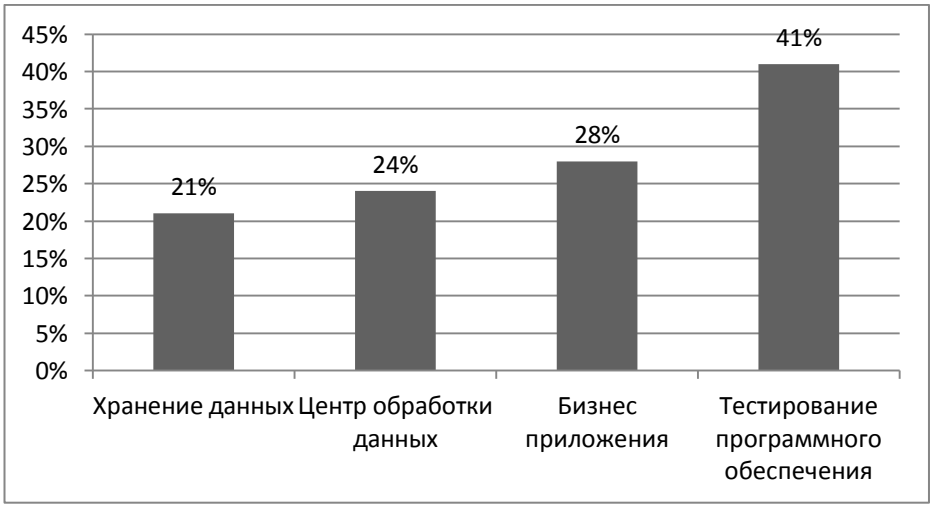


Рисунок 1. Распределение облачных сервисов в мире по видам использования

По результатам исследования, проведенного среди российских банков, почти три четверти респондентов обсуждают возможность перехода на «облачные» технологии, но большинство из них пока воздерживается от практических действий. Однако во всех без исключения банках возникла необходимость удаленного доступа к системам самообслуживания с гарантией высокой скорости и удобства работы клиентов. Поэтому, несмотря на открытые вопросы в сфере безопасности, банки являются одними из самых активных потребителей облачных решений [3].

Наряду с преимуществами существует и ряд недостатков, связанных с «облачными» сервисами:

- пользователь не является владельцем и не обладает доступом к «облачной» инфраструктуре, соответственно сохранность используемых данных полностью зависит от кампании, предоставляющей данные услуги;
- для получения качественных услуг необходим высокоскоростной Интернет;
- отсутствие общепринятых стандартов в области обеспечения безопасности «облачных» сервисов.

По данным ForresterResearch, половина организаций, не внедряющих «облачные» технологии, оправдывают свою позицию опасениями за безопасность личных данных. В сфере безопасности организации больше всего озабочены такими факторами, как защита данных, правильное функционирование систем и их доступность. При этом все большее значение приобретают задачи защиты приложений, оптимального мониторинга и аудита, а также соблюдение законодательных и нормативных требований [4].

Россия по показателю внедрения облачных технологий занимает в мире лишь 34 место, тому есть много причин. К примеру, территория РФ пока недостаточно покрыта высокоскоростным интернетом – непременным условием полноценного пользования «облачными» технологиями. Многие эксперты отмечают также особенности менталитета российского бизнеса – а именно, склонность неохотно доверять новым, не проверенным практикой техническим решениям.

Опасения в отношении «облачных» технологий вызывают и другие факторы. Несмотря на то, что многие крупные компании мира взялись за освоение «облачных» технологий, другие пока склонны переоценивать риски и относиться к данному направлению настороженно. Их вполне можно понять – перед «облачными» вычислениями сегодня стоят не только технические, но и организационно-юридические проблемы, необходимо развитие методик регулирования юридических вопросов, связанных с аспектами функционирования рассматриваемых систем [5].

Несмотря на опасения и недостатки «облачных» сервисов, перспективы внедрения их в России огромны. Согласно исследованиям, проведенным аналитиками Orange Business Services, доход российского рынка «облачных» услуг для бизнеса от 4,5 млрд р. в 2012 г. может увеличиться до 19 млрд р. в 2016 г. [3].

Крупные поставщики «облачных» услуг, такие как Amazon, IBM, Salesforce.com создали мощные механизмы безопасности. Они работают не только на прикладном, но и на инфраструктурном уровне и включают в свой состав такие инфраструктурные средства, как межсетевые экран и систем шифрования. Эти поставщики хранят в «облаке» петабайты конфиденциальных данных и пока не испытывают серьезных проблем в сфере безопасности.

Компании, предлагающие программное обеспечение для информационной безопасности, создали целый ряд межсетевых экранов и систем шифрования для защиты любых «облачных» услуг. Большинство решений для облачной безопасности перешло от защиты корпоративных сетей с помощью межсетевых экранов к защите точек доступа за счет сочетания межсетевых экранов и средств шифрования данных на пользовательском уровне [6]. В результате, каким бы устройством ни пользовался абонент для доступа в «облако», его коммуникации, загружаемые программы и передаваемые данные будут надежно защищены.

«Облачные» технологии развиваются стремительно и охватывают все больше и больше сфер деятельности, предоставляют практически безграничные возможности благодаря своим сервисам, начиная с простого хранения информации и заканчивая предоставлением сложных безопасных ИТ-инфраструктур. И так как сами технологии достаточно молоды, продолжаются исследования возможности их применения в различных областях жизни.

Литература:
1. Бизнес в облаках. Чем полезны облачные технологии для предпринимателя. Режим доступа: URL: https://kontur.ru/articles/225 (дата обращения: 21.02.2015).
2. Аджемов А.С. «Облачные технологии». Информационные технологии, связь и защита информации МВД России – 2012, 2012, № 1, с. 46-47.
3. Батаев А.В, Перспективы внедрения облачных технологий в банковском секторе России. Режим доступа: URL: http://institutiones.com/innovations/2345-perspektivy-vnedreniya-oblachnyx-texnologij-v-bankovskom-sektore-rossii.html (дата обращения: 20.02.2015).
4. Безопасность в облаке. // «Защита информации. Инсайд», 2011, № 6, с. 64-65.
5. Широкова Е.А. Облачные технологии // Современные тенденции технических наук: материалы международной научной конференции (г. Уфа, октябрь 2011 г.), 2011, с. 30-33.
6. К.Л. Костюченко Новые акценты в обеспечении информационной безопасности органов внутренних дел. – Вестник Уральского юридического института МВД России, 2014, № 4, с. 30-32.

О.Ю. Евсеева, *Аль-Аззави Эсса Мохаммед

МОДЕЛЬ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ В КЛАСТЕРИЗОВАННОЙ MESH-СЕТИ

Харьковский национальный университет радиоэлектроники,
*Одесская национальная академия связи им. А.С. Попова

Ключевые слова: беспроводные mesh-сети, кластеризованная сеть, динамическая маршрутизация, распределение канальных ресурсов.

Расширение зоны покрытия, повышение надежности и скорости передачи в рамках беспроводных одноранговых (mesh) сетей сопряжено с усложнением процесса управления ними. Одной из важных управленческих задач является маршрутизация, основными требованиями к решению которой выступают адаптивность, оптимальность, масштабируемость, а также высокая степень согласованности с процессом распределения канальных ресурсов (временных слотов). В соответствии с перечисленными требованиями в работе предложена математическая модель беспроводной mesh-сети, представленная в пространстве состояний, ориентированная с целью обеспечения масштабируемости на кластерную структуру сети. В рамках модели предполагается выделение каждому кластеру собственного пула временных слотов, распределение которых в пределах кластера не требует учета явления интерференции, что существенно упрощает задачу.

O.Yu. Yevsyeyeva, * Al-Azzawi Essa Mohammed

MODEL ON DYNAMIC ROUTING IN CLUSTERED MESH-NETWORK

Kharkiv National University of Radioelektronics,
*Odessa National Academy of Telecommunication named after A.S.Popov

Keywords: wireless mesh-network, clustered network, dynamic routing, link resources allocation.

Widening of covered area, increasing of reliability and capacity within the wireless mesh networks is associated with complication of control of them. One of the most important control problem is routing, the basic requirements for the solution of which are adaptability, optimality, scalability, as well as a high degree of consistency with the process of link resources (time slots) allocation. In accordance with the requirements a mathematical model of wireless mesh-network, represented in the state space, is offered. In order to provide scalability the model is oriented for clustered structure of the network. Each cluster has its own pool of time slots, which have to be allocated across the cluster. Because time slots allocation within a cluster does not require taking into account interference effect, the task of managing are greatly simplified.

Повышающаяся роль мобильности пользователей и растущие объемы передаваемого трафика, связанные с увеличением доли мультимедийной компоненты и количества используемых терминальных устройств, обеспечивают востребованность различных беспроводных технологий, среди которых отдельную нишу занимают одноранговые (mesh) сети. Их основным преимуществом является способность сочетать гибкость беспроводных технологий с высокими скоростями передачи трафика, надежностью и безопасностью, свойственными проводным сетям. Mesh-сети по уровню эффективности использования канальных ресурсов (будь то временные, частотные, или частотно-временные ресурсы), а также по размерам зоны покрытия существенно выигрывают по сравнению с сетями, построенными по принципу «точка-многоточка» (Point-to-Multipoint, PMP). С другой стороны своеобразной платой за расширение возможностей mesh-сетей является усложнение задач управления ними. Поскольку в PMP-режиме весь трафик в обязательном порядке должен быть передан через базовую станцию, то достаточно организовать восходящий и нисходящий каналы связи, в рамках которых возможно лишь перераспределение ресурсов в интересах тех или иных потоков трафика. В mesh-сетях понятие восходящего и нисходящего каналов связи в принципе отсутствует, любая mesh-станция может выступать как терминальное (оконечное) устройство, так и как транзитный маршрутизатор. Тогда для mesh-сетей актуальной является задача маршрутизации, которая, принимая во внимание специфику организации подобного рада сетей и беспроводной связи в целом, должна быть решена совместно, или по меньшей мере согласованно с задачей распределения ресурсов канального уровня, а учитывая ограниченность объема этих ресурсов, их нестационарность и высокую территориальную распределенность управляемой системы, в качестве основных требований к решению задачи маршрутизации выступают адаптивность, оптимальность и масштабируемость.

Формирование оптимального управляющего решения предполагает наличие строго формализованной математической модели объекта управления – беспроводной mesh-сети, вид которой существенно зависит от реализуемого в системе метода многостанционного доступа к общим ресурсам канального уровня. Для систем с временным разделением доступа к общему частотному ресурсу (Time-Division Multiple Access, TDMA), который определен семейством стандартов IEEE 802.16 как основа для mesh-режима сетей WiMax, оптимальное решение динамической маршрутизации может быть получено на основании модели в пространстве состояний, предложенной в [1]. Модель предполагает трактовку задачи маршрутизации как задачи оптимального распределения канальных ресурсов, в качестве которых выступают временные слоты. Основу модели составляет система разностных уравнений состояния:

$$q_{i,j}(k+1) = q_{i,j}(k) - \sum_{\substack{v \in S_i^1, \\ v \neq i}} \sum_{r=1}^{N_F} m_{i,v}(k) \tau_{i,v}^{r,j}(k) n + \sum_{\substack{g \in S_i^1, \\ g \neq i,j}} \sum_{r=1}^{N_F} m_{g,i}(k) \tau_{g,i}^{r,j}(k) n + \xi_{i,j}(k) \Delta t, \quad (1)$$

где $(i, j) \in E$; $i \neq j$; k=0, 1, 2...; $\Delta t = t_{k+1} - t_k$ – интервал дискретизации (период перерасчета и смены управляющих переменных); $q_{i,j}(k)$ – переменная состояния, отражающая объем данных, которые находятся на i-й станции и предназначены для передачи j-й станции в момент времени t_k; $\tau_{i,j}^{r,l}(k)$ – булева переменная, выполняющая роль управляющей: $\tau_{i,j}^{r,l}(k) = 1$, если в k-й момент времени в канале (i, j) r-й слот используется для передачи данных, адресованных l-й станции; $m_{i,j}(k)$ – количество бит пользовательских данных, которые могут быть переданы в k-й момент времени в канале (i, j) при использовании одного временного слота; S_i^1 – множество станций mesh-сети, смежных с i-й станцией; $\xi_{i,j}(k)$ – интенсивность поступления данных на i-ю станцию в момент времени t_k, адресованных j-й станции; n – количество фреймов, передаваемых в течение времени Δt, $n = \Delta t / T_F$; T_F – длительность фрейма; N_F – количество слотов в одном фрейме, используемых для передачи пользовательского трафика; E – множество каналов между станциями mesh-сети.

Уравнение (1) позволяет контролировать как буферные ресурсы сети (через переменные состояния $q_{i,j}(k)$), так и канальные ресурсы (через переменные управления $\tau_{i,j}^{r,l}(k)$), ограниченность которых требует выполнения ряда условий:

$$0 \le q_{i,j}(k) \le q_{i,j}^{\max} \quad \text{или} \quad 0 \le q_{i,j}(k), \sum_{\substack{j=1,\\ i \ne j}}^{N_v} q_{i,j}(k) \le q_i^{\max}, \tag{2}$$

$$\sum_{\substack{(i,j)\in E,\\ j\ne i}} \sum_{\substack{l=1,\\ l\ne i}}^{N_v} \tau_{i,j}^{r,l}(k) \le 1, \tag{3}$$

где $q_{i,j}^{\max}$ и $q_i^{\max}$ – максимальный размер отдельной j-й очереди на i-й станции и максимально допустимый размер суммарной очереди на i-й станции соответственно; N_v – общее количество станций в mesh-сети.

Тогда на основании модели (1) – (3) задача динамической маршрутизации и реализующего ее оптимального распределения канальных ресурсов может быть формализована как задача минимизации стоимостной функции J по переменным $\tau_{i,j}^{r,l}(k)$ при ограничениях (1) – (3), где целевая функция представляется традиционным в рамках теории оптимального управления квадратичным выражением

$$J = \sum_{k=1}^{a} \left[\vec{q}^{\,T}(k) W_q \vec{q}(k) + \vec{\tau}^{\,T}(k) W_\tau \vec{\tau}(k) \right] \to \min. \tag{4}$$

Здесь a – количество интервалов Δt, для которых осуществляется расчет управляющих переменных; $\vec{q}(k)$, $\vec{\tau}(k)$ – векторы, объединяющие переменные состояния и управления соответственно; W_q, W_τ – диагональные неотрицательно определенные весовые матрицы использования буферных и канальных ресурсов соответственно.

Управление, получаемое в результате решения задачи (1) – (4), допускает единоразовое использование каждого временного слота в рамках всей mesh-сети, что существенно ограничивает пропускную способность системы. С другой стороны повторное использование слотов требует усложнения модели и замену условия (3) выражением вида

$$\sum_{\substack{(i,j)\in E,\\ j\ne i}} \sum_{\substack{l=1,\\ l\ne i}}^{N_v} \tau_{i,j}^{r,l}(k) + \sum_{\substack{(g,j)\in E,\\ g\in S_i^2,\\ g\ne j}} \sum_{\substack{l=1,\\ l\ne i}}^{N_v} \tau_{g,j}^{r,l}(k) \le 1, \tag{5}$$

которое запрещает назначение одного и того же временного слота станциям, удаленным друг от друга на расстояние двух переприемов (2 hops) и менее [2].

Замена условия (3) на (5) сопряжена с изменением траектории поведения системы, что требует корректировки целевой функции, например, следующим образом:

$$J = \sum_{k=1}^{a} \left[\vec{q}^{\,T}(k) W_q \vec{q}(k) + \vec{\tau}^{\,T}(k) W_\tau \vec{\tau}(k) - \vec{\tau}^{\,T}(k) W_{reuse} \vec{\tau}(k) \right] \to \min, \tag{6}$$

где W_{reuse} – весовая матрица, отражающая выигрыш за счет повторного использования слотов.

Таким образом, в результате решения задачи (6) при ограничениях (1) – (2), (5) имеем оптимальную стратегию маршрутизации и распределения канальных ресурсов mesh-сети на основе временного множественного доступа, способную адаптивно подстраиваться под изменения структуры сети, сигнально-помеховой обстановки и интенсивностей поступающих на обслуживание пользовательских потоков, и нацеленную при этом на достижение максимальной производительности системы за счет повторного использования слотов. Однако, если рассматривать задачи (4) и (6) с точки зрения сложности получения численного решения,

применение модели (1) – (2), (5) – (6) обладает более низкой масштабируемостью, что ограничивает ее применение на практике.

Одним из наиболее эффективных инструментов в решении проблемы масштабируемости в телекоммуникациях является применение иерархических методов как построения самих систем, так и методов управления ними. В случае беспроводных сетей это сопряжено с кластеризацией и иерархической организацией кластеров в рамках единой системы. Как показывает анализ, кластеризация беспроводных сетей различного типа, в том числе и mesh-сетей, может базироваться на различных критериях. Поскольку в нашем случае причина снижения масштабируемости связана с необходимостью учета интерференции при повторном использовании слотов, целесообразно в качестве основного критерия кластеризации использовать именно это явление. В работе [3] предложен алгоритм кластеризации mesh-сети, в результате применения которого, все станции в кластере испытывают взаимную интерференцию, и, как результат, повторное использование слотов в рамках каждого отдельно взятого кластера является недопустимым. В то же время данный алгоритм выделяет в структуре сети кластеры, взаимное удаление которых позволяет использовать одинаковые наборы временных слотов. Это ведет к двухуровневой схеме управления mesh-сетью, верхний уровень в которой отвечает за назначение каждому кластеру собственного пула (набора) слотов, а на нижнем уровне предполагается динамическое закрепление слотов за конкретными mesh-станциями в рамках выделенного пула. Тогда задача маршрутизации в mesh-сети с целью облуживания поступающего в сеть трафика может быть формализована как задача минимизации (4) по переменным $\tau_{i,j}^{r,l}(k)$ при ограничениях (1) – (3), дополненных для каждого из кластеров сети системой неравенств вида

$$\sum_{r=1}^{N_F} \sum_{\substack{(i,j)\in E,\\ j\neq i}} \sum_{\substack{l=1,\\ l\neq i}}^{N_V} F_{i,j}^{A} \tau_{i,j}^{r,l}(k) \le N_{sl}^{A}(k), \qquad (7)$$

$$F_{i,j}^{A} = \begin{cases} 1, \text{если канал передачи (i, j) принадлежит кластеру A;} \\ 0, \text{в противном случае;} \end{cases}$$

где N_{sl}^{A} – количество слотов, выделяемых кластеру A на протяжении k-го интервала управления.

С точки зрения вычислительной сложности постановка задача оптимизации (1) – (4), (7), так же как и все выше описанные подходы принадлежащая к классу целочисленного программирования, существенно выигрывает по сравнению с моделью (1) – (2), (5) – (6). С точки зрения физики трактовка задачи динамической маршрутизации в виде (1) – (4), (7) представляет собой компромисс между максимизацией производительности беспроводной mesh-сети и масштабируемостью управляющих решений. В силу положенных в основу модели разностных уравнений состояния задача (1) – (4), (7) обеспечивает адаптивный выбор маршрутов и распределение временных слотов вдоль каждого из них, оптимальное в рамках заданного верхним уровнем пула слотов, алгоритм формирования которого представляет предмет дальнейших исследований.

Литература:

1. Yevsyeyeva O., Al-Azzawi Essa Mohammed Mathematical model for resource allocation in TDMA-based wireless meshnetworks // Eastern-European Journal of Enterprise Technologies, 2014, Vol. 3, N. 9(69), P. 4-9.

2. Hung-Yu Wei, Ganguly S., Izmailov R., Haas Z.J. Interference-aware IEEE 802.16 WiMax mesh networks // In proc. IEEE Vehicular Technology Conference, VTC 2005, Vol. 5, P. 3102 – 3106.

3. Yevsyeyeva O., Al-Azzawi Essa Mohammed An Algorithm for Clustering And Aggregation Of Wireless Mesh Network's Topology // In proc. First International IEEE Conference «Problems of Infocommunications. Science and Technology» PICS&T-2014, 14-17 October, 2014, P. 37–38.

У.Б. Амирсаидов

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ РАСЧЕТА ВАРИАЦИИ ЗАДЕРЖКИ IP-ПАКЕТОВ

Ташкентский университет информационных технологий, г.Ташкент, Узбекистан

Ключевые слова: услуги связи, качество обслуживания, задержка, вариация задержки, среднеквадратичное отклонение, моделирование, интенсивность обслуживания.

Описан метод расчета вариации задержки пакетов, приведенный в рекомендации МСЭ-Т Y.1541. Рассмотрены приближенные методы расчета вариации задержки. Приведен метод измерения вариации задержки пакетов. На основе имитационного моделирования определена аппроксимирующая гамма-функция распределения времени задержки пакетов в сети. Проведен расчет вариации задержки на основе гамма-распределения. Приведены результаты сравнительного анализа методов расчета вариации задержки пакетов. Даны рекомендации по использованию методов расчета и измерения вариации задержки пакетов.

U.B. Amirsaidov

COMPARATIVE ANALYSIS OF METHODS FOR CALCULATION OF DELAY VARIATION OF IP PACKETS

Tashkent University of information technology, Tashkent, Uzbekistan

Keywords: communication services, Quality of service, delay, delay variation, modeling, mean-squaredeviation,service rate.

The method is described delay variation of packets that is recommended in ITU-T Y.1541. Approximate methods are discussed for calculation of packet delay variation. Based on the imitation modeling, approximate gamma-function of distribution for packet delay variation is defined in IP network. Also, given delay variation based on the gamma-function. In addition, the results are given for comparative analysis of methods for calculation of packet delay variation. Recommendations are given for using methods of calculation and measuring packet delay variation.

Качество услуг связи является важным фактором, влияющим на конкурентоспособность операторов связи. Исходя из требований рынка, целесообразно развивать нормативную базу качества услуг. Методы оценки и нормы на качества обслуживания сетей IP приведены в рекомендации МСЭ-Т Y.1541 [1]. Основными показателями качества обслуживания мультимедийного трафика являются среднее значение задержки IP-пакета (IPTD- IP packet Transfer Delay) и вариация (джиттер) этой задержки (Jitter, IPDV- IP packet Delay Variation).

Целью данной работы является сравнительный анализ методов расчета вариации задержки пакетов.

Возникновение вариаций задержки – прямое следствие природы пакетной коммутации IP-сети. В соотвествии с Y.1541, вариация задержки пакетов рассчитывается по формуле:

$$J = t_p - t_{\min}, \tag{1}$$

где t_p -квантиль функции распределения времени задержки пакета (F(t)) уровня значимости 0.999 ($F(t_p) = 0.999$); $t_{\min}$ - минимальная длительность передачи пакета.

Расчет квантиля t_p с помощью метода, рекомендованного МСЭ-Т, проводится следующим образом. Вначале оцениваются среднее значение $\bar{t}_{çàäi}$, среднеквадратичное отклонение σ_i, третий центральный момент β_{3i} и асимметрия γ_i времени задержки пакетов на

каждой i-й фазе обслуживания. Далее для маршрута, содержащего N фаз (узлов коммутации), рассчитываются среднее значение $\bar{t}_{çàä\ ñ}$, среднеквадратичное отклонение $\sigma_{ñ}$ и асимметрия γ_c времени задержки по формулам:

$$\bar{t}_{çàä\ ñ} = \sum_{i=1}^{N} \bar{t}_{çàä\ i}, \tag{2}$$

$$\sigma_{ñ} = \sqrt{\sum_{i=1}^{N} \sigma_i^2}, \tag{3}$$

$$\gamma_{ñ} = \frac{\sum_{i=1}^{N} \beta_{3i}}{\sigma_c^3}. \tag{3}$$

Согласно Y.1541 t_p - квантиль функции распределения времени задержки пакетов в сети из N фаз обслуживания определяется соотношением:

$$t_p = \bar{t}_{çàä\ ñ} + \sigma_{ñ}(x_p - \frac{\gamma_c[1-(x_p)^2]}{6}), \tag{4}$$

где x_p - значение p -квантиля для стандартного нормального распределения.

Выражение (4) с учетом $x_p = 3.09$ ($p = 0.999$) можно записать в виде:

$$t_p = \bar{t}_{çàä\ ñ} + \sigma_c(3.09 + 1.425\gamma_c). \tag{5}$$

На основе имитационного моделирования определена аппроксимирующая гамма-функция распределения времени задержки пакетов в сети с зависимым потоком:

$$F_c(t) = \frac{1}{\theta^k \Gamma(k)} \int_0^t t^{k-1} e^{-t/\theta} dt, \tag{6}$$

где: $k =]1/v^2[$, $\theta = \bar{t}_{çàä\ ñ}/k$, $v = \sigma_c / \bar{t}_{çàä\ ñ}$ - коэффициент вариации; $\Gamma(k)$ - гамма-функция Эйлера.

Среднее время задержки пакетов в неэкспоненциальном узле i с зависимым потоком определяется в виде [2]:

$$\bar{t}_{çàäi} = \frac{1}{\mu_i(1-P_{îæi})}, \tag{7}$$

где μ_i - интенсивность обслуживания пакетов в узле i $P_{îæi}$ - вероятность ожидания пакетов в очереди узла i, $i = \overline{1,N.}$.

Среднее время задержки пакетов в сети определяется по формуле (2).

Значение t_p определяется из уравнения:

$$F_c(t_p) = 0.999 \quad (8)$$

Результаты расчетов t_p по формулам (5) и (8) почти одинаковые. Это подтверждает достоверность аппроксимирующей функции (6).

В работе [3] предложены следующие приближенные формулы для расчета вариации (джиттера) времени задержки:

$$J \approx t_{ç\max} - t_{ç\min}, \quad (9)$$

$$J \approx 6\sigma_c, \quad (10)$$

где $t_{ç\max}$ - максимальное время задержки пакетов.

В таблицу 1 сведены результаты расчетов джиттера по формулам (5), (9) и (10) при различных N и ρ.

Таблица 1 - Результаты расчета джиттера

N	Вариация (джиттер) задержки J		
	$t_{ç\max} - t_{ç\min}$	6σ	$t_p - t_{ç\min}$
	$\rho = 0.2$		
2	41.92	21.24	23.08
3	88.17	43.62	48.27
4	124.35	58.74	64.41
5	161.31	74.58	82.23
	$\rho = 0.5$		
2	159.12	100.08	110.97
3		141.78	154.31
4	291.56	183.3	199.41
5	347.99	225.84	243.31
	$\rho = 0.8$		
2	497.47	305.94	335.41
3	565.32	369.6	402.24
4	740.07	435.78	468.11
5	779.18	499.74	545.05

Анализ полученных результатов показывает, что приближенную формулу (10) можно использовать только при $N \le 5$ и $\rho \le 0.5$. Значения джиттера, рассчитанные с помощью приближенной формулы (9), в 1.5 – 2 раза больше, чем действительные значения.

Измерение, мониторинг и контроль значений сквозных показателей качества обслуживания IP – сети осуществляется аппаратно-программным комплексом IP Quality Monitor (IQM) [4]. Джиттер $J_{i,i-1}$ определяется как разница сквозных задержек пакетов i и $i-1$:

$$J_{i,i-1} = \left|(R_i - S_i) - (R_{i-1} - S_{i-1})\right|, \quad (1.35)$$

где R - время отправки пакета, S - время доставки пакета.

На основе рассылки тестовых пакетов и измерений определяется среднее значение джиттера $\overline{J}$.

Для определения $\overline{J}$ проведено имитационное моделирование последовательной сети в среде Anylogic. Результаты моделирования сети при различных N и ρ сведены в таблицу 2.

Таблица 2 - Результаты моделирования сети для определения $\overline{J}$

N	$\overline{J}$	$J_{\min} * 10^{-6}$	$J_{\max}$	σ_j
	$\rho = 0.2$			
2	3.57	0.08	54.48	3.6
3	4.92	2.66	86.31	5.08
4	6.12	2.5	113.28	6.48
5	7.14	2.95	134.06	7.77
	$\rho = 0.5$			
2	7.39	1.51	113.28	7.85
3	9.01	1.59	187.55	10.48
4	10.12	4.6	241.19	12.71
5	10.87	1.45	300.65	14.74
	$\rho = 0.8$			
2	9.53	1.34	206.54	10.48
3	10.26	2.58	332.68	12.59
4	10.62	4.89	344.88	14.31
5	10.8	3.48	538.09	15.75

Анализ полученных данных показывает, максимальное значение $J_{\max}$ и среднее квадратичное отклонение джиттера σ_j повышаются с увеличением N и ρ. Среднее значение джиттера $\overline{J}$ в 10-50 раз меньше, чем значения джиттера J, рассчитанного с помощью формулы (5) на основе рекомендации Y.1541. Вероятность того, что значение джиттера больше, чем среднее значение, равна 0.35. Поэтому для достоверной оценки J по результатам измерения необходимо построить гистограмму распределения джиттера. Далее, провести аппроксимацию гистограмм и определить J_p уровня значимости p. На основе сравнения J (таблица 1) и $J_{\max}$ (таблица 2) следует, что при тестовом испытании для приближенной оценки джиттера J можно использовать его максимальное значение $J_{\max}$.

Литература:

1. ITU-T. Network performance objectives for IP- based services. Recommendation Y.1541. Geneva, 2006.

2. Амирсаидов У.Б., Махмудов С.О., Мусоходжаева И.А. Метод расчета характериситик сети массового обслуживания с зависимым потоком.- Вестник ТУИТ, 2014, №3, с.63-69.

3. Никульский И.Е. Моделирование сегмента широкополосной сети доступа, использующего технологию пассивных оптических сетей GPON//Материалы Четвертой всероссийской научно-практической конференции по имитационному моделированию ИММОД-2009, Т.2.-СПб.,2009.- с.187-193.

4. Кузовлев А.В. Контроль качества в сетях IP.- Техника Связи , №3-4, 2009, с.20-24.

И.В. Щербань, *Д.Е. Антонов, *Р.В. Быкадоров

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ МИКРОЭЛЕКТРОМЕХАНИЧЕСКИХ АКСЕЛЕРОМЕТРОВ

Северо-Кавказский филиал Московского технического университета связи
и информатики, г.Ростов-на-Дону, Россия
*Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: микроэлектромеханическая система, калибровка, программное обеспечение, аппаратное обеспечение.

Реализован программно-аппаратный комплекс для исследования моделей статических погрешностей микроэлектромеханических (МЭМС) акселерометров. Экспериментальные исследования проведены на МЭМС-микросхеме LSM303DLH, включающей три акселерометра с ортогонально ориентированными измерительными осями.

I.V. Shcherban, *D.E. Antonov, *R.V. Bykadorov

THE TECHNICAL COMPLEX FOR THE RESEARCH OF THE CHARACTERISTICS OF MEMS ACCELEROMETERS

The North Caucasian Branch of the Moscow Technical University
of Communications and Informatics, Rostov-on-Don, Russia
*Southern Federal University, Rostov-on-Don, Russia

Keywords: microelectromechanical systems, sensor calibration, hardware, software.

The technical complex for the research of the models of the measurement disturbances of MEMS accelerometers have been realized. Experiments were carried out on the MEMS chip LSM303DLH, consisting of three accelerometers with orthogonally oriented measurement axes.

Перспективы современного приборостроения связаны с созданием функциональных элементов, обладающих малыми массой, габаритными размерами, энергопотреблением и себестоимостью при безусловном выполнении целевой функции с заданной точностью. Известно, что технологии микроэлектромеханических систем (МЭМС) обеспечивают высокий уровень функциональности, надёжности и низкую цену конструируемых на их основе измерительных преобразователей (ИП), например, инерциальных датчиков. Основными недостатками таких датчиков являются сравнительно низкая точность, зашумленность выходного сигнала, а также принципиальная невозможность формирования на сегодняшний день точных моделей погрешностей ИП МЭМС. Последний факт обусловлен нестабильностью этих моделей, сильной зависимостью модельных параметров от внешних условий – от температуры, характеристик источника питания и т.п. факторов. Таким образом требуется периодическая коррекция моделей погрешностей ИП МЭМС в ходе их эксплуатации. Соответственно, представляет интерес, разработанный программно-аппаратный комплекс для исследования статических погрешностей МЭМС микросхем, которые могут содержать до 3 акселерометров.

Аппаратная часть реализованного комплекса включает наклонно-поворотный стол (НПС), преобразователь выходных сигналов цифрового выхода микросхемы МЭМС в протокол UART 2.0 (рис. 1) и ЭВМ.

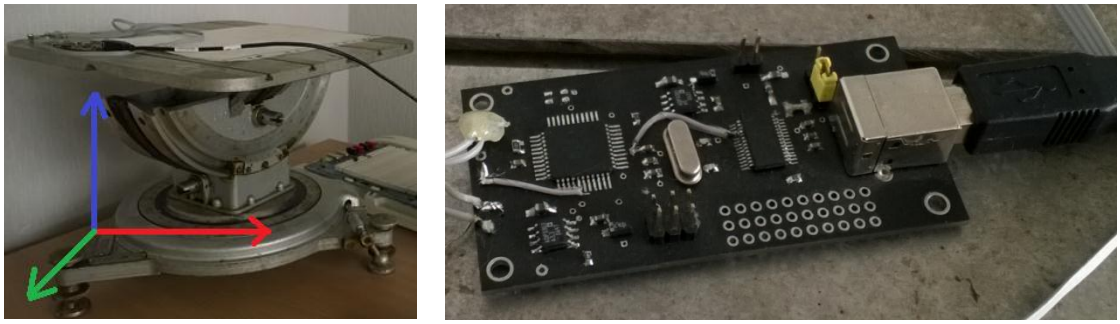


Рисунок 1. Наклонно-поворотный стол и преобразователь выходных сигналов в формат UART

НПС позволяет задавать требуемую ориентацию осей чувствительности (ОЧ) акселерометров относительно плоскости горизонта с точностью до 3 угл. мин. Указанной точности вполне достаточно для оценки погрешностей датчиков такого типа. Так, погрешности измерений точно рассчитываемого в месте испытаний гравитационного ускорения, обусловленные погрешностями выставки НПС, имеют в этом случае порядок 10^{-6} м/с^2. Шумовая же погрешность акселерометров микросхемы, например, LSM303DLH характеризуется среднеквадратичным отклонением (СКО) 0,015 м/с^2, что предопределяет порядок погрешностей в измерениях ускорений 10^{-2} м/с^2.

Программная часть комплекса реализована на основе технологии виртуальных приборов LabVIEW National Instruments. Разработанный виртуальный приборв (DG) обеспечивает съём информации с акселерометров и датчиков угловой скорости (при необходимости), перевод битов в физические величины, запись данных в файлы данных и их статистическую обработку.

Разработана методика статистической обработки измеренных данных. Выполняется проверка шумов ИП МЭМС на гауссовость, рассчитываются параметры шума – математическое ожидание, СКО. Фрагменты панели ВП и блок-диаграммы расчёта точечных характеристик шумов измерений, построения гистограмм распределения случайных величин представлены на рисунках 2-4.

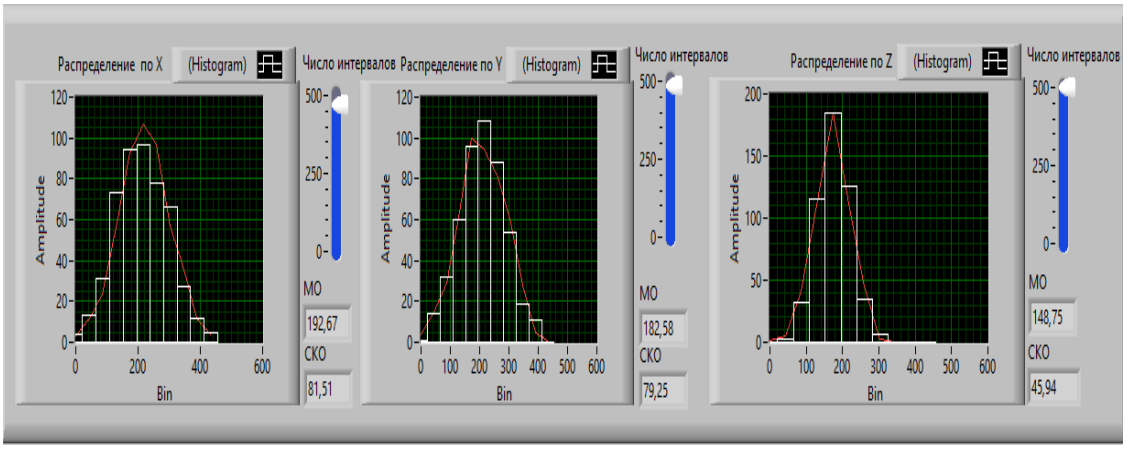
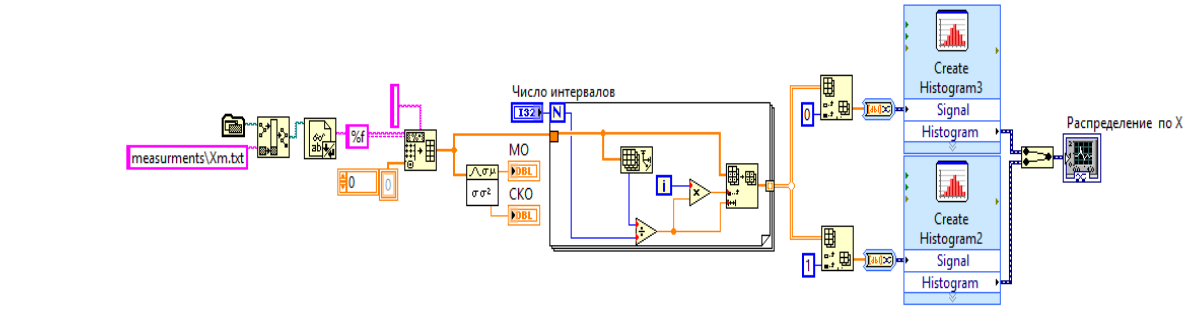
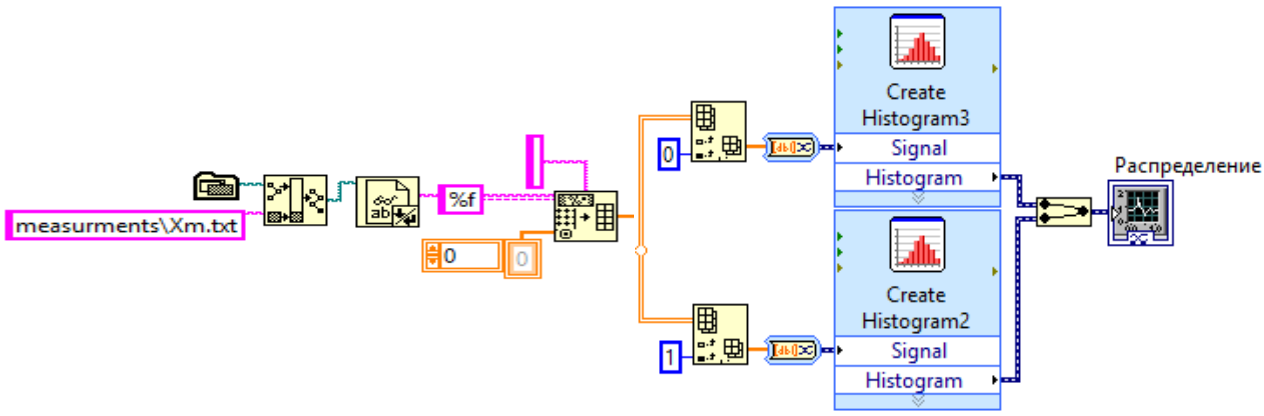


Рисунок 2. Фрагмент лицевой панели ВП



а)



б) в)

Рисунок 3.Фрагменты блок-диаграммы ВП:
а) расчет точечных характеристик шума измерений; б) считывание входных данных и их запись в массив; в) статистическая обработка измерений.

Разработанный программно-аппаратный комплекс позволяет проводить исследования моделей погрешностей акселерометров МЭМС микросхем. Микросхема может содержать до трех акселерометров.

Литература:

1. Распопов В.Я. Микромеханические приборы. М.: Машиностроение, 2007. 400с.
2. Коркишко Ю.Н. и др. Исследование работы БИНС в условиях высоких широт с учетом погрешностей реальных датчиков //Доклады XVI Санкт-Петербургской межд. конф. по интегрированным навигационным системам, 25-27 мая 2009, с. 57-60.

У.Х. Арипова

ИНЖЕКЦИОННО – ВОЛЬТАИЧЕСКИЙ УПРАВЛЯЕМЫЙ ГЕНЕРАТОР ТОКА

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан.

Ключевые слова: генераторы стабильного тока, фото-вольтаического эффекта, инжекционно-вольтаическим эффектом, биполярный транзистор.

Исследована возможность использования биполярного транзистора, работающего в инжекционно – вольтаическом режиме, в качестве управляемого генератора стабильного тока. Создан трехструктурный инжекционно – вольтаический транзистор, одновременно реализующий

усиление и высокое выходное сопротивление (режим генератора тока). Разработан управляемый сильноточный генератор тока на биполярном транзисторе.

U.H. Aripova

INJECTION-VOLTAIC CONTROLLED CURRENT GENERATOR

Tashkent University of Information Technologies, Tashkent, Uzbekistan.

Keywords: stable currentgenerators, photo-voltaiceffect, injection-voltaiceffect,thebipolar transistor.

Possibility of use of the bipolar transistor working in injection-voltaic a mode, as the operated generator of a stable current is investigated. It is created three-structural injection-voltaic the transistor simultaneously realizing strengthening and high-current resistance (a mode of the generator of a current). It is developed operated high-current the current generator on the bipolar transistor.

Теоретический анализ связи фото-вольтаического эффекта (ФВЭ) в солнечных элементах с инжекционно - вольтаическим (ИВ) эффектом (ИВЭ) в многослойных полупроводниковых *p-n* структурах и перспективы создания сильноточной и низковольтной (напряжение питания порядка контактной разности потенциалов) элементной базы устройств электроники приводятся в [1-3].

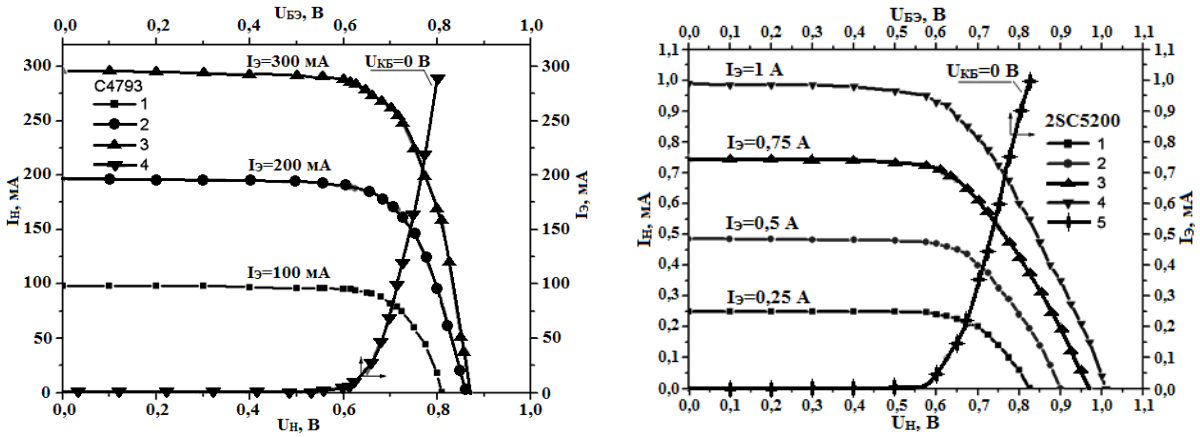
В полупроводниковой микроэлектронике широко используются генераторы стабильного тока [4], задача которых поддерживать величину выходного тока неизменной при изменениях значения нагрузки и входного, (питающего) напряжения. Идеальный генератор стабильного тока должен иметь на вольтамперной характеристике (ВАХ) горизонтальный участок, характеризующийся бесконечно большим значением динамического сопротивления. Генераторы стабильного тока, используемые в микроэлектронике, имеют малое значение генерируемого тока (до 1 мА). Мощные управляемые генераторы стабильного тока на основе биполярных транзисторов не разработаны. Вместе с тем, биполярный транзистор (БТ) в инжекционно-вольтаическом режиме (ИВР) работы уже является управляемым генератором тока (УГТ), на основе которого можно создать полупроводниковые устройства устойчивые при повышении рабочих температур и к нестабильности питания с высокими значениями выходного тока.

Управление генератором тока на основе БТ в ИВР можно осуществлять либо заданием напряжения эмиттер-база $E_Б$, либо токами эмиттера $I_Э$ или базы $I_Б$ БТ.

Моделирование работы БТ в ИВР проведено с использованием Multisim 10.1. Для моделирования использованы кремниевые БТ S4793 и 2SC5200 (*n-p-n* - структура), а также ZTX968 (*p-n-p* - структура).

На рис. 1 приведены экспериментальные нагрузочные и входные ВАХ БТ S4793 и 2SC5200. Они полностью подтверждают результаты моделирования и показывают, что в режиме ХХ при управлении током эмиттера сосредоточенное омическое сопротивление базы БТ $R_Б$ приводит к сдвигу напряжения ИВ ЭДС на величину падения напряжения $I_Б \cdot R_Б = I_Э \cdot R_Б$ [5,6].

Из рис. 1 б можно заключить, что при непосредственном последовательном соединении каскадов, одного, управляемого напряжением эмиттер база и второго, управляемого током эмиттера, входная характеристика выходит за пределы горизонтального участка соответствующего режиму генератора тока.



а) б)

Рисунок 1. Нагрузочные и входные ВАХ БТ С4793 (а) и SC5200 (б).

Следует отметить, что в данном случае транзистор, управляемый током, является нелинейной нагрузкой для транзистора, управляемого напряжением $E_Б$. Для того чтобы каскад, управляемый током, работал в режиме ограничения тока его входную характеристику необходимо сместить в область меньших напряжений каскада управляемого напряжением, что можно сделать включением источника напряжения смещения E_{CM} между базами каскадов.

Литература:

1. Арипов Х.К., Алимова Н.Б., Бустанов Х.Х., Объедков Е.В., Тошматов Ш.Т. - Инжекционно-вольтаический эффект на основе многослойных полупроводниковых структурах // Гелиотехника №1, 2009 г. С. 15-21.

2. Арипов Х.К., Алимова Н.Б., Бустанов Х.Х., Объедков Е.В., Тошматов Ш.Т. - Адаптированные электронные переключающие ячейки с питанием от солнечного элемента// Гелиотехника №2, 2009 г. С. 8-12.

3. Арипов Х.К., Алимова Н.Б., Бустанов Х.Х., Объедков Е.В., Тошматов Ш.Т. - Исследование усилительных свойств биполярного транзистора в инжекционно-вольтаическом режиме // Ахборот коммуникациялар: Тармоқлар-Технологиялар-Ечимлар, №1 (9), 2009й, С.22-25

4. Edwin W Greeneich. Analog Integrated Circuits-New York, Chapman & Hall, 1977. 341 p.

5. Арипов Х.К., Румянцев В.Д. Солнечные элементы с распределенными параметрами. 1. Вольтамперные характеристики при равномерном и неравномерном освещении // Гелиотехника. 1983, №4, С.6-10.

6. Арипов Х.К., Румянцев В.Д. Солнечные элементы с распределенными параметрами. 2. Эффективность фотоэлектрического преобразования // Гелиотехника. 1983, №5, С.6-10.

Арус Кинан, А.С. Еременко

ПРЕДОТВРАЩЕНИЕ ПЕРЕГРУЗКИ КАНАЛОВ СВЯЗИ ПРИ РЕАЛИЗАЦИИ ОТКАЗОУСТОЙЧИВОЙ МАРШРУТИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Харьковский национальный университет радиоэлектроники, г. Харьков, Украина

Ключевые слова: отказоустойчивость, маршрутизация, потоковая модель, схема резервирования, одноадресный поток.

Предложена модель отказоустойчивой одноадресной маршрутизации потоков в сети. Потоковая модель представлена алгебраическими уравнениями и неравенствами, которые характеризуют состояние сети, т.е. загруженность ее каналов связи. В модель заложены три основные схемы резервирования: защиты канала, узла и маршрута. Расчет основного и резервного маршрутов осуществляется в ходе решения оптимизационной задачи нелинейного

программирования. Предложенные условия предотвращения перегрузки позволяют учитывать случай, когда на резервные пути переключатся не все, а лишь некоторые из передаваемых потоков.

Arous Kinan, O.S. Yeremenko

LINKS OVERLOAD PREVENTION WITHIN FAULT-TOLERANT ROUTING IN TELECOMMUNICATION NETWORK

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Keywords: fault tolerance, routing, flow-based model, backup scheme, unicast flow.

A model of fault-tolerant unicast routing within the network proposed. Flow-based model is represented by algebraic equalities and inequalities that characterize the state of the network, i.e. utilization of its communication links. There are three main protection schemes in the proposed model: link, node and path. Calculation of the primary and backup routes is carried out with solving an optimization problem of nonlinear programming. Proposed conditions of overload prevention allows to consider the case when just some of the flows switched to the backup paths, but not all of them.

Важное место в общем комплексе мероприятий по обеспечению заданного качества обслуживания (Quality of Service, QoS) в современных мультисервисных телекоммуникационных сетях (ТКС) отводится средствам (моделям, методам и протоколам) маршрутизации. От эффективности решения маршрутных задач зависят ключевые показатели сквозного (end-to-end) QoS, такие как средняя задержка, джиттер, вероятность потерь пакетов и производительность ТКС в целом. Однако вдоль выбранного маршрута могут возникать отказы в обслуживании, вызванные перегрузкой или недостаточной эксплуатационной надежностью сетевого оборудования. В связи с этим, на первое место по своей актуальности выходят требования по повышению отказоустойчивости маршрутных решений. Учитывая то, что резервный путь рассчитывается одновременно с основным, реализуя определенную схему защиты – узла, канала, маршрута, время на переключение минимально, и определяется в основном скоростью обнаружения вероятных отказов. В данной работе развивается подход, ориентированный на решение проблем, связанных с предотвращением перегрузки каналов связи ТКС при реализации различных схем резервирования сетевых ресурсов в условиях мультипотокового трафика [1, 2]. В этой связи предлагается дальнейшее развитие потоковых моделей одноадресной отказоустойчивой маршрутизации [3, 4] за счет придания им функций борьбы с возможной перегрузкой.

Пусть при разработке потоковой модели маршрутизации структура ТКС описывается с помощью ориентированного графа $\mathbf{\Gamma} = (V, E)$, где $V = \{v_i, i = \overline{1,m}\}$ – множество вершин – узлов (маршрутизаторов) сети, а $(i, j) \in E$ – множество дуг графа, моделирующих каналы связи (КС) ТКС. Для каждого КС, моделируемого дугой $(i, j) \in E$, задана пропускная способность, измеряемая в пакетах в секунду (1/с), которая будет обозначаться как φ_{ij}. С каждым k-м потоком связано ряд параметров: r_k – средняя интенсивность потока на входе в сеть; s_k – узел-отправитель; d_k – узел-получатель. В ходе решения задачи маршрутизации необходимо рассчитать множество переменных x_{ij}^k, каждая из которых характеризует долю интенсивности k-го потока в КС $(i, j) \in E$; $k \in K$, где K – множество потоков в сети.

При однопутевой маршрутизации имеют место условия

$$x_{ij}^k \in \{0;1\}, \tag{1}$$

а при необходимости реализации многопутевых решений условия (1) заменяются на

$$0 \le x_{ij}^k \le 1. \tag{2}$$

Кроме того, с целью недопущения потерь пакетов на узлах и в сети в целом вводятся условия сохранения потока

$$\begin{cases} \sum\limits_{j:(i,j)\in E} x_{ij}^k - \sum\limits_{j:(j,i)\in E} x_{ji}^k = 0; \quad k \in K, \ i \neq s_k, d_k; \\ \sum\limits_{j:(i,j)\in E} x_{ij}^k - \sum\limits_{j:(j,i)\in E} x_{ji}^k = 1; \quad k \in K, \ i = s_k; \\ \sum\limits_{j:(i,j)\in E} x_{ij}^k - \sum\limits_{j:(j,i)\in E} x_{ji}^k = -1; \quad k \in K, \ i = d_k. \end{cases} \tag{3}$$

Для определения резервного пути необходимо, наряду с неизвестными x_{ij}^k, рассчитать дополнительные переменные $\bar{x}_{ij}^k$, которые характеризует долю k-го потока, протекающего в канале $(i,j) \in E$ резервного маршрута. На переменные $\bar{x}_{ij}^k$ также накладываются ограничения, подобные (1)-(3).

Кроме того, в структуру предлагаемой модели для предотвращения пересечения основного и резервного маршрутов с реализацией различных схем резервирования вводится ряд дополнительных условий-ограничений [3, 4]:

– при реализации схемы защиты (i,j)-канала в предлагаемую модель вводятся условия вида:

$$x_{ij}^k \bar{x}_{ij}^k = 0, \tag{4}$$

выполнение которых гарантирует использование (i,j)-канала лишь одним маршрутом – либо основным, либо резервным;

– при реализации схемы защиты i-го узла модель дополняется следующим условием:

$$\sum_{i:(i,j)\in E} x_{ij}^k \bar{x}_{ij}^k = 0, \tag{5}$$

выполнение которого гарантирует использование i-го узла (т.е. всех инцидентных ему каналов) либо основным, либо резервным маршрутом;

– для обеспечения защиты маршрута (маршрутов) в модель вводится условие:

$$\sum_{(i,j)\in E} x_{ij}^k \bar{x}_{ij}^k = 0, \tag{6}$$

что эквивалентно удовлетворению требований относительно отсутствия в основном и резервном маршрутах общих узлов и каналов (кроме узла-отправителя и узла-получателя).

Новизна модели состоит в том, что условие предотвращения перегрузки каналов связи записывается в виде:

$$\frac{1}{2}\sum_{k\in K} r^k \left((x_{ij}^k + \bar{x}_{ij}^k) + \sqrt{(x_{ij}^k - \bar{x}_{ij}^k)^2} \right) \le \varphi_{ij}, \ (i,j) \in E. \tag{7}$$

Использование условия (7) позволяет предотвратить перегрузку каналов и сети в целом даже в случае, когда на резервные пути переключатся не все, а лишь некоторые из передаваемых потоков.

Для расчета маршрутных переменных x_{ij}^k и при решении задач отказоустойчивой маршрутизации в ТКС необходимо минимизировать следующую целевую функцию:

$$F = \sum_{k\in K}\sum_{(i,j)\in E} c_{ij}^k x_{ij}^k + \sum_{k\in K}\sum_{(i,j)\in E} \bar{c}_{ij}^k \bar{x}_{ij}^k, \tag{8}$$

где c_{ij}^k и $\bar{c}_{ij}^k$ – маршрутные метрики каналов основного и резервного маршрутов соответственно. Функция (8) численно характеризует суммарные затраты на формирование и использование основного и резервного маршрутов между парой узлов отправитель-получатель.

Кроме того, в ходе исследования модели (1)-(8) установлена необходимость ее дополнения условием

$$\sum_{k\in K}\sum_{(i,j)\in E} c_{ij}^{k}x_{ij}^{k} \le \sum_{k\in K}\sum_{(i,j)\in E} \bar{c}_{ij}^{k}\bar{x}_{ij}^{k}, \quad (9)$$

выполнение которого гарантирует то, что основной путь (мультипуть) всегда будет эффективнее, т.е. производительнее или «короче» запасного в зависимости от выбора метрик c_{ij}^{k} и $\bar{c}_{ij}^{k}$.

Задача расчета маршрутных переменных при наличии ограничений (1), (3)-(6), (7), (9) с целевой функцией (8) относится к классу задач смешанного целочисленного нелинейного программирования. А при реализации многопутевой отказоустойчивой маршрутизации, то есть при учете условий (2) и (7) – это задача нелинейного программирования.

Эффективность предложенной модели (1)-(9) продемонстрируем на численном примере реализации схемы защиты канала (1, 3) при решении задачи однопутевой маршрутизации в сети, топология которой представлена на рис.1 для двух потоков. Сеть состоит из пяти узлов-маршрутизаторов и семи КС с пропускной способностью (пакетов в секунду, 1/с), показанной на дугах графа.

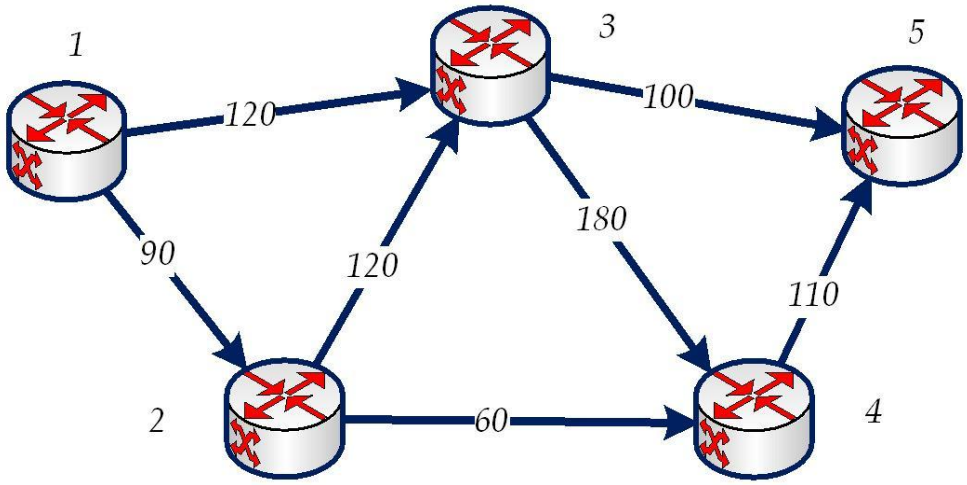


Рисунок 1. Топология анализируемой сети

Для первого потока: узел-отправитель – это первый маршрутизатор, узел-получатель – пятый маршрутизатор. Интенсивность потока – 80 1/с. Для второго потока: узел-отправитель – это второй маршрутизатор, узел-получатель – четвертый маршрутизатор. Интенсивность потока – 60 1/с. Метрика – число переприемов (hops), т.е. c_{ij}^{k} и $\bar{c}_{ij}^{k}$ равны единице.

В ходе решения задачи определено, что основной маршрут первого потока для указанной схемы будет включать в себя два переприема, проходя через узлы 1-3-5. Основной маршрут для второго потока будет включать лишь дугу 2-4. При реализации схемы защиты канала (1, 3) без учета условия (7) резервный маршрут для первого потока будет иметь три переприема и включать узлы 1-2-4-5. Однако использование канала (2, 4) первым и вторым потоками приведет к его перегрузке, т.к. суммарная интенсивность потока, протекающего по нем, будет составлять 140 1/с. Перегрузки удастся избежать, если при расчете резервного пути для первого потока принять во внимание условие (7), тогда искомый маршрут пройдет через узлы 1-2-3-5, не вызвав перегрузку сети.

Выводы.

Предлагается математическая модель отказоустойчивой маршрутизации для различных схем резервирования сетевых ресурсов (1)-(8). Модель представлена с линейными (1)-(3) и нелинейными (4)-(6), (7) условиями-ограничениями, которые совместно с целевой функцией (8) позволили сформулировать оптимизационную задачу по расчету искомых маршрутных переменных. В рамках модели заложена возможность реализации различных схем

резервирования: узла (5), канала (4) и маршрута (6). Новизна модели заключается в модификации условий предотвращения перегрузки каналов связи, по которым, в общем случае, одновременно могут протекать потоки как основных, так и резервных маршрутов. Использование условия (7) в ходе реализации многопутевой маршрутизации позволит предотвратить перегрузку каналов связи даже в случае, если только некоторые потоки будут переключаться из основных путей на резервные. Модель охватывает случай одноадресной (unicast) маршрутизации, но введенное условия (8) справедливо также и при организации многоадресной (multicast) и широковещательной (broadcast) маршрутизации, осуществляемой, например, в рамках модели, описанной в работах [5, 6].

Литература:

1. Hariyawan M. Y. Comparison Analysis of Recovery Mechanism at MPLS Network // International Journal of Electrical and Computer Engineering (IJECE), 2011, Vol.1, No.2, p. 151-160.

2. Xi K., Chao H. IP fast reroute for double-link failure recovery // Proceeding GLOBECOM'09 Proceedings of the 28th IEEE conference on Global telecommunications, 2009, p. 1035-1042.

3. Лемешко А.В., Романюк А.А., Козлова Е.В. Модель отказоустойчивой маршрутизации в MPLS-сети // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2013, с. 203-206.

4. Лемешко А.В., Козлова Е.В., Романюк А.А. Математическая модель отказоустойчивой маршрутизации, представленная алгебраическими уравнениями состояния MPLS-сети // Системи обробки інформації, Вип. 2 (109), 2013, с. 217-219.

5. Лемешко А.В., Кинан Моххамед Арус. Потоковая модель многоадресной маршрутизации // Материалы 23-й Международной конференции "СВЧ-техника и телекоммуникационные технологии" (КрыМиКо'2013), Севастополь, 8-13 сентября 2013 г., в 2 т. – Севастополь: Вебер, 2013, Т.1, с. 523-524.

6. Лемешко А.В. Потоковые модели многоадресной и широковещательной маршрутизации в телекоммуникационных сетях [Электронный ресурс] / А.В. Лемешко, К.М. Арус // Проблеми телекомунікацій, 2013, № 1 (10), с. 38 - 45. Режим доступа: http://pt.journal.kh.ua/2013/1/1/131_lemeshko_multicast.pdf.

О.О. Басов, Е.А. Васечкин, Д.А. Струев

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К ФОРМИРОВАНИЮ МНОЖЕСТВА СИСТЕМОТЕХНИЧЕСКИХ РЕШЕНИЙ ПО ПОСТРОЕНИЮ ПОЛИМОДАЛЬНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Академия Федеральной службы охраны Российской Федерации, г. Орел, Россия

Ключевые слова: полимодальная инфокоммуникационная система, эффективность, себестоимость, целостность информации.

На основе системного подхода рассмотрено обоснование рационального выбора системотехнических решений для построения полимодальных инфокоммуникационных систем (ПИКС). На основе предложенного подхода выполнена постановка задачи синтеза таких систем. Она заключается в формировании множества системотехнических решений, обеспечивающих при заданных условиях требуемую целостность информации. Представлены влияющие на нее ограничения. Сделан вывод о необходимости выбора конкретных вариантов реализации информационно-алгоритмической структуры ПИКС.

O.O. Basov, E.A. Vasechkin, D.A. Struev

METHODOLOGICAL APPROACH TO FORMING THE MULTITUDE OF THE CIRCUIT SOLUTIONS FOR CONSTRUCTING POLYMODAL INFOCOMMUNICATION SYSTEMS

Academy of Federal Agency of protection of Russian Federation, Orel, Russia

Keywords: polymodal infocommunication system, effectiveness, prime cost, information integtity.

The substantiation of the circuit solutions for polymodal infocommunication systems (PIS) construction rational choice is considered on the basis of the system approach. Based on the suggested approach the setting of such systems analysis task has been performed. It is confined in forming of the multitude of the circuit solutions which provide the required information integrity under given conditions. The limitations influencing the integrity are presented as well. The conclusion concerning the necessity of the choice of the PIS information-algorithmic structure specific variants realization is formed.

При проектировании систем инфокоммуникаций неизбежно возникают противоречия между желанием быстрого внедрения системы и получения требуемого эффекта при приемлемых затратах, желанием создавать систему традиционными методами и стремлением к принципиально новому подходу, исходя из сущности ПИКС [1, 2]. Под последними следует понимать взаимоувязанную совокупность систем обработки и хранения информации, телекоммуникационных сетей, их объединяющих, функционирующих под единым управлением с целью сбора, обработки, хранения, защиты, передачи и распределения, отображения и использования многомодальной информации, учитывающей смысл сообщаемых сообщений, личность абонентов (пользователей), их настроение, физиологическое и психоэмоциональное состояния и намерения.

При большом многообразии программно-аппаратных реализаций, способных обеспечить выполнение системных требований при максимуме внешней эффективности, возникает проблема их рационального выбора. Существующие и создаваемые программно-аппаратные средства характеризуются целым рядом различных показателей, которые различным образом могут влиять на структуру и принципы организации обмена полимодальной информацией.

Таким образом, возникает задача выбора рациональных системотехнических решений, а приведенные соображения требуют выработки общесистемного методологического подхода к формированию множества таких решений.

Методологический подход включает:

- обоснование перечня требований $P = \{p_i\}$, предъявляемых к ПИКС со стороны ее пользователей, на удовлетворение которых направлено множество услуг $S = \{s_i\}$;
- определение совокупности исходных условий $Z = \{z_i\}$ для проектирования сети передачи данных (СПД), включая возможности и тенденции ее развития;
- поиск оптимальных (квазиоптимальных) подходов к формированию множества Δ_α допустимых системотехнических решений;
- выбор показателя эффективности $Э^{ПИКС}$, отражающего способность ПИКС выполнять одну или несколько целевых функций с заданным качеством и являющегося функционалом $Э^{ПИКС} = F\{P, Z, \Delta_\alpha\}$.

Тогда в самом общем виде постановка задачи синтеза ПИКС заключается в отыскании такого варианта с параметрами $\overline{\alpha}_\alpha \subset \Delta_\alpha$, который при удовлетворении требованиям P с учетом заданных исходных условий Z обладал бы наибольшей эффективностью:

$$Э^{ПИКС} = \max_{\overline{\Delta}_\alpha}\left(F\{P, Z, \Delta_\alpha\}\right). \quad (1)$$

Сформулированная задача (1) по своему характеру является оптимизационной, поэтому множество Δ_α с формальных позиций теории исследования операций может трактоваться как множество оптимальных системотехнических решений.

Необходимо отметить, что на практике применительно к распределенным ПИКС строгое решение поставленной задачи (1) как оптимизационной в общем виде оказывается крайне затруднительным. Причинами этого служат различная степень важности показателей эффективности $Э^{ПИКС}$ современных инфокоммуникационных систем различного назначения и сложный вид их функциональной зависимости от параметров $\bar{\alpha}_\alpha \subset \Delta_\alpha$. Поэтому при выборе основных системотехнических решений по построению ПИКС может быть использован известный подход, состоящий, во-первых, в ее декомпозиции на подсистемы, во-вторых, в оптимизации одного из параметров при ограничениях на остальные, в-третьих, в обоснованном применении различных показателей эффективности $Э^{ПИКС}$ с учетом особенностей решаемых частных задач [3].

Предложенная в [2] декомпозиция показателя удельной себестоимости ПИКС позволяет представить задачу синтеза ПИКС (1) в виде:

$$\varsigma^{ИНФ} = \max_{\bar{\Delta}_\alpha}\left(F_1\left\{R, \Delta_\alpha\right\}\right) \tag{2}$$

при

$$\varsigma^{СПД} = \max_{y \in Y}\left(F_2\left\{Z, Y, H, V, O, X\right\}\right). \tag{3}$$

Здесь $\varsigma^{ИНФ}$ и F_1 – показатель и функционал удельной себестоимости информации; $R = \{r_k, k \in C\}$ – множество инфокоммуникационных ресурсов; $\varsigma^{СПД}$ и F_2 – показатель и функционал удельной себестоимости СПД; Y – множество управляемых переменных; H – множество неуправляемых переменных; $V \supset R$ – множество выходных переменных; O – множество частных задач (проектных операторов); X – граф, определяющий отношения между элементами перечисленных множеств.

Область допустимых значений Y задается системой ограничений:

$$\varpi_Y = \Psi_\xi(Y), \quad \xi = \overline{1, \Im}, \tag{4}$$

где $\Im$ – число функций-ограничений.

Выражение (3) представляет собой классическую задачу синтеза сети в рамках программно-целевого подхода [4], господствующего в области анализа и синтеза телекоммуникационных систем и сетей. Тогда при реализации принципа мультисервисности [5] задачи синтеза ПИКС заключаются в формировании множества $\bar{\alpha}_\alpha \subset \Delta_\alpha$, которое при удельной себестоимости $\varsigma^{СПД}$ (3), полученной в результате синтеза СПД, способствующей предоставлению заданных инфокоммуникационных ресурсов *R*, и ограничении приведенных затрат на обработку информации $C_{пр}^{ИНФ} \le C_{пр}^{ИНФ\,доп}$ обеспечивало требуемую целостность информации [2]:

$$Ц^{ИНФ} = \max_{\bar{\Delta}_\alpha}\left(F_1\left\{R, \Delta_\alpha\right\}\right). \tag{5}$$

На целостность полимодальной информации влияют следующие ограничения:

1. Со стороны абонента – на способы человеко-машинного взаимодействия, связанные с его навыками использования абонентским терминалом (интерфейсом), информационных технологий, личными предпочтениями и физическими ограничениями: $UC = \{UC_i, i \in X\}$;
2. Со стороны абонентского терминала – на способы человеко-машинного взаимодействия, связанные с его программно-аппаратными возможностями: $DC = \{DC_j, j \in Y\}$;

3. Среды человеко-машинного взаимодействия (тип помещения и уровень шумов в нем, число абонентов, расстояние между абонентом и абонентским терминалом и др.): $EC = \{EC_k, k \in Z\}$;
4. Предоставляемых услуг, связанные с предметной областью, наличием доступа к инфокоммуникационным ресурсам, их объемом и типом: $SC = \{SC_l, l \in V\}$.

Для формирования множества Δ_α введены подмножества декартовых произведений исходных множеств макромодели, задающих пространство альтернатив синтеза:

$$F_{UC}^{(\alpha)} \subseteq P^{(\alpha)} \times S^{(\alpha)} \times R^{(\alpha)} \times D^{(\alpha)} \times AS^{(\alpha)} \times NS^{(\alpha)}; \quad (6)$$

$$F_{DC}^{(\alpha)} \subseteq P^{(\alpha)} \times S^{(\alpha)} \times R^{(\alpha)} \times D^{(\alpha)} \times AS^{(\alpha)} \times NS^{(\alpha)}; \quad (7)$$

$$F_{EC}^{(\alpha)} \subseteq P^{(\alpha)} \times S^{(\alpha)} \times R^{(\alpha)} \times D^{(\alpha)} \times AS^{(\alpha)} \times NS^{(\alpha)}; \quad (8)$$

$$F_{SC}^{(\alpha)} \subseteq P^{(\alpha)} \times S^{(\alpha)} \times R^{(\alpha)} \times D^{(\alpha)} \times AS^{(\alpha)} \times NS^{(\alpha)}, \quad (9)$$

где $D = \{d_b, b \in H\}$ – множество устройств ввода/вывода сигналов различных модальностей, доступных абоненту; $AS = \{as_q, q \in E\}$ и $NS = \{ns_a, a \in U\}$ – множества потоков искусственных и естественных сигналов, использующихся для анализа входных $IM = \{IM_1, IM_2, ..., IM_{N_{IM}}\}$ и синтеза выходных $OM = \{OM_1, OM_2, ..., OM_{N_{OM}}\}$ модальностей.

С учетом этого задача синтеза ПИКС сводится к поиску оптимальных (квазиоптимальных) подходов к формированию множества Δ_α с учетом ограничений UC, DC, EC, SC, реализующих систему на базе множества модальностей $NM^{(\alpha)} = IM^{(\alpha)} \cup OM^{(\alpha)}$:

$$\Delta_\alpha^{\text{огр}} = \begin{cases} \langle p_i^{(\alpha)}, s_g^{(\alpha)}, d_b^{(\alpha)}, r_k^{(\alpha)}, as_q^{(\alpha)}, ns_a^{(\alpha)} \rangle; \\ \Phi^{(\alpha)} : F_{UC}^{(\alpha)} \cap F_{DC}^{(\alpha)} \cap F_{EC}^{(\alpha)} \cap F_{SC}^{(\alpha)} \to B_m; \\ W^{(\alpha)} : AS \times NS \times T \to AS^{(\alpha)} \times NS^{(\alpha)}, \end{cases} \quad (10)$$

где $W^{(\alpha)} = \{w_f, f \in O\}$ – множество преобразований, выполняемых при реализации услуги в режиме реального времени T, а элементы множества B_m принимают значения $\{0,1\}$ [6].

В рамках предлагаемого методологического подхода необходим обоснованный выбор конкретных вариантов реализаций отображения $\Phi^{(\alpha)}$ информационно-алгоритмической структуры ПИКС и конфигурации программно-аппаратного обеспечения, необходимого для ее реализации.

Литература:

1. Басов О.О., Саитов И.А. Основные каналы межличностной коммуникации и их проекция на инфокоммуникационные системы // Труды СПИИРАН, 2013. Вып. 1(32). – С.152–170.

2. Басов О.О., Саитов И.А. Качество функционирования и эффективность полимодальных инфокоммуникационных систем. // Труды СПИИРАН, 2014. Вып. 7(30). – С.122–140.

3. Зацаринный А.А., Ионенков Ю.С., Кондрашев В.А. Об одном подходе к выбору системотехнических решений построения информационно-телекоммуникационных систем // Системы и средства информатики. Вып. 16. – М.: Наука, 2006.

4. Царегородцев, А.В. Кислицын А.В. Основы синтеза защищенных телекоммуникационных систем / под ред. Е. М. Сухарева. – М.: Радиотехника, 2006. – 256 с.

5. Концептуальные положения по построению мультисервисных сетей на ВСС РФ // Утв. Первым заместителем министра РФ по связи и информатизации 25.01.02. – М.: Минсвязи РФ, 2002.

6. Басов О.О., Никитин В.В., Илюшин М.В. Теоретико-множественная модель полимодальной инфокоммуникационной системы // Новые информационные технологии в научных исследованиях: материалы XVIII Всероссийской научно-технической конференции

студентов, молодых ученых и специалистов. Рязанский государственный технический университет, 2013. – 344 с. – С.60–62.

К.А. Батенков

НАПРАВЛЕНИЯ РАЗВИТИЯ СОВРЕМЕННЫХ МЕТОДОВ МОДУЛЯЦИИ

Академия ФСО России, г. Орёл, Россия

Ключевые слова: дискретное отображение непрерывного канала связи, оператор, модуляция, демодуляция, непрерывный канал связи.

Показано, что синтез сигналов для современных систем связи осуществляется на основе хорошо разработанных так называемых быстрых алгоритмов цифровой обработки сигналов, например дискретного преобразования Фурье, сложения по модулю два и др. Выделена основная особенность существующих методов модуляции и демодуляции сигналов, заключающуюся в поэтапной обработке сигналов в форме операторов заданного класса. Указано, что каждый из этапов порождает информационные потери, существенно влияющие на общие показатели технического эффекта синтезируемой системы передачи.

K.A. Batenkov

DEVELOPMENT DIRECTION OF MODERN MODULATION TECHNIQUES

The Academy of Federal Security Guard Service of the Russian Federation, Orel

Keywords: continuous channel discrete mapping, operator, modulation, demodulation, continuous channel.

Signal design realization for modern communication systems on base of well-exploit so-called fast digital signal processing algorithms e. g. discrete Fourier transform, congruence addition of two etc. is demonstrated. Modern modulation and demodulation technique basic feature consisting in phased signal processing in fixed operator class form is dedicated. Information losses generating each of phase and severely influencing on technical effect indexes of transmission system synthesized are indicated.

Хорошо известно, что выбор метода модуляции определяется, в первую очередь, средой передачи, по которой предполагается осуществлять передачу информации. Именно среда передачи в совокупности с оборудованием аналоговых окончаний моделируется в форме непрерывного канала связи и определяет потенциальные характеристики системы связи в целом. Так, анализ доступной литературы [1, 2, 3, 4, 5, 6], показал наличие существенных отличий в используемых методах модуляции для различных сред передачи информации. При этом можно отметить следующие особенности.

Методы модуляции для оптоволоконных кабелей используют достаточно простые маломощные формы одномерных сигнальных созвездий, что, очевидно связано как со свойствами непрерывного канала связи, который в данном случае оказывается существенно отличным от чисто гауссовского, так и с возможностями современной оптоэлектронной техники с точки зрения обработки сигналов на подобных высоких скоростях передачи данных. Вдобавок ко всему прочему, показатели скорости и достоверности, достигаемые с помощью оптоволоконных технологий, в настоящее время оказываются даже несколько избыточными, что, в свою очередь, не вызывает стимула к дальнейшему их развитию и приближению к теоретически возможным пределам технического эффекта.

В противоположность оптическим системам передачи линии радиосвязи функционируют в условиях жесткой конкуренции за ресурс непрерывного канала связи [7]. В результате применение наиболее современных и, как следствие, вычислительно затратных методов модуляции именно для подобных линий оказывается целесообразным.

Данное заключение справедливо как с позиции типа сигнальных созвездий, так и с точки зрения количества и формы несущих колебаний, причем для последних оно оказывается наиболее ярко выраженным, поскольку использование подобных сложных несущих направлено на формирование сигнала в линии радиосвязи, согласованного с широкополосными свойствами самого непрерывного канала, и одновременно снижающего негативное воздействие довольно распространенных узкополосных помех различного происхождения.

Методы модуляции в медножильных и коаксиальных кабелях являются близкими по свойствам к используемым в радиолиниях. Однако вследствие сравнительно более простых свойств непрерывного канала связи методы модуляции не отличаются разнообразием форм применяемых несущих [8].

В целом следует подчеркнуть постепенный переход в современных системах передачи к использованию все более и более широкополосных сигналов, которые наиболее полно используют предоставляемый ресурс непрерывного канала связи [9]. Однако вследствие вычислительной сложности формирования общего вида подобных сигналов, их синтез осуществляется на основе хорошо разработанных так называемых быстрых алгоритмов цифровой обработки сигналов, например дискретного преобразования Фурье, сложения по модулю два. В свою очередь данное существенное снижение сложности расчетов приводит к шести весьма серьезным последствиям (особенностям).

Во-первых, любое быстрое преобразование подразумевает наличие некоторых базисных функций, линейная свертка которых и формирует результирующих сигнал, передаваемый по непрерывному каналу связи. В результате осуществляется фиксация класса используемых сигналов, а значит, возможности дальнейшей подстройки под свойства непрерывного канала связи несколько сокращаются.

Во-вторых, достаточно полезные свойства несущих колебаний на входе непрерывного канала, например ортогональности, значительно упрощающие вычислительные процедуры, практически всегда нарушаются на его выходе из-за неидеальности фильтрационных и помеховых характеристик канала связи. В итоге неизбежны неустранимые искажения передаваемого сигнала и как следствие, возникает необходимость использования достаточно сложных механизмов кодирования и одновременно сравнительно маломощных сигнальных конструкций.

В-третьих, быстрые алгоритмы подразумевают использование линейных детерминированных схем обработки сигналов, а нелинейные и рандомизированные процедуры оказываются под запретом. Естественно, данное обстоятельство существенно влияет на результирующие показатели технического эффекта систем передачи информации, правда, как показали проведенные исследования, основанных на сравнительно сложных моделях непрерывных каналов связи, отличных от гауссовских детерминированных.

В-четвертых, применение как на передаче, так и на приеме быстрых алгоритмов подразумевает необходимость последующей обработки принимаемых сигналов в других функциональных узлах, что, естественно предполагает разбиение на минимум два этапа процедуры демодуляции, что, естественно, с точки зрения технического эффекта приводит к системе, имеющей заведомо более низкие показатели вследствие разного рода информационных потерь.

В-пятых, быстрые алгоритмы модуляции и демодуляции, основываются на наиболее общих свойствах непрерывного канала связи, например полосе пропускания или типа воздействующей помехи, а детальный учет характеристик канала, как правило, осуществляется другими функциональными узлами системы передачи информации. В результате оптимизация модулятора и демодулятора, в лучшем, случае осуществляется раздельно, а зачастую вообще, оптимизируется лишь приемная часть системы передачи.

В-шестых, достаточно эффективные современные методы пространственной обработки сигналов так же основываются на ограниченных классах сигналов, что влечет как формирование результирующего пространственно-временного сигнала в виде совокупности одномерных сигналов, так и необходимость выполнения временных и пространственных операций последовательно, а не совместно.

Таким образом, целесообразно выделить основную особенность существующих методов модуляции и демодуляции сигналов, заключающуюся в поэтапной обработке сигналов в форме операторов заданного класса. В результате каждый из этапов порождает информационные потери,

существенно влияющие на общие показатели технического эффекта синтезируемой системы передачи.

Литература:

1. Broadband optical access networks / Leonid G. Kazovsky, Ning Cheng, Wei-Tao Shaw, [et al.]. – Hoboken, New Jersey : John Wiley & Sons, Inc, 2011. – 283 p.

2. Horak, R. Telecommunications and data communications handbook / Ray Horak. – Hoboken, New Jersey : John Wiley & Sons, Inc, 2007. – 791 p.

3. MIMO-OFDM for LTE, WiFi, and WiMAX : coherent versus non-coherent and cooperative turbo-transceivers / L. Hanzo, J. Akhtman, L. Wang, M. Jiang. – UK : John Wiley & Sons Ltd, 2011. – 658 p.

4. Fazel, K. Multi-carrier and spread spectrum systems: from OFDM and MC-CDMA to LTE and WiMAX / K. Fazel, S. Kaiser. – 2nd ed. – Chichester : John Wiley & Sons Ltd, 2008. – 260 p.

5. Krouk, E. Modulation and coding techniques in wireless communications / E. Krouk, S. Semenov. – Chichester : John Wiley & Sons Ltd, 2011. – 662 p.

6. Батенков, А. А. Синтез многомерных ансамблей сигналов для гауссовского дискретного канала связи / А. А. Батенков, К. А. Батенков // Вестник Рязанского государственного радиотехнического университета. – 2008. – № 25. – С. 7–14.

7. Батенков, К. А. Математическое моделирование непрерывных многопараметрических каналов связи в операторной форме // Телекоммуникации. – 2013. – № 10. – С. 2–4.

8. Батенков, К. А. Алгоритм формирования несущих колебаний для линейного канала связи с аддитивным белым гауссовским шумом // Телекоммуникации. – 2008. – № 3. – С. 10–15.

9. Батенков, К. А. Необходимые условия оптимальности операторов модуляции и демодуляции // Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов: сб. ст. / [сост. А.В. Калачев, В.В. Белозерских]. – Барнаул : Барнаул, 2013. – С. 58–62.

С.А. Бережной, Ю.А. Карпенко,
Р.Н. Сулейманов, Н.В. Руденко, *Н.Я. Половинчук

ЭЛЕКТРОННЫЙ ПРАКТИКУМ: СРЕДСТВА И АЛГОРИТМ РАЗРАБОТКИ

Донской государственный технический университет, г. Ростов-на-Дону, Россия
*Ростовский филиал Московского государственного университета
гражданской авиации, г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, электронный практикум, алгоритм, математическое моделирование, виртуальная модель электрической цепи.

Предложены программные средства и алгоритм разработки электронного практикума по электротехническим дисциплинам. В качестве примера рассмотрен алгоритм расчёта цепи синусоидального тока в программе *Mathcad.* Показана целесообразность проверки расчета цепи в программе *Multisim.* Полное совпадение показаний приборов виртуальной модели, реализованной в программе *Multisim,* с соответствующими результатами расчета в программе *Mathcad* свидетельствует о верности полученных результатов. Предложенный алгоритм позволяет преподавателю высшего учебного заведения разрабатывать качественные электронные практикумы по электротехническим дисциплинам.

S.A. Berezhnaya, Yu.A. Karpenko,
R.N. Suleymanov, N.V. Rudenko, *N.Ya. Polovinchuk

ELECTRONIC PRACTICAL WORK: MEANS AND ALGORITHM OF DEVELOPMENT

Don State Technical University, Rostov-on-Don, Russia
*Rostov branch of Moscow State University civil aviation, Rostov-on-Don, Russia

Keywords: information technologies, electronic practical work, algorithm, mathematical modeling, virtual model of an electric chain.

Software and algorithm of development of an electronic workshop on electrotechnical disciplines are offered. As an example the algorithm of calculation of a chain of sinusoidal current in the Mathcad program is considered. Expediency of check of calculation of a chain is shown in the Multisim program. Full coincidence of indications of devices of the virtual model realized in the Multisim program to the corresponding results of calculation in the Mathcad program testifies to fidelity of the received results. The offered algorithm allows the teacher of a higher educational institution to develop qualitative electronic workshops on electrotechnical disciplines.

Постановка задачи. Формирование компетенций выпускников в соответствии с ФГОС ВПО третьего поколения - важнейшая задача ВУЗа. Среди этих компетенций особое место занимают компетенции, связанные с владением выпускниками информационными технологиями. В настоящее время отсутствует общепринятый алгоритм разработки электронного практикума для проведения практических или лабораторных занятий по электротехническим дисциплинам. Эти дисциплины являются базовыми для формирования будущих специалистов в таких областях как радиотехники, связь, автоматика, электротехники, поэтому разработки указанного алгоритма актуальна. В данной статье обобщен опыт преподавателей ДГТУ и РФ МГТУ ГА в форме алгоритма разработки электронного практикума для проведения практических или лабораторных занятий.

Материалы исследования. При разработке электронного практикума преподавателю ВУЗа целесообразно использовать [1, с.303; 2, с.5]: основную образовательную программу (ООП) по направлению подготовки и рабочую программу дисциплины (РПД); курс лекций по дисциплине; информационную среду обучения. На основе анализа литературы и опыта авторов предлагается **следующий алгоритм разработки электронного практикума по электротехническим дисциплинам**.

1. Учебный материал дисциплины разбивается на модули в соответствии с дидактическими единицами содержания дисциплины согласно ООП и РПД.
2. В каждом модуле для практических и лабораторных занятий выбираются объекты исследования, формулируется темы, цели и задачи исследования (расчёта) с учетом необходимости формирования требуемых компетенций согласно ООП и РПД;
3. Выбирается программное обеспечение с учётом возможностей ВУЗа;
4. Разрабатывается и отлаживается виртуальная модель объекта, например, в системе *Mathcad* - в форме математической модели (системы уравнений) и программы её решения; в системе *Multisim* - в форме схемотехнической модели, содержащей виртуальные приборы.
5. Разрабатывается методика исследования виртуальной модели и форма представления результатов исследования (расчёта).
6. Разрабатываются методические рекомендации для преподавателей и студентов в электронном виде по организации и выполнению исследования (расчётов), а также по формулированию выводов.
7. Предлагаются контрольные вопросы (тесты - при дистанционном обучении) для контроля усвоения учебного материала и формирования компетенций.

Рассмотрим применение алгоритма на примере разработки практического занятия на тему «Расчет цепи синусоидального тока символическим методом» по дисциплине «Основы теории цепей» для бакалавров по направлению подготовки «Радиотехника».

В качестве программного обеспечения целесообразно использовать систему компьютерной математики *Mathcad* и систему схемотехнического моделирования *Multisim*. Главное их достоинство - простота и наглядность использования для учебных целей [3, с.16]. Так *Mathcad* позволяет вводить математические выражения с помощью встроенного редактора формул, причём в виде, максимально приближённому к общепринятому, и тут же получить результат [3, с.16]. На занятии студентам предлагается по вариантам выполнить расчет цепи, схема замещения которой представлена на рисунке 1. Необходимо определить токи в ветвях, активную, реактивную и полную мощности всей цепи, составить баланс мощностей, построить векторную диаграмму напряжений и токов, записать выражения для мгновенных значений всех токов и напряжений, изобразить временную диаграмму тока, напряжения и мощности источника.

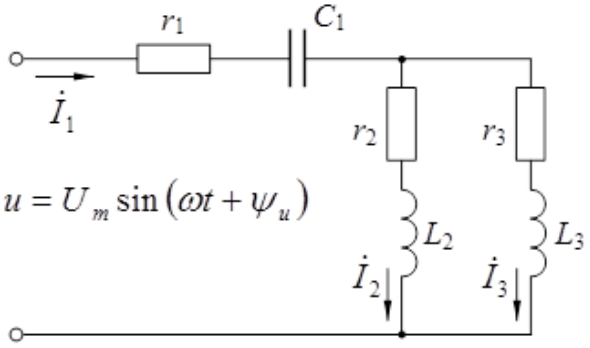


Рисунок 1. Схема замещения цепи синусоидального тока

Алгоритм расчёта в системе *Mathcad* содержит следующие этапы.

1. Ввод исходных данных в программу (рисунок 2). Для каждого студента задаётся индивидуальный вариант параметров цепи и напряжения источника.

$U_m := 141V$ $r_1 := 9ohm$ $L_2 := 9.55mH$

$\psi_u := 30deg$ $r_2 := 2ohm$ $L_3 := 0.04henry$

$f := 50Hz$ $r_3 := 12ohm$ $C_1 := 320\mu F$

Рисунок 2. Ввод исходных данных в программу

2. Расчет реактивных сопротивлений цепи и перевод сопротивлений участков цепи и напряжения в комплексную форму (рисунок 3).

$\omega := 2\cdot\pi\cdot f$ $\omega = 314.159\,s^{-1}$ $x_{L2} := \omega\cdot L_2$ $x_{L2} = 3\,ohm$

$x_{L3} := \omega\cdot L_3$ $x_{L3} = 12.566\,ohm$ $x_C := \frac{1}{\omega\cdot C_1}$ $x_C = 9.947\,ohm$

$Z_1 := r_1 - j\cdot x_C$ $Z_1 = (9 - 9.947i)\,ohm$

$Z_2 := r_2 + j\cdot x_{L2}$ $Z_2 = (2 + 3i)\,ohm$

$Z_3 := r_3 + j\cdot x_{L3}$ $Z_3 = (12 + 12.566i)\,ohm$

$U := \frac{U_m}{\sqrt{2}}\cdot\exp(j\cdot\psi_u)$ $U = (86.345 + 49.851i)\,V$

$Z_{общ} := \frac{Z_2\cdot Z_3}{Z_2 + Z_3} + Z_1$ $Z_{общ} = (10.734 - 7.508i)\,ohm$

Рисунок 3. Расчет реактивных сопротивлений цепи и перевод сопротивлений участков цепи и напряжения в комплексную форму.

3. Расчёт комплексных значений токов в ветвях и напряжений на участках схемы выполняется на основе закона Ома и Кирхгофа (рисунок 4)

$$I_1 := \overrightarrow{\left(\frac{U}{Z_{общ}}\right)} \quad I_1 = (3.22 + 6.897i)\,A \qquad U_1 := \overrightarrow{(I_1 \cdot Z_1)} \quad U_1 = (97.586 + 30.04i)\,V$$

$$U_{ab} := \overrightarrow{(U - U_1)} \quad U_{ab} = (-11.241 + 19.811i)\,V \qquad I_2 := \overrightarrow{\left(\frac{U_{ab}}{Z_2}\right)} \quad I_2 = (2.842 + 5.642i)\,A$$

$$I_3 := \overrightarrow{\left(\frac{U_{ab}}{Z_3}\right)} \quad I_3 = (0.378 + 1.255i)\,A$$

Рисунок 4. Расчет искомых комплексных значений токов в ветвях и напряжений.

4. Расчёт действующих значений и начальных фаз токов в ветвях и напряжений на участках цепи (рисунок 5)

$$Iэ_1 := |I_1| \quad Iэ_1 = 7.612\,A \qquad \psi_1 := \arg(I_1) \quad \psi_1 = 64.972\,deg$$

$$Uэ_1 := |U_1| \quad Uэ_1 = 102.105\,V \qquad \psi_2 := \arg(I_2) \quad \psi_2 = 63.26\,deg$$

$$Uэ_{ab} := |U_{ab}| \quad Uэ_{ab} = 22.778\,V \qquad \psi_3 := \arg(I_3) \quad \psi_3 = 73.251\,deg$$

$$Iэ_2 := |I_2| \quad Iэ_2 = 6.317\,A \qquad \psi_4 := \arg(U_1) \quad \psi_4 = 17.11\,deg$$

$$Iэ_3 := |I_3| \quad Iэ_3 = 1.311\,A \qquad \psi_5 := \arg(U_{ab}) \quad \psi_5 = 119.572\,deg$$

Рисунок 5. Расчёт действующих значений токов в ветвях и напряжений на участках цепи.

5. Расчёт активной, реактивной и полной мощности потребителей. Проверка решения методом баланса мощностей (рисунок 6)

$$Pп := Iэ_1^2 \cdot r_1 + Iэ_2^2 \cdot r_2 + Iэ_3^2 \cdot r_3 \quad Pп = 621.858\,W$$

$$Qп := -Iэ_1^2 \cdot x_C + Iэ_2^2 \cdot x_{L2} + Iэ_3^2 \cdot x_{L3} \quad Qп = -434.977\,V{\cdot}A\,p$$

$$Sп := \sqrt{Pп^2 + Qп^2} \quad Sп = 758.889\,V{\cdot}A$$

$$Sи := U \cdot \overline{I_1} \quad Sи = (621.858 - 434.977i)\,V{\cdot}A$$

$$Pи := Re(Sи) \quad Pи = 621.858\,W$$

$$Qи := Im(Sи) \quad Qи = -434.977\,V{\cdot}A\,p$$

$$Sи := |Sи| \quad Sи = 758.889\,V{\cdot}A$$

Рисунок 6. Расчёт активной, реактивной и полной мощности источника. Проверка решения методом баланса мощностей.

Баланс мощностей сходится, следовательно, расчёт токов выполнен правильно.

6. Построение векторной диаграммы токов и напряжений. Используется алгебраическую форму записи (рисунок 7)

$$I_j := \begin{pmatrix} 3.197 + 6.895i \\ 2.812 + 5.665i \\ 0.385 + 1.23i \end{pmatrix} \qquad U_j := \begin{pmatrix} 86.345 + 49.851i \\ 97.715 + 30.087i \\ -11.371 + 19.764i \end{pmatrix}$$

$$k := 0..2$$

$$Ix_k := \begin{pmatrix} 0 \\ Re(I_{j_k}) \end{pmatrix} \qquad Iy_k := \begin{pmatrix} 0 \\ Im(I_{j_k}) \end{pmatrix}$$

$$Ux_k := \begin{pmatrix} 0 \\ Re(U_{j_k}) \end{pmatrix} \qquad Uy_k := \begin{pmatrix} 0 \\ Im(U_{j_k}) \end{pmatrix}$$

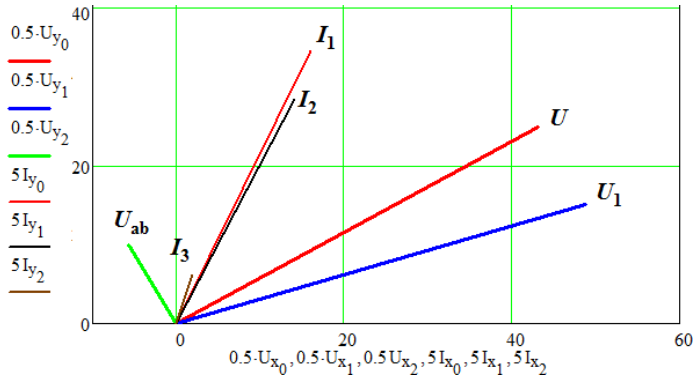


Рисунок 7. Векторная диаграмма напряжений и токов.

8. Записываются выражения для мгновенных значений токов в ветвях и напряжений на участках цепи (рисунок 8):

$$i_1 = 7.612\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 64.972^{o}\right) \qquad u_1 = 102.105\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 17.11^{o}\right)$$
$$i_2 = 6.317\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 63.26^{o}\right) \qquad u_{ab} = 22.778\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 119.572^{o}\right)$$
$$i_3 = 1.311\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 73.251^{o}\right) \qquad u = 100\cdot\sqrt{2}\cdot\sin\left(314.159\cdot t + 30^{o}\right)$$

Рисунок 8. Мгновенные значения токов в ветвях и напряжений на участках цепи.

9. Изображаются временные диаграммы напряжения, тока и мгновенной мощности источника (рисунок 9)

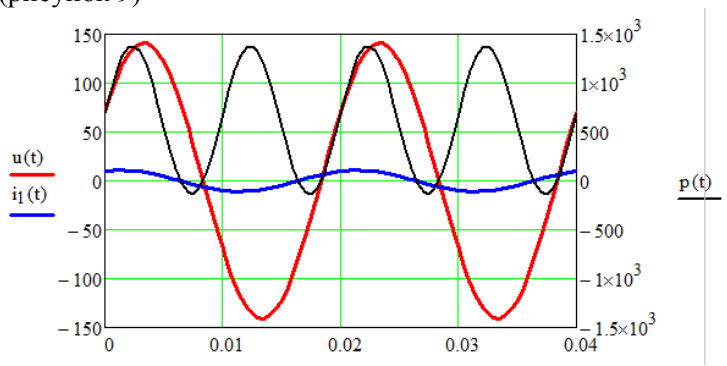


Рисунок 9. Временная диаграмма напряжения, тока и мгновенной мощности источника.

Проверка расчета цепи переменного тока символическим методом может быть выполнена в программной среде *Multisim*. Виртуальная модель цепи переменного тока, реализованная в программе *Multisim* в соответствии с изложенным алгоритмом, приведена на рисунке 10. Результаты её моделирования представлены на рисунке 11.

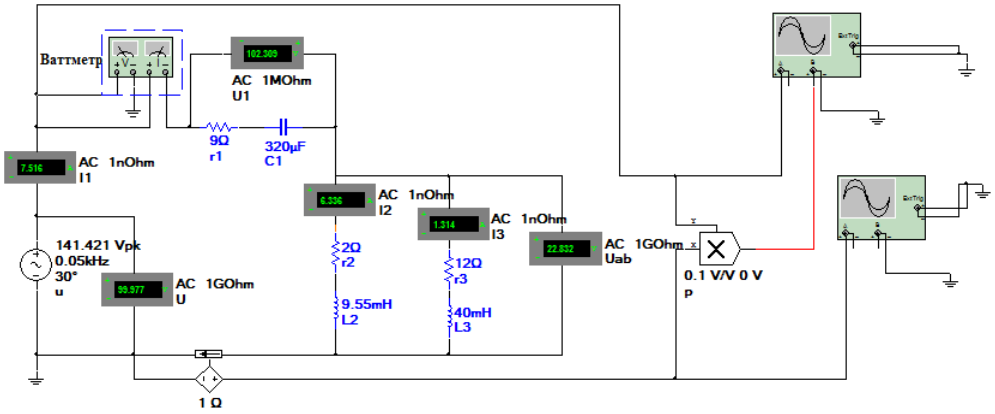


Рисунок 10. Виртуальная модель цепи переменного тока.

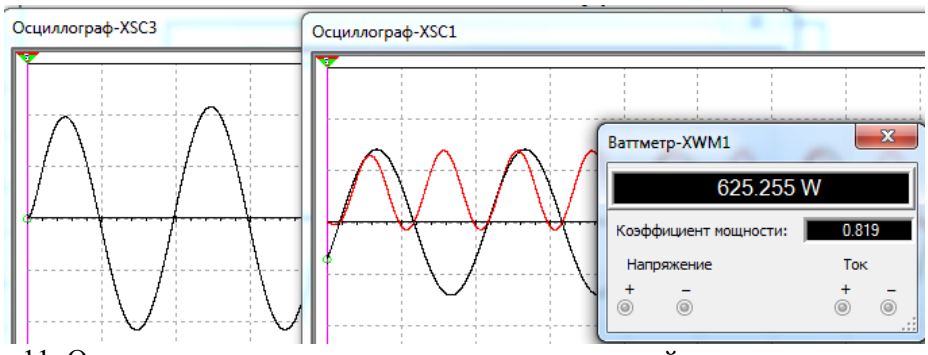


Рисунок 11. Осциллограммы тока, напряжения и мгновенной мощности источника ЭДС виртуальной модели цепи.

Сравнительный анализ свидетельствует о том, что показания приборов виртуальной модели, реализованной в программе *Multisim*, полностью совпадают с соответствующими результатами расчета в программе *Mathcad.*

Вывод. Предложенный алгоритм позволяет преподавателю разрабатывать качественные электронные практикумы по электротехническим дисциплинам, как для очной формы обучения, так и для дистанционной.

Литература:

1. Миронов В.Н. Разработка и внедрение электронного практикума по дисциплине «Электротехнические материалы» // Вестник Астраханского ГТУ. 2007. № 2. С. 302-305.
2. Руденко Н.В., Половинчук Н.Я., Семергей С.В. Основы теории цепей. Лабораторный практикум. - Ростов-на-Дону: РИО РТИСТ ФГБОУ ВПО «ЮРГУЭС», 2012. 92 с.
3. Любимов Э.В. Теория и практика электротехнических расчётов в среде *Mathcad* и *Multisim.* СПб.: Наука и Техника, 2012. 400 с.

Э.А. Бинеев, А.В. Бородин

ОЦЕНКА ВРЕДНОСТИ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ

Северо-Кавказский филиал Московского технического университета связи и информатики, Россия, г. Ростов-на-Дону,

Ключевые слова: электромагнитное поле, напряженность электрического поля

Аннотация: Приведен анализ методов измерения напряженности низкочастотных электрических полей, а также полей радиочастотного диапазона. Рассмотрены факторы, влияющие на выбор, погрешность и методику измерений.

E.A. Bineev, A.V. Borodin

ASSESSMENT OF HARMFULNESS OF ELECTROMAGNETIC FIELDS

North Caucasian branch of the Moscow Technical University of Communications and Informatics, Russia, Rostov-on-Don

Keywords: electromagnetic field, the electric field strength

Abstract: An analysis of methods for measuring the intensity of low-frequency electric fields and radio frequency fields. The factors influencing the choice, accuracy and measurement technique.

Пространство около источника переменного электромагнитного поля (ЭМП) делится на две зоны: ближнюю, или зону индукции, и волновую зону излучения. В зоне индукции работающие подвергаются воздействию различных по величине электрических и магнитных полей, поэтому их интенсивность оценивается раздельно величинами напряженности электрической (*Е, В/м*) и магнитной (*Н, А/м*) составляющих. Эти поля имеют место при работе с источниками низко-, высоко- и ультравысокочастотных излучений. В диапазоне частот 300 МГц – 300 ГГц интенсивность ЭМП характеризуется плотностью потока энергии (ППЭ, $Вт/м^2$). Нормативные значения ЭМП приведены в [1,2].

Для уменьшения потерь при передаче электроэнергии на большие расстояния растут уровни передаваемых по воздушным линиям электропередач (ЛЭП) напряжений, которые уже достигли 1150 кВ. При этом возникает ряд проблем, связанных, во- первых, с необходимостью развития соответствующих систем изоляции техники передачи электроэнергии, а во- вторых, с возрастающим воздействием на окружающую среду и человека низкочастотных электрических полей (ЭП), создаваемых как самими энергетическими установками, так и воздушными ЛЭП сверхвысокого и ультравысокого напряжения. В этой же связи, в последнее время, стали

рассматриваться ЭП, генерируемые электрифицированным транспортом, которые дают основной вклад в электрическое окружение плотно населенной городской среды. Ввиду негативных воздействий низкочастотных ЭП как на окружающую среду и человека, так и на систему изоляции техники передачи электроэнергии возникает необходимость разработки надежных средств измерения напряженности ЭП.

Техническое состояние изоляции и электрооборудования определяется с учетом распределения напряженности ЭП на их поверхностях. Распределение вектора напряженности ЭП в объемах или вблизи поверхности изоляторов электротехнического и другого оборудования является одной из важнейших характеристик электрического состояния материалов, устройств, аппаратуры, отвечающих современным требованиям по надежности, простоте и экономичности. Знание реальной картины распределения напряженности ЭП на поверхности электрооборудования позволяет правильно оценивать запас электрической прочности изоляции, анализировать конструктивные параметры, определять объективные возможности электрооборудования, как на стадии изготовления, так и на стадии эксплуатации.

Знание напряженности ЭП требуется и в других областях – в нефтяной (при перекачке, транспортировке и хранении нефтепродуктов), в химической, технической и электронной промышленности. Т. е. там, где возникает вероятность появления электрических зарядов, приводящих к вероятности взрыва или пожара, а также в технологических процессах, сопровождаемых применением или появлением ЭП, в области изучения атмосферного электричества, в экологии, медицине и др.

Методы измерения напряженности ЭП определяются характером контролируемого объекта, окружающей средой (воздух, газ и смеси газов; проводящие и диэлектрические жидкости; твердые и сыпучие тела), их состоянием, размерами, а также требуемой погрешностью измерения. В результате патентного поиска за последние тридцать лет установлено, что все методы можно разбить на две группы: методы измерения на моделях и методы внесения пробного тела.

Методы измерения на моделях предполагают замену реальных условий, условиями аналогового моделирования с использованием геометрически подобных моделей, электролитической ванны или напряженной мембраны. Однако такие методы не могут давать большой точности измерения. Скорее они могут применяться только для получения качественной картины поля.

Исторически одними из первых появились методы измерения, основанные на внесении в исследуемое пространство пробного тела. Первоначально под пробным телом понимались геометрические тела из различных материалов, диэлектрические нити, электрический заряд и др. Пробное тело испытывало силовое воздействие со стороны поля, вызывающее его линейное и угловое перемещение, пропорциональное напряженности ЭП. В дальнейшем понятие «пробное тело» стало рассматриваться более широко. Под ним, в общем случае, стали понимать еще вещество, газы, зонды, датчики различных конструкций, или другими словами все то, что вносится в ЭП и реакция на его воздействие пропорциональна напряженности поля.

Методы внесения пробного тела можно разделить на методы направленного и ненаправленного приема. При таком делении «методов внесения пробного тела» под направленным и ненаправленным приемом, понимается зависимость или независимость результатов измерения или преобразования от ориентации пробного тела (датчика) в измеряемом поле соответственно.

В зависимости от того, сколько составляющих вектора напряженности одновременно или разновременно позволяет измерять (определять) данный метод, все методы направленного приема разделены на три группы: методы измерения одной, двух и трех составляющих. Большинство выявленных методов направленного приема являются методами, основанными на различных физических эффектах и измеряющими одну составляющую вектора напряженности ЭП. Особенностью измерения напряженности ЭП по одной составляющей заключается в том, что для определения модуля вектора напряженности ЭП необходимо выделять максимальную его составляющую.

Любое проводящее тело, внесенное в ЭП, искажает его. Это происходит за счет того, что на проводящем теле, находящемся в ЭП, индуцируются электрические заряды. Эти заряды создают собственное поле, которое, накладываясь на исходное ЭП, искажают последнее. В связи с этим датчик преобразовывает уже «искаженное» ЭП, что является причиной возникновения

погрешности измерения напряженности ЭП. И чем сильнее искажения, тем больше погрешность измерения. При построении трехкоординатных датчиков необходимо выбрать такую его форму, которая бы: а) вносила незначительные искажения в ЭП во всех направлениях; б) была симметрична по всем пространственным направлениям; и, кроме того: в) позволяла достаточно точно рассчитывать нормальную составляющую напряженности ЭП на проводящей поверхности датчика с учетом его взаимодействия с источником поля, а следовательно и вносимые датчиком в поле искажения, учитывающие в виде коэффициента искажения [3]. Можно выделить три основные формы проводника, используемые для построения датчиков напряженности ЭП - плоскую, цилиндрическую и сферическую. Анализируя указанные формы проводников, можно заключить, что плоская форма проводника удобней для построения однокоординатных, цилиндрическая – двухкоординатных, а сферическая – трехкоординатных датчиков напряженности ЭП. Однако сферическая форма проводника является универсальной, т.к. пригодна для построения одно-, двух- и трехкоординатных датчиков, и отвечает всем предъявляемым к ней требованиям. Кроме этого у сферической формы отсутствуют острые грани, что не будет приводить к образованию электрической короны в полях с высокой напряженностью [4].

Измерение полей радиочастотного диапазона проводят в местах установки устройств автоматических и автоматизированных систем технологического управления в частотном диапазоне от 1 до 1000 МГц. Измеряют также напряженности электромагнитного поля от переносных и стационарных радиопередающих станций, которые используются персоналом энергообъекта. Измеряют зависимость напряженности поля от расстояния до источника электромагнитного излучения и ослабление поля искусственными преградами (стены, экраны, корпуса шкафов и т.д.).

Для измерения помех в радиочастотном диапазоне обычно используют перестраиваемые селективные высокочастотные вольтметры с соответствующим набором антенн. Для сигналов вертикальной поляризации в диапазоне 26-300 МГц возможно использование биконических антенн с круговой диаграммой направленности и входным сопротивлением 50 Ом. Для сигналов с горизонтальной поляризацией следует использовать дипольные антенны с входным сопротивлением 50 Ом. Существенным для правильных измерений является хорошее согласование антенно-фидерного тракта с вольтметром во всем диапазоне измеряемых частот. Значение коэффициента стоячей волны напряжения не должно превышать 3.

Для измерения сигналов в диапазоне частот 300-1000 МГц возможно использование калиброванной измерительной антенны, рупорной измерительной антенны П-6-33 с входным сопротивлением 50 Ом. Эта антенна позволяет принимать сигналы любой линейной поляризации, но обладает ограниченной диаграммой направленности ($\pm 45^{o}$). Для сигналов с горизонтальной поляризацией можно также использовать калиброванную широкополосную антенну в виде конического диполя ДП-3 из измерительного комплекса FSM-8,5. Этот диполь имеет входное сопротивление 50 Ом и коэффициент стоячей волны не более 2.

Таким образом, при выборе методов измерения электромагнитных полей различных частот следует учитывать все многообразие факторов, влияющих на выбор, погрешность и методику измерений.

Литература:

1. СанПиН 2.2.4.723-98. Переменные магнитные поля промышленной частоты (50 Гц) в производственных условиях. – М.: Инф.-изд. Центр Минздрава РФ, 1998.

2. СанПиН 2.2.4./2.1.8.055-96. Электромагнитные излучения радиочастотного диапазона. – М.: Инф.-изд. Центр Минздрава РФ, 1996.

3. Зимин Е.Ф. Измерение параметров электрических и магнитных полей в проводящих средах / Е.Ф.Зимин, Э.С.Кочанов. -М.:Энергоатомиздат, 1985. -256 с.

4. Камра А.К. Сферический прибор для измерения вектора электрического поля в полевых условиях / А.К.Камра // Приборы для научных исследований. -1983. -№10. -С.144-149.

А.Н. Буренин, *О.Е. Нестеренко, *К.Е. Легков

К ВОПРОСУ МОДЕЛИРОВАНИЯ ПРОЦЕССА МОНИТОРИНГА ПАРАМЕТРОВ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Открытое акционерное общество «Научно-исследовательский институт «Рубин»,
г. Санкт-Петербург, Россия
* Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Ключевые слова: инфокоммуникационная сеть специального назначения, модель мониторинга, автоматизированная система управления, контроль объектов управления.

Рассмотрена математическая модель процесса мониторинга параметров управления инфокоммуникационных сетей специального назначения. Выбран стохастический образ потока передачи запросов и данных параметров по подсети обмена информацией в инфокоммуникационной сети специального назначения. Получена вероятность поступления ответов на запросы параметров на интервале Δt. Приведены выводы по результатам аналитического моделирования.

A.N. Burenin, *O.E. Nesterenko, *K.E. Legkov

TO THE QUESTION IS MODELLING PROCESS MONITORING OF MANAGEMENT PARAMETERS SPECIAL PURPOSE INFOCOMMUNICATION NETWORKS

Public corporation research Institute of "Rubin", St. Petersburg, Russia
* Military space academy, St. Petersburg, Russia

Keywords: special purpose infocommunication networks, monitoring model, automated control system, control of objects of management.

The mathematical model of process monitoring is parameters management of special purpose infocommunication networks is considered. The stochastic image a stream of transfer requests and data parametres on a subnet exchange information special purpose infocommunication is chosen. The probability of receipt of answers to inquiries of parameters on Δt interval is received. Conclusions by results of analytical modeling are given.

В соответствии с целями и задачами проведения мониторинга инфокоммуникационных сетей специального назначения (ИКС СН) можно представить формальную схему взаимодействия при сборе информации о параметрах объектов контроля при организации их эксплуатации, рис. 1.

Пусть имеется М объектов контроля ИКС СН. Каждый j-й объект контроля (объект мониторинга для целей эксплуатации) характеризуется множеством, в общем, случайных параметров $П_j = \{П_{ji}\}$, каждый элемент $П_{ji}$ которого представляет собой случайную величину, задаваемую либо рядом распределения (если параметр $П_{ji}$ представляет собой дискретную величину), либо плотностью распределения (если параметр $П_{ji}$ представляет собой непрерывную величину). Для общности будем считать, что известна функция распределения каждого параметра $П_{ji}$.

Программа комплекса сбора данных (КСИ) производит опрос каждого j-го объекта либо циклически в определенной очередности опрашивая все параметры, либо асинхронно – когда следующий запрос на последующий параметр посылается только после получения предыдущего (естественно при ограничении на время ожидания).

При организации циклического опроса параметров $П_j = \{п_{ji}\}$ суммарное время опроса каждого j-го объекта контроля ИКС СН постоянно и составит $Δt_{цj}$, а время, выделенное в каждом цикле опроса для каждого параметра $п_{ji}$ составит $Δt_{цj}/_{nj}$, где n_j – число параметров в j-м объекте контроля и управления ИКС СН.

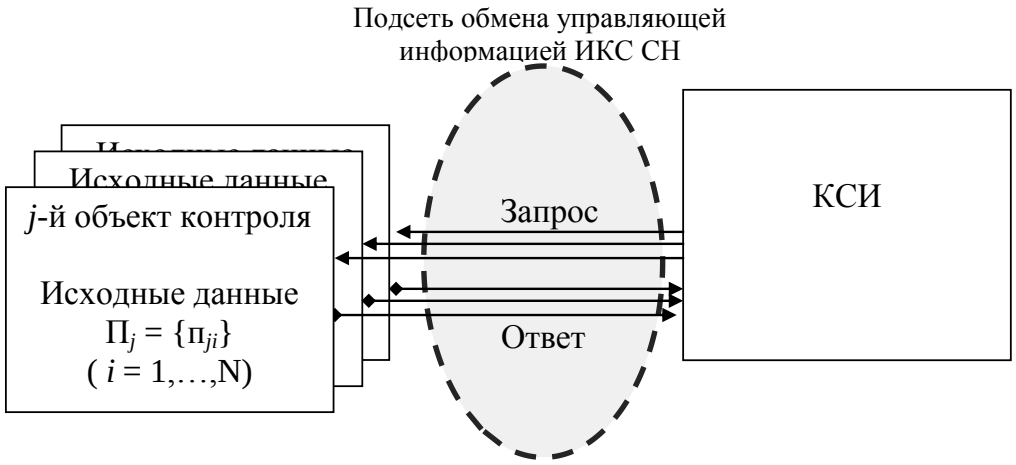


Рисунок 1. Схема взаимодействия при организации контроля объектов управления и эксплуатации ИКС СН

Однако, в силу влияния разных случайных и непредвиденных факторов во время функционирования ИКС СН при запросе определенного i-го параметра он может быть не получен за время, выделенное на данный запрос (т.е. за $\Delta t_{цо}/n_{ji}$). В этом случае в определенном цикле опроса в принципе число полученных данных о запрошенных параметрах будет менее n_{ji}, что показывает степень полноты процедур мониторинга параметров j-го объекта ИКС СН.

Функция распределения случайного числа своевременно полученных значений параметров в каждом цикле опроса j-го объектов контроля будет иметь следующий вид:

$$F(m) = 1/B(m+1, n_{ij}-m)\int x_m(1-x_m)^{n_{ij}-m-1}dx, \quad (1)$$

где B(m+1, n_{ji}-m) – бэта-функция.

В более частных случаях, характерных для подавляющего числа объектов ведомственных или корпоративных ИКС СН, для которых число контролируемых параметров n достаточно велико, возможны два варианта.

В первом варианте наряду с большим количеством контролируемых параметров n_{ji} (в практических случаях достаточно иметь n_{ji} = 50 - 100) и достаточно большом значении вероятности P(Ã) > 0,8 справедливо нормальное приближение для данного полученного вида распределения.

Во втором варианте наряду с большим количеством контролируемых параметров n_{ji} (n_{ji} = 50 - 100) и сравнительно небольшим значением P($Ã_{ji}$), характерным при интенсивных воздействиях противника на контролируемый объект ИКС СН, модель описывается приближением Пуассона.

Рассматривая модель взаимодействия одного КСИ с целым рядом объектов мониторинга и эксплуатации 1,…,M, следует признать, что на КСИ поступает (в силу влияния множества случайных факторов) случайный поток данных опрашиваемых параметров $\Pi_1 = \{n_{1i}\}$, $\Pi_2 = \{n_{2i}\}$, …., $\Pi_M = \{n_{Mi}\}$. Ясно, что в общем случае этот поток данных обладает свойствами, связанными с ординарностью или неординарностью, стационарностью или нестационарностью, отсутствием или наличием последействия. Так как поток данных, поступающий от M объектов мониторинга и управления на КСИ, вызван запросами самого КСИ, то можно считать его для данного цикла стационарным потоком. Очевидно, что в силу влияния целого ряда случайных факторов, связанных со случайным временем передачи запросов и данных параметров по подсети обмена информацией ИКС СН возможны случаи практически одновременного поступления данных опроса параметров, т.е. поток строго является неординарным и с ограниченным последействием и в общем виде обладает теми или иными свойствами самоподобия. Однако при этом следует обоснованно выбрать стохастический образ этого потока. В целом наиболее общим и наиболее поглощающим различные типы реальных потоков с описанными свойствами является стохастический поток Бернулли, для которого вероятность поступления в интервале ровно γ ответов с параметрами объектов мониторинга составит:

$$P_\gamma = \frac{1}{\gamma!}\frac{d^\gamma}{dz^\gamma}\prod_{j=1}^{M_n}[1+(z-1)F_j(\Delta t)] \quad , \qquad (2)$$

где П… - производящая функция;

$M_n = \Sigma n_{ji} M$ – общее число контролируемых данным КСИ параметров в М объектах контроля ИКС СН.

Тогда вероятность поступления ровно γ ответов на запросы параметров на интервале Δt составит:

$$P_\gamma(\Delta t) = C_\gamma^{M_n}\left(\frac{\Delta\tau}{\Delta t}\right)^{M_n}\left(1-\frac{\Delta\tau}{\Delta t}\right)^{\gamma-M_n} \quad . \qquad (3)$$

В соответствии с данным выражением можно оценить как вероятность получения полных сведений о контролируемых параметрах, так и вероятность потерянных данных. Кроме того можно оценить требуемую производительность КСИ по обработке данных параметров объектов мониторинга и эксплуатации.

Каждый j-й объект мониторинга и управления ИКС СН должен обладать такой производительностью, чтобы он не стал причиной задержки своевременного получения значений оцениваемых параметров $П_j = \{n_{ji}\}$. Для этого необходимо определить загрузку каждого j-го объекта контроля, для опроса которого выделяется интервал с длительностью цикла $\Delta t_{Цj} = \Delta t_Ц/M$. Так как каждый запрос о параметрах обрабатывается объектом за в общем случайное время $t_{оз(j)}$, то, учитывая особенности функционирования большинства объектов при взаимодействии с КСИ, обоснованно считать его распределенным по усеченному нормальному закону с достаточно малой дисперсией.

Поэтому для оценки загрузки каждого j-го объекта контроля ИКС СН можно взять математическое ожидание этого времени, т.е. $M[t_{оз(j)}]$. Суммарное случайное время отработки каждым j-м объектом ОМУ запросов КСИ составит $T_{оз(j)} = n_j\ t_{оз(j)}$, а его среднее значение $M[T_{оз(j)}] = M[n_j t_{оз(j)}] = n_j M[t_{оз(j)}]$.

Приведенные выше аналитические модели организации процедур сбора информации ИКС СН, в принципе позволяют оценить основные вероятностно-временные характеристики различных вариантов организация взаимодействий источников и потребителей оперативных и ретроспективных данных мониторинга при эксплуатации комплексов технических средств и оборудования ИКС СН.

Приведенные результаты аналитического моделирования позволяют сделать следующие выводы:

- если функции распределения вероятности значений основных параметров таковы, что вероятность их изменения за время опроса достаточно велика (0,7 – 0,9 и выше), то более предпочтителен вариант циклического (синхронного) опроса параметров;
- если функции распределения вероятности значений основных параметров таковы, что вероятность их изменения за время опроса мала (менее 0,2 – 0,3), то более предпочтителен вариант асинхронного опроса параметров;
- если функции распределения вероятности значений параметров таковы, что для одних вероятность их изменения за время опроса мала, а для других наоборот – велика, или значение этих вероятностей составляет средние значения (0,4 – 0,6), альтернативные варианты могут применяться равноправно или раздельно для разных групп параметров;
- если осуществляется выборочный контроль параметров, то целесообразно применять асинхронный опрос параметров;
- при выборе вариантов размещения шлюзов для взаимодействия открытых и защищенных секторов ИКС СН целесообразен второй вариант централизованного его размещения, т.к. распределенный вариант размещения, лишь незначительно разгружает центральный шлюз, существенно загружает защищенные сети обмена, значительно увеличивает время, требующееся на сбор информации о параметрах объектов контроля и, кроме того, потребует больших материальных затрат, связанных с оснащением узлов ИКС СН шлюзами.

Литература:

1. Легков К.Е., Буренин А.Н. К вопросу управления эффективностью инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 1. – С. 38–43.

2. Легков К.Е. Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 4. – С. 38–43.

3. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 5. – С. 34–40.

4. Легков К.Е., Скоробогатова О.А. Основные направления развития автоматизированных систем управления специального назначения и требования предъявляемые к ним системой управления // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 1. – С. 40–45.

5. Буренин А.Н., Легков К.Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 3. – С. 12–17.

6. Буренин А.Н., Легков К.Е. Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 4. – С. 46–50.

7. Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 5. – С. 8–12.

8. Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 6. – С. 22–28.

9. Буренин А.Н. , Легков К.Е., Мясникова А.И. Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 11–13.

10. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 14–16.

11. Легков К.Е., Буренин А.Н. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 2. – С.4–7.

12. Буренин А.Н., Легков К.Е. К вопросу управления рисками при обеспечении безопасности инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 17–19.

13. Легков К.Е., Мясникова А.И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 20–22.

А.Н. Буренин, *К.Е. Легков

К ВОПРОСУ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ КАЧЕСТВОМ ФУНКЦИОНИРОВАНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Открытое акционерное общество «Научно-исследовательский институт «Рубин»,
г. Санкт-Петербург, Россия
* Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Ключевые слова: инфокоммуникационная сеть специального назначения, модель управления качеством, автоматизированная система управления, контроль объектов управления.

Рассмотрены модели мониторинга управления качеством функционирования управляемых и неуправляемых инфокоммуникационных сетей специального назначения с учётом различных качественных показателей состояния управления. Получены выражения для получения случайных значений времен проведения технических операций по предоставлению конкретному пользователю соответствующей информационной или телекоммуникационной услуги.

A.N. Burenin, *K.E. Legkov

TO THE QUESTION IS MODELLING PROCESS IS MANAGEMENT OF QUALITY SPECIAL PURPOSE INFOCOMMUNICATION NETWORKS

Public corporation research Institute of "Rubin", St. Petersburg, Russia
* Military space academy, St. Petersburg, Russia

Keywords: special purpose infocommunication networks, quality management model, automated control system, control of objects management.

Models monitoring of quality management is function operated and uncontrollable special purpose infocommunication networks taking into account various quality indicators of a condition is management are considered. Expressions for obtaining casual values in times carrying out technical operations on granting to the specific user of the corresponding information or telecommunication service are received.

Каждая служба инфокоммуникационной сети специального назначения (ИКС СН) при проведении $O(i)$ операции должна обеспечить соответствующим объектам ведомственной или корпоративной автоматизированной системы управления (АСУ) определенный уровень услуг связи, который требует соответствующей организации этих служб. В условиях функционирования служб при конфликте и обострении обстановки их параметры, в общем случае, являются случайными величинами, а случайное время предоставления соответствующей услуги может быть получено при рассмотрении основных схем информационного взаимодействия компонент службы и будет равно сумме случайного числа случайных значений времен проведения технических операций по получению и предоставлению конкретному пользователю (должностным лицам (ДЛ) или прикладному процессу пункта управления (ПУ) АСУ) соответствующей информационной или телекоммуникационной услуги:

$$T_{Servis}^{O(i)} = \sum_{j=1}^{N_{O(i)}} t_{tex\ oper}^{(j)}, \quad (1)$$

где $t_{tex\ oper}^{(j)}$ – j-я техническая операция по получению и предоставлению соответствующей информационной или телекоммуникационной услуги.

Для приведенных основных служб ИКС СН могут быть получены соответствующие выражения:

$$T_{IPT\Phi}^{O(i)} = \sum_{j=1}^{N^{IPT\Phi}_{O(i)}} t_{tex\ oIPT\Phi}^{(j)}. \quad (2)$$

$$T_{PD}^{O(i)} = \sum_{j=1}^{N^{PD}_{O(i)}} t_{tex\ oPD}^{(j)}. \quad (3)$$

$$T_{EM}^{O(i)} = \sum_{j=1}^{N^{EM}_{O(i)}} t_{tex\ oEM}^{(j)}. \quad (4)$$

$$T_{FT}^{O(i)} = \sum_{j=1}^{N^{FT}_{O(i)}} t_{tex\,oFT}^{(j)} \quad . \tag{5}$$

$$T_{VKS}^{O(i)} = \sum_{j=1}^{N^{VKS}_{O(i)}} t_{tex\,oVKS}^{(j)} \quad . \tag{6}$$

Вместе с тем, учесть случайное число технических операций по предоставлению соответствующей информационной или телекоммуникационной услуги ИКС СН на практике достаточно сложно, поэтому, т.к. для большинства используемых служб при организации обслуживания дисперсия случайного числа технических операций невелика, целесообразно использовать величину среднего значения числа операций $\overrightarrow{N}_{O(i)}^{...}$, т.е.

$$T_{IPT\Phi}^{O(i)} = \sum_{j=1}^{\overrightarrow{N}^{IPT\Phi}_{O(i)}} t_{tex\,oIPT\Phi}^{(j)} \quad . \tag{7}$$

$$T_{PD}^{O(i)} = \sum_{j=1}^{\overrightarrow{N}^{PD}_{O(i)}} t_{tex\,oPD}^{(j)} \quad . \tag{8}$$

$$T_{EM}^{O(i)} = \sum_{j=1}^{\overrightarrow{N}^{EM}_{O(i)}} t_{tex\,oEM}^{(j)} \quad . \tag{9}$$

$$T_{FT}^{O(i)} = \sum_{j=1}^{\overrightarrow{N}^{FT}_{O(i)}} t_{tex\,oFT}^{(j)} \quad . \tag{10}$$

$$T_{VKS}^{O(i)} = \sum_{j=1}^{\overrightarrow{N}^{VKS}_{O(i)}} t_{tex\,oVKS}^{(j)} \quad . \tag{11}$$

Как правило, для каждой технической операции длительностью $t_{tex\,oIPT\Phi}^{(j)}$, $t_{tex\,oPD}^{(j)}$, $t_{tex\,oEM}^{(j)}$, $t_{tex\,oFT}^{(j)}$, $t_{tex\,oVKS}^{(j)}$ может быть задана функция распределения случайного времени ее проведения $F\left(t_{tex\,oIPT\Phi}^{(j)} \le T_{tex\,oIPT\Phi}^{(j)}\right)$, $F\left(t_{tex\,oPD}^{(j)} \le T_{tex\,oPD}^{(j)}\right)$, $F\left(t_{tex\,oEM}^{(j)} \le T_{tex\,oEM}^{(j)}\right)$, $F\left(t_{tex\,oFT}^{(j)} \le T_{tex\,oFT}^{(j)}\right)$, $F\left(t_{tex\,oVKS}^{(j)} \le T_{tex\,oVKS}^{(j)}\right)$.

Применяя преобразование Лапласа-Стильтьеса (ПЛС) к выражениям (12)–(16), можно оценить вид функций распределения случайных времен $T_{IPT\Phi}^{O(i)}, T_{PD}^{O(i)}, T_{EM}^{O(i)}, T_{FT}^{O(i)}, T_{VKS}^{O(i)}$ либо непосредственно, либо на основе четырехмоментной аппроксимации с последующим применением семейства распределений Пирсона.

$$\mathrm{extr}\overline{Q}_{ИКС}^{O(i)} = \min[\, f_1^{O(i)}(\overrightarrow{T}_{IPT\Phi}^{O(i)}, \overline{T}_{PD}^{O(i)}, \overline{T}_{EM}^{O(i)}, \overline{T}_{FT}^{O(i)}, \overline{T}_{VKS}^{O(i)})] \tag{12}$$

Выбор критериев эффективности стратегий управления ИКС СН не может быть формализован и базируется на результатах обоснования основных качественных показателей ее функционирования. Так если выбраны такие свойства ИКС СН как $P\{t \le t_{доп}\}$ (вероятность своевременной предоставления соответствующей услуги и $T_{Д}^{*}$ (среднее время предоставления услуги), то в качестве критериев оптимальности выработанного плана управления услугами, нужно выбирать такие, которые бы производили учет этих параметров при формировании плана управления, а процедура управления услугами в ИКС СН позволяла формировать план управления

по максимальному значению оценки величины $P^*_{cд}=P\{t \le t_{доп}\}$ или минимальному значению величины $t^*_д \le t^*_{д\,доп}$. Естественно, что тогда в качестве показателя эффективности плана управления выбирается $P^*_{cд}$ или $t^*_д$, а правило выбора плана управления будет состоять в выборе исходящего направления в соответствии с критерием максимального $P^*_{cд}$ или минимального $t^*_д \le t^*_{д\,доп}$ значения информации агрегированной по конкретному показателю эффективности ИКС СН, представленной в виде матриц $\mathbf{P}^*(t)=\left|P^*_{cдij}(t)\right|$ или $\mathbf{T}^*_Д=\left|t^*_{дij}\right|$.

При выборе критерия оптимальности плана управления необходимо учитывать и степень сложности получения численного значения соответствующего показателя. Так получение достоверной (состоятельной) оценки вероятности своевременного предоставления услуги для всей ИКС СН представляет собой задачу достаточной сложности, практическое выполнение которой потребует значительных временных и вычислительных затрат и, самое главной, не позволяет использовать эти значения при организации оперативного управления качеством функционирования ИКС СН. Это же справедливо и для такого показателя эффективности как вероятность отказа в предоставлении услуги, вероятность отказа в обслуживании требования и т.д.

В этом плане выбор показателя $t^*_д$ более предпочтителен и для каждого фрагмента ИКС СН с однотипными технологиями формируются частные планы управления $\gamma_{дij}\,|_0^{T_u} \in \Gamma\,|_0^{T_u}$, в качестве критериев оптимальности которых, выбираются либо $\mathbf{T}^*_{Д\min}=\left|min\,(t^*_{д\,ij})\right|$, либо $\mathbf{T}^*_{Д\min}=\left|min\,(t^*_{уст\,ij})\right|$. При этом возможны два варианта применения этих критериев при построении плана управления эффективностью.

Первый вариант представляет собой непосредственное построение планов управления в ИКС СН по выбранному показателю $\mathbf{T}^*_Д$. Он предусматривает уточнение текущих оценок показателей $\mathbf{T}^*_Д=\left|t^*_{д\,ij}\right|$ или $\mathbf{T}^*_Д=\left|t^*_{уст\,ij}\right|$ при обслуживании каждого пользователя после успешно обслуженного требования. Вместе с тем данный вариант в явном виде не учитывает структурные изменения в ИКС СН в результате воздействий. Поэтому для оперативной реакции на них при управлении эффективностью ИКС СН необходимо вводить соответствующие механизмы управления, которые блокируют на время восстановления вычисление оценок средних значений величин $t^*_{д\,kq}$ или $t^*_{уст\,kq}$.

Второй вариант связан с получением аналитических выражений для средних времен обслуживания. Действительно среднее время обслуживания зависит от среднего времени задержки его на каждом узле услуг ИКС СН, среднего времени его непосредственного обслуживания, от длины трассы обслуживания, измеренной в числе обслуживаемых участков и времени передачи требования на трассе обслуживания.

Время обслуживания будет величиной случайной. Пусть известны вероятности соответствующих состояний узлов обслуживания ИКС СН $P_{io}(t_c),\ldots P_{ir}(t_c),\ldots P_{in}(t_c),\ldots P_{i,\ n+s}(t_c)$. В соответствии с этим задержка обслуживания возникает только тогда, когда вновь поступившее требование застанет все каналы обслуживания соответствующего узла услуг ИКС СН занятыми. Тогда среднее время задержки и обработки обслуживания на узле услуг ИКС СН составит:

$$\overline{t_з}=\sum_{j=n}^{n+s-1} t_з(r=j)P_{ij}+\sum_{j=n}^{n+s-1}\frac{(j-n+1)Q}{n\nu_{эф}}\,P_{ij} \qquad (13)$$

Полученные аналитические выражения для средних времен обслуживания выделяют те параметры плана управления качеством функционирования ИКС СН, которые влияют на качество

обслуживания. Так, чем меньше в трассе обслуживаемых узлов услуг, тем при прочих равных условиях меньше среднее время обслуживания.

Таким образом, исходя из определенного существенного свойства ИКС СН – среднего времени обслуживания пользователей, возможно выделить параметры (показатели), по которым необходимо осуществлять оптимизацию плана управления и строить исходя из этого стратегию и процедуры управления методами многокритериальной оптимизации либо по Парето, либо скаляризацией и получением одного интегрального показателя (свертка).

Литература:

1. Легков К.Е., Буренин А.Н. К вопросу управления эффективностью инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 1. – С. 38–43.
2. Легков К.Е. Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 4. – С. 38–43.
3. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 5. – С. 34–40.
4. Легков К.Е., Скоробогатова О.А. Основные направления развития автоматизированных систем управления специального назначения и требования предъявляемые к ним системой управления // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 1. – С. 40–45.
5. Буренин А.Н., Легков К.Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 3. – С. 12–17.
6. Буренин А.Н., Легков К.Е. Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 4. – С. 46–50.
7. Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 5. – С. 8–12.
8. Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 6. – С. 22–28.
9. Буренин А.Н. , Легков К.Е., Мясникова А.И. Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 11–13.

А.Н. Буренин, *И.А. Ледянкин, *К.Е. Легков

МЕТОД ОЦЕНКИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Открытое акционерное общество «Научно-исследовательский институт «Рубин»,
г. Санкт-Петербург, Россия
* Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Ключевые слова: программа, информация, автоматизация, управление, ресурсы, ошибка.

По мере развития автоматизированных систем управления специального назначения (АСУ СН), основанных на использовании электронно-вычислительных машин (ЭВМ), возникают все более серьезные требования к надежности программного обеспечения (ПО) в автоматизированных

системах обработки данных и локальных вычислительных сетях специального назначения. Проблема безотказной работы, как самой системы, так и надежного функционирования ее программного обеспечения с появлением сложных АСУ СН, связанных с автоматизированным вводом, хранением, обработкой и выводом информации, приобретает все большее значение. В статье авторами предложены основные подходы к оценке надежности программного обеспечения автоматизированных систем управления специального назначения.

A.N. Burenin, *I.A. Ledyankin, *K.E. Legkov

METHOD OF ASSESSMENT SOFTWARE RELIABILITY AUTOMATED CONTROL SYSTEMS SPECIAL PURPOSE

Public corporation research Institute of "Rubin", St. Petersburg, Russia
* Military space academy, St. Petersburg, Russia

Keywords: program, information, resources, management, automation, error.

With the development of automated control systems for special purposes (ACS SP) based on the use of computers (PC), there are increasing demands for reliability of software in the automated data processing systems and local area networks for special purposes. Problem uptime, as the system itself, and reliable operation of its software with the advent of sophisticated ACS SP associated with automated input, storage, processing and output of information is becoming increasingly important . In the article the authors proposed the main approaches to assessing the reliability of software for automated control systems for special purposes.

Обеспечение надежного функционирования комплексов программ, а следовательно выработка требований предъявляемых к программным комплексам в современных условиях выходит на передовые позиции. Проблема безотказной работы, как самой системы, так и надежного функционирования ее программного обеспечения приобретает все большее значение. Этому способствует:

- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств вычислительной техники;
- сосредоточение в единых базах данных информации различного назначения и принадлежности;
- расширение круга лиц, имеющих доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;
- усложнение режимов функционирования технических средств вычислительной системы: широкое внедрение многопрограммного режима, режима разделения времени и реального времени;
- автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях;
- увеличение количества технических средств и связей в автоматизированных системах управления и обработки данных.

В настоявшее время программное обеспечение является неотъемлемой частью любой вычислительной системы входящей в состав АСУ СН.

Последствия внешних воздействий, проявляющиеся со стороны различных природных факторов и неправильного взаимодействия человека–оператора с техническими средствами, а также внутренние процессы, происходящие в самой системе негативно влияющие на работу ПО, могут носить весьма серьезный, а порой и катастрофический характер.

Необходимость в разработке надежного комплекса программ связана с проведением мероприятий обеспечивающих необходимые показатели надежности. Прежде всего, с учетом динамических характеристик системы и инерционности объектов управления должны быть определены и сформулированы основные требования к надежности конкретного комплекса программ:

- необходимая наработка на отказ;
- допустимая длительность восстановления;
- коэффициент готовности.

На основе этих данных производится распределение ресурсов на отладку программ и на разработку средств оперативного контроля и восстановления.

При оценки надежности АСУ следует учитывать множество различных факторов, которые влияют непосредственно как на всю систему, так и на само программное обеспечение, которое входит в состав системы.

Для получения технико-экономических характеристик создания программ обычно применяют методы экспертных оценок, ретроспективного анализа, фактографический метод накопления и обработки реальных измеряемых данных.

Рассмотрим сущность приведенных методов.

Метод экспертных оценок заключается в сборе информации путем специалистов, при этом достоверность данных полностью определяется уровнем знаний и справедливостью суждений опрашиваемых. Этот метод обычно используется для оценки отдельных стадий жизненного цикла программ: проектирования, разработки, сопровождения. Существует большое количество методов обеспечения надежности и связанных с ними методов оценки надежности на различных стадиях жизненного цикла программных средств.

На этапе проектирования и разработки ПО используются методы внесения избыточности; на этапе функционирования - различные методы контроля программ и данных, программного восстановления и испытаний на надежность; на этапе сопровождения - методы обеспечения сохранности корректности внесения изменений в программы.

Изучение статистики первичных ошибок в комплексах программ различного назначения позволяет выявить основные факторы и показатели определяющие надежность ПО.

Общая средневзвешенная ошибка функционирования ПО вследствие невыявленных первичных ошибок определяется соотношением:

$$\sigma(\tau) = \sum_{j=1}^{q} x_j \sigma_j(\tau) = \sum_{j=1}^{q} x_j \sum_{k=1}^{m} P_k^{(1)}(\tau)\Delta k_j \qquad (1)$$

где τ - длительность отладки комплекса программ;

σ_j - вторичная ошибка в *j*-х результатах решения задачи за счет пропущенных при отладке первичных ошибок, т.е. ошибка, выявленная при отладке программ;

$P_к^{(1)}(\tau)$ - вероятность наличия в программе первичной ошибки *k*-го типа, которая при использовании программы вносит в результирующую *j*-ю переменную дополнительную ошибку Δk_j;

m - полное количество типов не выявленных в программе первичных ошибок;

x_j - условный взвешенный коэффициент последствия ошибок;

q - полное количество типов выходных величин.

Результаты анализа ПО встроенных систем управления показывают, что первичные программные ошибки вследствие неправильной записи на языке программирования и ошибок трансляции составляют до 25% общего числа ошибок в программах. Количество и типы этих ошибок определяются степенью автоматизации программирования и глубиной формализованного контроля тестов программ. Количество программных ошибок зависит от квалификации разработчиков, общего объема комплексов программ и ряда других факторов. Согласно статистическим данным, 80% программ систем управления в настоящее время разработаны на автокодах. Программные ошибки при разработке программ на автокодах можно классифицировать следующим образом: ошибки типов операций, ошибки переменных, ошибки управления и циклов. Ошибки, обусловленные неполным учетом всех условий решения задачи, являются наиболее частыми и составляют до 70% всех ошибок в исходных текстах программ.

Динамика количества выявленных ошибок в зависимости от времени отладки может быть представлена экспоненциальной моделью.

На практике число оставшихся первичных ошибок в комплексе программ оценивается соотношением:

$$n_0 = N_0 \exp(-k\tau) \qquad (2)$$

где n_o - число ошибок, оставшихся к моменту времени отладки τ (n_o пропорционально интенсивности обнаружения ошибок $dn/d\tau$ с точность коэффициента *k*); *n*- число устраненных

первичных ошибок; N_0- начальное число первичных ошибок; k - коэффициент темпа выявления ошибок.

Ошибки в программах тесно связаны с используемыми моделями надежности (рис.1).

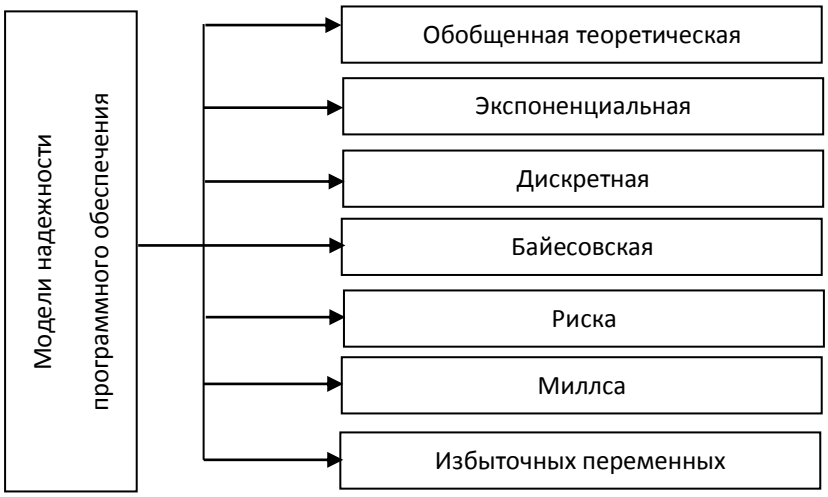


Рисунок 2. Модели надежности программного обеспечения

Количество моделей надежности на сегодняшний день превышает сотню и продолжает расти. В зависимости от точки зрения на понятие надежности и глубины исследования выявляются различные критерии и нюансы.

Поэтому построение полной схемы моделей может основательно запутать процесс.

Представленная схема классификации моделей надежности ПО не является единственной.

В заключении хочется отметить, что несмотря на очевидную актуальность, вопрос оценки надежности ПО не привлекает должного внимания. Вместе с тем даже поверхностный анализ проблемы с теоретико-вероятностной точки зрения позволяет выявить некоторые закономерности.

Литература:

1. Легков К.Е. Основные теоретические и прикладные проблемы технической основы системы управления специального назначения и основные направления создания инфокоммуникационной системы специального назначения.// Телекоммуникации и транспорт. Вып. № 6. Москва, 2013. С. 43-47.

2. Легков К.Е., Буренин А.Н. К вопросу управления эффективностью инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 1. – С. 38–43.

3. Легков К.Е. Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 4. – С. 38–43.

4. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 5. – С. 34–40.

5. Легков К.Е., Скоробогатова О.А. Основные направления развития автоматизированных систем управления специального назначения и требования предъявляемые к ним системой управления // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 1. – С. 40–45.

6. Буренин А.Н., Легков К.Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 3. – С. 12–17.

7. Буренин А.Н., Легков К.Е. Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 4. – С. 46–50.

8. Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 5. – С. 8–12.

9. Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 6. – С. 22–28.

10. Буренин А.Н. , Легков К.Е., Мясникова А.И. Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 11–13.

11. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 14–16.

12. Легков К.Е., Буренин А.Н. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 2. – С.4–7.

13. Буренин А.Н., Легков К.Е. К вопросу управления рисками при обеспечении безопасности инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 17–19.

14. Легков К.Е., Мясникова А.И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 20–22.

А.Н. Буренин, *К.Е. Легков, *Д.В. Негодин

МОДЕЛИ МОНИТОРИНГА ПАРАМЕТРОВ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Открытое акционерное общество «Научно-исследовательский институт «Рубин»,
г. Санкт-Петербург, Россия
*Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Ключевые слова: инфокоммуникационная сеть специального назначения, модель мониторинга, автоматизированная система управления, контроль объектов управления.

Рассмотрены модели мониторинга параметров управления инфокоммуникационных сетей специального назначения для двух вариантов размещения и применения шлюза передачи данных в элементах импорта данных состояния и с учётом основных факторов, которые оказывают влияние на функционирование модели (таких как: количество узлов, объем данных мониторинга, получаемых от источника, и интенсивность их получения, влияние обработки данных открытого сегмента на производительность средств сбора в закрытом сегменте, пропускная способность трактов передачи, увеличение объема трафика при передаче данных по закрытому тракту, производительность всех средств сбора).

A.N. Burenin, *K.E. Legkov, *D.V. Negodin

MODELS OF MONITORING PARAMETERS MANAGEMENT SPECIAL PURPOSE INFOCOMMUNICATION NETWORKS

Public corporation research Institute of "Rubin", St. Petersburg, Russia
*Military space academy, St. Petersburg, Russia

Keywords: special purpose infocommunication networks, monitoring model, automated control system, control objects of management.

Models monitoring parameters management special purpose infocommunication networks for two options placement and application a lock data transmission in elements import data a condition and taking into account major factors which influence model functioning (such as are considered: number of knots, volume of data of the monitoring received from a source, and intensity of their receiving, influence data processing an open segment on productivity means of collecting in the closed segment, capacity paths transfer, increase in volume a traffic at data transmission on the closed path, productivity of all means collecting).

Функционирование инфокоммуникационных сетей специального назначения различных министерств, ведомств или корпораций с требуемыми уровнями устойчивости и эффективности в условиях всевозможных воздействий, возможно осуществить только при организации качественной подсистемы управления эксплуатацией комплексов технических средств и оборудования сетей в составе инфокоммуникационных сетей специального назначения (ИКС СН), в контуре которых участвуют должностные лица и оперативно-технический персонал служб эксплуатации.

Чрезвычайно возросшая сложность самих создаваемых ИКС СН и комплексов технических средств в их составе, а также существенно возросшие возможности противника по проведению целого комплекса разрушающих и информационных воздействий на ИКС СН, значительно усложняют организацию процессов их эксплуатации, связанных с необходимостью оперативного мониторинга эксплуатационного состояния многочисленного оборудования комплексов и средств ИКС СН.

В принципе, в связи с тем, что в любой ИКС СН существуют сегменты закрытой информации и сегменты открытой информации, возможными вариантами построениями архитектур подсистем мониторинга ИКС СН могут быть варианты, связанные с:

- способом размещения и применения шлюзов передачи данных в элементах импорта данных состояния эксплуатируемого комплекса;
- организацией взаимодействий источников и потребителей данных мониторинга.

При этом целесообразны два возможных варианта размещения и применения шлюза передачи данных в элементах импорта данных состояния:

- вариант 1 – шлюз размещается на каждом узле ИКС СН;
- вариант 2 – шлюз размещается только в центре управления ИКС СН.

В первом варианте трафик мониторинга на каждом узле ИКС СН поступает от средств сбора данных открытого сегмента в средства сбора данных закрытого сегмента (создавая для них дополнительную вычислительную нагрузку) и передается в центр управления по защищенной информационной подсети, где общесетевые для ИКС СН средства сбора получают, обрабатывают весь поступающий трафик и заносят результаты обработки в БД.

Во втором варианте трафик мониторинга передается в центр управления ИКС СН по открытой и по закрытой подсетям – в зависимости от того, в каком секторе узла собраны данные мониторинга, а в центре управления имеются два общесетевых средства сбора данных – по одному в каждом сегменте, и общесетевое средство закрытого сегмента получает через шлюз данные открытого сегмента, затрачивая на их получение определенную долю своего вычислительного ресурса.

При этом должно учитывается, что:

- каждое средство выполняется на отдельной ПЭВМ;
- задержки данных на передачу через шлюз зависят (линейно) только от объема передаваемых данных;
- передача данных по закрытой подсети увеличивает время передаваемого трафика за счет служебного шифрования данных, используемых при передаче в зависимости от объема передаваемых «полезных» данных;
- закрытый тракт передачи является «наложенным» на открытый, то есть в открытом тракте одновременно передаются и открытый, и закрытый трафик;
- сетевые средства сбора данных разделяют свой ресурс на все выполняемые подпроцессы получения и обработки данных, логически независимые друг от друга.

Целесообразно моделирование осуществить для обоих вариантов с целью определения зависимости оперативности поступления данных мониторинга (периода времени от момента

получения данных от источника до момента занесения их в базу данных) и трафика в трактах передачи данных.

Основными факторами, влияние которых подлежит учету в моделях, являются:

- количество узлов;
- объем данных мониторинга, получаемых от источника, и интенсивность их получения (случайные величины);
- влияние обработки данных открытого сегмента на производительность средств сбора (узловых и сетевых) в закрытом сегменте (линейно зависит от объема данных);
- пропускная способность трактов передачи (тракты к узлам считаются независимыми друг от друга);
- увеличение объема трафика при передаче данных по закрытому тракту;
- производительность всех средств сбора, линейно зависящая от объема обрабатываемых данных.

При этом организация взаимодействий источников и потребителей оперативных и ретроспективных данных мониторинга предполагает выбор дисциплины получения данных программами сбора данных и имеется один или более однотипных источников данных, каждый из которых по запросу программы комплекса сбора данных (КСИ) предоставляет значения всех параметров, изменившихся с момента предыдущего запроса. Как правило, зависимости факта и объема изменения данных от времени известны. КСИ взаимодействует с источниками данных посредством циклического выполнения следующего процесса:

- формирование запроса (используется известный фиксированный вычислительный ресурс КСИ);
- передача запроса по такту передачи данных к источнику данных (время передачи фиксировано и известно, все тракты независимы друг от друга);
- обработка запроса источником данных, длительность которой определяется фиксированной известной составляющей и переменной составляющей, линейно зависящей от объема изменений в данных, подлежащих передаче КСИ;
- передача ответа по тракту передачи данных к КСИ (время передачи определяется аналогично времени обработки запроса источником);
- обработка ответа КСИ (используется вычислительный ресурс КСИ, зависит от фиксированной известной составляющей и переменной составляющей, линейно зависящей от объема изменений в данных, подлежащих обработке).

КСИ использует два способа организации опросов:

- взаимодействие с каждым источником осуществляется логически отдельным подпроцессом, для которого известно фиксированное время паузы между окончанием обработки предыдущего опроса и началом формирования следующего (период повтора опроса), а все продпроцессы конкурируют за вычислительный ресурс КСИ – он распределяется на все активные подпроцессы (подпроцессы в фазе формирования запроса или обработки ответа);
- КСИ выполняет процессы взаимодействия с источниками в цикле последовательно – опрос первого источника, второго источника и т.д., пауза на период повтора опроса, опрос первого источника и т.д.

Модель мониторинга позволит получить следующие оценки для двух описанных выше вариантов:

- загрузки источников, КСИ и трактов передачи данных;
- оперативность сбора данных – время от изменения параметра до окончания обработки ответа источника, содержащего изменившееся значение;
- вероятность пропуска изменения значения параметра, то есть ситуации, когда параметр изменил свое значение между двумя последовательными опросами более, чем один раз.

Литература:

1. Легков К.Е., Буренин А.Н. К вопросу управления эффективностью инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 1. – С. 38–43.

2. Легков К.Е. Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 4. – С. 38–43.

3. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 5. – С. 34–40.

4. Легков К.Е., Скоробогатова О.А. Основные направления развития автоматизированных систем управления специального назначения и требования предъявляемые к ним системой управления // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 1. – С. 40–45.

5. Буренин А.Н., Легков К.Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 3. – С. 12–17.

6. Буренин А.Н., Легков К.Е. Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 4. – С. 46–50.

7. Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 5. – С. 8–12.

8. Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 6. – С. 22–28.

9. Буренин А.Н. , Легков К.Е., Мясникова А.И. Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 11–13.

10. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 14–16.

11. Легков К.Е., Буренин А.Н. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 2. – С.4–7.

12. Буренин А.Н., Легков К.Е. К вопросу управления рисками при обеспечении безопасности инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 17–19.

13. Легков К.Е., Мясникова А.И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 20–22.

И.В. Щербань, * Р.В. Быкадоров

РЕАЛИЗАЦИЯ КОМПЛЕКСА ДЛЯ КАЛИБРОВКИ МИКРОЭЛЕКТРОМЕХАНИЧЕСКИХ МАГНИТОМЕТРОВ АППАРАТНО-ПРОГРАММНЫМИ СРЕДСТВАМИ NATIONAL INSTRUMENTS

Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия
*Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: калибровка, аппаратно-программный комплекс, микроэлектромеханический (MEMS) магнитометр, National Instruments LabVIEW.

Реализован измерительный комплекс для калибровки и подготовки к работе и измерениям MEMS магнитометров, с использованием аппаратных и программных средств National Instruments

LabVIEW и Delphi 7.0. Проведены испытания комплекса, содержащего в своем составе трехосный магнитометр на базе MEMS L3G4200D.

I.V. Shcherban, *R.V. Bykadorov

THE TECHNICAL COMPLEX FOR THE MEMS MAGNETOMETR'S CALIBRATION, BASED ON THE NATIONAL INSTRUMENTS SOFTWARE AND HARDWARE

The North Caucasian Branch of the Moscow Technical University
of Communications and Informatics, Rostov-on-Don, Russia
*Southern Federal University, Rostov-on-Don, Russia

Keywords: calibration, National Instruments hardware and software, microelectromechanical (MEMS) magnetometer.

Implemented a measurement system for calibration, setup, and measurements MEMS magnetometers, using hardware and software, National Instruments LabVIEW and Delphi 7.0. The tests of the complex, containing in its composition of three-axis magnetometer based on MEMS L3G4200D.

Микроэлектромеханические (MEMS) датчики – это устройства, производимые по технологии, схожей с технологией производства обычных полупроводниковых элементов, что и обуславливает привлекательность их характеристик, например, низкие стоимость и энергопотребление, миниатюрность, простота использования и другие. В частности, к таким датчикам относятся акселерометры и магнетометры.

Основными недостатками MEMS-датчиков являются сравнительно низкая точность, зашумленность выходного сигнала, а также принципиальная невозможность формирования точных моделей погрешностей. Последний факт обусловлен нестабильностью этих моделей, сильной зависимостью модельных параметров от внешних условий – от температуры, характеристик источника питания и т.п. факторов. Поэтому требуется периодическая коррекция моделей погрешностей MEMS-датчиков в ходе их эксплуатации.

Соответственно, представляет интерес разработанный комплекс для калибровки и подготовки к работе любого, от одноосного до трехосного, MEMS магнитометра. Аппаратная часть комплекса включает наклонно-поворотный стол (НПС), преобразователь выходных сигналов цифрового выхода микросхемы MEMS в протокол UART 2.0 и ЭВМ. Размещение калибруемой микросхемы на НПС позволяет задавать требуемую ориентацию осей чувствительности магнитометра относительно земных координат с точностью до 3 угл. мин.

Калибровка магнитометра включает предварительную процедуру нормировки выходных сигналов. Для этого микросхема поворачивается на 360° вокруг перпендикуляра к поверхности Земли для определения максимума и минимума в потоке выходных цифровых данных. Далее рассчитывается угол магнитного наклонения (УМН). Он изменяется в зависимости от широты места испытаний L:

$$\lambda = \mathrm{tg}^{-1}\left(2\,\mathrm{tg}\,L\right). \tag{1}$$

Вследствие влияния магнитного поля Земли измеренное значение УМН отличается от реального. Расширенный угол магнитного наклонения (РУМН) определялся как

$$\lambda' = \mathrm{tg}^{-1}\left(-\frac{\overline{X}_{mc}\sin\theta\sin\varphi+\cos\theta\,\mathrm{tg}\psi+\overline{Y}_{mc}\cos\theta}{\sin\theta\cos\varphi\,\mathrm{tg}\psi-\sin\varphi}\right). \tag{2}$$

Далее нормирование производится при найденном УМН:

$$\overline{X}_{mc} = \left(X_{mc} - B_{iasx}\right)SF_x; \tag{3}$$

$$B_{iasx} = \frac{X_{max}+X_{min}}{2}; \tag{4}$$

$$SF_x = \frac{2\cos\lambda}{X_{max}-X_{min}}, \tag{5}$$

где: X – координатная ось; X_{mc} – измеренная величина (выходной сигнал датчика); $\overline{X}_{mc}$ – нормированная величина; $X_{\max}$ и $X_{\min}$ – измеренные максимальное и минимальное значение измеренной величины в горизонтальной плоскости, соответственно; B_{iasx} – напряжение смещения x-датчика, SF_x – масштабирующий множитель.

Углы крена θ и наклона φ рассчитываются как

$$\theta = \sin^{-1}\left(\frac{a_x}{g}\right); \quad \varphi = \sin^{-1}\left(\frac{-a_x}{g\cos\theta}\right), \tag{6}$$

где a_x – выходной сигнал акселерометра исследуемой микросхемы; g – точно рассчитываемое в месте испытаний земное ускорение;

$$\psi = \mathrm{tg}^{-1}\left(-\frac{\sin\lambda\sin\varphi + \overline{X}_{mc}\sin\theta\sin\varphi - \overline{Y}_{mc}\cos\theta}{\sin\lambda\sin\theta\cos\varphi + \overline{X}_{mc}\cos\varphi}\right). \tag{7}$$

Информация о 3-х координатах измерения нормируется и дополняется на основе расчетов УМН, РУМН, углов θ, φ, ψ. По окончании расчетов полученные измерения MEMS-магнитометра сравниваются с заранее известными базовыми направлениями НПС и, далее, рассчитываются погрешности измерений.

Использована технология виртуальных приборов National Instruments LabVIEW. Синтезированный виртуальный прибор обеспечивает съём информации с магнитометра, перевод битов в физические величины, запись данных в соответствующие файлы данных и их обработку. Панель виртуального прибора содержит все необходимые элементы для вывода и ввода данных. Входными данными прибора является измерения магнитометра, а также значения широты и долготы места испытаний. Фрагменты панели виртуального прибора (ВП) представлены на рисунках 1, 2.

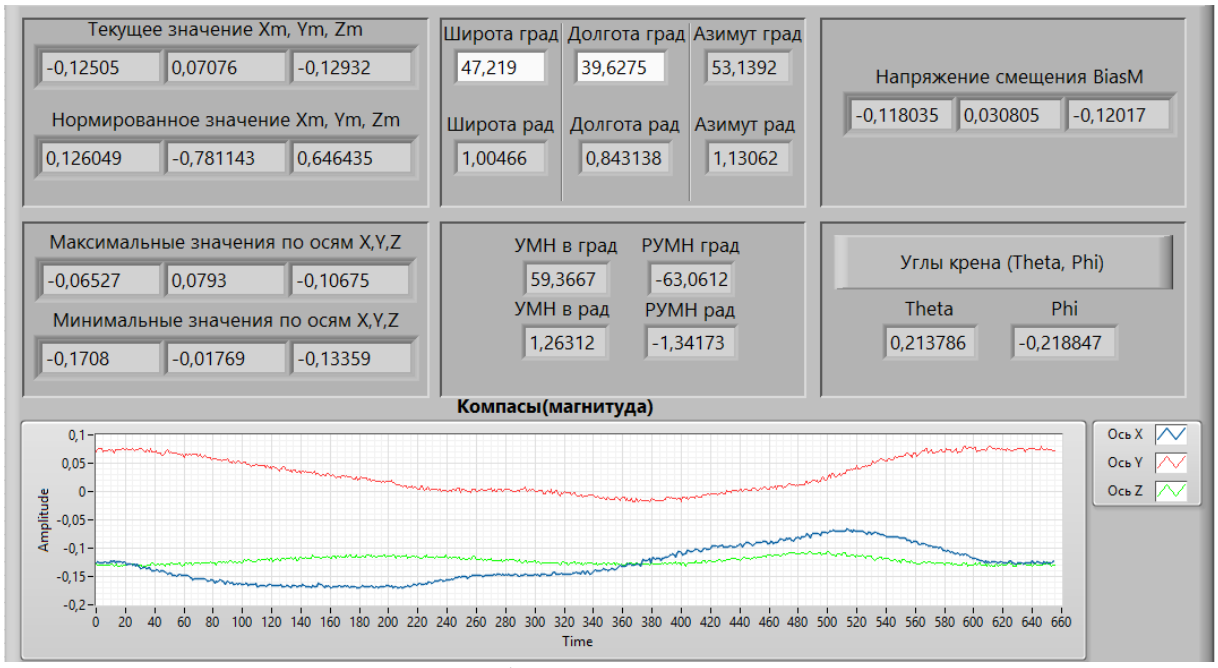


Рисунок 1.Лицевая панель ВП

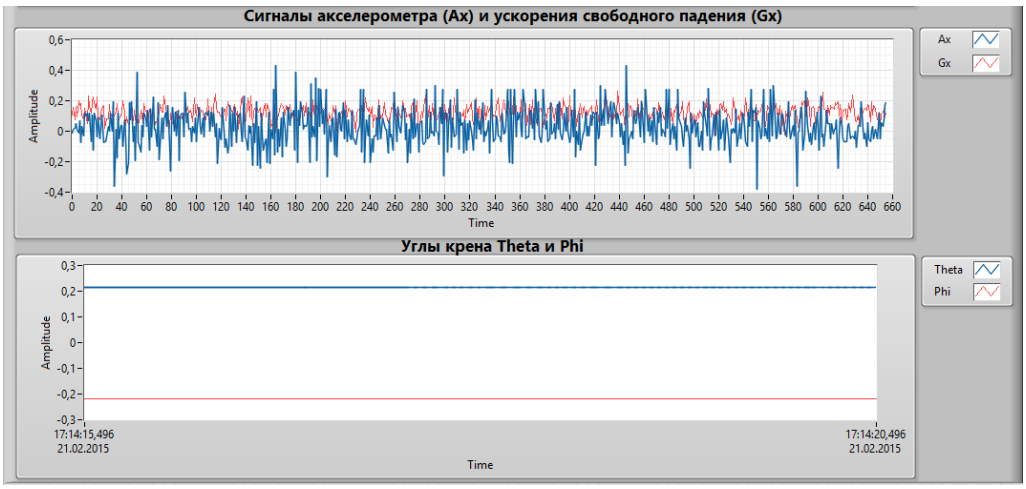


Рисунок 2. Графики функций выходных сигналов магнитометра на панелях ВП

Вычислительная часть ВП разбита на три секции, блок-диаграммы которых представлены на рисунках 3,4,5, где определяются минимальные $X_{\min}$ и максимальные $X_{\max}$ значения магнитуды при вращении микросхемы, вычисляются напряжение смещения B_{iasx}, значения УМН и угла θ, азимут. В результате ВП вычисляет РУМН и строит по полученным значениям соответствующие графики.

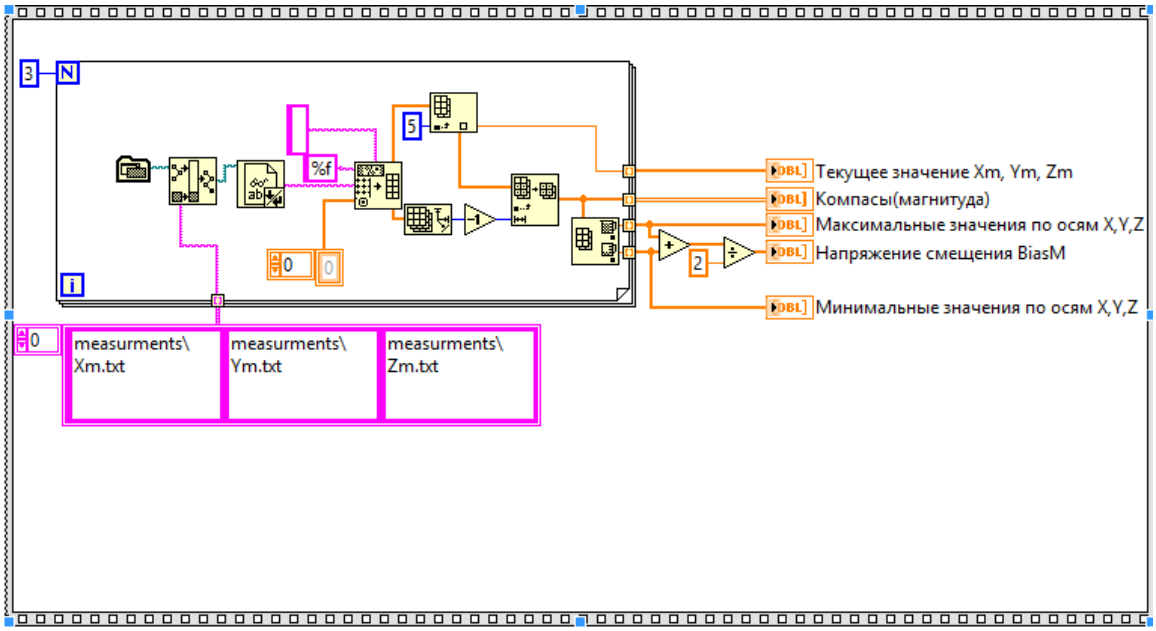


Рисунок 3. Фрагмент блок-диаграммы ВП: ввод данных

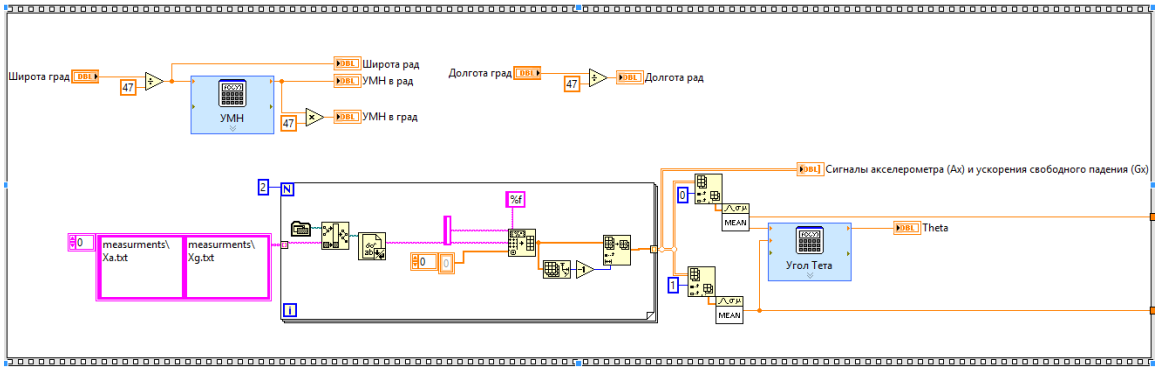


Рисунок 4. Фрагмент блок-диаграммы ВП: расчет широты и долготы

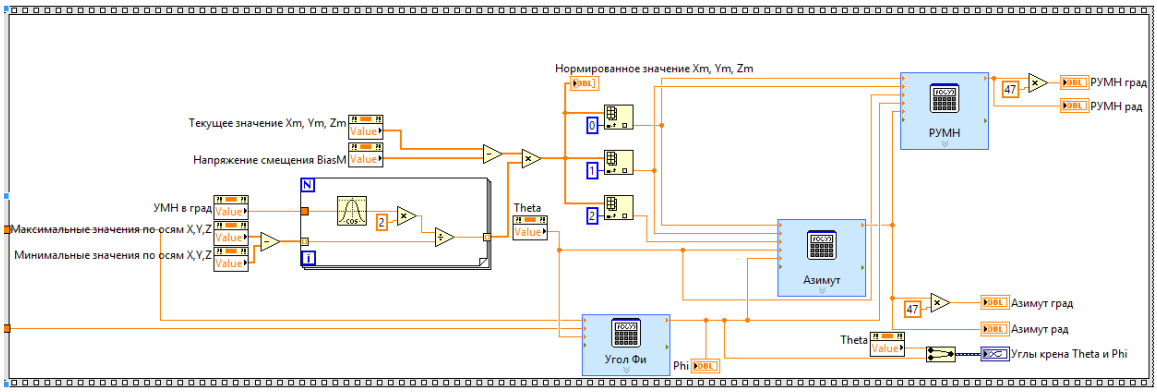


Рисунок 5. Фрагмент блок-диаграммы ВП: расчет УМН и РУМН

При испытаниях исследовалась MEMS-микросхема L3G4200D, содержащая в своем составе, в том числе, трехосный магнитометр. Динамический диапазон измерений магнитометра составляет ±250/±500/±2000 градусов в секунду по соответствующим каналам. Для оценки точности измерений магнитометра использовался MEMS-датчик, включающий трехосные акселерометр, гироскоп и компас AK8963, объединенные в составе микросхемы MPU-6515. Компас здесь имеет тот же динамический диапазон, но более высокую точность. Результаты испытаний подтвердили работоспособность разработанного комплекса и возможность его эффективного использования для калибровок MEMS-магнитометров.

Литература:

1. Seong Yun Cho A Calibration Technique for a Two-Axis Magnetic Compass in Telematics Devices // ETRI Journal, Vol. 27, № 3. June 2005. P. 280-288.

А.Н. Вакказова

ИССЛЕДОВАНИЕ И ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ VoIP-ТРАФИКА НА ГОЛОСОВЫХ ПЛАТФОРМАХ (IVR)

Поволжский Государственный Университет Телекоммуникаций и Информатики (ПГУТИ), г. Самара

Ключевые слова: корпоративная телефонная инфраструктура, интерактивная информационно-справочная система, автоматическая телефонная станция, телефонный сценарий.

Рассмотрен новый метод организации IVR-платформы с использованием «облачных» технологий, позволяющий значительно сократить финансовые затраты благодаря внедрению такого комплекса в телефонную инфраструктуру компании. Предлагаемый подход может быть реализован в открытой телекоммуникационной сети. Механизм оценки качества работы IVR-системы в зависимости от параметров канала передачи данных дает возможность формировать численные требования к характеристикам канала при выборе оператора связи предоставляющего услуги доступа в открытую сеть.

A.N. Vakkazova

THE STUDY AND MANAGEMENT OF VoIP TRAFFIC ON VOICE PLATFORMS (IVR)

Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara

Keywords: corporate telephony infrastructure, interactive informational system, automatic telephone exchange, a telephone script.

A new method of arranging the IVR platform using cloud-based technologies that significantly reduce the financial costs due to the implementation of such a complex in the telephone company's infrastructure. The proposed approach can be implemented in an open telecommunications network. The mechanism for evaluating the performance of the IVR system depending on the parameters of the data channel allows the numerical requirements for the characteristics of the channel selecting operator provides access to the public network.

Исследуем актуальность использования автоматизированных систем обработки запросов по телефону. Функционирование большинства современных компаний ориентировано на обслуживание клиентов [1, 3]. В большинстве случаев заявки от потенциальных заказчиков поступают по телефону. Благодаря быстрому и оперативному реагированию на такие заказы создается имидж компании и складывается впечатление об эффективности ее работы с клиентами и партнерами. Ведь каждый не обработанный (по ряду причин) звонок – подарок конкурентам. В связи с этим, целесообразно говорить об актуальности программного решения по автоматизации процесса обработки заявок в системах массового обслуживания [1 – 5]. В данной статье предложены результаты разработки экономичного, с точки зрения финансовых затрат, варианта системы обработки звонков клиентов, основанного на использовании открытых, свободных программных продуктов, обеспечивающих базовую функциональность IVR (Interactive voice response – интерактивные информационно-справочные) систем. Одно из решений автоматизации обработки звонков – использование IVR-систем в телефонной инфраструктуре компании [6]. Интерактивные информационно-справочные системы обладают широкими возможностями: от простого проигрывания мелодии до голосовой верификации клиента [7]. Они поддерживают следующие функции:

1. Text-to-speech – преобразование текста в речь или синтезатор речи [8]; Speech recognition (распознавание речи) – технология преобразования речевого сигнала в текстовый поток [4];
2. Voice Verification (верификация по голосу) – аутентификация клиента по голосовой модели [8]. Данная технология активно применяется в банковской и страховой сферах услуг. Теперь клиенты могут не запоминать длинные лицевые счета и пароли;
3. Direct talk – распознавание речи «на лету» в режиме реального времени [8].

Рассмотрим решение организации IVR-платформы. Причем его можно реализовать непосредственно в телефонной инфраструктуре компании или в виде удаленного сервиса с использованием «облачных» технологий, т.е. организовать IVR-платформу на «облачных» серверах. Анализ и результаты исследования характеристик и ограничений, накладываемых на канал связи, приводятся ниже. Новый метод предусматривает использование языка разработки VoiceXML, свободных программных продуктов, предоставляющих базовую функциональность IVR-систем, и открытой (бесплатной) программной автоматической телефонной станции (АТС). При этом специализированное оборудование не требуется. Программные компоненты устанавливаются на обычный ПК, позволяя тем самым существенно снизить затраты на покупку дополнительного оборудования, как это делалось для существующих решений в крупном бизнесе. В этом случае от компании-заказчика требуется только подключить компьютер в свою телефонную сеть. На компьютере устанавливается бесплатная программная АТС и интерпретатор языка VoiceXML. Данное решение является IVR-платформой, на которой работают приложения, обрабатывающие телефонные звонки. В качестве готового решения был выбран свободный программный продукт Asterisk компании Digium.

Проанализируем качество работы IVR-системы. «Облачное» использование предлагаемого IVR-решения накладывает ряд требований на характеристики и параметры среды передачи данных и, в первую очередь, на параметры сети связи, по которой передается голосовой трафик к удаленному VoIP-серверу. Качество голосовой связи в сетях передачи данных определяется параметрами доставки голосовых пакетов и качеством обмена сигнальными сообщениями [9 – 11]. Можно выделить факторы, влияющие на качество IP-телефонии: задержка доставки пакета – промежуток времени, требующийся для передачи пакета через сеть; джиттер (вариация задержки) – промежуток времени между доставкой двух последовательных пакетов; пропускная способность сети; вероятность потери пакетов.

Суммарная задержка доставки пакетов складывается из ряда составляющих – постоянных и переменных. К задержкам с постоянным значением времени относятся те, что возникают при кодировании, декодировании, инкапсуляции, декапсуляции и буферизации пакетов, их приеме и передаче. Значение задержки варьируется при постановке пакетов в очередь и передаче их по сети [11]. В предлагаемом подходе организации IVR-платформы обработка голосового трафика происходит на удаленных «облачных» серверах. Голосовой трафик передается по интернет-каналам. Все данные конечного пользователя – RTP (Real-time Transport Protocol) трафик маршрутизируются по аналогии с другими типами потоков данных, некритичным к задержкам и потерям (HTTP, FTP). Многообразие технологий обеспечения качества сервиса, несогласованность параметров QoS между операторами связи и отсутствие единства в реализациях протоколов у разных производителей оборудования не позволяют гарантировать необходимое качество обслуживания в данной ситуации, а механизмы управления трафиком, использующиеся в корпоративных сетях связи здесь просто неприменимы. Проблему повышения качества передачи голосового трафика в открытых сетях частично можно решить за счет перехода на более скоростные тарифы доступа к сети, однако качество сервиса в любом случае не будет гарантированным. Сегодня единственная возможность обеспечения требуемого уровня голосовой связи в открытых сетях – использование услуг провайдера, предлагающего гарантированную скорость линии доступа независимо от времени суток [11]. Для реализованной IVR-системы в открытой сети был проведен анализ ее работоспособности на основе оценки достоверности распознавания речи – одной из основных функций данных платформ. Оценка достоверности распознавания речи определялась процентным отношением количества корректно распознанных фрагментов речи к общему количеству произнесенных. Параметры канала связи (временная задержка, потеря пакетов, джиттер и т.д.), в первую очередь, оказывают влияние на качество передаваемого голосового трафика и как следствие на достоверность распознанных данных. Было исследовано влияние потери пакетов в открытом канале связи на достоверность распознавания данных IVR-системой, находящейся на «облачных» серверах. Для этого эмулировалась ситуация с различным процентом потерь в канале связи при передаче по нему голосового трафика к IVR. Определение оценки достоверности распознавания речи в зависимости от величины потерянных пакетов производилось с использованием заранее записанных голосовых образцов речи клиентов на электронный носитель. Данные образцы «сообщались» IVR-системе по открытому каналу связи, эмулируя тем самым поведение реального клиента, сообщающего данные системе распознавания по телефону. При этом в канале связи моделировалась ситуация потери пакетов. Эмулирование потери пакетов осуществлялось с помощью операционной системы Linux (Ubuntu 9.10). Подробное описание метода формирования задержек и потерь в Linux приводится в [12]. При тестировании IVR-платформы в канале связи, где отсутствует потеря пакетов, среднее значение достоверности распознавания речи составило 96,7%. На рисунке 1 показаны результаты тестирования реализованной IVR-системы с функцией распознавания речи. Моделировалась ситуация при которой изменялась процентная величина потери пакетов в канале (10, 20, 30 и 40%) и для каждого значения вычислялась достоверность распознавания. При каждом измерении системе «сообщалось» определенное предложение, после чего вычислялось процентное соотношение корректно распознанных выражений. Как видно из полученных результатов (рисунок 1), при увеличении процента потери пакетов достоверность распознавания уменьшается.

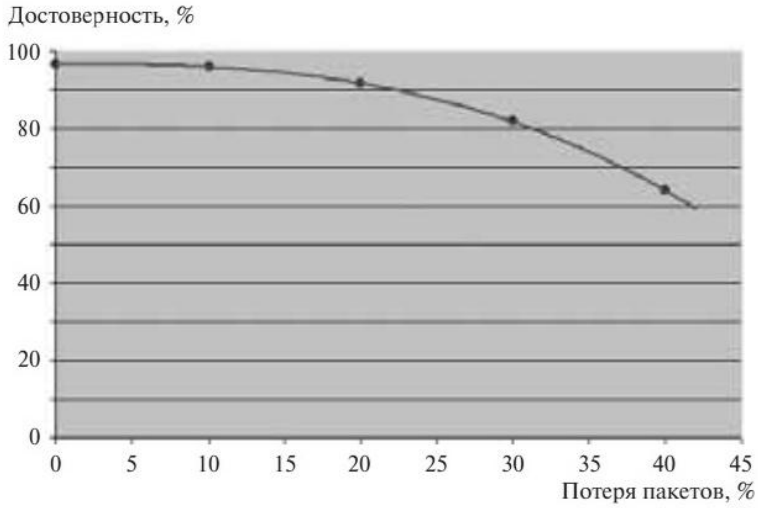


Рисунок 1. Достоверность распознавания в открытом канале связи

При малом проценте потерь пакетов в канале связи значение достоверности распознавания изменяется незначительно. Приблизительно до 30% потери пакетов, достоверность распознавания превышает 80%, что считается хорошим показателем для систем распознавания речи [12]. Допустимое значение достоверности распознавания речи IVR-системой может задаваться непосредственно заказчиком при формировании технического задания на внедрение IVR-системы в телефонную инфраструктуру. Компания-заказчик сама может определять приемлемый для нее процент корректно распознанных данных. Предложенный метод оценки достоверности позволяет заказчикам определять численные требования и ограничения к характеристикам канала связи и может использоваться при выборе оператора связи, предоставляющего услуги доступа в сеть Интернет при размещении IVR на «облачных» серверах.

В заключении можем отметить, что нами рассмотрен новый метод организации IVR-платформы с использованием «облачных» технологий, позволяющий значительно сократить финансовые затраты благодаря внедрению такого комплекса в телефонную инфраструктуру компании. Предлагаемый подход был реализован в открытой телекоммуникационной сети. Механизм оценки качества работы IVR-системы в зависимости от параметров канала передачи данных дает возможность формировать численные требования к характеристикам канала при выборе оператора связи предоставляющего услуги доступа в открытую сеть.

Литература:

1. Росляков, А.В. Анализ гомогенной модели распределенного центра обслуживания вызовов как единой команды / А.В. Росляков, Е.В. Глушак // T-Comm. Телекоммуникации и транспорт. - 2013. - №7. – С. 102 – 105.

2. Глушак, Е.В. Анализ гомогенной модели распределенного центра обслуживания вызовов / Е.В. Глушак, А.В. Росляков // Инфокоммуникационные технологии. – 2013. – Т.12, №3. – С. 23 – 26.

3. Глушак, Е.В. Оценка эффективности применения алгоритма интеллектуального управления входящими вызовами при различных вариантах информированности о состоянии центров обслуживания вызовов / Е.В. Глушак // Инфокоммуникационные технологии. – 2014. – Т.12, №2. – С. 25 – 31.

4. Глушак, Е.В. Экспериментальное исследование модели РЦОВ на основе имитационного моделирования / Е.В. Глушак, А.В. Росляков // T-Comm. Телекоммуникации и транспорт. - 2014. - №11. – С. 42 – 46.

5. Глушак, Е.В. Исследование рефлексивной модели функционирования распределенных центров обслуживания вызовов / Е.В. Глушак // Труды Международной молодежной научно-практической конференции СКФ МТУСИ «ИНФОКОМ-2013», Ростов-на-Дону, 2013. – С. 381 – 384.

6. Синтез русской речи [Электронный ресурс]. – Режим доступа: http://www.speechpro.ru/technologies/synthesis (дата обращения: 22.01.15).

7. Слепич, А.Н. Результаты работы первого семинара «Обеспечение расследования, раскрытия и профилактики преступлений с использованием фоноскопических экспертиз» / А.Н. Слепич, И.В. Рыжкова // Речевые технологии. – 2008. - №2. – С. 73–78.
8. Nuance Voice Biometrics [Электронный ресурс]. – Режим доступа: http://www.nuance.com/for-business/by-solution/customer-service-solutions/solutions-services/inbound-solutions/voice-authentication-biometrics/index.htm (дата обращения: 27.01.15).
9. Asterisk (PBX) [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Asterisk_%28PBX%29 (дата обращения: 02.02.15).
10. The VoiceXML Browser for Asterisk [Электронный ресурс]. – Режим доступа: http://www.i6net.com/wp-content/fi les/documents/I6NET-VXI-developer-guide-en-2010-11.pdf (дата обращения: 05.02.15).
11. Качество речи в IP-сетях [Электронный ресурс]. – Режим доступа: http://www.ccc.ru/magazine/depot/07_12/read.html?Wcd7dcbe937f87.htm (дата обращения: 02.02.13).
12. Эмуляция влияния задержек глобальных сетей в Linux [Электронный ресурс]. – Режим доступа: http://www.opennet.ru/base/net/network_mess_emulation.txt.html (дата обращения: 01.02.15).

А.С. Вартанян, В.В. Бурдюг, В.В. Харченко

ИСПОЛЬЗОВАНИЕ МАГНИТОДИЭЛЕКТРИКОВ ДЛЯ УЛУЧШЕНИЯ ХАРАКТЕРИСТИК И ПАРАМЕТРОВ АНТЕНН

Военный учебно-научный центр ВВС «ВВА», Воронеж

Ключевые слова: антенна, магнитодиэлектрик, радиосвязь.

В работе предлагается использование интеллектуальных покрытий, построенных на основе магнитодиэлектрических материалов, позволяющих управлять характеристиками и параметрами антенных систем. Приведен анализ результатов проведенных авторами исследований по оценке влияния параметров указанных покрытий на характеристики излучения и энергетические параметры цилиндрической антенны. На основе полученных данных сформулированы предложения по эффективному применению интеллектуальных покрытий в антенных системах перспективных комплексов радиосвязи, радиолокации и радионавигации.

A.S. Vartanyan, V.V. Burdyug, V.V. Kharchenko

THE USE OF MAGNETODIELECTRICS TO IMPROVE CHARACTERISTICS AND PARAMETERS OF ANTENNAS

Military Science and Education Centre of air force, Voronezh

Keywords: antenna, magnetodielectric, radio communication.

The paper proposes the use of smart coatings that are based on magnetodielectric materials, allow to control the characteristics and parameters of antenna systems. The analysis of the results of the authors of studies to assess the impact of these parameters on the coating characteristics of the radiation and energy parameters of the cylindrical antenna. Based on these results the proposals for the effective application of intelligent coatings antenna systems perspective complexes radio, radar and navigation.

В настоящее время интенсивно развивается теория и практика использования различного рода защитных покрытий в антенной технике. В антенной технике изначально покрытия выполняли лишь защитные функции излучающего раскрыва от механических повреждений и негативного влияния окружающей среды. Однако, с развитием науки в области структур, обладающих одновременно и диэлектрическими, и магнитными свойствами, указанные выше покрытия стали рассматривать с точки зрения возможности изменения параметров и характеристик как передающих, так и приемных антенн [1]. Электроны в материале движутся

вперед и назад под действием электрического поля и по кругу под действием магнитного. Степень взаимодействия определяется двумя характеристиками вещества: диэлектрической проницаемостью ε и магнитной проницаемостью μ. Первая показывает степень реакции электронов на электрическое поле, вторая - степень реакции на магнитное. У подавляющего большинства материалов ε и μ больше нуля. В настоящее время достаточно большое количество работ посвящено применению покрытий, созданных на базе магнитодиэлектриков (значения диэлектрической ε и магнитной μ проницаемостей покрытия отличны от единицы). Также интересным и с теоретической и практической точек зрения, является вопрос разработки и применения интеллектуальных покрытий на основе недавно созданных, и в настоящее время интенсивно развивающихся, метаматериалов (ε и μ могут принимать отрицательные значения) [2]. Однако в любом случае актуальным является вопрос соотношения значений параметров указанных покрытий для эффективного управления характеристиками и параметрами антенных систем.

Как правило, основной целью применения магнитодиэлектрического покрытия является повышение помехозащищенности и помехоустойчивости антенной системы за счет значительного снижения уровня боковых лепестков диаграммы направленности при незначительном увеличении или сохранении ее ширины [2; 3]. Проведенные авторами исследования позволили оценить влияние параметров ε и μ покрытия на диаграмму направленности и КПД цилиндрической антенной решетки. Выбор цилиндрической конструкции объясняется перспективностью использования неплоских раскрывов. Антенны, размещенные на цилиндрических или сферических поверхностях, выигрывают по ряду показателей у антенн, размещенных на плоских поверхностях, например, появляется возможность электрического перемещения сканирующего луча, что по понятным причинам, повышает надежность функционирования антенных систем в комплексах радиолокации, навигации и связи.

На рисунке 1 приведены диаграммы направленности цилиндрических антенных решеток (ЦАР) щелевых излучателей. При этом сплошными кривыми изображены диаграммы направленности цилиндрической АР без покрытия со спадающим амплитудно-фазовым распределением в раскрыве антенны, а штриховыми линиями – диаграммы направленности ЦАР с магнитодиэлектрическим покрытием с параметрами $\varepsilon = 1.5$ и $\mu = 2$ при равномерном амплитудно-фазовом распределении.

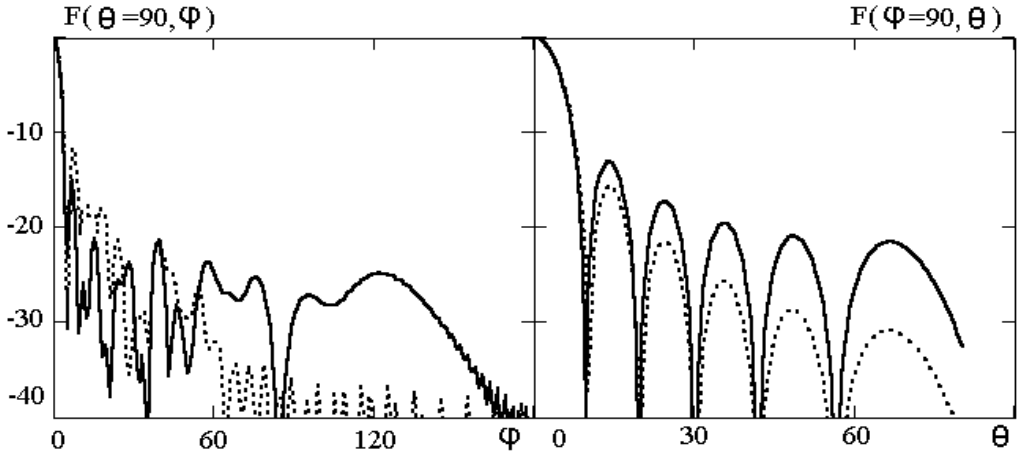


Рисунок 1. Диаграммы направленности антенных решеток

Из рисунков видно, что использование магнитодиэлектрического покрытия позволяет значительно изменять характеристики излучения ЦАР. В частности, из приведенного примера видно, что применение покрытия с указанными параметрами позволяет значительно снизить уровень бокового и заднего излучения в азимутальной плоскости (в диапазоне углов 30-180 градусов) и угломестной плоскости в диапазоне от 0 до 90 градусов.

Степень влияния параметров покрытия на энергетические характеристики ЦАР можно оценить через КПД данной антенны.

На рисунках 2, 3 приведены зависимости значений КПД ЦАР без покрытия (сплошные линии) и КПД ЦАР с магнитодиэлектрическими покрытиями (штриховые линии) от угла θ. Зависимости приведены для различных параметров магнитодиэлектрических покрытий и различных значений волнового сопротивления фидера $W_ф$. На рисунке 2 представлены зависимости при параметрах $\varepsilon = 3$, $\mu = 1$, $W_ф = 150$; на рисунке 3 – при параметрах $\varepsilon = 2$, $\mu = 1.5$, $W_ф = 150$.

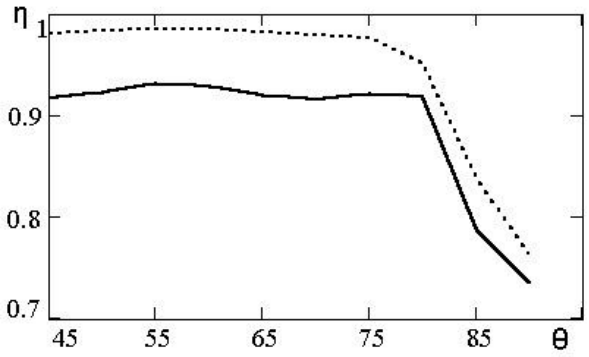


Рисунок 2. Зависимости КПД антенн при $\varepsilon = 3$, $\mu = 1$, $W_ф = 150$

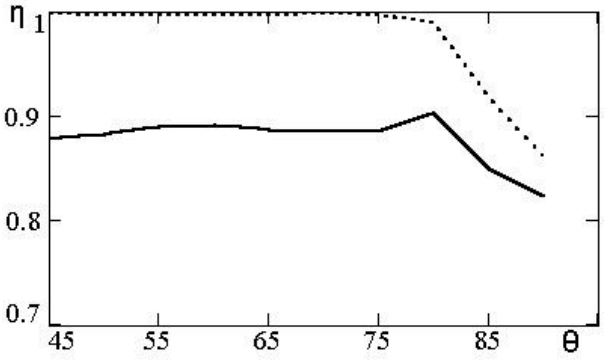


Рисунок 3. Зависимости КПД антенн при $\varepsilon = 2$, $\mu = 1.5$, $W_ф = 150$

Из приведенных результатов следует, что подбор параметров магнитодиэлектрического покрытия позволяет добиться улучшения согласования излучающего раскрыва с фидерным трактом.

Таким образом, могут быть найдены значения электродинамических и геометрических параметров покрытия, при которых обеспечивается как снижение уровня боковых лепестков, так и улучшение согласования в секторе сканирования. Это позволяет обеспечить повышение коэффициента усиления антенны на краю сектора сканирования по сравнению с ЦАР без покрытия.

Литература:

1. Габриэльян Д.Д., Звездина М.Ю., Харченко В.В. Влияние параметров магнитодиэлектрического покрытия на излучение продольной щели на цилиндре // Физика волновых процессов и радиотехнические системы. – 2004. – Т.7. №4.

2. Немцович Л.В., Шадров В.Г. Нанокристаллические ферромагнетики - новый класс магнитолегких материалов. - Зарубежная радиоэлектроника. Успехи современной радиоэлектроники, 2003, №3.

3. Габриэльян Д.Д., Звездина М.Ю. Взаимное сопротивление продольных вибраторов вблизи импедансного кругового цилиндра // Радиотехника. - 2000. - №5. - С.67-69.

В.А. Васильев, А.Н. Буренин, *К.Е. Легков

МОДЕЛИ УПРАВЛЕНИЯ КАЧЕСТВОМ ФУНКЦИОНИРОВАНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Открытое акционерное общество «Научно-исследовательский институт «Рубин»,
г. Санкт-Петербург, Россия
* Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Ключевые слова: инфокоммуникационная сеть специального назначения, модель управления качеством, автоматизированная система управления, контроль объектов управления.

Рассмотрены модели мониторинга управления качеством функционирования управляемых и неуправляемых инфокоммуникационных сетей специального назначения с учётом различных качественных показателей состояния управления. Предложен общий подход к формированию моделей управления для всех уровней управления. Получен вариант рациональной организации процедур управления комплексом услуг инфокоммуникационных сетей специального назначения (ИКС СН), которому соответствует тот или иной уровень качества функционирования ИКС СН.

V.A. Vasiliev, A.N. Burenin,*K.E. Legkov

MODELS OF QUALITY MANAGEMENT IS FUNCTION SPECIAL PURPOSE INFOCOMMUNICATION NETWORKS

Public corporation research Institute of "Rubin", St. Petersburg, Russia
* Military space academy, St. Petersburg, Russia

Keywords: special purpose infocommunication networks, quality management model, automated control system, control of objects of management.

Models monitoring quality management is function of operated and uncontrollable special purpose infocommunication networks taking into account various quality indicators of a condition management are considered. The general approach to formation of models management for all levels are management is offered. The option of the rational organisation procedures management is received by a complex of services to which there corresponds this or that level of quality is function.

Среди основных задач управления инфокоммуникационными сетями специального назначения (ИКС СН) задача управления качеством их функционирования является наиболее сложной, т.к. связана с необходимостью учета многих факторов, характеристик и параметров сложных процессов, протекающих в ИКС СН. Поэтому при построении моделей управления качеством функционирования ИКС СН целесообразно декомпозировать эту задачу на две подзадачи и разрабатывать модели управления для этих подзадач, рис. 1.

В настоящее время известно значительное число способов организации управления сетями и услугами, которые не всегда применимы и эффективны при управлении ИКС СН в силу ее сложности, многоуровневости и мультисервисности. Поэтому, и с учетом того, что архитектура современных ИКС СН содержит три основных уровня, управление качеством функционирования ею также целесообразно организовать по трем уровням управления. Вместе с тем целесообразно предложить общий подход к формированию моделей управления для всех уровней.

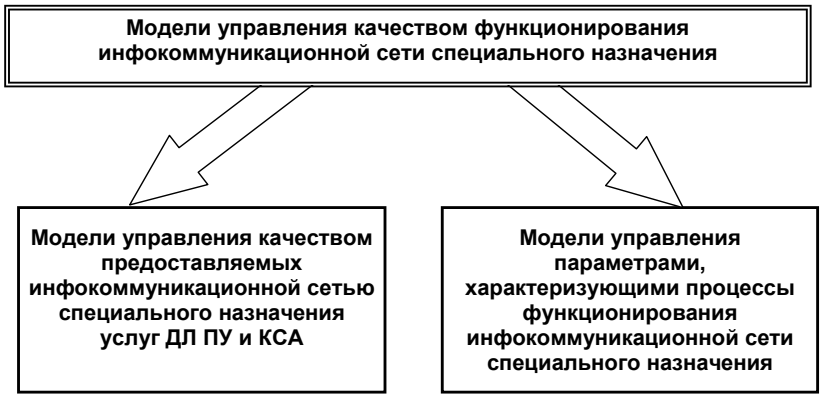


Рисунок 1. Декомпозиция моделей управления качеством функционирования ИКС СН

Из всех процессов управления, каждый из которых в той или иной степени влияет на эффективность ИКС СН, непосредственно влияют на параметры, отражающие ее качественные характеристики, только процессы управления качеством функционирования.

Функционирование ИКС СН с определенными качественными показателями, при которых ее основные цели выполняются, характеризуются определенным состоянием управления $\overline{\overline{S}}$, при этом все состояния управления, которые могут встречаться в процессе управления ИКС СН, можно подразделить на два подмножества – управляемых, при которых заданная цель ИКС СН $\mathbf{C}_{ICN}$ всегда достигается, и неуправляемых, когда эта цель $\mathbf{C}_{ICN}$ не достигается.

Обозначим $\{\overline{\overline{S}}\}$ множество всех возможных состояний управления $\overline{\overline{S}}$, встречающихся в процессе управления ИКС СН. Пусть $\{\overline{\overline{S}}_{\text{r}}\}$ – подмножество множества состояний управления $\{\overline{\overline{S}}\}$, где ИКС СН неуправляема, т.е. не все цели из $\mathbf{C}=\{\mathbf{C}_{ICN}\}$ достигаются, а $\{\overline{\overline{S}}_{\text{s}}\}$ – подмножество состояний управления, где ИКС СН управляема, т.е. все цели из $\mathbf{C}=\{\mathbf{C}_{ICN}\}$ достигаются.

Очевидно, что

$$\{\overline{\overline{S}}_{\text{s}}\}\bigcup\{\overline{\overline{S}}_{\text{r}}\}=\{\overline{\overline{S}}\}. \quad (1)$$

Каждому элементу множества $\{\overline{\overline{S}}\}$ целесообразно поставить в соответствие число, не превышающее 1 из множества $P\{\overline{\overline{S}}\}$, которое определяет вероятность появления этого состояния. В силу чрезвычайной сложности ИКС СН число элементов множества $\{\overline{\overline{S}}\}$ настолько велико, что под $P\{\overline{\overline{S}}\}$ допустимо понимать плотность вероятности, т.е.:

$$\int_{\overline{\overline{S}}} P\{\overline{\overline{S}}\}\, d\overline{\overline{S}}=1. \quad (2)$$

Соотношение (2) определяет, что вне области $\{\overline{\overline{S}}\}$ не могут встретиться реальные состояния управления ИКС СН.

Для выполнения целей при управлении качеством функционирования ИКС СН необходимо соответствующим образом (с помощью управления) изменить состояние управления $S_c=F\left(U_c Z_c\right)$, которое зависит от управления U_c и совокупности внешних воздействий на ИКС СН Z_c.

При выборе определенного управления $U_{c\,fics}$ получается вполне конкретное качество обслуживание пользователей, т.е. вполне определенное значение качественных показателей функционирования ИКС СН $Q(.....)$, а это приводит к некоторой экстремальной задаче:

$$Q\left(Z_c, S_c\right)\rightarrow \max_{U_{c\,fics}\in\Xi}. \quad (3)$$

Решение этой экстремальной задачи − некоторое управление $\mathbf{U}^{*}_{c\,fics}$, являющееся оптимальным управлением качеством функционирования ИКС СН. В этом решении использована модель ИКС СН и учтен ресурс, выделяемый на управление Ξ.

Многоуровневое управление ИКС СН в сложных условиях обстановки невозможно без гибкого оперативного распределения предоставляемых пользователям услуг в реальном масштабе времени. При этом обеспечение гибкости, масштабируемости и возможности наращивания номенклатуры требуемых услуг при управлении ИКС СН невозможно без рациональной организации процедур управления комплексом предлагаемых услуг.

Для выполнения конкретной задачи в различных сложных условиях, каждому ПУ ведомственной или корпоративной АСУ требуется определенное соотношение предоставляемых ИКС СН гарантированных информационных и телекоммуникационных услуг, которому соответствует тот или иной уровень качества функционирования ИКС СН, определяемый в плоскости предоставляемых услуг, в конечном счете, значениями показателей качественного функционирования соответствующих служб ИКС СН (IP-телефония, ПД, ЭП, ФО, ВКС и пр.), т.е. соответственно $Q_{IPT\Phi}, Q_{PD,} Q_{EM,} Q_{FT,} Q_{VKS}$:

$$Q^{O(i)} = f^{O(i)}(Q_{IPT\Phi}, Q_{PD,} Q_{EM,} Q_{FT,} Q_{VKS}) \quad (4)$$

где $O(i)$ - *i*-я операция.

Таким образом, необходимо решить многокритериальную задачу по такой организации управления услугами ИКС СН (совокупности предоставляемых услуг пользователям – ДЛ и прикладным процессам ПУ ведомственных или корпоративных АСУ), которая обеспечит экстремум показателю эффективности функционирования ИКС СН при проведении $O(i)$ операции, т.е.:

$$\mathrm{extr} Q_{ICN\,SN}^{O(i)} = \mathrm{extr}[\, f^{O(i)}(Q_{IPT\Phi}, Q_{PD,} Q_{EM,} Q_{FT,} Q_{VKS})]. \quad (5)$$

В принципе, эта задача может быть решена методами многокритериальной оптимизации по Парето (решением задачи оптимизации является множество Парето) или приведением к единому показателю как взвешенной сумме частных показателей (свертка).

Литература:

1. Легков К.Е., Буренин А.Н. К вопросу управления эффективностью инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 1. – С. 38–43.
2. Легков К.Е. Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 4. – С. 38–43.
3. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2014. № 5. – С. 34–40.
4. Легков К.Е., Скоробогатова О.А. Основные направления развития автоматизированных систем управления специального назначения и требования предъявляемые к ним системой управления // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 1. – С. 40–45.
5. Буренин А.Н., Легков К.Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 3. – С. 12–17.
6. Буренин А.Н., Легков К.Е. Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 4. – С. 46–50.
7. Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 5. – С. 8–12.
8. Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. № 6. – С. 22–28.
9. Буренин А.Н. , Легков К.Е., Мясникова А.И. Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 11–13.

10. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 1. – С. 14–16.

11. Легков К.Е., Буренин А.Н. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 2. – С.4–7.

12. Буренин А.Н., Легков К.Е. К вопросу управления рисками при обеспечении безопасности инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 17–19.

13. Легков К.Е., Мясникова А.И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2012. № 3. – С. 20–22.

В.Д. Меерович, *С.В. Гусишная

АЛГОРИТМ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ НАВИГАЦИОННЫХ СПУТНИКОВЫХ ИЗМЕРЕНИЙ

Ростовский государственный университет путей сообщения, г. Ростов-на-Дону, Россия
*Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: спутниковая навигация, погрешности измерения псевдодальностей, координаты спутников.

Предложен способ определения расстояний между спутниками и погрешностей взаимной синхронизации часов навигационных спутников, которые используются для компенсации помех в сигнале навигационного приемника объекта.

V.D. Meerovitch, *S.V. Gusishnaya

ALGORITHM OF PARAMETER IDENTIFICATION NAVIGATION SATELLITE MEASUREMENTS

Rostov State Transport University, Rostov-on-Don, Russia
* North-Caucasian branch of the Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: satellite navigation, pseudorange measurement errors, the coordinates of satellites

A method for determining the distance between the satellites and mutual synchronization errors hours of navigation satellites, which are used to compensate for signal interference navigation receiver object is offered.

Введение. Ошибки решения спутниковой навигационной задачи в значительной мере зависят как от ошибок определения текущих координат спутников, так и от степени подавления помех, возникающих при приеме-передаче спутниковых сообщений. В общем случае информационная структура спутникового измерения псевдодальности Z_R, используемого в качестве основного сигнала при позиционировании объектов, с учетом помех, в наибольшей степени влияющих на точность позиционирования, имеет вид:

$$Z_R = \sqrt{(\xi - \xi_c)^2 + (\eta - \eta_c)^2 + (\zeta - \zeta_c)^2} + c(\Delta\tau - \Delta T) + W_{ИТ} + W_{П}, \quad (1)$$

где ξ_c, η_c, ζ_c - текущие координаты спутника в гринвичской системе координат (ГрСК),

ξ, η, ζ - текущие координаты объекта в ГрСК,

С - номинальное значение скорости света в вакууме,

$\Delta\tau$ - погрешность часов навигационного приемника,

ΔT - погрешность часов спутника,

$W_{ИТ}$ - погрешности, обусловленные прохождением радиосигнала через ионосферу и тропосферу,

$W_{П}$ – инструментальные погрешности навигационного приемника.

Ниже рассмотрим возможность компенсации приведенного спектра погрешностей, среди которых значительный удельный вес имеют инструментальные погрешности навигационного приемника и ошибки часов спутника и приемника. Так, например, несмотря на установку атомных часов на навигационных спутниках, среднеквадратическое значение ошибки взаимной синхронизации бортовых шкал времени может достигать 20 и более нс [1].

В настоящее время для компенсации погрешности часов применяются различные алгоритмы, построенные на основе ее аппроксимации временными полиномами. Например, в СНС ГЛОНАСС ошибка часов спутника ΔT аппроксимируется линейной зависимостью от времени с заданными параметрами (в GPS применяется квадратичная зависимость):

$$\Delta T = \alpha_0 + \alpha_{1t} + T_{\Gamma} + T_P \,, \tag{2}$$

где t- время расчета погрешности на момент поступления спутниковой информации,

α_0, α_1 - известные параметры модели ошибки часов спутника,

T_{Γ} – время задержки спутникового сигнала,

T_P – релятивистская поправка, определяемая в процессе вычисления координат спутника.

Как видно из (2), компенсационная модель содержит 4(!) параметра, требующих дополнительного непростого их определения с различной периодичностью, снижающего общую эффективность применения модели (2). В связи с этим рассмотрим ниже способ компенсации ошибок часов спутника ΔT и приемника $\Delta\tau$, а также инструментальных погрешностей навигационного приемника, позволяющий осуществлять компенсацию их текущих значений непосредственно в навигационном приемнике без использования каких-либо аппроксимирующих моделей.

Алгоритм идентификации параметров спутника. Существующие навигационные системы ГЛОНАСС и GPS с целью повышения точности решения навигационной задачи проходят в настоящий момент усиленную модернизацию, позволяющую, в частности, определять с помощью бортовых измерительных средств расстояния между спутниками, находящимися в зоне прямой видимости.

Так, например, навигационные спутники ГЛОНАСС-М оснащаются бортовой аппаратурой межспутниковых измерений [2], а навигационные спутники ГЛОНАСС-К - приемоформирующим устройством межспутниковой радиолинии [3]. Формирующая часть устройства межспутниковой радиолинии осуществляет формирование и излучение информационно-измерительных радиосигналов, структура которых аналогична структуре навигационного сигнала ГЛОНАСС. В приемной части осуществляется усиление радиосигналов и измерение псевдоскорости и псевдодальности между навигационными спутниками системы ГЛОНАСС и выделение цифровой информации из принимаемого информационно-измерительного сигнала.

Повышение точности определения положения навигационных спутников возможно также при использовании лазерных дальномеров [4,5], в основе которого лежит принцип измерения времени распространения лазерных импульсов.

При этом очевидно, что сигналы измерения псевдодальностей между *i*-м и *j*-мспутниками будут свободны от погрешностей, обусловленных прохождением сигнала через ионосферу и тропосферу как в (1), и будут иметь вид:

$$Z_{ij} = R_{ij} + c(\Delta T_i - \Delta T_i) = R_{ij} + \Delta T_{ji} \,, \tag{2}$$

где Z_{ij} – псевдодальность, измеренная на j-м спутнике,

R_{ij} - истинная дальность между i-м и j-м спутниками,

ΔT_i - погрешность часов i-госпутника,

ΔT_j - погрешность часов j-го спутника,

$\Delta T_{ji} = c(\Delta T_j - \Delta T_i)$ - погрешность, обусловленная ошибкой взаимной синхронизации часов i-го и j-го спутников.

Перед построением алгоритма идентификации искомых пространственно-временных параметров спутников предварительно определим число спутников N, необходимое и достаточное для их полной идентификации. Число всех возможных расстояний между N спутниками (равное числу ребер графа с N вершинами) определяется известным выражением: $N(N-1)/2$. При обоюдном измерении расстояний между двумя спутниками число измеренных межспутниковых дальностей будет равно, соответственно, $N(N-1)$. В полученных измерениях содержатся следующие неизвестные переменные: $N(N-1)/2$ истинных расстояний между N спутниками и $(N-1)$ линейно независимых ошибок взаимной синхронизации часов N спутников (остальные $(N-1)(N/2-1)$ определяются их линейными комбинациями), т.е. общее число неизвестных переменных составляет $N(N-1)/2+N-1$. Приравнивая общее число измерений к числу неизвестных переменных, имеем следующее уравнение:

$N(N-1)/2 = N-1$

или

$N^2 - 3N + 2 = 0$,

откуда легко определяется число спутников, необходимое и достаточное для решения поставленной задачи идентификации:

N=2.

В принятых обозначениях измеренные расстояния (псевдодальности) Z_{ij}между двумя навигационными спутниками А и В могут быть представлены следующим образом:

$$Z_{BA} = R_{AB} + \Delta T_{AB},$$
$$Z_{AB} = R_{AB} + \Delta T_{BA}, \qquad (3)$$

где ΔT_{AB}, ΔT_{BA} – погрешности взаимной синхронизации часов спутников А и В,

R_{AB} - истинная дальность между спутниками.

Учитывая очевидное соотношение:

$\Delta T_{AB} = -\Delta T_{BA}$,

система (3) из 2-х уравнений с 3-мя неизвестными может быть сведена к системе 2-х уравнений с 2-мя неизвестными – истинной дальностью R_{AB} и погрешностью взаимной синхронизации часов спутников:

$$Z_{BA} = R_{AB} + \Delta T_{AB},$$
$$Z_{AB} = R_{AB} - \Delta T_{AB}, \qquad (4)$$

и легко решается непосредственно на борту каждого из спутников А и В.

В данном случае решается не только задача текущего определения погрешностей взаимной синхронизации часов всех спутников, используемых, как показано далее, для компенсации помех в сигнале навигационного приемника объекта, но и расстояний между спутниками, используемых, в свою очередь, в качестве дополнительной информации для повышения точности измерения текущего местоположения спутников.

Алгоритм технической реализации предложенного подхода рассмотрим по шагам на примере спутника А.

1. Передача навигационных сообщений к спутнику В.

2. Прием навигационных сообщений от спутника В (выполняется одновременно с п.1).
3. Определение псевдодальности Z_{BA} до спутника В.
4. Передача полученного значения псевдодальности Z_{BA} на спутник В.
5. Прием значения псевдодальности Z_{AB} от спутника В (выполняется одновременно с п.4).
6. Решение системы уравнений (4) и вычисление истинной дальности R_{AB} и погрешности взаимной синхронизации часов ΔT_{AB}.
7. Передача в спутниковом навигационном сообщении погрешностей взаимной синхронизации часов ΔT_{AB}.

Алгоритм компенсации погрешностей спутникового сообщения в навигационном приемнике. Для решения навигационной задачи спутниковые сообщения принимаются, как правило, не менее, чем от четырех спутников [1,2], что позволяет формировать различные линейные комбинации сигналов, принимаемых от разных спутников. Так, разность сигналов псевдодальностей, принятых от двух спутников – *i*-го и *j*-го, с учетом (1) имеет вид:

$$Z_{Ri} - Z_{Rj} = \sqrt{(\xi - \xi_{ci})^2 + (\eta - \eta_{ci})^2 + (\zeta - \zeta_{ci})^2} - \sqrt{(\xi - \xi_{cj})^2 + (\eta - \eta_{cj})^2 + (\zeta - \zeta_{cj})^2} + \\ + \Delta T_{ij} \quad , \qquad (5)$$

где принято вытекающее из практики спутниковой навигации допущение об идентичности помех, обусловленных прохождением через ионосферу и тропосферу радиосигналов спутников, находящихся в зоне видимости одного и того же объекта.

Как видно из (5), разность сигналов $Z_{Ri} - Z_{Rj}$ любых двух спутников содержит помеховую составляющую ΔT_{ij}, которая уже известна из принятого спутникового сообщения и может быть скомпенсирована (при этом разность сигналов не содержит остальных помех, приведенных в (1): ошибок часов приемника, его инструментальных погрешностей и др.). В результате, обработке – применению стандартной итеративной процедуры решения системы нелинейных уравнений (5) относительно координат $\xi,\ \eta,\ \zeta$ [1,2], подлежат сигналы, содержащие только истинную информацию о координатах объекта, что позволяет существенно повысить общую точность решения навигационной задачи.

Заключение. Предложенный подход к идентификации пространственно-временных параметров навигационныхспутников позволяет, используя простые методы радио- и лазерных измерений, во-первых, существенно повысить точность синхронизации хода часов на всех навигационных спутниках группировки (что особенно важно для системы ГЛОНАСС, наземные станции синхронизации времени которой расположены только на территории РФ), а во-вторых, повысить общую точность решения навигационной задачи за счет компенсации основных помех в принятом навигационном сообщении.

Литература:

1. ГЛОНАСС. Интерфейсный контрольный документ / Навигационный радиосигнал в диапазонах L1, L2 с открытым доступом и частотным разделением (Редакция 5.1). 2008. – 74с.

2. ГЛОНАСС. Принципы построения и функционирования / Под ред. А.И. Перова, В.Н. Харисова. – 3-е изд., перераб. – М.: Радиотехника, 2005 . – 688 с.

3. Ступак Г. Г., Ревнивых С. Г., Игнатович Е. И., Куршин В. В., Бетанов В. В., Панов С.С., Бондарев Н.З., Чеботарев В. Е., Решетнёва М. Ф., Балашова Н. Н., Сердюков А. И., Синцова Л. Н. // Выбор структуры орбитальной группировки перспективной системы ГЛОНАСС // Космонавтика. №3-4 (6). 2013. С. 4–11.

4. Чубыкин А.А., Рой Ю.А., Корнишев О.М., Падун П.П. Использование бортовых лазерных измерительно-связных средств для повышения точности и оперативности ЭВО спутников системы ГЛОНАСС // ЭВ & ЭС. Т. 12. 2007. С. 25–30.

5. Шаргородский В.Д., Чубыкин А.А., Сумерин В.В. Межспутниковая лазерная навигационно-связная система // Аэрокосмический курьер. 2007. № 1 (49). С. 88–89.

Е.С. Власенко

ПРОГНОЗИРОВАНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ ДОСТУПА

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, г.Санкт-Петербург, Россия

Ключевые слова: сеть доступа, прогнозирование, пропускная способность, сценарий развития, прогнозирование временного ряда, вейвлет-аппроксимация.

В статье рассматриваются существующие методы прогнозирования показателей сети. Анализируются изменения пропускной способности сети доступа в странах с разным уровнем экономического развития. Предложен гибридный метод прогнозирования данного показателя. В нем предлагается использовать три сценария развития изменений: оптимистический, прагматический и пессимистический. Прагматический сценарий предлагается строить на базе вейвлет-аппроксимации временного ряда для возможности учета локальных особенностей. Сценарий наилучшего развития событий строится на базе закона Нильсена, а наихудший – из роста объема передаваемого видеотрафика. На основе данного метода сделан краткосрочный прогноз для России.

E.S. Vlasenko

FORECASTING BANDWIDTH SPEED OF ACCESS NETWORK

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg, Russia

Keywords: access network, forecasting, bandwidth speed, scenario of development, prediction of time series, wavelet-approximation.

The article deals with existing methods of forecasting network indicators. Changes of bandwidth speed of access network in countries with different level of economic development are analyzed. A hybrid method of forecasting is offered for this indicator. It is proposed to use three scenarios of changes: optimistic, pragmatic and pessimistic. Pragmatic scenario is based on wavelet-approximation of the time series for the possibility of taking into account local peculiarities. The best scenario development is based on the Nielsen's law and the worst - of the growth of video traffic. Short-term forecast is made for Russia with this method.

Введение

Прогнозирование необходимо при планировании сети и выполняется для ее основных показателей. Оценки их изменений в будущем могут привести к высоким рискам принятого оператором сценария развития сети. Поэтому развитие методологии прогнозирования является одной из важнейших задач исследования в области планирования сетей.

Сегодня существуют разные подходы к оценке и прогнозированию развития сетей. Одним из самых распространенных является контроль изменения количества подключенных к сети оконечных устройств. Их количественное изменение во времени обычно описывается логистическим законом роста. Это позволяет сделать прогноз будущего развития. Другим подходом является использование для прогнозирования статистической зависимости плотности оконечных устройств и внутреннего валового продукта на душу населения (ДВВП). Впервые такой подход был применен Джиппом для телефонии и отражен в виде одноименной диаграммы. Эти методы позволяют оценить изменение числа оконечных устройств, но не требований к сети доступа. Рассмотрим процесс развития широкополосного доступа (ШПД). Для его оценки уже

недостаточно рассматривать только плотность оконечных устройств, так как при том же их количестве наблюдается увеличение требований к пропускной способности сети. Причиной являются изменения объемов трафика, в том числе вследствие появления новых услуг, а также возможности имеющихся устройств.

Анализ изменений пропускной способности во времени

Рассмотрим зависимость пропускной способности уровня доступа нескольких стран от времени, предварительно сгруппировав их по уровню развития экономики, в соответствии с делением, которое приводит МСЭ [1]. Для анализа будем использовать статистические данные о скорости загрузки в сети Интернет базы данных NetIndex [2]. Так как максимальная скорость передачи данных участка сети доступа определяет возможность получения пользователем услуг и, в большинстве случаев, именно она выступает в роли ограничителя, то положим, что эта часть сети обладает наименьшей пропускной способностью на всем пути передачи данных. Поэтому будем соотносить информацию из базы данных со значениями пропускной способности этого участка. Проанализируем зависимости изменения максимальной скорости передачи от времени за период с 2008 по 2014 год для обеих групп. Они имеют схожий характер изменений, но в группе развитых стран значения пропускной способности выше, чем в развивающихся.

Процесс изменения пропускной способности сети абонентского доступа имеет логистическую функцию тренда следующего вида:

$$y = \frac{A}{1+e^{-\frac{t-t_0}{B}}}, \quad (1)$$

где A – асимптотическое значение функции y, B – коэффициент, определяющий скорость роста y с t, t_0 – расположение во времени. Определим параметры в уравнениях кривой для России и некоторых стран из обеих групп. Результаты отражены в таблице 1.

Таблица 1. Параметры уравнений кривых тренда разных стран

Страна	A	B	t_0	Коэффициент регрессии, %
Россия	52739,30	50,251	562,31	98.46
Норвегия	66729,90	45,45	525,45	98,54
Сингапур	253371	25,64	384,10	98.77
Судан	4613,48	38,46	461,54	91,61
Катар	52246,70	34,48	463,45	97,72

Итак, экономически более развитые страны имеют большие скорости передачи на уровне доступа, чем развивающиеся. В аналитической записи аппроксимирующих кривых эта особенность отражается величиной коэффициента B. Таким образом, в странах с более высоким уровнем экономики при больших начальных значениях рост пропускной способности уровня доступа происходит медленнее, чем в менее развитых со значительно меньшими начальными величинами.

Сценарии краткосрочного развития изменений пропускной способности

Краткосрочный период развития обычно принимают равным 3-5 годам. Будем рассматривать горизонт планирования сроком в 3 года.

Выше было показано, что изменение пропускной способности может быть описано с помощью логистической кривой. Но чтобы учесть локальные особенности изменения и повысить точность приближения будем использовать вейвлет-аппроксимацию временного ряда. Разложим его на аппроксимирующую и набор детализирующих составляющих с помощью многократного стационарного дискретного вейвлет-преобразования. Проведем независимое прогнозирование каждой компоненты на заданный период упреждения. Прогноз изменений исходного временного ряда на заданном горизонте планирования получим путем объединения соответствующих будущих значений компонент на нем. Полученный результат будем использовать в качестве прагматического сценария прогноза значений максимальной скорости передачи сети доступа в будущем для заданного периода упреждения. Прогноз для России представлен на рис.1.

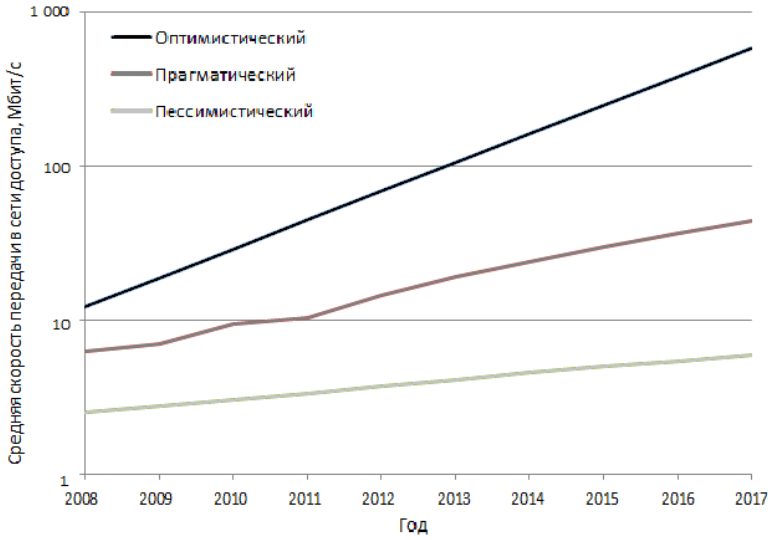


Рисунок 1. Сценарии прогноза изменения пропускной способности сети доступа

По данным Cisco Visual Networking Index [3] для региона Центральной и Восточной Европы прогноз пропускной способности на 2018 год составляет 45 Мбит/с, а в 2013 она принимала значение 17,5 Мбит/с. Цифры полученного прогноза и составленного компанией Cisco близки, что повышает правомерность сделанных расчетов. Однако неопределенность данного развития в будущем служит поводом к разработке альтернативных сценариев.

Оптимистический сценарий получим, используя закон Нильсена [4]. В соответствии с данным законом о динамике скорости передачи данных на уровне доступа: пропускная способность этого участка сети увеличивается на 50% каждый год. Поэтому построим, в соответствии с ним, прогноз для России. Его можно задать с помощью следующей функции:

$$y = 185{,}23 \cdot e^{0{,}43 \cdot x}. \quad (2)$$

Оптимистический сценарий прогноза представлен на рис.1.

По данным TeleGeography [5] максимальная скорость, определяемая на одно подключение в долгосрочных проектах операторов, больше 1 Гбит/с. Сопоставив эти значения с данными полученными по закону Нильсена, можно утверждать, что данная зависимость подтверждается.

Под пессимистическим сценарием прогноза будем понимать вариант развития, предполагающий наименьший рост пропускной способности в сети доступа. Минимальную скорость передачи можно определить как среднюю скорость доступа из расчета на одно подключение необходимую для предоставления запланированных услуг. Как правило, сегодня предоставление услуг по отдельности уступает место пакетному. Для него требуется предусмотреть пропускную способность уровня доступа, позволяющую предоставлять потоковые и интерактивные услуги. Также учтем, что включение Интернета Вещей в существующую сеть позволит предоставлять новые услуги, для которых пока неясно какая пропускная способность будет необходима для их предоставления. Предположим, что передача видео среди них будет самой ресурсоемкой (например, передача видео с камеры в операционной). Таким образом, пропускную способность требуемую для предоставления услуг потокового вещания с поддержкой интерактивности будем рассматривать как необходмую для реализации и самую ресурсоемкую. Поэтому полоса пропускания должна обеспечивать скорость, превышающую требуемую для этой услуги.

Требования к полосе пропускания при передаче видео зависят от способа кодирования и сжатия, а также параметров передаваемого изображения. В последние десятилетия наблюдается устойчивый рост требований к параметрам передаваемого изображения. Например, вследствие увеличения его четкости, значительно вырос объем данных для незакодированного видео HD по сравнению с UHD. Подобный тренд приводит к росту необходимой скорости передачи, несмотря на создание все более эффективных по сжатию методов кодирования. Другой причиной увеличения необходимой скорости является рост потребности в более высокой степени сжатия видео для таких приложений, как потоковая передача в интернете и телевизионное вещание.

По данным компании Cisco [6] в 2013 году объем видео в общем IP трафике составлял 66%, а к 2018 прогнозируется рост до 79%. Таким образом, видео трафик является самым требовательным по необходимой скорости передачи. Поэтому для оценки необходимой пропускной способности нужно знать доли видео разной четкости. Для подобной оценки воспользуемся прогнозом компании Cisco (рис.2).

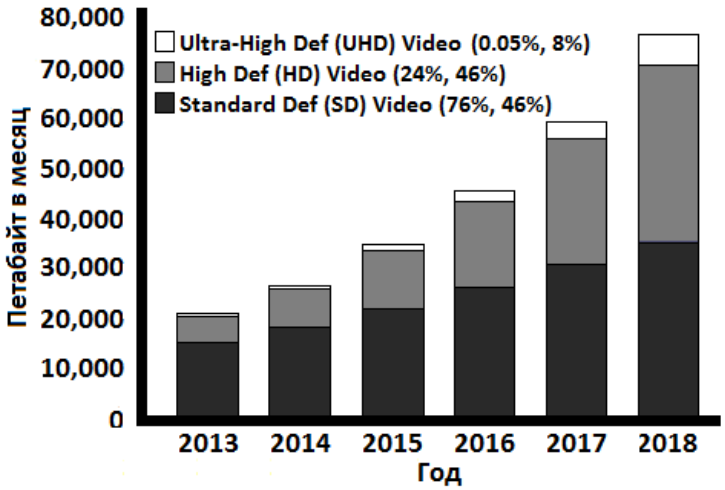


Рисунок 2. Рост мирового объема видео в Интернете [6]

Разработанный в виде трех сценариев прогноз изменений пропускной способности сети доступа для России приведен на рис.1.

Заключение

В работе были рассмотрены способы прогнозирования одного из показателей сети. Использование только метода количественного прогнозирования не учитывает возможности появления новых факторов, которые могут повлиять на процесс и не рассматривались при составлении прогноза. Таким образом, требуется предусмотреть возможность качественных изменений в будущем. Поэтому следует рассматривать несколько сценариев развития процесса в будущем, что было продемонстрировано выше. Подобный подход можно охарактеризовать как гибридный. Его применение позволяет получить наиболее полную картину будущих изменений.

Литература:

1. Country classifications / ITU. – URL: http://www.itu..int/en/ITU-D/Statistics/Pages/definitions/regions.aspx (дата обращения: 09.02.2015).

2. NetIndex. – URL: http://www.netindex.com/ (дата обращения: 02.02.2015).

3. Cisco Visual Networking Index / Cisco. – URL: http://share.cisco.com/vni14/ (дата обращения: 25.12.2014).

4. Nielsen's Law of Internet Bandwidth. – URL: http://www.nngroup.com/articles/law-of-bandwidth/ (дата обращения: 09.02.2015).

5. Authoritative Telecom Data: CommsUpdate / TeleGeography. – URL: https://www.telegeography.com/products/commsupdate/ (дата обращения: 25.12.2014).

6. Cisco Visual Networking Index and VNI Service Adoption: Global Forecast Update 2013–2018 / Cisco. – 2014. – URL: http://www.ciscoknowledgenetwork.com/files/448_06-24-14-VNI_Traffic_and_Service_Adoption_Forecast_Presentation__CKN_MOBILITY_.pdf?PRIORITY_CODE= (дата обращения: 09.02.2015).

С.В. Гаркуша, Е.В. Гаркуша

КОМПЛЕКСНОЕ РЕШЕНИЕ ЗАДАЧ РАСПРЕДЕЛЕНИЯ ЧАСТОТНЫХ КАНАЛОВ И ПОТОКОВОЙ МАРШРУТИЗАЦИИ В MESH-СЕТЯХ СТАНДАРТА IEEE 802.11, ПРЕДСТАВЛЕННЫХ В ВИДЕ ГИПРЕГРАФА

Полтавский университет экономики и торговли, г. Полтава, Украина

Ключевые слова: многоканальная многоинтерфейсная mesh-сеть, потоковая маршрутизация, распределение частотных каналов, гиперграф, граф Кенига.

Предложен подход к использованию гиперграфов и графов Кенига при моделировании многоканальных многоинтерфейсных mesh-сетей стандарта IEEE 802.11. Это, в свою очередь, позволило более полно и детально описать возможные конфигурации как всей mesh-сети в целом, так и отдельных ее элементов при решении задачи распределения неперекрывающихся частотных каналов в виде гиперграфа, а также в виде разнородных вершин графа Кенига при решении задачи маршрутизации. Основываясь на гиперграфовом, а также плоском кениговом представлении mesh-сети, в работе выполняется согласованное решение задач распределения неперекрывающихся частотных каналов и потоковой маршрутизации.

S.V. Garkusha, E.V. Garkusha

DEVELOPING A MODEL OF CONSISTENT SOLUTION THE DISTRIBUTION OF NONOVERLAPPING FREQUENCY CHANNELS AND FLOW ROUTING IN MULTICHANNEL MULTIRADIO MESH-NETWORK IEEE 802.11

Poltava University of Economics and Trade, Poltava, Ukraine

Keywords: multichannel multiradio mesh-network, flow routing, distribution of frequency channels, hypergraph, graph Koenig.

An approach to the use of hypergraphs and graphs Koenig for modeling multilchannel multiradio mesh-networking standard IEEE 802.11. This, in turn, allowed for a fuller and describe in detail all the possible configurations of mesh-network as a whole and its individual elements in solving the problem of distribution of non-overlapping frequency channels in the form of a hypergraph as well as dissimilar vertices of Koenig in solving the problem of routing. Based on hypergraph and flat koenigs representation of multi- multilchannel multiradio mesh-network in the work performed consistent solution of problems of distribution of non-overlapping frequency channels and stream routing.

Одним из наиболее эффективных средств повышения производительности беспроводных mesh-сетей (Wireless Mesh Network, WMN) стандарта IEEE 802.11 является подход, основанный на использовании многоканального многоинтерфейсного режима ее построения и функционирования (Multi-Radio Multi-Channel Wireless Mesh Networks, MR MC WMN) с эффективным решением задач распределения неперекрывающихся частотных каналов [1; 2] и маршрутизации. В результате анализа известных решений топологического описания MR MC WMN стандарта IEEE 802.11 установлено, что все они базируются на использовании графового представления. Использование теории графов обеспечивает максимальную наглядность при моделировании MR MC WMN, так как множеству станций ставится в однозначное соответствие множество вершин графа, а множеству радиоканалов – множество ребер (дуг) графа. Использование графового представления MR MC WMN целесообразно в случае использования на mesh-станциях направленных антенн, так как между ними формируется радиоканал, который может быть представлен в виде ребра графа. Однако в случае использования на mesh-станции не направленных антенн, графовое представление MR MC WMN не обеспечивает адекватный учет их особенностей, с учетом формирования кластерной структуры.

Таким образом, при моделировании MR MC WMN необходимо использовать более эффективные, хотя, возможно, и более сложные, способы представления mesh-сети с использованием топологических идей. В качестве таких подходов предложено использовать математический аппарат теории гиперграфов, что позволяет провести теоретическое описание

задач распределения частотных каналов и маршрутизации в MR MC WMN с учетом станционного размера, степени перекрытия и неоднородности зон устойчивого приема на этапе постановки задач, а также анализа станционных размеров создаваемых доменов коллизий и их связности на этапе анализа результатов решения.

Предложенная топологическая модель MR MC WMN стандарта IEEE 802.11, которая позволила более полно и подробно описать возможные конфигурации как всей mesh-сети в целом, так и отдельных ее элементов представленных в виде вершин и ребер гиперграфа. В рамках гиперграфового представления, как было показано в работах [3], MR MC WMN ставится в соответствие гиперграф $H(I, J; R)$, где I – множество вершин, J – множество ребер, R – предикат, определяющий смежность станций с зонами устойчивого приема (Transmission Range, TR). $I = \{n_i, i = \overline{1, N}\}$, где n_i – элемент множества I, моделирующий mesh-станции MR MC WMN, N – их общее количество в mesh-сети. $J = \{z_j, j = \overline{1, Z}\}$, где z_j – элемент множества J, моделирующий зону устойчивого приема, Z – их общее количество в MR MC WMN. Предикат R, являясь инцидентором гиперграфа H, определяет принадлежность i-й станции j-й зоне устойчивого приема. Так в случае, если i-я mesh-станция участвует в формировании j-й зоны устойчивого приема, то предикат $R(n_i, z_j)$ – истинный, т.е. равный единице, в противном случае $R(n_i, z_j)$ – ложный, т.е. равный нулю. В результате этого описание MR MC WMN может быть произведено с использованием конечного гиперграфа $H(I, J; R)$, состоящего из пары множеств вершин $I = \{n_i, i = \overline{1, N}\}$ и ребер $J = \{z_j, j = \overline{1, Z}\}$ вместе с двуместным предикатом $R \Leftrightarrow R(n_i, z_j)$, определенным для всех $n_i \in I$ и $z_j \in J$ [4; 5].

Приобрела новую формализацию задача определения связности. По сравнению с использованием графового представления возможной конфигурации WMN, нет необходимости проводить поиск независимых путей между всеми парами вершин графа. При использовании гиперграфового подхода решения задачи связности сводится к поиску максимального числа станций, удаление которых приведет к разделению WMN на несколько несвязных компонент. Использование гиперграфов также позволяет определить место той или иной станции в составе WMN, в отличие от графового представления, невольно «уравнивающего» основные элементы системы.

Также предложена модель комплексного решения задач распределения неперекрывающихся частотных каналов и потоковой маршрутизации в MR MC WMN стандарта IEEE 802.11 с использованием гиперграфов и графов Кенига. Если в приведенных ранее решениях задача распределения неперекрывающихся частотных каналов была ориентирована на получение связной сбалансированной по пропускной способности структуры mesh-сети, то в рамках предложенной модели решение указанных задач подчинено единой общей цели – повышению межконцевого качества обслуживания по показателям производительности за счет согласованного использования сетевых ресурсов многоканальных многоинтерфейсних mesh-сетей, что особенно проявлялось при увеличении степени перекрытия зон устойчивого приема, числа радиоинтерфейсов на mesh-станциях и количества поддерживаемых частотных каналов в сети. На рис. 1 приведен пример mesh-сети, которая была получена в результате комплексного решения задач распределения неперекрывающихся частотных каналов и потоковой маршрутизации, а на рис. 2 и рис. 3 ее представление в виде гиперграфа и графа Кенига.

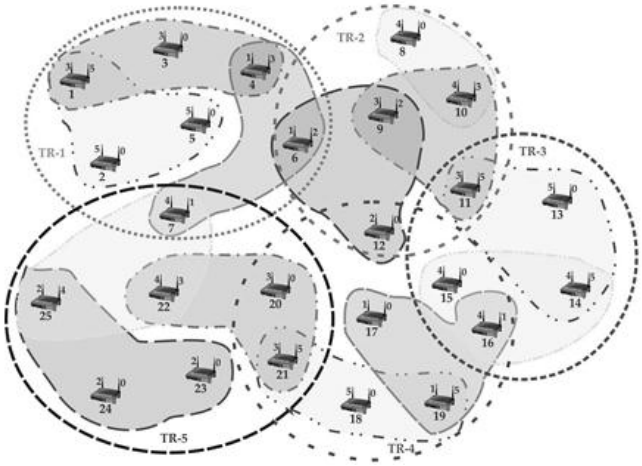


Рисунок 1. Пример MR MC WMN, полученой в результате согласованного решения задач распределения неперекрывающихся частотных каналов и потоковой маршратизации

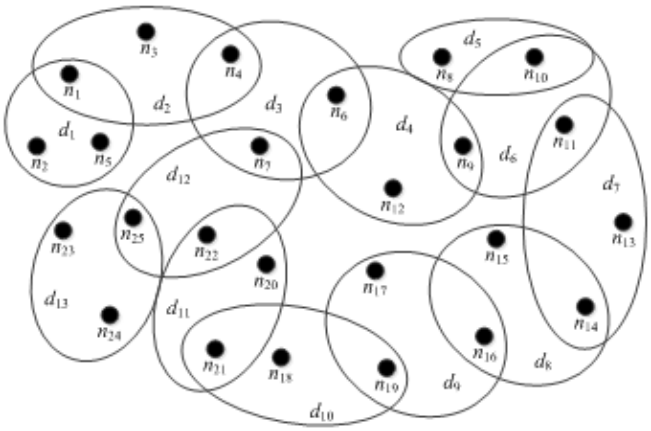


Рисунок 2. Гиперграфовое представление MR MC WMN, приведенной на рис. 1

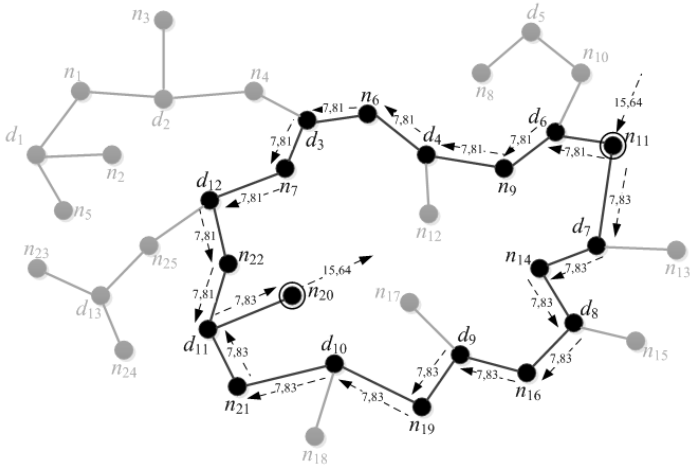


Рисунок 3. Кениговое представление MR MC WMN, приведенной на рис. 1

В результате сравнительного анализа установлено, что в случае использования MR MC WMN с уровнем связности равным единице (1-связная mesh-сеть) выигрыш при использовании согласованного решения задач распределения неперекрывающихся ЧК и потоковой маршрутизации отсутствует. В случае использования 3-связной MR MC WMN выигрыш составил 75-100%, а для 7-связной mesh-сети – 80-100% (табл. 1).

Таблица 1. Результаты сравнительного анализа согласованного и последовательного решения задач распределения неперекрывающихся ЧК и потоковой маршрутизации

Пример конфигурации MR MC WMN	Связность гиперграфа (MR MC WMN)	Количество используемых неперекрывающихся ЧК	Выигрыш по производительности, %
№1	1-связный	3	0
		4	0
		5	0
№2	3-связный	3	85-100
		4	80-100
		5	75-100
№3	7-связный	3	85-100
		4	83-100
		5	80-100

Также в результате сравнительного анализа установлено, что повышению производительности MR MC WMN способствует увеличение количества радиоинтерфейсов на станциях mesh-сети. Это вызвано тем, что mesh-станция источник может производить передачу данных одновременно по нескольким доменам коллизий, количество которых соответствует количеству радиоинтерфейсов на ней.

Проанализированы характеристики возможных конфигураций mesh-сетей, а также характеристики их структур, на основе чего определены условия, влияющие на производительность MR MC WMN при согласованном решении задач распределения неперекрывающихся частотных каналов и потоковой маршрутизации: уменьшение размера зоны устойчивого приема приводит к увеличению количества формирующихся доменов коллизий, а также уменьшению числа станций, входящих в состав каждого из них, что способствует повышению общей производительности mesh-сети; использование однородной MR MC WMN позволяет сформировать сбалансированные друг относительно друга домены коллизий; уменьшение степени перекрытия зон устойчивого приема, а также увеличение количества неперекрывающихся частотных каналов приводит к формированию большего количества доменов коллизий, способствует уменьшению их размеров, а также повышению производительности mesh-сети в целом; увеличение числа радиоинтерфейсов на mesh-станциях способствует формированию большего количества независимых маршрутов.

Литература:

1. Гаркуша С.В. Разработка и анализ двухиндексной модели распределения частотных каналов в многоканальной mesh-сети стандарта IEEE 802.11 [Електронный ресурс] // Проблемы телекоммуникаций, 2011, № 3 (5), С. 38-57. – Режим доступа к журн.: http://pt.journal.kh.ua/2011/3/1/113_garkusha_mesh.pdf .

2. Лемешко А.В., Гаркуша С.В. Классификация методов распределения частотных каналов в многоинтерфейсных многоканальных mesh-сетях стандарта IEEE 802.11 [Электронный ресурс] // Проблеми телекомунікацій. – 2011. – № 2 (4). – С. 139–149. – Режим доступа к журн.: http://pt.journal.kh.ua/2011/2/1/112_lemeshko_classification.pdf.

3. Гаркуша С.В. Разработка потоковой модели маршрутизации в многоканальных многоинтерфейсных mesh-сетях стандарта IEEE 802.11, представленных в виде графа Кенига [Електронний ресурс] / С.В. Гаркуша // Проблеми телекомунікацій. – 2014. – № 1 (13). – С. 20-34. – Режим доступу до журн.:http://pt.journal.kh.ua/2014/1/1/141_garkusha_routing.pdf .

4. Berge C. Graphs and Hypergraphs. – New York: Elsevier, 1973. – 528 p.

5. Berge C. Hypergraphs: The Theory of Finite Sets. – Amsterdam, Netherlands: North-Holland, 1989. – 256 p.

Д.Э. Гладков, В.А. Дунаев

НАСТРОЙКА ПОДКЛЮЧЕНИЙ К УДАЛЕННЫМ РАБОЧИМ СТОЛАМ С МАНДАТНЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

Академия ФСО России, г. Орёл, Россия

Ключевые слова: мандатное разграничение доступа, удаленные рабочие столы, защищенное взаимодействие, облачный сервис, методика.

Описана проблема защищенного взаимодействия с удаленными пользователями на основе операционной системы AstraLinuxSE и возможность организации такого сервиса. Приведены преимущества облачных вычислений, их роль и необходимость в повседневной жизни. Дана краткая методика по настройке облачного сервиса с использованием открытых архитектур, таких как Kernel-BasedVirtualMachine и OpenStack.

D.E. Gladkov, V.A. Dunaev

CONFIGURINGTHE CONNECTIONTOTHE REMOTE DESKTOP ACCESSDIFFERENTIATIONCREDENTIALS

Academy FSO Russia, Orel, Russia

Keywords: access control credential, remote desktops, secure communication, cloud service, technique.

Described the problem of secure interaction with remote users on the basis of the operating system Astra Linux SE and the possibility of organizing such a service. The advantages of cloud computing, their role and the need for daily life. A brief procedure for setting up a cloud service using open architectures such as Kernel-Based Virtual Machine and OpenStack.

В наше время телекоммуникационная индустрия развивается очень высокими темпами. Все больше компаний переходят на облачные вычисления, которые объединяют в себе как файловые хранилища, текстовые, графические редакторы, так и личное пространство пользователей для полноценной работы. Данные технологии позволяют объединить множество программных и аппаратных реализаций в единое целое, это повышает удобство пользования всеми средствами, обеспечивает доступность к необходимым данным тогда, когда это необходимо, а также уменьшает финансовые затраты, но вопросы разграничения доступа в таких системах, как правило, остаются не решенными. С другой стороны, операционная система AstraLinuxSE используется в организациях, где требуется разграничение доступа к данным. Это делает необходимым создание защищенного облачного сервиса с мандатным разграничением доступа [1, 2].

Данные технологии актуальны тем, что облачные вычисления сокращают финансовые затраты как для конечных пользователей, так и для организаций, обеспечивают повсеместную доступность из любой точки при наличии подключения к интернету. Мандатное разграничение доступа к удаленным рабочим столам позволяет пользователям получать доступ только к той информации, которая предназначена только для них.

В настоящее время в публичном доступе нет методики, которая раскрывает правила настройки облачного сервиса для защищенной операционной системы AstraLinuxSE с последующей настройкой мандатного разграничения доступа. Все имеющиеся подходы содержат в себе только отдельные выдержки по установке и настройке гипервизоров и открытой структуры OpenStack, необходимой для развертывания облака [3, 4].

Предлагаемая авторами методика, совмещающая в себе установку и настройку гипервизора, развертывание облака и конфигурирование мандатного разграничения доступа, позволяет создавать защищенное взаимодействие удаленных пользователей с рабочим столом, при котором участники взаимодействия получают доступ к ресурсам в соответствие с их полномочиями.

В настоящей методике делается попытка интеграции облачных вычислений и защищенной операционной системыAstraLinuxSE.

На рисунке 1 представлена обобщенная структура организации защищенного удаленного доступа к рабочим столам. Методика для реализации этой структуры в общем виде должна содержать следующие шаги [5, 6]:

1. Установка гипервизора KVM (в новых версиях является частью ОС Linux).
2. Установка интерфейса виртуализации (библиотека libvirt) для более простого управления виртуальными машинами.
3. Для организации работы виртуальных машин необходимо установить OpenStack, а именно, самый главный компонент - Nova, отвечающий за распределение ресурсов виртуальной машины, работоспособность, соединение с внешним миром, управление гипервизором и доступом к нему.

Полученные результаты позволят организовать защищенное удаленное взаимодействие пользователей с рабочими столами AstraLinuxSE, разграничить доступ этих пользователей к виртуальным машинам и данным.

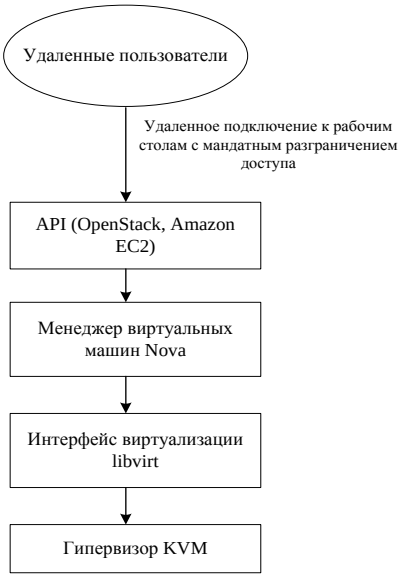


Рисунок 1. Структура организации удаленного доступа к рабочим столам

Литература:

1. Немет Э. Unix и Linux. Руководство системного администратора. /Э.Немет, Г. Снайдер, Т. Хейн, Б. Уэйли. – Вильямс, 2013. – 1312 с.

2. Облачные вычисления: Инфраструктура как сервис (Infrastructureas a Service, IaaS) [Электронный ресурс] – Режим доступа: http://ibm.com – Заглавие с экрана. – (Дата обращения: 20.02.2015)

3. Облачные вычисления: Основы [Электронный ресурс] – Режим доступа: http://ibm.com – Заглавие с экрана. – (Дата обращения: 20.02.2015)

4. Гипервизоры, виртуализация и облако: О гипервизорах, виртуализации систем и о том, как это работает в облачной среде [Электронный ресурс] – Режим доступа: http://ibm.com – Заглавие с экрана. – (Дата обращения: 20.02.2015)

5. Знакомство с OpenStack : архитектура, функции, взаимодействия [Электронный ресурс] – Режим доступа: http://ibm.com – Заглавие с экрана. – (Дата обращения: 20.02.2015)

6. Защищенная облачная платформа [Электронный ресурс] – Режим доступа: http://astra-linux.com – Заглавие с экрана. – (Дата обращения: 20.02.2015)

Е.В. Глушак

ИССЛЕДОВАНИЕ И ОЦЕНКА СХОДИМОСТИ ТЕОРЕТИКО-ИГРОВОГО АЛГОРИТМА ИНТЕЛЛЕКТУАЛЬНОГО ПЕРЕНАПРАВЛЕНИЯ ЗАЯВОК В РАСПРЕДЕЛЕННЫХ ЦЕНТРАХ ОБСЛУЖИВАНИЯ ВЫЗОВОВ

Поволжский Государственный Университет Телекоммуникаций и Информатики (ПГУТИ), г. Самара, Россия

Ключевые слова: распределенные центры обслуживания вызовов, алгоритм интеллектуальной маршрутизации, сходимость, теоретико-игровые модели, равновесие по Нэшу, информированность.

Предложен алгоритм интеллектуального перенаправления вызовов. Рассмотрены варианты информированности. Представлены условия и результаты проведения имитационного моделирования в программной среде Matlab/Simulink. Произведена оценка сходимости полученных результатов с теоретическими значениями. Доказанная безусловная устойчивая сходимость разработанного теоретико-игрового алгоритма интеллектуальной маршрутизации вызовов в распределенном центре обслуживания вызовов позволяет рекомендовать использовать его на практике для повышения качества обслуживания вызовов.

E.V. Glushak

STUDY AND EVALUATION OF THE CONVERGENCE OF GAME-THEORETIC ALGORITHM FOR INTELLIGENT FORWARDING OF APPLICATIONS IN DISTRIBUTED CALL CENTERS

Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia

Keywords: distributed call centers, the algorithm intelligent routing, convergence, game-theoretic model, Nash equilibrium, the awareness.

The algorithm intelligent redirection of calls. The variants of awareness. Presents the conditions and results of the simulation software Matlab/Simulink. The assessment of the convergence of the obtained results with the theoretical values. Proven unconditionally stable convergence of the developed game-theoretic algorithm for an intelligent call routing in a distributed call center can be recommended to use it in practice to improve the quality of the service calls.

Под распределённым центром обслуживания вызовов (РЦОВ) понимается совокупность территориально разнесенных и информационно связанных между собой региональных ЦОВ, предоставляющих услуги клиентам с помощью операторов или автоматически и использующих единые правила обработки и маршрутизации вызовов [1].

При имитационном моделировании РЦОВ можно представить как открытую сеть массового обслуживания. Элементами этой сети являются многоканальные системы массового обслуживания (СМО), которые моделируют отдельные центры обслуживания вызовов (ЦОВ). На вход каждой такой СМО поступает не только собственные вызовы, но и вызовы от других центров. Поступив в систему, вызовы могут сразу же попасть на обслуживание к операторам центра или ожидать в очереди, если все операторы заняты. Для обслуживания поступающих в РЦОВ вызовов необходимо обеспечить минимально возможное время обслуживания, для чего требуется определенное количество операторов в центрах и оптимальное распределение поступающей нагрузки по различным центрам. Для этого разработана теоретико-игровая модель РЦОВ и алгоритм интеллектуальной перемаршрутизации, реализованные в программной среде MATLAB [2].

Процесс перераспределения входящих вызовов для минимизации времени ожидания в очереди и равномерного распределения поступающей нагрузки в РЦОВ между локальными центрами называется «интеллектуальным» управлением вызовами [3].

На рисунке 1 представлен алгоритм принятия решений в *i*-ом ЦОВ, основанный теоретико-игровых моделях, предложенных в [2], где действия каждого ЦОВ из состава РЦОВ интерпретируются как работа в команде.

На каждом шаге работы локальные центры в составе распределенного принимают решения, используя информацию о занятости друг друга, полученную на предыдущем шаге, а также субъективные значения параметров принятия решения предыдущего периода времени. Не берется в расчет лишь тот случай, когда принятие решений по перенаправлению вызовов реализовывается на основании всей предыстории поступления и обслуживания вызовов.

Обозначим используемые параметры алгоритма:

$x_i\left(r_{ijn}\right)$ - действия отдельных центров при знании $\mathbf{r}$;

$W_i^t\left(x_i^t\right)$ - текущее состояние загруженности *i*-го ЦОВ с периодом сбора информации о загрузке операторов ЦОВ *t* ;

I_i^t - знание (информированность) *i*-го ЦОВ о состоянии загрузки других центров в РЦОВ за тот же период *t*, *t = 0, 1, 2, …* , $i \in N$;

I_i^{t+1} - информированность *i*-го ЦОВ о состоянии других центров в следующий период времени t+1;

I_i^{t-1} - информированность *i*-го ЦОВ о состоянии других центров в предыдущий период времени t–1;

γ_i^t – некоторый коэффициент в границах [0;1], интерпретируемый как "величина шага" к минимальным затратам на обработку вызова;

ρ - общая загруженность операторов каждого центра;

θ_i, $\theta_i \in \Omega$ - представление *i*-го ЦОВ об общей загруженности всех ЦОВ;

θ_{ij}, $\theta_{ij} \in \Omega, j \in N$ - представления *i*-го ЦОВ о представлениях других о параметре ρ ;

θ_{ijk}, $\theta_{ijk} \in \Omega, j,k \in N$ - представления *i*-го ЦОВ о представлении *j*-го ЦОВ о представлении *k*-го ЦОВ, и т.д.;

$\theta_{ij_1 \ldots j_l}$, где $j_1,\ldots,j_l \in N$, а $\theta_{ij_1 \ldots j_l} \in \Omega$ - структура информированности I_i *i*-го ЦОВ;

Ω – множество возможных значений коэффициента загруженности каждого ЦОВ;

I – множество значений информированности для всех ЦОВ.

Наряду с информированностью $I_i, i \in N$ можно рассматривать информированность I_{ij} (информированность *j*-го ЦОВ в представлении *i*-го ЦОВ), I_{ijk} и т.д. При поступлении вызова в ЦОВ запускаются счетчики числа входящих вызовов *M* и времени пребывания вызова в системе *T*. Также используется счетчик длины очереди *q*, который в начале моделирования равен 0, параметры τ – длительность обслуживания и l – счетчик, отмечающий число нетерпеливых клиентов.

Могут быть следующие варианты информированности:

1. Полная информированность - каждому ЦОВ известны все параметры о других ЦОВ в предыдущий I_i^{t-1} и последующий I_i^{t+1} периоды времени, включая выбранные действия каждого ЦОВ о перенаправлении вызовов.
2. Отсутствие информированности - у каждого ЦОВ нет никаких знаний о состоянии других центров. Из-за неточности или отсутствии данных о состоянии других ЦОВ каждый центр анализирует только собственные параметры *q* и $t_{ож}$. И при условии $q >> q_{ср.}$ и $t >> t_{ср.}$ ЦОВ перенаправляет вызов в другой центр, не зная состояние его загруженности и его действия по перенаправлению вызовов.
3. Информированность неполная - у ЦОВ есть информация лишь о некоторых параметрах других центров.

Изменяя во входных параметрах имитационной модели данные об информированности, исследовалось перераспределение нагрузки между всеми ЦОВ на разных этапах и при различных известных параметрах загрузки центров.

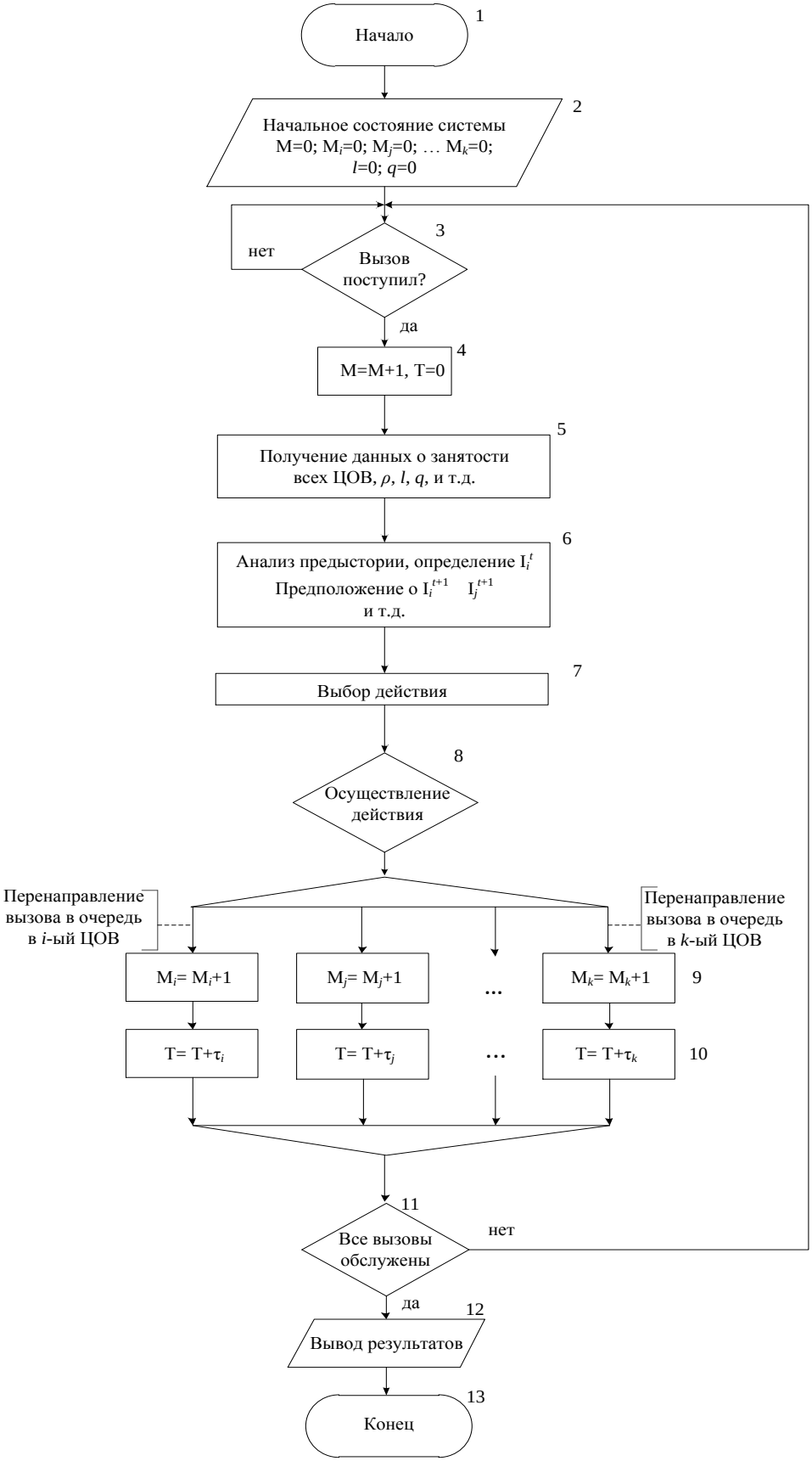


Рисунок 1. Алгоритм реализации принятия решений в *i*-ом ЦОВ из состава РЦОВ

Эксперимент проводился с пятью локальными центрами, входящими в состав распределенного. Процесс моделирования разбивался на m=20 серий по $N=10^4$ испытаний в каждой, исследование проводилось с разной интенсивностью входящей нагрузки и фиксированными интенсивностью обслуживания вызовов μ=1 1/с и максимальным временем ожидания вызовов в очереди w =180 с.

Результаты имитационного моделирования позволили убедиться в сходимости средних результатов к теоретическим значениям выигрышей, основываясь на работе [3]. Сначала были найдены оптимальные по Нэшу решения в смешанных стратегиях [2], далее оценивалось средние возможные результаты игры при случайном перемешивании стратегий с найденными оптимальными по Нэшу пропорциями (среднее время обслуживания вызовов в каждом ЦОВ при фиксированной загрузке и при определенной информированности) [3]:

$$\overline{f_1} = \overline{f_2} = \overline{f_3} = \overline{f_4} = \overline{f_5} = \overline{f_{общ.}} = 50{,}023. \quad (1)$$

Рисунок 2 подтверждает сходимость средних результатов игры всех центров к теоретическим значениям. Как видно из приведенных данных, безусловная устойчивая сходимость наблюдается после числа повторений игры n свыше 450, хотя при рассматриваемой статистической имитации хорошее совпадение с теоретическими расчётами наблюдалось также при n=70 и n=270, что можно считать случайным совпадением.

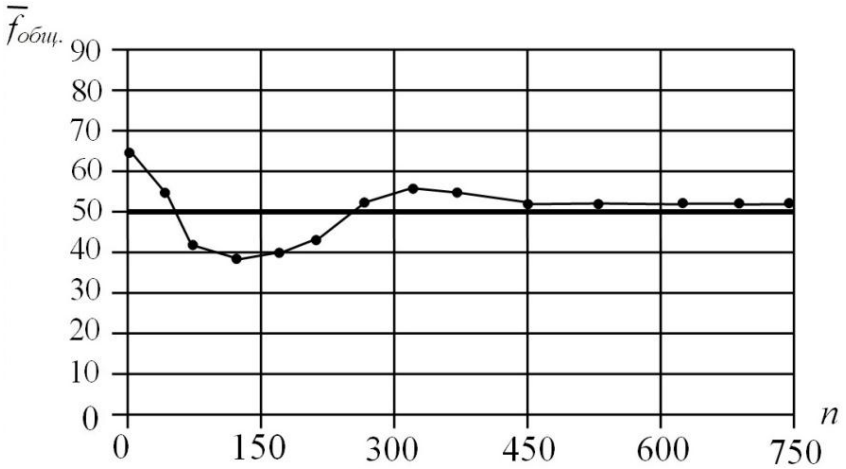


Рисунок 2. Сходимость средних выигрышей всего РЦОВ

Таким образом, доказанная безусловная устойчивая сходимость разработанного теоретико-игрового алгоритма интеллектуальной маршрутизации вызовов в РЦОВ позволяет рекомендовать использовать его на практике для повышения качества обслуживания вызовов.

Литература:

1. Глушак, Е.В. Анализ гомогенной модели распределенного центра обслуживания вызовов / Е.В. Глушак, А.В. Росляков // Инфокоммуникационные технологии. – 2013. – Т.12, №3. – С. 23 – 26.

2. Глушак, Е.В. Оценка эффективности применения алгоритма интеллектуального управления входящими вызовами при различных вариантах информированности о состоянии центров обслуживания вызовов / Е.В. Глушак // Инфокоммуникационные технологии. – 2014. – Т.12, №2. – С. 25 – 31.

3. Глушак, Е.В. Экспериментальное исследование модели РЦОВ на основе имитационного моделирования / Е.В. Глушак, А.В. Росляков // T-Comm. Телекоммуникации и транспорт. - 2014. - №11. – С. 42 – 46.

В.А. Головской, А.А. Мозоль

ПОРЯДОК РАСЧЕТА ОСЛАБЛЕНИЯ РАДИОПОМЕХ ЗА СЧЕТ ЧАСТОТНОЙ РАССТРОЙКИ

Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия

Ключевые слова: электромагнитная совместимость, радиопомеха, эмиттер радиопомехи.

В докладе представлен краткий анализ нормативных документов, регламентирующих порядок расчета ослабления непреднамеренных радиопомех, воздействующих на радиоэлектронное средство, за счет частотной расстройки. Выявлены неточности в одном из документов при учете различных типов радиопомех. Предложен способ интерполяции характеристик частотной избирательности и спектров излучения радиоэлектронных средств, направленный на повышение точности решения задачи обеспечения объектовой электромагнитной совместимости. Приведены результаты численного моделирования.

V.A. Golovskoy, A.A. Mozol`

THE PROCEDURE OF CALCULATING RADIO DISTURBANCE ATTENUATION DUE TO FREQUENCY DETUNING

The Federal government institution scientific and production association special equipment and telecoms of the Ministry of the Internal Affairs of the Russian Federation, Rostov-on-Don, Russia

Keywords: electromagnetic compatibility, radio disturbance, emitter of radio disturbance.

The report provides a brief analysis of the regulations governing the procedure for calculating the attenuation of unintentional radio interference affecting radio-electronic facility, at the expense of the frequency detuning. Revealed inaccuracies in one of the documents, taking into account the different types of interference. Provides a method of interpolation frequency selectivity characteristics and emission spectra of radio-electronic means, to improve the accuracy of solving the problem of on-site to ensure electromagnetic compatibility. The results of numerical simulation.

При решении задач объектовой электромагнитной совместимости (ЭМС) радиоэлектронных средств (РЭС) важное значение имеет учет воздействия непреднамеренных радиопомех (НРП), генерируемых эмиттером радиопомех (ЭРП), на защищаемое (ЗРЭС). Потенциальная опасность воздействия НРП определяется их частотными и энергетическими характеристиками [1, С.19]. Основными нормативными документами, определяющими порядок расчета частотно-зависимого подавления, являются Рекомендация МСЭ-R SM.337-6 «Частотный и территориальный разнос» [2] и ГОСТ В 25838-83 «Совместимость радиоэлектронных средств электромагнитная. Методы комплексной оценки электромагнитной совместимости радиоэлектронных средств, размещаемых на объектах и в локальных группировках» [3].

Для определения уровня НРП на входе радиоприемника (РПМ) ЗРЭС рекомендуется [2, С.3] использовать величину $FDR(\Delta f)$, дБ, представляющую собой сумму двух членов: подавление на частоте настройки OTR, дБ, и подавление вне частоты настройки $OFR(\Delta f)$, дБ, которое является дополнительным подавлением из-за частотной расстройки Δf между НРП и ЗРЭС

$$FDR(\Delta f) = OTR + OFR(\Delta f), \quad (1)$$

$$OTR = 10 \lg \frac{\int_0^\infty P(f)\,\mathrm{d}f}{\int_0^\infty P(f)\,|H(f)|^2\,\mathrm{d}f}, \qquad OFR(\Delta f) = 10 \lg \frac{\int_0^\infty P(f)\,|H(f)|^2\,\mathrm{d}f}{\int_0^\infty P(f)\,|H(f+\Delta f)|^2\,\mathrm{d}f},$$

где $P(f)$ – эквивалентная спектральная плотность мощности НРП на промежуточной частоте, дБ/Гц; $H(f)$ – избирательность РПМ, дБ; $\Delta f = |f_j - f_i|$, f_j – частота настройки ЭРП, Гц; f_i – частота настройки РПМ, Гц. Функцию OTR предлагается аппроксимировать следующим образом [2, С.3]:

$$OTR \approx K \lg\left(\frac{\Delta f_j}{\Delta f_i}\right), \quad \text{при } \Delta f_i \le \Delta f_j, \tag{2}$$

где $K = 20$ как для некогерентных, так и для импульсных НРП; Δf_j – полоса частот ЭРП на уровне минус 3 дБ, Гц; Δf_i – полоса пропускания РПМ на уровне минус 3 дБ, Гц.

Однако определение величины $FDR(\Delta f)$ согласно (1) на практике может быть затруднительно, поскольку, во-первых, значение спектральной плотности мощности НРП не всегда указывается в форме №1, во-вторых, спектральная плотность мощности зависит от таких факторов, как используемый метод модуляции и ширина полосы информационного сигнала для аналоговых систем и скорость передачи данных – в случае цифровых систем [2, С.4]. А скорость передачи данных в современных системах может изменяться в зависимости от отношения «сигнал/шум» в канале за счет изменения типа манипуляции, что не позволяет воспользоваться табулированными значениями для типичных систем.

Согласно [3, С.46] коэффициент ослабления воздействия НРП на ЗРЭС за счет частотного разноса Δf определяется как

$$K(\Delta f) = 10^{\frac{F(\Delta f)}{10}}, \tag{3}$$

где $F(\Delta f)$ – функция ослабления мощности НРП за счет частотного разноса, дБ, определяемая при $\Delta f \ge \frac{\Delta f_j(p) + \Delta f_i}{2}$ как

$$F(\Delta f_p) = \begin{cases} X_i(\Delta f_p), & \text{если } \Delta f_i \square\ \Delta f_j(p), \\ \tilde{K} \lg \frac{\Delta f_i}{\Delta f_j(p)} + X_j(\Delta f), & \text{если } \Delta f_i \le \Delta f_j(p), \end{cases} \tag{4}$$

где $X_i(\Delta f)$ – относительное ослабление НРП при частотной расстройке Δf, обусловленное характеристикой частотной избирательности (ХЧИ) РПМ, дБ; $\tilde{K}$ – коэффициент, определяемый типом НРП, $\tilde{K} = 10$ для шумоподобной НРП и $\tilde{K} = 20$ для импульсной НРП; Δf_i – ширина полосы пропускания i-го РПМ на уровне минус 3 дБ, Гц; $\Delta f_j(p)$ – полоса частот радиоизлучения j-го ЭРП на уровне минус 3 дБ на частоте НРП $\Delta f_{jП}$, Гц; $X_j(\Delta f)$ – относительное изменение мощности излучения на частоте $\Delta f_{jП} + \Delta f$ по сравнению с частотой и $\Delta f_{jП}$, дБ; $f_{jП} = p f_j$ – частота НРП, Гц; p – порядковый номер гармоники несущей частоты ЭРП.

При $\Delta f < \frac{\Delta f_j(p) + \Delta f_i}{2}$ функция ослабления мощности НРП определяется как

$$F(\Delta f) = \tilde{K} \lg \frac{\Delta f_c}{\Delta f_j(p)}, \quad (5)$$

где $\Delta f_c = \left| \Delta f_p - \frac{\Delta f_j(p) + \Delta f_i}{2} \right|$ – ширина полосы совпадения.

Ширина полосы частот радиоизлучения j-го РПДУ $\Delta f_j(p) = \Delta f_i$ при $p = 1$, а при $p > 1$ ее определяют экспериментально [3, С.47; 4, С.158].

Функция $X_i(\Delta f)$ определяется по ХЧИ или, при отсутствии данных о таких характеристиках, вычисляется следующим образом [4, С.158]:

$$X_i(\Delta f) = \frac{X_i + 3}{K_{iПР} - 1}\left(\frac{2\Delta f}{\Delta f_i} - 1\right) - 3, \quad (6)$$

где X_i – уровень, относительно которого определялась полоса пропускания i-го РПМ при расчете его коэффициента прямоугольности $K_{iПР}$, дБ.

Значения X_i и $K_{iПР}$ определяются по ГОСТ В 24911-81 «Радиоприемники. Требования по частотной избирательности» [3, С.47] или согласно таблице [4, С.158].

Таблица 1.

	Узкополосная система связи	Широкополосная система связи	Остальные РЭС
X_i, дБ	60	60	30
$K_{iПР}$	1,5–2,5	2,5–3,5	2,0

Функция $X_j(\Delta f)$ зависит от класса излучения ЭРП, и определяется экспериментально. При отсутствии экспериментальных данных рекомендуется [4, С.157] определять значения $X_j(\Delta f)$ из аппроксимации спектра излучения ломаной линией. Кроме ломаной линии в качестве аппроксимирующей функции нелинейных элементов трактов используют тригонометрические функции, степенные ряды [5, С.24] и др.

Совместный анализ [2] и [3] показал:

- рекомендация [2] в основных моментах опирается на [3];
- русскоязычная версия [2] содержит ошибки и неточности;
- в [3] корректнее учитывается тип помехи (шумоподобная или импульсная).

Так как аппроксимация спектра излучения и ХЧИ ломаной линией снижает точность расчета $K(\Delta f)$, то для построения зависимостей $X_j(\Delta f)$ и $X_i(\Delta f)$ предлагается применять процедуры интерполяции для значений рабочих частот и ширины полосы излучения ЭРП и полосы пропускания (усилителя промежуточной или радиочастоты) РПМ на уровнях минус 3 дБ, минус 30 дБ и X дБ относительно нулевого уровня. Указанные данные берутся из формы №1 ГКРЧ.

Для интерполяции на неравномерной сетке, каковой является ось частот f, предлагается использовать частный случай интерполяционного многочлена Эрмита [6, С.136] – кубический интерполяционный многочлен Эрмита [7, С.78; 8, С.356]

$$H(x) = c_1 + c_2(f - f_i) + c_3(f - f_i)^2 + c_4(f - f_i)^3, \quad (7)$$

где $c_1 = h_i, c_2 = \dot{h}_i, c_3 = \left(3\Delta_i - \dot{h}_{i+1} - 2\dot{h}_i\right)(\Delta f_i)^{-1}, c_4 = \left(\dot{h}_{i+1} + \dot{h}_i - 2\Delta_i\right)(\Delta f_i)^{-2}$, h_i – значения функции $h(f)$ в узлах интерполирования, $\dot{h}_i = h'(f_k)$, а величины $\Delta f_i, \Delta h_i, \Delta_i$ определяются системой $\Delta f_i = f_{i+1} - f_i, \Delta h_i = h_{i+1} - h_i, \Delta_i = \Delta h_i (\Delta f_i)^{-1}$.

Рисунок иллюстрирует результат интерполяции спектра излучения ломаной линией и кубическим интерполяционным многочленом Эрмита, обозначенные в области легенды рисунка ЛИ и КЭИ соответственно.

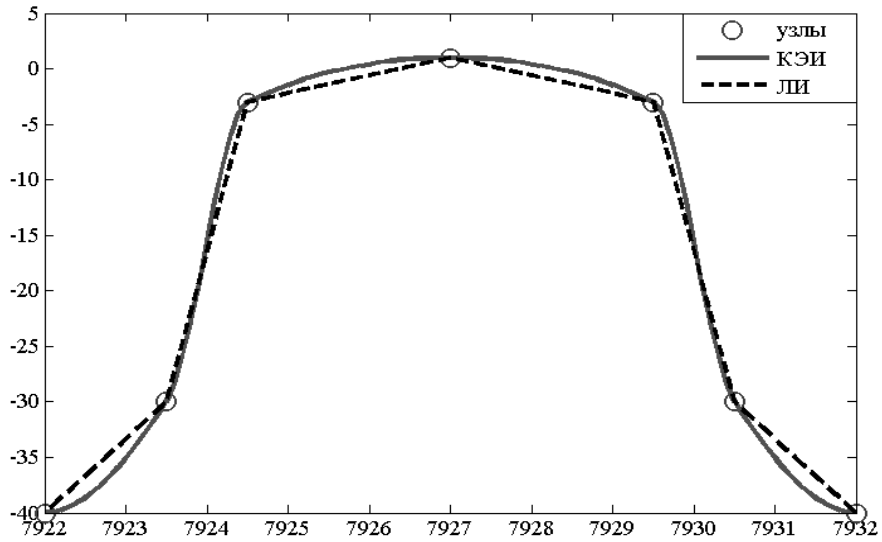


Рисунок 1. Результаты интерполяции

Интерполяция кубическим многочленом Эрмита дает выигрыш несмотря на кажущуюся незначительность отличий. Во-первых, ХЧИ и спектры излучений не имеют точек разрыва первого рода, и интерполяция кубическим многочленом Эрмита обеспечивает адекватное описание ХЧИ и спектров излучений. Во-вторых, вследствие адекватного описания ХЧИ и спектра излучения более точно будут проводиться процедуры учета влияния НРП. В-третьих, кубическая Эрмитова интерполяция позволяет предъявлять требования к производным интерполянта, что может быть полезно при построении характеристик различных широкополосных систем.

Результаты анализа позволяют сделать следующие выводы:

- для расчета частотно-зависимого подавления целесообразно использовать математический аппарат (3)–(6), базирующийся на требованиях [3];
- для интерполяции ХЧИ каскадов ЗРЭС и спектра излучения ЭРП целесообразно использовать интерполяцию кубическим многочленом Эрмита.

Литература:

1. Лемешко Н.В. Методология моделирования сертификационных испытаний радиоэлектронных средств по эмиссии излучаемых радиопомех [Текст]: дис. … докт. техн. наук : 05.12.04 / Николай Васильевич Лемешко. – Москва, 2014. – 486 с.

2. Recommendation ITU-R SM.337-6 Frequency and distance separations [Электронный ресурс]. – Режим доступа: http://www.itu.int/rec/r-rec-sm.337-6-200810-i/en.

3. ГОСТ В 25838-83. Совместимость радиоэлектронных средств электромагнитная. Методы комплексной оценки электромагнитной совместимости радиоэлектронных средств, размещаемых на объектах и в локальных группировках. – М. 1983.

4. Теория и методы оценки электромагнитной совместимости радиоэлектронных средств / Под ред. Ю.А. Феоктистова. – М. : Радио и связь, 1988. – 216 с.

5. Бобков А.М. Реальная избирательность радиоприемных трактов в сложной помеховой обстановке. – СПб. 2001. – 216 с.

6. Самарский, А.А., Гулин А.В. Численные методы. – М. : Наука. Гл. ред. физ-мат.лит., 1989. – 432 с.

7. Утешев А.Ю., Тамасян Г.Ш. К задаче полиномиального интерполирования с кратными узлами // Вестник Санкт-Петербургского университета. Серия 10: Прикладная математика. Информатика. Процессы управления. – 2010. – Сер. 10, вып. 3. – С. 76–85.

8. Gasparo M.G., Morandi R. Piecewise cubic monotone interpolation with assigned slopes // Computing, 1991, Volume 46, Issue 4, pp. 355–365.

В.А. Григорьев, А.В. Щаднев

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ РАЗЛИЧНЫХ СРЕДСТВ СВЯЗИ И УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ УСТРОЙСТВАМИ

Ростовский Государственный Экономический Университет, г. Ростов-на-Дону, Россия

Ключевые слова: роботы, коммуникации, «железо», каналы связи, XBee, Wi-Fi

В данной работе решается проблема выбора каналов управления робототехническими устройствами на базе микроконтроллеров были рассмотрены такие способы управления роботами, как: управление при помощи звука, радио, управление с помощью электромагнитных волн различного вида, и другие. Были отдельно выделены и описаны следующие, оказавшиеся потенциально более эффективными, способы: Управление с помощью Wi-Fi, управление с помощью Bluetooth, управление с помощью XBee. Указаны их достоинства и по результатам проведенного анализа даны рекомендации по использованию.

V.A. Grigoriev, A.V. Shchadnev

COMPARATIVE ANALYSIS OF POSSIBILITES OF DIFFERENT MEANS OF COMMUNICATIONS AND CONTROL OF ROBOTIC DEVICES

Rostov State University of Economics, Rostov-on-Don, Russia

Keywords: robots, communications, hardware, data links, XBee, Wi-Fi

This article shows different control channels of robotic devices using microcontrollers. They are: sound control, radio control, control by different kind of electromagnetic waves, etc. Some more effective ways of control were selected and described more thoroughly: Wi-Fi control, Bluetooth control, control with XBEE. Their advantages are elaborated and analysis concluded, after which practical recommendations are given.

В настоящее время вопросы обмена данными между различными устройствами, активно используемыми людьми как для выполнения функциональных обязанностей, так и повышения личной эффективности, становятся всё более актуальными. Проникновения робототехнических устройств, программируемых систем и микроконтроллеров («Интернет вещей» [1]) во все сферы деятельности человека означает, что к каналам связи и управления предъявляется масса требований, зачастую противоречивых, но которые необходимо принять во внимание. При этом лимитирующим фактором выступает самый первый уровень организации информационных коммуникаций – уровень «железа».

Студенческое конструкторское бюро РГЭУ в рамках своей деятельности по созданию робототехнических устройств на базе Arduino приобрело практический опыт использования различных протоколов и средств коммуникаций. По результатам проведенного анализа были сделаны определенные выводы о возможностях организации каналов обмена данными, которые нашли своё отражение в данной работе.

Были выделены основные классы каналов передачи данных:

1. Управление при помощи звука
2. Управление по радио
   - 2.1. Xbee
   - 2.2. Радиомодули
   - 2.3. Bluetooth
   - 2.4. Управление по Wi-Fi
3. Инфракрасное управление
4. Управление с использованием видеоинформации

Давайте рассмотрим их более подробно.

1. Управление звуком:

Существует два основных варианта. Для выполнения первого нужно реализовать:

1. Запись звука в файл .wav

2. Автоматическая отправка файла в сервис Google

3. Вывод распознанного аудио в виде текстовой строки

4. Поиск по строке схожих команд из выборки уже заложенных

5. Выполнение команды

6. Подтверждение выполнения команды.

7. Повтор пункта 1 (цикл).

Существует ещё один вариант: реализовать обработку звукового файла на самом устройстве.

В первом случае, главный недостаток, необходимость постоянного интернет соединения, то есть мы всё равно будем вынуждены ставить дополнительные контроллеры, обеспечивающие его. Во втором, необходимость выделять значительные ресурсы на саму обработку, не говоря уже о том, что придётся создавать собственные программы для этого.

2. Управление по радио

Управление осуществляется путём передачи команд на специальные модули с последующей их обработкой на контроллере в понятный управляемым модулям вид. Таким образом команды достаточно оперативно приводятся в исполнение.

2.1. XBee

XBee — это модуль, дающий вашему устройству возможность использования протокола ZigBee [2]. Это стандарт беспроводной передачи данных, аналогичен Wi-Fi и Bluetooth, но ориентирован на экономию электроэнергии и большую защищённость канала за счет меньшей скорости.

Большая часть материалов в сети о коммуникации между модулями XBee относится к их первому поколению: «Series 1» или просто «S1». Но они всё сильнее вытесняются новой, более совершенной линейкой второго поколения «Series 2» или просто «S2».

При попытке сконфигурировать S2 точно так же, как и S1, ошибка возникает при попытке установить параметр MY. Так например, команда ATMY=1111 вернёт ошибку. В модулях второго поколения этот параметр стал доступным только для чтения.

Работа с XBee организована как пересылка сообщений через последовательное (serial) соединение.

Дальность передачи- 120 м на улице и до 35 м в помещении.

Скорость обмена данными- до 250 кбит/с.

Энергопотребление- 2,8 - 3,4 В, потребляет 45 мА в режиме приёма, 50 мА в режиме передачи и 0,01 мА в режиме энергосбережения.

Цена модуля- 3690 руб.

2.2. Радиомодули

Существует огромный выбор радиомодулей. Разброс как цены, так и характеристик очень значительный, по этому каждый сможет подобрать себе то, что ему нужно для решения конкретной задачи.

Дальность передачи- до 1800 м.

Скорость обмена данными- до 18,75 кбит/с.

Энергопотребление- 3,3 - 5 В, потребляет 30 мА.

Цена модуля- от 290 до 3705 руб.

2.3. Bluetooth

Bluetooth 4.1 – новая версия технологии Bluetooth, выпущенная в конце 2013 года. Стандарт предоставляет скорость передачи данных в 1 Мбит/с. В новой версии максимально возможное расстояние между двумя соединенными между собой объектами возросло до 100 метров, скорость установления соединения составляет около 5 миллисекунд. Также новая версия улучшает совместную работу Bluetooth и LTE. Также важным нововведением является возобновление соединения при возвращении в зону покрытия. Отличительной особенностью является встроенный механизм шифрования AES 128, поддержка режимов пониженного энергопотребления. Цена микрочипа RN4020 составляет 5255 рублей.

2.4. Управление по Wi-Fi

Для управления по Wi-Fi понадобится беспроводный маршрутизатор. К примеру, TP-LINK TL-MR3020, который стоит всего 1500 рублей. Легко настраивается и прошивается. Достоинства

метода – довольно высокая скорость подачи сигналов, однако возможны сильные помехи от рядом расположенной электронной аппаратуры. Управление осуществляется следующим способом:

Посылаем сигнал с компьютера (ноутбука). Роутер отправляет сигнал микроконтроллеру. Микроконтроллер получает сигнал от роутера и управляет самой платой.

3. Инфракрасное управление

Инфракрасное излучение — электромагнитное излучение, занимающее спектральную область между красным концом видимого света и микроволновым радиоизлучением. Инфракрасный канал, в отличие от радиоканала, нечувствительным к электромагнитным помехам. Однако, недостатком ИК канала является низкая скорость передачи сигнала, также не обеспечивается скрытность передачи информации. В условиях прямой видимости ИК канал может обеспечить связь до нескольких километров. Для управления используется приемник инфракрасного (ИК) излучения TSOP стоимостью в 59 рублей.

4. Управление с использованием видеоинформации Управление видео работает следующим образом. После анализа изображения и распознавания образов происходит деление объектов окружающей среды на пассивные и активные.

В случае если робот видит какое либо препятствие – он выполняет запланированное действие. Если это препятствие подходит под объект из его БД, то он опять же выполняет действие, предписанное данной ситуации.

Возможно и активное управление. К примеру, если перед ним махнуть рукой вправо – то он поедет вправо.

Краткий сравнительный анализ различных каналов связи по двум основным параметрам приведен в Таблице 1.

Таблица 1.

Тип связи	Дальность действия	Цена устройства
Wi-Fi	30 метров	1500 рублей
Bluetooth 4.1	100 метров	5255 рублей
Радиосвязь	До 1800 метров	До 3700 рублей
XBEE	35-120 метров	3690 рублей

Как видно из таблицы, характеристики модулей и их цены весьма различны. У этих типов связи есть как преимущества, так и недостатки. Выбирать тип связи уже следует исходя из поставленной задачи.

Например, если нам не критична скорость передачи данных, лучше всего выбрать модули радиосвязи. Большинство из них дёшевы и дают самую лучшую дальность передачи сигнала.

Если ставятся цели не только передавать сигналы управления, но и принимать, к примеру, видеоинформацию от робота, самым лучшим выбором будут Wi-Fi модули или Bluetooth, так как именно они позволяют вести передачу с наивысшей скоростью.

XBEE же следует использовать в случаях, когда требуется относительно защищённый канал передачи информации.

Также можно поставить вопрос о легкости подбора управляющих устройств. Учитывая данный фактор, приведенные выше, а также распространённость и стоимость технологии, в настоящее время своей работе наше конструкторское бюро РГЭУ использует Wi-Fi модули. Это позволяет решать все задачи, стоящие перед используемыми робототехническими устройствами.

Литература:

1. Леонид Черняк. Интернет вещей: новые вызовы и новые технологии // «Открытые системы», № 04, 2013.

2. http://en.wikipedia.org/wiki/XBee

И.Д. Григорьев

ПЕРСПЕКТИВЫ РАЗВИТИЯ КОНЦЕПЦИИ «ИНТЕРНЕТ ВЕЩЕЙ»

Московский Технический Университет Связи и Информатики, г. Москва, Россия

Ключевые слова: интернет вещей, сенсорные сети, сетевые технологии, информационные системы.

Описаны базовые понятия и выделены ключевые свойства концепции «Интернет вещей». Сделана попытка спрогнозировать сферы применения технологии на основе существующих исследований.

I.D. Grigoryev

PROSPECTS FOR THE ELABORATION OF THE INTERNET OF THINGS CONCEPT

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: Internet of Things (IoT), Wireless Sensor Network (WSN), network technologies, information systems.

Describes the basic terms and key features of the Internet of Things concept. An attempt is made to predict the scope of the technology based on existing researches.

Под термином Internet of Things – Интернет вещей (IoT) понимается такая концепция вычислительной сети, при которой частью этой сети являются физические объекты реального мира, способные обмениваться информацией в сети Интернет. IoT стал важным технологическим трендом [1], который предполагает расширение Интернет из сети, соединяющей оконечные пользовательские устройства, до сети, которая в том числе соединяет и физические объекты, позволяя им взаимодействовать друг с другом и с пользователями. Таким образом, вводится термин «Thing», который включает в себя следующие параметры:

1. Некоторое физическое воплощение и характеристики (форма, объем и т. д.);
2. Минимальный набор коммуникационных функций — возможность обнаружения, приёма и ответа на сообщения;
3. Уникальный идентификатор;
4. Объект должен иметь название и как минимум один адрес. Название — это описание объекта в формате, удобном для человека, а адрес — это строка, представляемая в виде, удобном для вычислительных устройств, используемая для связи с объектом;
5. Объект должен обладать вычислительными способностями. Вычислительная мощность объекта может варьироваться в зависимости от назначения устройства;
6. Может иметься возможность регистрировать какие-либо физические явления (температуру, уровень освещения, уровень радиации и т. д.) или физически влиять на окружение.

Последний пункт является определяющим в классификации типов вычислительных сетей. Таким образом, если объекты сети удовлетворяют этим условиям, то сеть называется сенсорной.

Включение таких объектов в глобальную сеть кардинально меняет архитектурные и алгоритмические принципы сети Интернет. Фактически, это означает достижение нового уровня гетерогенности сети из-за присоединения к ней устройств, которые имеют минимальные вычислительные и коммуникационные возможности [2]. Это означает частичную или полную непригодность существующих сетевых протоколов и приложений для нового типа сетей. Также существующая топология сети Интернет может подвергнуться серьезным изменениям в связи с новой вводимой спецификой работы.

С системной точки зрения IoT можно рассматривать как крайне динамическую и широко распределенную систему, состоящую из огромного количества объектов, производящих и обрабатывающих информацию. Возможность взаимодействия с реальным миром достигается путем использования устройств, которые способны предоставлять интерфейс к своему

физическому окружению и преобразовывать получаемую информацию в поток данных и наоборот.

Таким образом можно выделить следующие ключевые свойства IoT:

1. *Гетерогенность используемых устройств*. IoT может быть охарактеризован огромным количеством устройств, подключенных к сети и взаимодействующих друг с другом;
2. *Масштабируемость*, подразумевающая под собой масштабируемость адресного пространства, вычислительных способностей, полосы пропускания;
3. *Широкая поддержка обмена данными с помощью беспроводных технологий* – они играют ключевую роль в IoT;
4. *Энергосберегающие технологии* играют важную роль по той причине, что в качестве узлов сети используются устройства с автономным питанием;
5. *Автономная работа.* Сложность и распределенность топологии сети подразумевает под собой существование множества сценариев работы с ней. В том числе, если какое-то устройство будет отключено от глобальной или локальной сети, оно должно уметь продолжать свою работу и обеспечивать максимально возможный функционал в любой ситуации;
6. *Возможность обработки разных типов информации.* Любая вычислительная сеть занимается обработкой информацией, и концепция IoT подразумевает обработку больших массивов разнородных данных, приведение их к некоторой общей форме, понятной для разрабатываемых приложений;
7. *Средства безопасности и конфеденциальности* сейчас идут рука об руку с любой разрабатываемой технологией. Таким образом, каждый участок сети, принадлежащий одному пользователю, должен быть логически изолирован в передаче конфеденциальных данных от глобальной сети.

Рассмотрим концепцию IoT с точки зрения распределенной сетевой инфраструктуры. Требуется создать распределенную сеть, которая позволяла бы легко реализовывать нужные специфические для какой-либо области сервисы. Проектирование распределенной архитектуры и протоколов – это ключевой вопрос для любых сетей, в том числе и для IoT.

Реализация распределенных протоколов маршрутизации является одним из фундаментальных блоков сетевых систем. Как было описано выше, вопросы масштабируемости, разнородности обрабатываемых данных, гетерогенности и т.д. не позволяют создать готовое цельное решение для IoT в настоящее время. Сейчас проводятся обширные исследования на эту тему [3,4].

Огромные массивы данных об окружающем мире, вливающиеся в Интернет будут требовать больших вычислительных способностей для их обработки. На самом деле, контроль такого количества информации является большой проблемой, к решению которой стремятся вычислительные устройства и их программное обеспечение. Отказоустойчивость будет являться одной из главных областей IoT: требуется контролировать ошибки соединения, ошибки программного обеспечения и аппаратной части, целостность данных, синхронизацию работы устройств.

Важной задачей является возможность адресации устройств с использованием уникальных идентификаторов. Концепция Object Name Service [5] (ONS) призвана расширить существующую систему Domain Name Service (DNS) для использования с объектами реального мира.

С прикладной точки зрения концепция IoT может совершить огромный толчок во всей индустрии инфокоммуникаций. Следует определить те области рынка, где решения IoT могут создать конкурентоспособную альтернативу существующим:

1. *«Умный» дом, «умное» здание.* Реализация IoT для работы внутри здания может помочь сократить постоянные расходы вроде затрат на электричество и увеличить комфорт пребывания людей в таком помещении. Ключевую роль в такой реализации будут играть сенсоры, которые используются для мониторинга окружающей среды и выявления нужд людей. Такой сценарий включает в себя большое количество разных подсистем, эффективно взаимодействующих между собой.
2. *«Умный город»* может использоваться для оптимизации использования реальной городской инфраструктуры – дороги, энергосистема и т. д. IoT технологии могут быть использованы для продвинутых систем контроля дорожного траффика –

система будет способна отслеживать движение автомобилей в больших городах и регулировать его с целью избегания заторов. В данном представлении в качестве «умных» объектов будут выступать автомобили. Данный пример является всего лишь единственным среди многих возможных.

3. *Мониторинг окружающей среды* предполагает использование возможностей сенсоров в качестве ключевого инструмента системы. Таким образом можно будет отслеживать температуру, скорость ветра, влажность воздуха и т. д. и использовать эти данные в большой гетерогенной вычислительной сети разными приложениями.
4. *Здравоохранение.* Пациенты могут носить на себе некоторое количество медицинских сенсоров, которые бы отслеживали таки параметры, как температура тела, кровяное давление, дыхательную активность. Другие сенсоры (акселерометры, гироскопы) могут быть использованы для мониторинга активности пациента. Вся информация будет собираться и отправляться в удаленные медицинские центры, которые будут использовать ее по назначению Также возможен вариант и с персонализированным здравоохранением – данные не отправляются в медицинский центр, а представляются на экране персонального устройства.

На самом деле, сфера применения IoT является крайне широкой, а приложения, используемые поверх существующей архитектуры, позволят увеличить пользу любых решений в разы.

В заключение можно сказать, что концепция IoT может спровоцировать большой скачок в инфокоммуникационной индустрии. Возможность взаимодействия реального и виртуального миров с помощью встроенных систем и вычислительных устройств открыла бы большие возможности для ведения дальнейших исследований и привела бы к большим изменениям в жизни каждого человека.

Литература:

1. The Internet of Things, ITU Internet Reports, 2005. .

2. L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

3. R.C. Shah, S. Roy, S. Jain, W. Brunette, Data mules: modeling a threetier architecture for sparse sensor networks, in: Proceedings of IEEE International Workshop on Sensor Networks Protocols and Applications, 2003, pp. 30–41.

4. F. De Pellegrini, C. Moiso, D. Miorandi, I. Chlamtac, R-P2P: a data centric dtn middleware with interconnected throwboxes.

5. Object Naming Service (ONS) Standard.

В.В. Гуров, В.Г. Орлов

ОБЗОР И СРАВНЕНИЕ ПРОТОКОЛОВ MPTCP И CMT-SCTP

Московский технический университет связи и информатики, г. Москва

Ключевые слова: множественная адресация, многопоточность, многопутевая передача данных, CMT-SCTP, MPTCP.

Были рассмотрены расширения транспортных протоколов, поддерживающие множественную адресацию, многопоточность и одновременную многопутевую передачу данных. Проведен анализ внесенных изменений в механизмы протоколов TCP и SCTP, на которых основаны расширения, а также сравнение принципов работы CMT-SCTP и MPTCP.

V.V. Gurov, V.G. Orlov

REVIEW AND COMPARISON OF PROTOCOLS MPTCP AND CMT-SCTP

Moscow Technical University of Communications and Informatics, Moscow

Keywords: multi-homing, multiple streams, multipath data transmission, SMT-SCTP, MPTCP.

The article discusses extensions of transport protocols that supports multi-homing, multi-threading and concurrent multipath transmission. Aanalysis was performed of the changes in the mechanisms of TCP and SCTP, and comparison principles of operation CMT-SCTP and MPTCP.

Традиционные протоколы транспортного уровня, широко применяемые в IP-сетях сегодня, являются морально устаревшими. Сегодня IP-сети могут быть построены на различных технологиях, при этом устройство в такой сети может иметь более одного адреса. Например, ноутбук может быть подключен к сети Интернет одновременно разными способами: через кабель по Ethernet, беспроводной USB-модем по 3G/4G и через Wi-Fi. При этом, имея выбор из IP-адресов и, как следствие, сетей доступа к сети Интернет, большинство приложений будут использовать только один путь в глобальную сеть и один IP-адрес.

Таким образом, имея множественную адресацию, пользователь не получает от нее тех преимуществ, которые она может предоставить, а именно: утилизацию всех возможных путей передачи данных и резервирование, которое в случае ошибок на основном пути позволяет перенаправить данные по резервному пути, минимизировав возникший простой в передаче данных.

Для того чтобы реализовать преимущества множественной адресации сегодня развиваются 2 протокола-расширения: MPTCP (Multipath TCP) и CMT-SCTP(Concurrent Multipath Transfer SCTP). Оба протокола поддерживают множественную адресацию и многопоточность, однако их реализация отличается, так как эти расширения основаны на разных протоколах.

Протокол TCP появился в середине 1970х годов и был предназначен для установления виртуального соединения и упорядоченной, гарантированной доставки данных в IP-сетях. Для установления TCP-соединения используется механизм трехэтапного согласования, который, несмотря на простоту, подвержен атакам.

TCP представляет поступающие от приложения данные в виде последовательного потока байт. Используя номера байт в последовательности (поле sequence number в заголовке TCP), получатель может упорядочить принятые данные, а также отправить подтверждение (поле acknowledgement number) другой стороне о том, что данные были доставлены.

Для контроля за процессом доставки и скоростью приема-передачи используется механизм скользящего окна. Размером этого окна определяется количество байт, которое может принять другая сторона, что влияет на скорость передачи, а продвижение этого окна относительно потока происходит только тогда, когда принимающая сторона подтвердила прием отправленных сегментов данных. При такой системе не допускается пробелов в последовательности. Если окно позволяет отправить 4 сегмента, а получатель получит только 3 из них, при этом не получит первого, то возникнет ситуация блокировки начала очереди (head of line blocking), так как окно не сможет продвинуться дальше и передача данных будет временно приостановлена ожиданием подтверждения первого сегмента. Другим недостатком является то, что внутри байтового потока TCP протокол прикладного уровня должен разделять свои сообщения. Несмотря на эти недостатки, протокол TCP до сих пор является одним из основных транспортных протоколов в IP-сетях.

Протокол SCTP появился в 2000 году и был результатом работы группы IETF SIGTRAN, которая занималась решением проблемы взаимодействия традиционной телефонии и VoIP. SCTP реализует лучшие возможности существующих транспортных протоколов TCP и UDP. Таким образом, SCTP, как и TCP ориентирован на соединение, обеспечивает упорядоченную доставку данных, имеет механизмы управления потоком, схожие с TCP, использует механизм подтверждений для обеспечения гарантированной доставки данных.

Сходство возможностей с протоколом TCP позволяет применять SCTP для приложений, которым необходимо, чтобы получатель принял все отправленные данные в том порядке, в

котором они были отправлены. SCTP также реализует возможности UDP: может использовать неупорядоченную доставку данных и сохраняет границы сообщений приложений.

Но SCTP не только совмещает в себе лучшее от существующих протоколов, он также поддерживает множественную адресацию и многопоточность. Использование множественной адресации зачастую подразумевает резервирование путей доступа в сеть, а не распределение нагрузки между этими путями, так как в случае различных по характеристикам путей, решение задачи эффективного распределения нагрузки становится отдельной проблемой.

SCTP без расширений реализует только резервирование путей. Таким образом, передача данных между приложениями двух устройств идет по пути, который был выбран основным, при этом на резервных путях постоянно происходит проверка доступности сторон. Благодаря этому, в случае проблем на основном пути, весь трафик будет передаваться по резервному пути.

Для установления соединения или SCTP-ассоциации SCTP использует механизм 4-х этапного согласования с использованием маркера (cookie). Это позволяет избавиться от атак, подобных SYN-flood в TCP, так как выделение ресурсов произойдет только тогда, когда другая сторона корректно ответит на полученный маркер.

Процесс передачи данных в SCTP отличается от передачи данных TCP. Прежде всего, SCTP представляет данные приложения в виде сообщения, а не байтового потока, как в TCP. Данная особенность позволяет приложению распределить свои сообщения на различные потоки, которых может быть до 65536. Сообщения в SCTP называются фрагментами (chunk), различают фрагменты, содержащие управляющую информацию и фрагменты данных, причем фрагменты с управляющей информацией всегда идут перед фрагментами данных. Несколько сообщений могут быть объединены в один фрагмент, а большое сообщение может быть разделено по нескольким фрагментам. Фрагменты данных характеризуются тремя идентификаторами: TSN (Transmission Sequence Number) – номер в последовательности переданных данных, используется для упорядочивания переданных данных и повторной передачи фрагментов, SID (Stream Identifier)-идентификатор потока, к которому относится данное сообщение, SSN (Stream Sequence Number) – номер в последовательности внутри потока.

Пакет SCTP может содержать несколько фрагментов, следовательно, если какой-либо из пакетов будет утерян, то будут простаивать только те потоки, сообщения которых содержались в пакете. Благодаря этому минимизируется время блокировки начала очереди. Кроме того, SCTP может использовать неупорядоченную доставку для потока, что позволяет не использовать SSN и сразу передавать полученные данные приложению. Также SCTP изначально поддерживает механизм выборочных подтверждений, подобный расширению SACK у TCP.

Благодаря ориентированности на сообщения, SCTP довольно просто расширять, добавляя в реализацию новые типы управляющих фрагментов. API сокета SCTP позволяет быстро адаптировать приложения, использующие TCP к использованию SCTP, однако при этом не будет многопоточности SCTP, поддержки состояния полузакрытого соединения TCP и экстренной доставки данных, хотя подобная проблема может быть частично решена использованием отдельного потока для срочных сообщений.

Реализуя поддержку множественных путей передачи данных, нужно учитывать, что протокол должен будет поддерживать многопоточность, способен работать не хуже однопоточных решений и адаптироваться к изменению условий на путях передачи данных. Кроме того, должен быть механизм аутентификации сторон и механизм автоматического добавления и удаления путей передачи данных.

В случае с MPTCP к реализации многопоточности также накладываются требования к работе в современной сети Интернет и возможности возврата к TCP, если другая сторона не поддерживает MPTCP. Структурно MPTCP представляет собой мета-сокет, который управляет подсокетами TCP или подпотоками TCP. Каждый такой подпоток является обыкновенным TCP-соединением, а передача управляющей информации заложена в поле параметры (options) заголовка TCP.

При установлении соединения к трехэтапному согласованию TCP добавляется параметр MP_CAPABLE [1], благодаря которому стороны могут определить поддерживается ли MPTCP. Также в этом параметре стороны обмениваются ключами, которые будут использоваться для установления нового подпотока по другому пути. Добавление нового подпотока может производиться двумя путями: установлением TCP соединения и уведомлением о наличии дополнительных адресов, чтобы другая сторона установила соединение по новому адресу.

Фактически добавление подпотока означает установление нового TCP-соединения, но с 4-х этапным согласованием и обменом аутентификационными сообщениями, основанными на хеш-кодах ключей сторон.

CMT-SCTP не изменяет процесс четырехэтапного согласования SCTP, во время которого сторонами перечисляются поддерживаемые параметры и расширения. Для динамической конфигурации адресов может использоваться расширение Dynamic Address Reconfiguration. Несмотря на то, что SCTP изначально поддерживает множественную адресацию, разрешение одновременной отправки фрагментов данных по всем путям не принесло бы ожидаемого роста скорости. В связи с этим, CMT-SCTP вносит 3 модификации в SCTP[2]:разделенные быстрые повторные передачи (Split Fast Retransmissions), подходящий рост окна перегрузки(Appropriate Congestion Window Growth) и задержанные выборочные подтверждения (Delayed SACKs). Эти модификации направлены, прежде всего, на устранение проблемы различных задержек на путях, которые затрагивают механизмы контроля перегрузки и повторных отправок.

Для поддержки многопоточности в TCP, MPTCP будет разделять нумерацию на уровне данных и уровне подпотока. Таким образом, кроме Sequence Number в заголовке TCP на подпотоке, будет использоваться также Data Sequence Number, который передается в параметре DSS. В данном параметре определяется соответствие между номером на уровне подпотока и номером на уровне данных. Это позволяет в случае проблем на подпотоке пересылать данные через другой подпоток. Еще одной особенностью MPTCP является то, что он использует единый размер окна для всех подпотоков, что позволяет отправлять данные с подпотока до тех пор, пока другая сторона намерена принимать данные, если б на каждом подпотоке использовалось одно окно, это привело бы к ситуации когда одни потоки загружены, а другие простаивают.

В сравнении расширений CMT-SCTP и MPTCP [3] было обнаружено, что MPTCP создает подпотоки, используя все доступные адреса, а CMT-SCTP использует непересекающиеся пары адресов для многопутевой передачи (показано на рисунке 1). При этом пропускная способность MPTCP была заметно выше, чем у CMT-SCTP. Также было выявлено, что у CMT-SCTP на достижение наибольшей пропускной способности значительно влияет выбор пары адресов, с которых устанавливается соединение. Стоит отметить также и то, что данные расширения пока не позволяют получить пропускную способность, равную суммарной пропускной способности интерфейсов, а также при наличии серьезной разницы в задержках на путях оба протокола могут работать даже хуже однопоточного протокола.

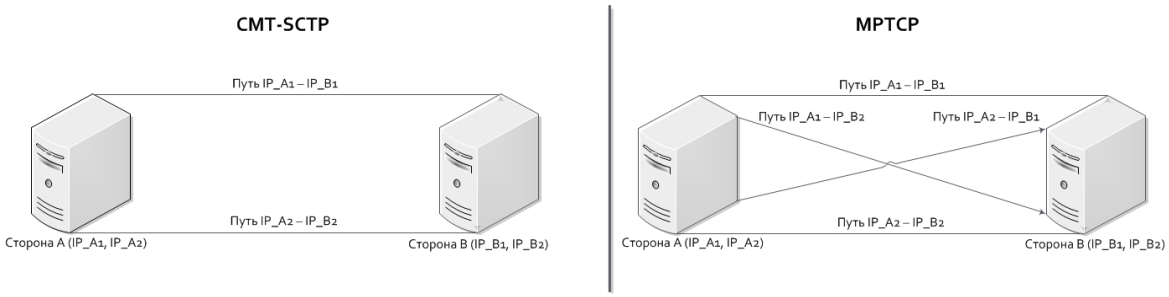


Рисунок 1 - Различие принципа построения путей передачи данных CMT-SCTP(слева) и MPTCP (справа).

Несмотря на то, что SCTP изначально был многопоточным и поддерживал множественную адресацию, добавление одновременной многопутевой передачи потребовало решения новых проблем. На сегодняшний день CMT-SCTP находится в стадии рабочего проекта IETF, и не имеет реализаций, доступных в широком доступе. MPTCP напротив уже имеет свой экспериментальный RFC в IETF и имеет несколько реализаций, более быстрое развитие MPTCP обусловлено также тем, что потребность в многопоточности и поддержке множественной адресации SCTP так и не получила широкого распространения. Однако все может измениться для SCTP и его расширений с массовым внедрением IPv6 или внедрением поддержки NAT для SCTP в оборудование. В связи с этим, для реализации преимуществ многопутевой передачи данных, привлекательнее выглядит MPTCP, так как для его внедрения требуется только поддержка данного расширения сторонами, тем не менее, разработчикам предстоит еще долгая работа по оптимизации.

Литература:
1. TCP Extensions for Multipath Operation with Multiple Addresses https://tools.ietf.org/html/rfc6824
2. Load Sharing for the Stream Control Transmission Protocol (SCTP) https://tools.ietf.org/html/draft-tuexen-tsvwg-sctp-multipath-09
3. Comparison of Multipath TCP and CMT-SCTP based on Intercontinental Measurements, Global Communications Conference (GLOBECOM), 2013 IEEE

В.А. Данилов, *Л.В. Данилова

АМПЛИТУДНЫЕ ХАРАКТЕРИСТИКИ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАТЕЛЕЙ ДЛЯ ПОДАВЛЕНИЯ НЕГАУССОВСКИХ УЗКОПОЛОСНЫХ ПОМЕХ

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия
*Ростовский государственный университет путей сообщения, г. Ростов-на-Дону, Россия

Ключевые слова: негауссовская помеха, нелинейная обработка, подавление помех.

Работа посвящена обоснованию вида амплитудной характеристики (АХ) нелинейного преобразователя (НП) для амплитудного подавления негауссовской помехи узкополосного типа. В задачах оптимального приема слабых сигналов на фоне негауссовских помех было установлено [1-3], что основным элементом помехозащиты является безынерционный нелинейный преобразователь, включаемый на входе той части приемника, которая является оптимальной при приеме сигнала на фоне белого гауссовского шума. Подавление негауссовской помехи путем нелинейного преобразования входных сигналов является, в сущности, процессом амплитудного подавления (АП) [2]. Установлено, что структура АП существенно зависит от вероятностных характеристик помехового колебания и от его спектра.

V.A. Danilov, *L.V. Danilova

AMPLITUDE CHARACTERISTICS OF NONLINEAR FUNCTION GENERATORS FOR THE INTEFERENCE NON-GAUSSIAN NARROWBAND SUPPRESSION

North-Caucasus Branch Federal Government Education Budget Establishment High Professional Education Moscow Technical University of Communications and Information Technology, Rostov-on-Don, Russia
*Rostov state university of transport communications, Rostov-on-Don, Russia

Keywords: non-Gaussian interference, nonlinear processing, interference suppression.

The work investigates the explanation of amplitude characteristic type of nonlinear generator for the amplitude suppression of non-Gaussian narrowband noise. In the problems of optimal weak signals detection against the background of non-Gaussian noise we proved [1-3] that the base element of interference elimination is the nonlinear inertialess transformer, which switches on that port of receiver, which is optimal in the signal reception against the background of white Gaussian noise. The non-Gaussian noise suppression by the instrumentality of nonlinear transformation of input signal is the amplitude suppression process [2]. The dependence of amplitude suppression structure of the probabilistic characteristics of oscillation and the spectrum is obtained.

Рассмотрим особенности построения схем АП для негауссовских помех широкополосного типа. Теоретическое обоснование алгоритма нелинейной обработки принимаемого сигнала $x(t)$

$$f_0(x) = -\frac{d}{dx}\ln w_1(x), \quad (1)$$

обеспечивающего подавление негауссовских помех с одномерной плотностью вероятности (ПВ) $w_1(x)$ в когерентном тракте обработки при обнаружении слабых сигналов впервые было сделано в работе [1]. В [4] были определены условия асимптотической оптимальности такого алгоритма. Его оптимальность доказана для помех, которые можно представить в виде стационарного процесса с независимыми отсчетами, что практически соответствует процессам с видеочастотной формой спектра. Поэтому применительно к радиотехническим системам нелинейная обработка (1) обладает оптимальными свойствами, если она применяется после синхронного (фазового) детектора [5]. Применение её в радиочастотном тракте на несущей или промежуточной частоте не гарантирует максимального подавления помехи процедурой нелинейного безынерционного преобразования.

Алгоритм нелинейной безынерционной обработки сигнала, предназначенный для подавления помех в радиочастотном тракте, обоснован в [2] и имеет вид

$$f_{0p}(x) = \int_0^x \frac{d[A \cdot g_0(A)]}{\sqrt{x^2 - A^2}}, \quad x \geq 0; \qquad (2)$$
$$f_{0p}(-x) = -f_{0p}(x),$$

где

$$g_0(A) = -\frac{d}{dA} \ln \left[\frac{W_A(A)}{A}\right], \qquad (3)$$

$W_A(A)$ – плотность вероятности огибающей помеховой составляющей в принимаемом сигнале. Данная характеристика является основной при описании помехового колебания узкополосного типа. Функция $W_A(A)$ может быть определена посредством интегрального соотношения вида [6]

$$\frac{W_A(A)}{A} = \int_0^\infty Q_1(v)\, J_0(Av) v dv, \qquad (4)$$

где $Q_1(v)$ – характеристическая функция (ХФ) для одномерной ПВ вида $w_1(x)$; $J_0(z)$ - функция Бесселя первого рода нулевого порядка.

Отметим здесь, что функция $g_0(A)$ в форме (3) определяет оптимальную колебательную характеристику (КХ) по первой гармонике принимаемого колебания. Данная функция позволяет определить оптимальную АХ НП в форме (2). Функции (2) и (3) связаны между собой интегральным соотношением [2] вида

$$g_0(A) = \frac{1}{\pi} \int_0^{2\pi} f_{0p}(A \cos\psi) \cos\psi \, d\psi, \qquad (5)$$

которое можно трактовать как интегральное уравнение типа Абеля [7].

Асимптотическая оптимальность алгоритма (2) доказана для помех, являющихся случайным процессом с узкополосной формой спектра, комплексную огибающую которой можно представить процессом с независимыми отсчетами. Алгоритм (2) эффективнее (1) при использовании нелинейной обработки в радиочастотном тракте.

Алгоритмы (1) и (2) применимы в тех случаях, когда спектр помехи существенно превышает спектр сигнала. В том случае, когда спектр помехи соизмерим со спектром сигнала, структура оптимальной обработки видоизменяется, и она исследована в работе [8]. Оптимальный обнаружитель в данном случае становится двухканальным. В каждом из этих каналов присутствуют нелинейные преобразовательные элементы, определяемые в соответствии с (1) и (3).

Двухканальная схема обнаружителя может быть сведена к одноканальной по схеме последовательного соединения НП и согласованного фильтра (СФ) в том случае, когда спектр помехи соизмерим со спектром сигнала [8].

В работе [9] показано, что в этом случае АХ определяется в два этапа. Сначала находится КХ по первой гармонике, а затем определяется искомая АХ. Вид КХ для помехи узкополосного типа в том случае, когда спектр помехи соизмерим со спектром сигнала, обоснован в работе [9] и имеет вид

$$h_0^2(A) = g_0^2(A) - \frac{2}{\pi} \int_0^A \frac{f_0^2(x) dx}{\sqrt{A^2 - x^2}}. \qquad (6)$$

В последней формуле характеристика $g_0(A)$ определяется соотношением (3), а функция $f_0(x)$ находится с помощью (1). Характеристику в форме (6) будем называть комбинированной колебательной характеристикой (ККХ), так как определяется она с помощью комбинации двух функций $g_0(A)$ и $f_0(x)$. Найденная ККХ позволяет теперь записать искомую АХ вида $f_1(x)$ для рассматриваемого случая. Функции $h_0(A)$ и $f_1(x)$ связаны между собой интегральным соотношением аналогичным формуле (5). Рассматривая (5) как интегральное уравнение типа

Абеля, можем найти искомую функцию $f_1(x)$ путем обращения соответствующего интегрального соотношения [7]

$$f_1(x) = \begin{cases} \frac{M(0)}{2x} + \frac{1}{2}\int_0^x \frac{d[zh_0(z)]}{\sqrt{x^2-z^2}}, & x > 0; \\ f_1(-x) = -f_1(x), \end{cases} \quad (7)$$

где $M(z) = zh_0(z)$.

Рассмотрим пример расчета с использованием найденных соотношений. Допустим, что в качестве помехового колебания рассматривается нормальный случайный процесс. В этом случае распределение $W_A(A)$ описывается законом Рэлея [6]

$$W_A(A) = \frac{A}{\sigma^2} exp(-\frac{A^2}{2\sigma^2}), \quad (8)$$

а функция $w_1(x)$ имеет вид

$$w_1(x) = \frac{1}{\sqrt{2\pi\sigma^2}} exp\left(-\frac{x^2}{2\sigma^2}\right). \quad (9)$$

Подставляя функции (8), (9) в соотношения (1), (3), получаем

$$g_0(A) = A/\sigma^2; \quad f_0(x) = x/\sigma^2.$$

Подставляя найденные значения в формулу (6), после вычисления интеграла с помощью [10], найдем

$$h_0(A) = \frac{A}{\sqrt{2}\sigma^2}.$$

Принимая во внимание найденное значение, с помощью (7) получаем

$$f_1(x) = \frac{x}{\sqrt{2}\sigma^2}.$$

Таким образом, искомая АХ для гауссовского случайного процесса является линейной, как и следовало ожидать.

На основании вышеизложенного можно сделать следующие выводы. Обоснован вид амплитудной характеристики НП для подавления негауссовской помехи узкополосного типа. Найденная АХ структурно определяется на базе оптимальной ККХ в форме (6), которая рассчитывается с помощью комбинации двух функций $f_0(x)$ и $g_0(A)$, определяемых по формулам (1) и (3). Эффективность предлагаемого метода АП может быть существенно больше эффективности исследованных ранее процедур, использующих характеристики в форме (1) и (2).

Литература:

1. Антонов О.Е. Оптимальное обнаружение сигналов в негауссовых помехах. Обнаружение полностью известного сигнала. // Радиотехника и электроника. 1967. Т.12. № 4. 579-587.

2. Валеев В.Г., Гонопольский В.Б. Метод амплитудного подавления негауссовских помех.// Радиотехника и электроника. 1981. Т. 26. №11. с. 2301-2315.

3.Акимов П.С., Бакут П.А., Богданович В.А. и др. Теория обнаружения сигналов /под ред. П.А. Бакута.- М.: Радио и связь, 1984, 440с.

4. Левин Б.Р., Кушнир А.Ф. Асимптотически оптимальные алгоритмы обнаружения и различения сигналов на фоне помех // Радиотехника и электроника. 1969. Т. 14. №2. С. 249-257.

5. Валеев В.Г., Корнилов И.Н. Нелинейная обработка сигналов для подавления помех в приемном тракте радиоэлектронных систем // Радиотехника. 2010. № 6. С. 37-42.

6. Тихонов В.И. Статистическая радиотехника. – М.: Радио и связь, 1982. 624 с.

7. Забрейко П.П., Кошелев А.И., Красносельский М.А. и др. Интегральные уравнения.- М.: Наука.1968. 448 с.

8. Валеев В.Г., Данилов В.А. Оптимальное обнаружение сигналов на фоне коррелированных радиопомех. // Известия высших учебных заведений. Радиоэлектроника. 1991. № 7. С. 30-34.

9. Данилов В.А., Данилов А.В. Оптимальное обнаружение сигналов на фоне негауссовских узкополосных помех // Известия вузов России. Радиоэлектроника. 2013. Вып. 3. С.15-23.

10. Градштейн И.С., Рыжик И.М. Таблицы интегралов, сумм, рядов и произведений.- М.: Наука, 1971. 1108 с.

В.А. Данилов, Ю.В. Жабинский, В.Л. Львов

КВАДРАТУРНО-НЕЛИНЕЙНЫЙ МЕТОД ПОДАВЛЕНИЯ УЗКОПОЛОСНЫХ НЕГАУССОВСКИХ ПОМЕХ

Северо-Кавказский филиал Московского государственного технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: негауссовская помеха, амплитудное подавление, эффективность подавления, амплитудная характеристика.

Рассмотрены принципы построения квадратурно-нелинейного метода подавления негауссовских помех в радиоканалах с некогерентным накоплением сигнала. Исследуются вопросы оптимизации нелинейного преобразователя и в том числе при выполнении нелинейной обработки полиномиальными преобразователями. Возможности метода иллюстрируются на примере подавления помех гармонического типа.

V.A. Danilov, Y.V. Jabinskiy, V.L. Lvov

QUADRATURE NONLINEAR METHOD OF NARROW BAND NON-GAUSSIAN INTERFERENCE SSUPPRESSION

The North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: non-Gaussian interference, amplitude suppression, efficiency of suppression, amplitude characteristic.

The paper considers principles of buildingquadraturenonlinearmethodofnon-Gaussianinterferencessuppression in radio channels with a non coherent signal integration. We examine the issues of nonlinear converter optimizationincluding the conditions of nonlinear processing with polynomial converters. The possibilities of this method are illustrated by the examples based on the harmonic interferences suppression.

В задачах с негауссовскими воздействиями особый интерес представляют вопросы исследования помехозащищенности некогерентных трактов обработки радиосигналов. Применение метода амплитудного подавления (АП), основанного на использовании безынерционных нелинейных преобразователей [1], может быть эффективным в том случае, когда помеха по спектру превосходит спектр сигнала. При действии полосовых помех эффективность безынерционных АП реализуется лишь только с помощью полосовых фильтров, что не всегда желательно.

Выполненные авторами статьи исследования показали, что путем некоторой модификации метода АП, связанной с применением идеального преобразователя Гильберта [2], можно обеспечить эффективность подавления негауссовских помех в некогерентных каналах, близкую к потенциальной, но уже без использования фильтровых систем. Безынерционный нелинейный преобразователь (НП) модуля аналитического сигнала будем называть квадратурным нелинейным преобразователем (КНП).

Статья посвящена обоснованию помехозащитных свойств метода КНП коррелированных негауссовских помех в радиоканалах с некогерентным накоплением сигнала. Рассмотрены вопросы оптимизации КНП и в том числе при выполнении нелинейной обработки полиномиальными преобразователями. Возможности метода иллюстрируются на примере подавления помех гармонического типа.

Рассмотрим прохождение аддитивной смеси *U(t)* сигнала *S(t)* и помехи *x(t)* через КНП, приведенный на схеме (рисунок1). Схема содержит идеальный преобразователь Гильберта H[·], устройства возведения в квадрат (КВ), сумматор (+), формирователь статистики

$$R(U_1, U_2) = \sqrt{U_1^2 + U_2^2}, \tag{1}$$

где $U_1 = U(t); \quad U_2 = H[U(t)];$

и безынерционный НП с амплитудной характеристикой g(R).

Будем считать, что входной сигнал *S(t)*удовлетворяет следующим ограничениям:

$$\langle S_1 \rangle = \langle S_2 \rangle = \langle S_1 S_2 \rangle = \langle S_2 S_1 \rangle = 0, \tag{2}$$

$$\langle S_1^2 \rangle = \langle S_2^2 \rangle = P_C, \tag{3}$$

где $S_1 = S(t); \quad S_2 = H[S(t)]$; $\langle * \rangle$ - усреднение по времени; P_c - мощность сигнала на входе приемника.

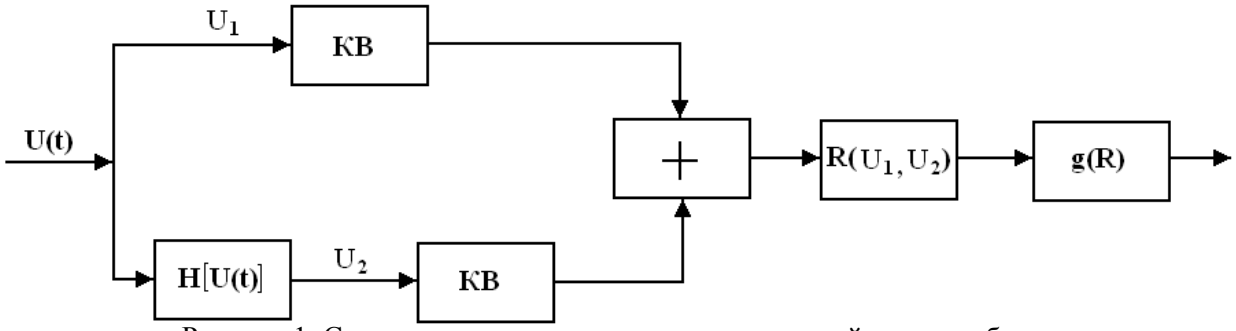


Рисунок 1. Структурная схема квадратурного нелинейного преобразователя

Помеха - стационарный эргодический процесс, заданный совместной плотностью вероятности $w_2(x_1, x_2)$ квадратурных составляющих $\{x_1 = x(t); x_2 = H[x(t)]\}$ с коэффициентом корреляции $r(\tau) = B_x(\tau) / B_x(0),$ где $B_x(\tau)$ - корреляционная функция квадратурных компонент помехи. Помеха и сигнал статистически независимы, отношение мощности сигнала к мощности помехи на входе приемника $q_{вх} = P_C / P_П$.

Представим процесс на выходе НП разложением в ряд

$$g[R(U_1, U_2)] \approx g[R(x_1, x_2)] + \left(\frac{\partial g}{\partial x_1} S_1 + \frac{\partial g}{\partial x_2} S_2 \right) + \frac{1}{2} \left[\frac{\partial^2 g}{\partial x_1^2} S_1^2 + 2 S_1 S_2 \frac{\partial^2 g}{\partial x_1 \partial x_2} + \frac{\partial^2 g}{\partial x_2^2} S_2^2 \right]. \tag{4}$$

Наличие сигнала на входе НП приводит к изменению среднего значения $M\{g[R(x_1 + S_1, x_2 + S_2)]\} \neq 0$, где $M\{*\}$ - статистическое усреднение. Предположим, что характеристика НП удовлетворяет условию

$$M\{g[R(x_1, x_2)]\} = 0. \tag{5}$$

Произведя в (4) усреднение во времени с учетом (2),(3), а затем усреднение по координатам с учетом (5), получаем

$$M\{g[R(x_1 + S_1, x_2 + S_2)]\} = \frac{P_C}{2} M\left[\frac{\partial^2 g}{\partial x_1^2} + \frac{\partial^2 g}{\partial x_2^2} \right].$$

К помехе относим лишь первое слагаемое (4) и, таким образом, отношение сигнал-помеха на выходе НП примет вид:

$$q = \frac{P_C^2}{4} \cdot \frac{\left(M\left[\frac{\partial^2 g}{\partial x_1^2} + \frac{\partial^2 g}{\partial x_2^2} \right] \right)^2}{M\{g^2[R(x_1, x_2)]\}}. \tag{6}$$

Статистическое усреднение в (6) производится по совокупности переменных (x_1, x_2) с учетом совместного распределения квадратурных компонент помехи. Так, например, для знаменателя (6) запишем

$$M\left[g^2(R)\right] = \int_{-\infty}^{\infty}\int g^2\left[R(x_1, x_2)\right] w_2(x_1, x_2)\, dx_1 dx_2. \tag{7}$$

Переходя в (7) к полярным координатам R,Θ по формулам $x_1 = R\cos\theta, x_2 = R\sin\theta$, принимая во внимание (1), получаем

$$M\left[g^2(R)\right] = \int_0^{\infty} g^2(R) W(R) dR \tag{8}$$

где

$$W(R) = R\int_0^{2\pi} w_2\left(R\cos\theta, R\sin\theta\right) d\theta \tag{9}$$

- распределение статистики $R(x_1, x_2)$ из (1). Производя таким же образом усреднение в числителе (6), учитывая (1),(9), получаем

$$M\left[\frac{\partial^2 g}{\partial x_1^2} + \frac{\partial^2 g}{\partial x_2^2}\right] = \int_0^{\infty}\left(\frac{d^2 g}{dR^2} + \frac{1}{R}\cdot\frac{dg}{dR}\right) W(R) dR. \tag{10}$$

Подставляя (8), (10) в (6), найдем

$$q = \frac{P_C^2}{4}\cdot\frac{\left[\int_0^{\infty}\left(\frac{d^2 g}{dR^2} + \frac{1}{R}\cdot\frac{dg}{dR}\right) W(R) dR\right]^2}{\int_0^{\infty} g^2(R) W(R) dR}. \tag{11}$$

Выражение (11) определяет отношение сигнал-помеха на выходе КНП, содержащего НП с характеристикой $g(R)$. Найдем вид характеристики НП, при которой достигается максимум коэффициента (11). Выполняя преобразования в числителе (11) с применением формулы интегрирования по частям, накладывая дополнительное условие

$$g'(R)W(R)\Big|_0^{\infty} + g(R)\left[W(R)/R - W'(R)\right]_0^{\infty} = 0, \tag{12}$$

можно показать [1], что максимум коэффициента (11) достигается при

$$g(R) = g_0(R) = \frac{W'(R)}{W(R)} - \frac{1}{R}\cdot\frac{d}{dR}\ln\left[\frac{W(R)}{R}\right] \tag{13}$$

и равняется

$$\max q = q(g = g_0) = \frac{P_C^2}{4}\int_0^{\infty} g_0^2(R) W(R) dR \tag{14}$$

Следовательно, для КНП, максимизирующего отношение сигнал-помеха на выходе НП, амплитудная характеристика НП должна быть согласована с распределением $W(R)$ статистики $R(x_1,x_2)$, формируемой в соответствии с (1). Это положение относится к помехам с произвольной шириной и формой спектра.

Необходимо сделать следующие замечания. Оптимальные решения (13),(14) существуют, если плотность вероятности $W(R)$из (9) удовлетворяет условиям, вытекающим из (12) с учетом (13). Формула (13) совпадает с выражением для оптимальной характеристики детектирования при АП помех в некогерентном полосовом обнаружителе [1]. Разница состоит только в том, что характеристика детектирования выражается через распределение $W_A(A)$огибающей $A(t)$ помехового колебания. Следовательно, если распределение $W(R)$статистики $R(x_1,x_2)$ из (1) будет совпадать с распределением огибающей помехи, то КНП на рисунке 1 в оптимальном случае будет

иметь те же энергетические характеристики, что и амплитудный подавитель помех в некогерентном полосовом обнаружителе сигналов [1].

Высказанные положения иллюстрируются на примере коррелированных квадратурных компонент по закону Хойта [3] и для синусоиды со случайной фазой. На рисунке 2 представлена характеристика эффективности подавления в функции от *r* для распределения Хойта. Эффект нелинейного подавления помехи в схеме КНП весьма ощутим, особенно при больших значениях *r*.

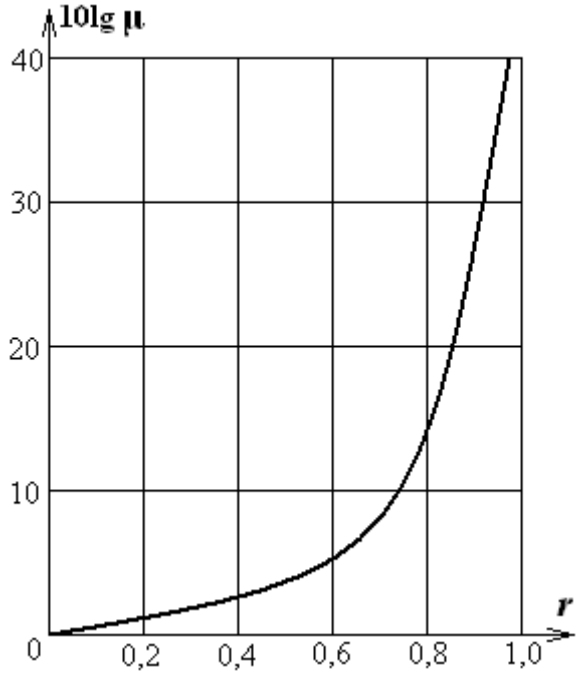


Рисунок 2. Характеристика эффективности подавления помехи для распределения Хойта

На рисунке 3 отражены результаты расчета эффективности КНП при воздействии негауссовской помехи с распределением квадратурных компонент по закону Райса [3].

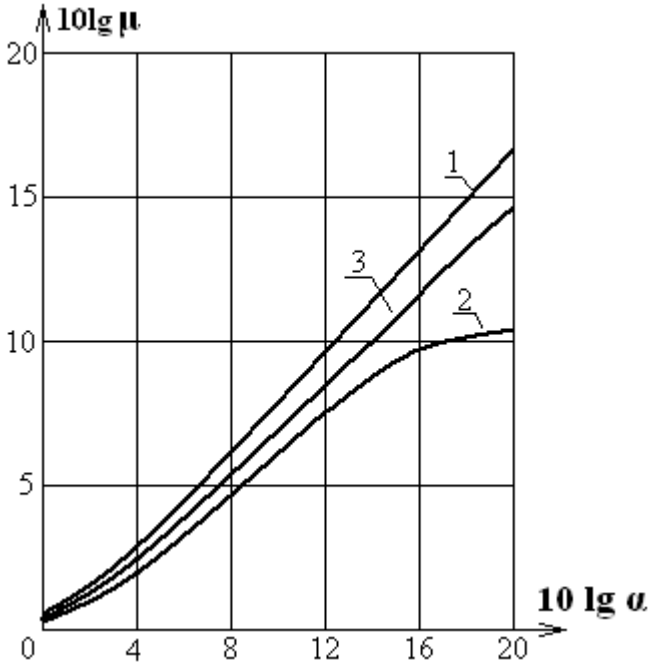


Рисунок 3. Результаты расчета эффективности КНП при воздействиинегауссовской помехи с распределением квадратурных компонент по закону Райса (1 – оптимальная характеристика, 2 – полином второй степени, 3 – полином третьей степени, α – параметр помехи)

Полученные результаты позволяют заключить, что метод КНП обеспечивает подавление негауссовской помехи до уровня шума. Применение полиномиального преобразователя с оптимизированными коэффициентами практически не отличается по эффективности от оптимального НП уже для полинома третьей степени.

Метод КНП может быть эффективным как для гауссовских, так и для негауссовских помех с произвольным спектром, и эта эффективность в каналах с некогерентным накоплением сигнала может быть достигнута уже без использования фильтровых систем.

Литература:

1. Акимов П.С., Бакут П.А., Богданович В.А. и др. Теория обнаружения сигналов/ Под ред. П.А. Бакута - М.: Радио и связь, 1984.
2. Тихонов В.И. Нелинейные преобразования случайных процессов – М.: Радио и связь, 1986.
3. Левин Б.Р. Теоретические основы статистической радиотехники - М.: Радио и связь, 1989.
4. Рытов С.М. Введение в статистическую радиофизику - М.: Наука, 1976.
5. Градштейн И.С., Рыжик И.М. Таблицы интегралов, сумм, рядов и произведений - М.: Наука, 1971.

А.М. Джамбеков

К ВОПРОСУ УЧЕТА НЕСТАЦИОНАРНОСТИ ПРИ УПРАВЛЕНИИ ПРОЦЕССОМ КАТАЛИТИЧЕСКОГО РИФОРМИНГА

Астраханский государственный технический университет, г. Астрахань, Россия

Ключевые слова: каталитический риформинг, нечеткое множество, нечеткий регулятор, стабилизационная колонна, стационарный случайный процесс, математическое ожидание, элементарная случайная функция.

В данной работе было изложено состояние вопроса учета нестационарности при управлении процессом каталитического риформинга. На основе разработанной ранее системы управления с нечетким регулятором температуры стабилизационной колонны риформинга была предложена структура системы управления с компенсатором случайной составляющей сигнала. Было получено аналитическое описание входного воздействия системы, которое представляет собой стационарный случайный процесс. Полученная система регулирования температуры колонны установки риформинга открывает возможности для качественного управления данной частью установки с компенсацией случайной составляющей входного сигнала.

A.M. Dzhambekov

THE ISSUE IN THE MANAGEMENT ACCOUNTING NONSTATIONARITY CATALYTIC REFORMING PROCESS

Astrakhan State Technical University, Astrakhan, Russia

Keywords: catalytic reforming, fuzzy set, fuzzy control, stabilization column stationary random process, the expectation elementary random function.

In this paper, was described state of the problem of nonstationarity in the management accounting catalytic reforming process. Based on previously developed control system with fuzzy temperature controller reformer stabilizer column was proposed control architecture with a compensator of the random component of the signal. It was an analytical description of the impact of the input system, which is a stationary random process. The resulting temperature control system of the column reformer opens

opportunities for quality control of this part of the installation with compensation of the random component of the input signal.

В настоящее время в нефтегазовой отрасли страны особое место занимают новые малозатратные технологии, которые позволяют с большой эффективностью использовать сырье в переработке газа и нефти и обеспечивать увеличение характеристик качества и понижение стоимости выпускаемой продукции.

Данное требование выполнимо при условии наиболее полного ресурсного использования на существующих установках нефте- и газоперерабатывающих заводов. В этом направлении набольшие возможности представляют установки каталитического риформинга. Каталитический риформинг (КР) бензинов является одним из самых важных процессов современной нефтеперерабатывающей промышленности. Его основное предназначение состоит в получении бензинов с высоким октановым числом [0].

Задача управления установкой КР является достаточно сложной по целому ряду причин. На технологический режим процесса КР влияет большое количество режимных переменных. Помимо этого, имеют место действующие на процесс существенные возмущения. Также, происходит непрерывное изменение качества сырья, поступающего на установку. Экспериментальный поиск оптимальных управлений влечет за собой большие затраты ресурсов установки КР.

При разработке оптимальных систем управления процессом КР важной задачей является построение адекватной математической модели процесса КР. Основная проблема построения таких моделей заключается в наличии большого количества информации о процессе, которую невозможно формализовать традиционными методами. К ней относится информация о качественном составе сырья и топливного газа, состоянии оборудования и пр. Большие возможности в вопросе формализации качественной информации и управления на базе данной информации открывает теория нечетких множеств.

Построение математической модели процесса КР с совместным использованием количественной и качественной информации открывает значительные перспективы для расширения возможностей оптимального управления процессом [0].

В работе [0] была построена система регулирования температуры стабилизационной колонны установки КР с цифровым нечетким регулятором (НР). При этом информация экспертов из базы знаний НР не учитывала случайные изменения управляющего сигнала системы θ (t) и протекающих процессов. В качестве входного воздействия m(t) был принят единичный ступенчатый сигнал.

Структурная схема системы управления с цифровым нечетким регулятором (НР) была представлена следующим образом [0]:

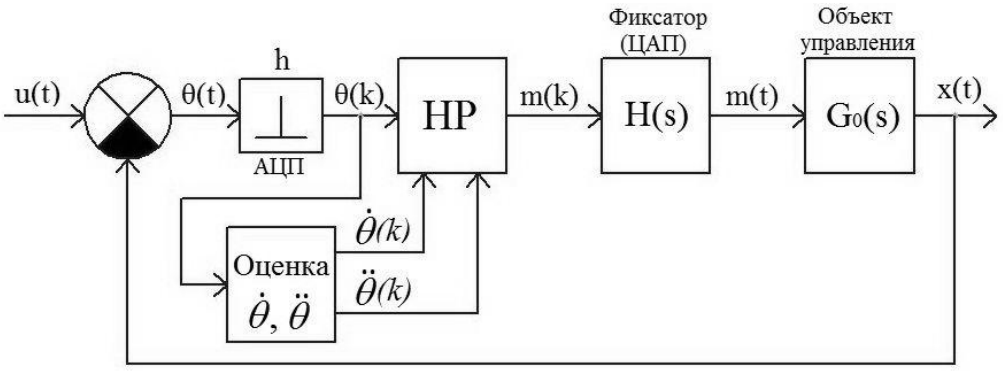


Рисунок 1. Структурная схема системы управления с цифровым НР

В качестве управляющего воздействия θ (t) в нечеткой системе выступает ошибка регулирования температуры, измеряемой на выходе из трубчатой печи подогрева сырья колонны. Температура на выходе печи подогрева должна поддерживаться в заданных пределах: 220÷256 ^{0}C. После выработки управляющего воздействия НР получаем значение ошибки регулирования температуры m(t) печи подогрева, которое будет подано на исследуемую, в системе Matlab Simulink, модель стабилизационной колонны. На выходе объекта управления мы получаем

значение ошибки регулирования температуры x(t) низа колонны. На регулирование температуры низа стабилизационной колонны также накладываются ограничения: 200÷250 ^{0}C.

Для учета нестационарности процесса необходимо спроектировать надстройку базы знаний НР [0]. Как было отмечено выше, к основным причинам нестационарности процесса КР относятся колебания параметров входного сырья. К одному из наиболее важных параметров относится температура входного потока. Поэтому, необходимо получить аналитическое описание входного воздействия системы m(t), которое представляет собой стационарный случайный процесс [0].

Допущение о стационарности протекания температуры m(t) как случайного процесса связано с тем, что данная величина для колонны стабилизации в большинстве случаев изменяется во времени приблизительно однородно и имеет вид непрерывных случайных колебаний вокруг некоторого среднего значения, причем ни средняя амплитуда, ни характер этих колебаний не обнаруживают существенных изменений с течением времени [0].

Для нахождения статистических характеристик данной случайной функции воспользуемся результатами, полученными в [0]. Здесь была получена совокупность реализаций колебания температуры колонны риформинга (рис.2), работающей на НПЗ. Используем тот фрагмент реализаций m(t), который удовлетворяет требуемым интервалам времени t= (0; 30) мин и температуры u(t)=(199÷277) ^{0}C. Это требование необходимо в целях дальнейшего вычисления аналитического выражения, куда входит величина T(t) с интервалами времени t= (0; 30) мин и температуры T(t)=(220÷256) ^{0}C.

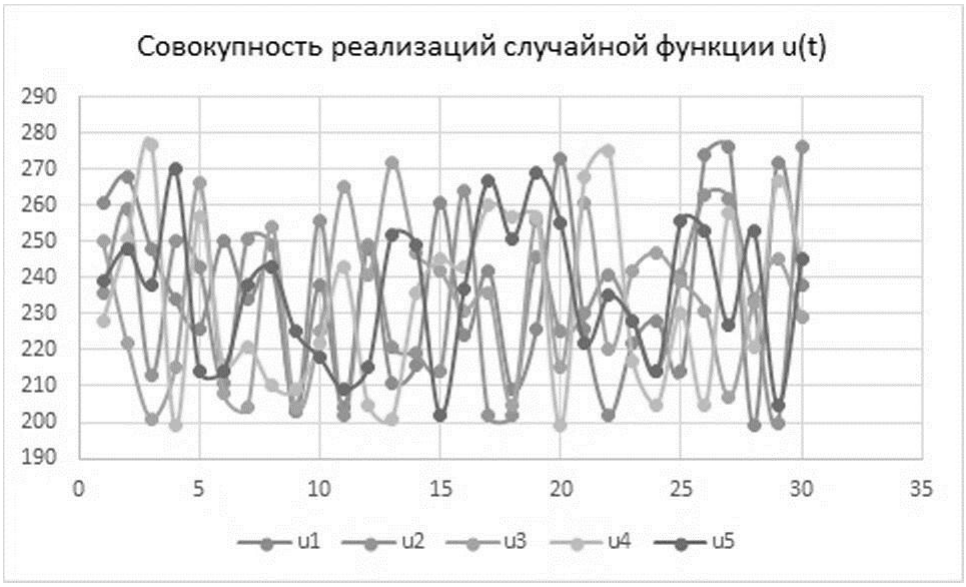


Рисунок 2. Совокупность реализаций случайной функции u(t)

Производим оценки математических ожиданий для каждой из 30-ти случайных величин (рис. 3).

Рисунок 3. Математическое ожидание случайной функции u(t)

Для получения аналитического выражения случайной функции u(t) воспользуемся *методом канонических разложений*, разработанным В.С. Пугачевым [0].

Идея метода канонических разложений состоит в том, что случайная функция, над которой нужно произвести те или иные преобразования, предварительно представляется в виде суммы так называемых *элементарных случайных функций*. Учитывая небольшой разброс значений функции u(t) и ее математического ожидания $u_x(t)$ на заданном интервале времени может быть использована только одна элементарная функция:

$$U(t) = V\varphi(t), \tag{1}$$

где V – обычная случайная величина, $\varphi(t)$ - обычная (неслучайная) функция.

В качестве функции $\varphi(t)$ будет выступать зависимость, полученная в ходе полиномиальной аппроксимации кривой математического ожидания $u_x(t)$:

$$\varphi(t) = 0{,}0028 \cdot t^3 - 0{,}1233 \cdot t^2 + 1{,}6342 \cdot t + 231{,}56 \cdot t$$

Итак, получаем выражение для элементарной функции:

$$U(t) = V \cdot (0{,}0028 \cdot t^3 - 0{,}1233 \cdot t^2 + 1{,}6342 \cdot t + 231{,}56 \cdot t)$$

Именно случайная величина V является тем параметром, который требует корректирование базы знаний НР для полной или приближенной компенсации случайной составляющей. Идея состоит в том, что нужно производить периодическое отслеживание изменения значения случайной величины V и в случае ее изменения с помощью надстроечного компенсатора создавать необходимое управляющее воздействие (рис.4).

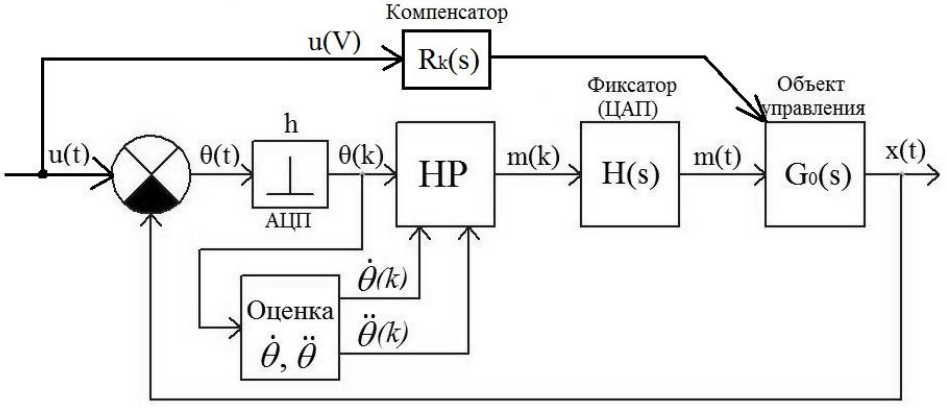


Рисунок 4. Структурная схема системы управления с цифровым НР и компенсатором

Руководствуясь методикой упомянутой выше работы необходимо произвести расчет системы регулирования на базе НР, учитывая в структурной схеме системы и при построении переходных процессов случайную величину V. Полученная система регулирования температуры стабилизационной колонны установки КР позволит производить качественное управление данной частью установки с компенсацией случайной составляющей входного сигнала.

Литература:

1. Имашев У.Б. Особенности развития процесса каталитического риформинга в России / У.Б. Имашев, А.А. Тюрин, Е.А. Удалова // Башкирский химический журнал. - 2009. - Т. 16. № 4. - С. 184-186.

2. Джамбеков А.М. Разработка нечеткой системы управления процессом вторичной бензина / А.М. Джамбеков, И.А. Щербатов // Геология, география и глобальная переработки энергия, № 3(54), 2014. - С.89-93.

3. Джамбеков А.М. Управление процессом каталитического риформинга на основе экспертной информации / А.М. Джамбеков, И.А. Щербатов // Системы. Методы. Технологии, № 4 (24), 2014. С. 103-111.

4. Гостев В.И. Нечеткие регуляторы в системах автоматического управления / В.И. Гос-тев. К.: «Радіоаматор», 2008. 972 с.

5. Штовба С.Д. Проектирование нечетких систем средствами Matlab / С.Д. Штовба. М.: Горячая линия - Телеком, 2007. 288 с.

6. Вентцель Е.С. Теория вероятностей: Ечебник для студ. вузов / Е.С. Вентцель. – М.: Академия, 2005. – 576 с.

7. Вентцель Е. С. Теория случайных процессов и ее инженерные приложения / Е.С. Вентцель, Л.А. Овчаров. - М.: Высшая школа, 2000. - 383 с.

8. Каракулов А.Г. Мониторинг установки каталитического риформинга бензинов Ачинского НПЗ с использованием компьютерной моделирующей системы / А.Г. Каракулов, Е.С. Шарова, Э.Д. Иванчина, А.Я. Сваровский, Д.А. Кульбов // Известия Томского политехнического университета. - 2013. - Т. 322. № 3. - С. 32-34.

9. Пугачев В.С. Применение канонических разложений случайных функций к определению оптимальной линейной системы / В.С. Пугачев // Автоматика и телемеханика, 1956, Т. 17, вып. 6. – С.489–499.

О.Ю. Евсеева, Е.Н. Ильяшенко

МОДЕЛЬ ВИРТУАЛИЗАЦИИ РЕСУРСОВ ТРАНСПОРТНОЙ ОПТИЧЕСКОЙ СЕТИ И МЕТОД УПРАВЛЕНИЯ НИМИ

Харьковский национальный университет радиоэлектроники, Харьков, Украина

Ключевые слова: транспортная оптическая сеть, программно-конфигурируемые сети, оптимальное управление ресурсами, виртуализация ресурсов.

Виртуализация ресурсов и абстрагирование от нижележащего транспортного уровня являются основой концепции программно-конфигурируемых сетей (Software-Defined Network, SDN). В работе предлагается математическая модель, обеспечивающая оптимальное динамическое формирование пула виртуальных ресурсов SDN на основе пакетной оптической транспортной сети и распределения этих ресурсов между поступающими на обслуживание запросами с учетом взаимосвязи уровней WDM и IP. Для получения численных решений предлагается декомпозиционный алгоритм, предполагающий последовательное, но взаимосогласованное решение задач управления физическим и виртуальными ресурсами.

O.Yu. Yevsyeyeva, Y.N. Ilyashenko

MODEL ON VIRTUALIZATION OF RESOURCES IN TRANSPORT OPTICAL NETWORK AND METHOD FOR CONTROLLING THEM

Kharkiv National University of Radioelektronics, Kharkiv, Ukraine

Keywords: optical transport network, software-defined network, optimal resource control, resource virtualization.

Resource virtualization and underlying transport network's abstraction are the basis of the concept of Software-Defined Network (SDN). In order to provide optimal dynamic creation of a pool of virtual resources in SDN that is based on packet-optical transport network and in order to allocate these resources among the incoming service requests a mathematical model that covers WDM and IP levels in couple was offered. To obtain numerical solutions of optimization problem a decomposition algorithm was proposed; the algorithm intends consistent, but mutually agreed solution to problems of control of physical and virtual resources.

Новейшими концепциями в области построения информационных систем являются облачные технологии, а в области телекоммуникаций – программно-конфигурируемые сети (Software-Defined Network, SDN). Примечательно, что в основе и облачных технологий, и обеспечивающих их техническую реализацию SDN лежит идея виртуализации ресурсов, выделяемых «по требованию». Виртуализация позволяет отделить управление сервисами от управления транспортной инфраструктурой и свести задачу выделения требуемых тому или иному приложению (сервису) пропускных способностей к задаче их назначения из общего виртуального пула транспортных ресурсов. В целом это призвано повысить эффективность использования ресурсов, поскольку в этом случае видимая на уровне сервисов «виртуальная» сеть, ее структура и пропускные способности, «эластично» подстраиваются под требования обслуживаемого трафика. В рамках SDN задача виртуализации возлагается на контроллер управления транспортной программно-конфигурируемой сети (transport SDN), который через сетевой API-интерфейс обеспечивает контроль и распределение ресурсов транспортной сети в соответствии с запросами, поступающими с уровня сервисов. Сама же транспортная SDN зачастую представляет собой пакетную IP-сеть на основе оптической инфраструктуры. В свете тенденций конвергенции и создания единых транспортных платформ одной из наиболее перспективных на сегодня является концепция IP-over-OTN, где функции оптической коммутации (Optical Transport Network, OTN) и волнового мультиплексирования (Wavelength Division Multiplexing, WDM) совмещены в рамках реконфигурируемой оптической сети, поверх которой через Ethernet-интерфейсы обеспечивается передача IP-пакетов. Таким образом, задача управления ресурсами пакетной оптической трансформируется в задачу формирования пула виртуальных ресурсов, т.е. динамического создания определенного набора виртуальных трактов передачи (световых путей), обладающих заданной пропускной способностью в соответствии с поступающими в сеть запросами. В свою очередь решение данной задачи тесно взаимосвязано с реализуемым на IP-уровне порядком управления трафиком, поскольку именно порядок распределения виртуальных ресурсов между обслуживаемыми запросами будет определять требования к создаваемой на оптическом уровне виртуальной топологии. Таким образом, имеем две актуальные тесно взаимосвязанные задачи: виртуализации ресурсов оптической сети и управления ними, которые должны быть решены совместно (или, по меньшей мере, согласованно), при этом в соответствии с концепцией SDN решение должно быть динамическим, масштабируемым и оптимальным, что может быть достигнуто в рамках предлагаемой математической модели.

Физическими ресурсами оптической транспортной сети являются несущие (световые волны), с целью управления которыми введем булеву переменную $w_{i,j}^{l,m,n}(k)$, принимающую единичное значение, если на k-м временном интервале управления предполагается использование l–й несущей в оптическим тракте (m,n) для создания светового пути между маршрутизаторами i и j. В рамках оптической сети переменные $w_{i,j}^{l,m,n}(k)$ связаны законом сохранения потока, вид

которого определяется способом организации связи между оптическими мультиплексорами. В случае реализации многоскоростной передачи (режим Mixed-Line Rate, MLR) необходимо учитывать, что разные линейные скорости при одинаковых расстояниях передачи сопряжены с разными уровнями битовых ошибок, а потому не каждая оптическая несущая может быть использована для установления светового пути:

$$\sum_{\substack{n=1,\\ n\neq m}}^{N}\sum_{l=1}^{N_{m,n}^{w}}\gamma_{i,j}^{l,m,n}c^{l,m,n}w_{i,j}^{l,m,n}(k)-\sum_{\substack{g=1,\\ g\neq m}}^{N}\sum_{l=1}^{N_{g,m}^{w}}\gamma_{i,j}^{l,m,n}c^{l,r,m}w_{i,j}^{l,r,m}(k)=\begin{cases} f_{i,j}(k), & if \quad m=i; \\ 0, & if \quad m\neq i,\ j; \\ -f_{i,j}(k), & if \quad m=j, \end{cases} \tag{1}$$

где $c^{l,m,n}$ – пропускная способность l-й оптической несущей в тракте передачи (m,n); $\gamma_{i,j}^{l,m,n}=\{0,1\}$ – коэффициент, отражающий приемлемость использования l-й несущей в оптическим тракте (m,n) для создания светового пути (i,j) в соответствии с допустимым порогом BER; $N_{m,n}^{w}$ – число оптических несущих в тракте передачи (m,n); N – число мультиплексоров в сети WDM; $f_{i,j}(k)$ – пропускная способность формируемого светового пути (i,j).

В традиционном односкоростном режиме (Single-Line Rate, SLR) условие сохранения потока упрощается и принимает вид:

$$\sum_{\substack{n=1,\\ n\neq m}}^{N}\sum_{l=1}^{N_{m,n}^{w}}cw_{i,j}^{l,m,n}(k)-\sum_{\substack{g=1,\\ g\neq m}}^{N}\sum_{l=1}^{N_{g,m}^{w}}cw_{i,j}^{l,r,m}(k)=\begin{cases} f_{i,j}(k), & if \quad m=i; \\ 0, & if \quad m\neq i,\ j; \\ -f_{i,j}(k), & if \quad m=j, \end{cases} \tag{2}$$

где c – пропускная способность оптической несущей.

Поскольку количество оптических несущих в каждом тракте передачи ограничено и каждая из них может быть использована один раз, переменная $w_{i,j}^{l,m,n}(k)$ кроме системы уравнений (1) или (2) должна удовлетворять условиям:

$$\sum_{i=1}^{N}\sum_{\substack{j=1,\\ j\neq i}}^{N}\sum_{l=1}^{N_{m,n}^{w}}w_{i,j}^{l,m,n}(k)\le N_{m,n}^{w}, \qquad \sum_{i=1}^{N}\sum_{\substack{j=1,\\ j\neq i}}^{N}w_{i,j,h}^{l,m,n}(k)\le 1. \tag{3}$$

Фигурирующая в выражениях (1) – (2) величина $f_{i,j}(k)$ должна удовлетворять требованиям относительно связности между маршрутизаторами на уровне IP, т.е.

$$f_{i,j}(k)\ge b_{i,j}(k), \tag{4}$$

где $b_{i,j}(k)$ – требуемая пропускная способность светового пути (i,j).

В свою очередь величина $b_{i,j}(k)$ определяется текущими объемами поступающего в сеть трафика и может быть рассчитана на основе выражений:

$$x_{i,j}(k+1)=x_{i,j}(k)-\sum_{\substack{l=1\\ l\neq i}}^{N^r}b_{i,l}(k)\cdot\Delta t\cdot u_{i,l}^{j}(k)+\sum_{\substack{m=1\\ m\neq i,j}}^{N^r}b_{m,i}(k)\cdot\Delta t\cdot u_{m,i}^{j}(k)+y_{i,j}(k), \tag{5}$$

$$0\le x_{i,j}(k), \qquad \sum_{\substack{j=1,\\ j\neq i}}^{N^r}x_{i,j}(k)\le x_i^{\max}, \qquad 0\le u_{i,l}^{j}(k)\le 1, \qquad \sum_{n=1}^{N^r}u_{i,l}^{n}(k)\le 1, \tag{6}$$

где $i, j = \overline{1, N^r}$, $i \neq j$; $\Delta t = t(k+1) - t(k)$ $x_{i,j}(k)$ – объем данных, которые находятся на i-м маршрутизаторе и предназначены для передачи j-му маршрутизатору в момент времени t_k; $u_{i,l}^{j}(k)$ – маршрутная переменная, которая указывает на долю пропускной способности канала (i,l), выделяемую в момент времени t_k для передачи потока с адресом j; $y_{i,j}(k)$ – объем нагрузки, поступающей в момент времени t_k на маршрутизатор i и предназначенной для передачи маршрутизатору j; N^r – количество маршрутизаторов в сети; $x_i^{\max}$ – максимально допустимая длина очереди на i-м маршрутизаторе.

Дополнительно с целью поддержки услуг гарантированного качества в модель могут быть введены полученные в рамках тензорного описания телекоммуникационных систем условия, выполнение которых обеспечивает требуемые значения скоростных, временных и надежностных показателей качества обслуживания [1]. Таким образом, предложенная математическая модель содержит управляющие переменные трех типов: $u_{i,l}^{j}(k)$, $b_{i,j}(k)$ и $w_{i,j}^{l,m,n}(k)$, где $u_{i,l}^{j}(k)$ определяют порядок распределения пула виртуальных ресурсов между поступающими на обслуживание IP-потоками, $b_{i,j}(k)$ – отвечают за виртуальные ресурсы, доступные на IP-уровне, $w_{i,j}^{l,m,n}(k)$ – отражают физические ресурсы оптической транспортной сети. Численные значения переменных управления всех типов могут быть получены в результате решения оптимизационной задачи, связанной с минимизацией суммарной потребляемой сетью электроэнергии $P_{\Sigma}(k)$ при ограничениях (1) – (6), где величина $P_{\Sigma}(k)$ рассчитывается, например, согласно [2].

Поскольку сформулированная задача является нелинейной и при этом содержит целочисленные переменные с целью ее дальнейшей практической реализации целесообразно рассматривать численные методы решения, позволяющие получить реализуемое в любой момент времени управление, в той или иной степени приближенное к оптимальному. В этой связи в соответствии с физическим смыслом рассматриваемой проблемы заслуживает внимания подход, предполагающий декомпозицию исходной задачи на ряд решаемых последовательно подзадач (рис.1).

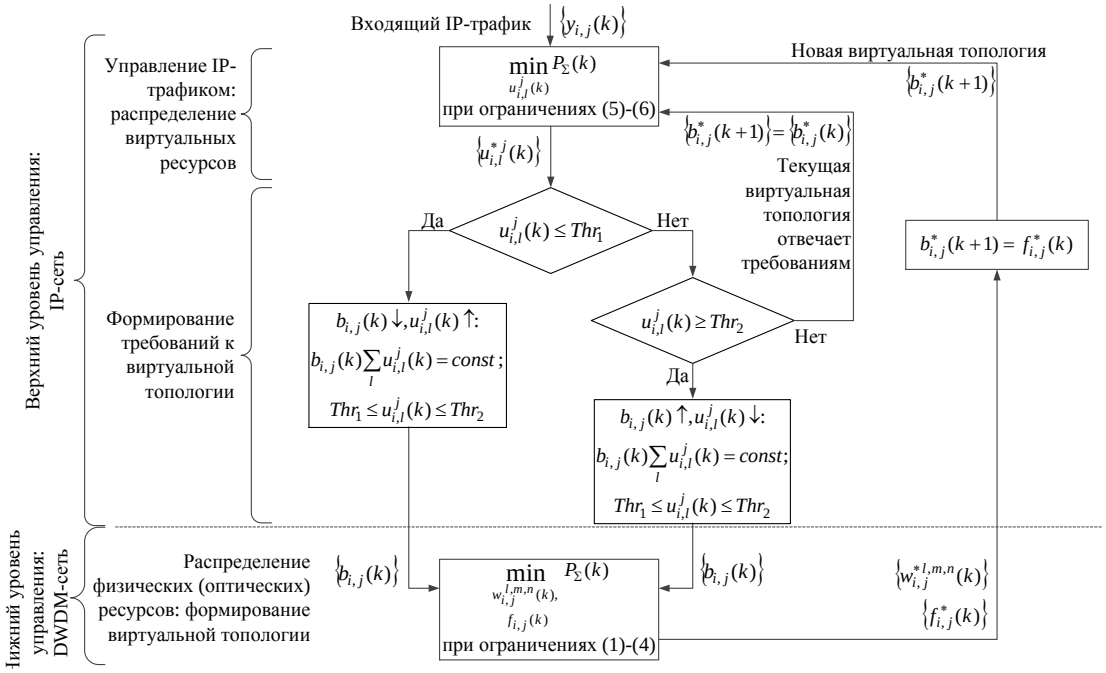


Рисунок 1. Алгоритм управления ресурсами транспортной оптической сети

Так на верхнем уровне управления пул виртуальных ресурсов, отображающий доступную на IP-уровне виртуальную топологию, предполагается известным; решаемая задача заключается в оптимальном их распределении между IP-потоками. Математически это формализуется как задача минимизации $P_{\Sigma}(k)$ по переменным $\left\{u_{i,l}^{j}(k)\right\}$ при ограничениях (5) – (6) при фиксированных значениях $\left\{b_{i,j}^{*}(k)\right\}$. На основании полученного оптимального порядка управления IP-потоками корректируются требования к пулу виртуальных ресурсов, т.е. осуществляет пересчет переменных $\left\{b_{i,j}(k)\right\}$. При этом следует исходить из допустимых нижнего (Thr_1) и верхнего (Thr_2) пороговых значений, которые указывают на недостаток или, напротив, избыток виртуальных ресурсов на отдельных направлениях. Скорректированные требования к виртуальной топологии спускаются на нижний уровень управления, где происходит перераспределение оптических несущих оптической транспортной сети и установление световых путей $\left\{f_{i,j}^{*}(k)\right\}$ в ходе решения задачи минимизации $P_{\Sigma}(k)$ по переменным $\left\{w_{i,j}^{l,m,n}(k)\right\}$ при ограничениях (1) – (4) в соответствии с новыми требованиями, т.е. полученными от верхнего уровня $\left\{b_{i,j}(k)\right\}$.

Таким образом, предлагаемый на основе математической модели (1) – (6) алгоритм нацелен на динамическое оптимальное распределение физических ресурсов транспортной оптической сети и их виртуализацию в соответствии с концепцией SDN, а применяемый при этом декомпозционный подход и последовательное рассмотрение задач управления физическими и виртуальными ресурсами обеспечивают масштабируемость решений.

Литература:

1. Лемешко А.В., Евсеева О.Ю. Тензорная модель многопутевой маршрутизации с гарантиями качества обслуживания одновременно по множеству разнородных показателей // Проблемы телекоммуникаций, 2012, № 4 (9), С. 16 - 31.

2. Yevsyeyeva O., Ilyashenko Y. Cross-Layer Design for Optimal Energy Effective Resource Allocation in IP-over-DWDM Networks // Proceedings of XIIIth International IEEE conference «The experience of designing and application of CAD systems in microelectronics», CADSM'2015, P. 414-418.

М.А. Елфимов, Н.А. Резниченко,
А.В. Позднякова, Н.В. Руденко, С.В. Иванов

ВЫБОР МЕСТА РАЗМЕЩЕНИЯ ВОЗОБНОВЛЯЕМЫХ ИСТОЧНИКОВ ЭНЕРГИИ ДЛЯ ЭНЕРГОСНАБЖЕНИЯ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: возобновляемые источники энергии, электроснабжение, средства мобильной связи, автоматизированная база данных, солнечные и ветровые энергетические установки.

Предложено применение автоматизированной базы данных для решения задачи выбора места размещения солнечных и ветровых энергоустановок, обеспечивающих энергоснабжение средств мобильной связи. При этом используются статистические данные о среднегодовой скорости ветра и распределении вероятности скорости ветра, а также продолжительности солнечного света. На примере Ростовской области показано, что наибольший поток ветровой энергии наблюдается с ноября по апрель, а наибольшая солнечная активность - с марта по ноябрь, что доказывает целесообразность использования комбинированных солнечно-ветровых энергетические установок для гарантированного автономного электроснабжения средств мобильной связи.

M.A. Elfimov, N.A. Reznichenko,
A.V. Pozdnyakova, N.V. Rudenko, S.V. Ivanov

CHOICE OF THE LOCATION OF RENEWABLE SOURCES ENERGY FOR POWER SUPPLY OF MEANS OF MOBILE COMMUNICATION

Don State Technical University, Rostov-on-Don, Russia

Keywords: renewables, power supply, means of mobile communication, the automated database, solar and wind power installations.

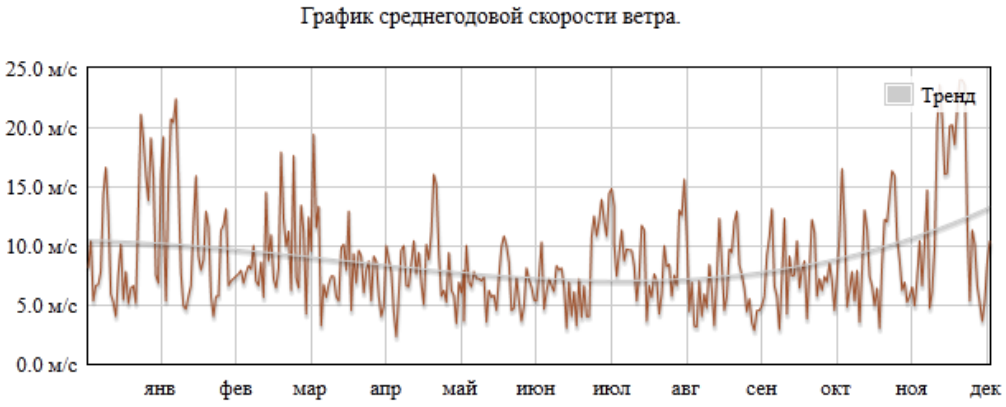
Application of the automated database for the solution of a problem of a choice of a location of the solar and wind power installations providing power supply of means of mobile communication is offered. Thus statistical data on the average annual speed of a wind and distribution of probability of speed of a wind, and also sunlight duration are used. On the example of the Rostov region it is shown that the greatest stream of wind energy is observed from November to April, and the greatest solar activity - from March to November that proves expediency of use of the installations combined solar and wind power for the guaranteed autonomous power supply of means of mobile communication.

Постановка задачи. Одним из перспективных путей надежного электроснабжения автономных объектов мобильной связи (сотовых базовых станций, мобильных коммутаторов, систем беспроводной связи с антеннами радио и сотового сигнала, приемопередатчиков и др.), удалённых от Госэнергосистемы, является применение электроэнергетических установок, использующих энергию ветра и солнца. Ресурсный потенциал возобновляемых источников энергии в России составляет порядка 5 млрд. т условного топлива в год, а экономический потенциал в самом общем виде достигает не менее 270 млн. т условного топлива [1]. В связи с этим задача выбора места размещения солнечных (СЭУ) и ветровых (ВЭУ) энергетических установок, обеспечивающих энергоснабжение средств мобильной связи (СМС) является актуальной.

Материалы исследования. Задача формулируется следующим образом. Обосновать выбор места размещения солнечных и ветровых энергетических установок для электроснабжения СМС с суммарной мощностью электроприёмников до 5 кВт [2, с.44; 3, с.395]. В качестве прототипа может быть выбрана ВЭУ на базе трехфазного генератора с постоянными магнитами со следующими техническими характеристиками [4, с.116; 5]:

- номинальной мощностью - 5 кВт;
- максимальная мощность - 7 кВт;
- начальная скорость ветра - 3 м/с (на высоте мачты 9 м);
- рабочий диапазон скорости ветра - от 3 м/с до 25 м/с;
- среднегодовая эффективная скорость ветра - 4 м/с;
- номинальная скорость ветра - 10 м/с.

С целью обоснования возможности и применения выбранной ВЭУ может быть использован Интернет-ресурс [6], который является автоматизированной базой данных, позволяющей получить данные о климате различных городов России в табличной или графической форме. Так для региона г. Ростова-на-Дону могут быть получены графики среднегодовой скорости ветра и распределения вероятности скорости ветра (Рисунок 1).



а)

б)

Рисунок 3. Графики среднегодовой скорости ветра (а) и распределения вероятности скорости ветра (б) в 2012 году

Анализ аналогичных графиков за 5 лет позволяет сделать следующие выводы:

- средняя наиболее вероятная скорость ветра за 5 лет составляет 7,2 м/с, что выше эффективной (4 м/с) скорости ветра; это свидетельствует о том, что в регионе г. Ростова-на-Дону эффективно применение выбранной ВЭУ;
- наибольшая скорость ветра, а, следовательно, вырабатываемая энергия может быть получена с ноября по апрель;
- поскольку возможная вырабатываемая мощность пропорциональна кубу скорости ветра [1], то с учётом номинальных характеристик выбранной ВЭУ и средней вероятной скорости ветра за 5 лет (7,2 м/с) можно рассчитать, что возможная средняя вырабатываемая мощность составит около 1,9 кВт.

Следовательно, для гарантированного энергоснабжения СМС с суммарной мощностью приёмников до 5 кВт в регионе г. Ростова-на-Дону целесообразно дополнительно использовать СЭУ, в качестве прототипа которой может быть выбрана установка со следующими характеристиками [4, с. 118; 7]:

- номинальная мощность солнечной генерации - 5 кВт;
- пиковая мощность потребления - 5 кВт;
- запас энергии - 10 кВт* ч;
- номинальное напряжение системы - 96 В;
- средняя производительность в месяц - 650 кВт *ч;
- совместимость с ветрогенератором - 96 В, 2 кВт.

Стандартная система солнечных батарей автономного электроснабжения состоит из солнечных панелей общей мощностью 5 кВт. Подобная система позволяет надежно обеспечить потребности в электричестве приёмники СМС. В месяц эта система вырабатывает в среднем от 500 до 1000 кВт*ч, что достаточно для работы любых электроприборов в нормальном режиме использования [8].

Известно, что для нормальной работы солнечных батарей СЭУ необходимо получать солнечный свет на протяжении 6-7 часов [9]. С помощью указанного Интернет-ресурса [6] может быть получен график средней продолжительности солнечного света в Ростовской области (Рисунок 2) в течение года.

Рисунок 2. График продолжительности солнечного света (горизонтальная линия соответствует уровню солнечной активности для нормальной работы солнечных батарей)

Анализ полученного графика позволяет сделать следующие выводы:

- среднегодовая продолжительность солнечного света составляет 9 часов, что позволяет использовать СЭУ как основной источник энергии в регионе;
- наибольшая солнечная активность, а, следовательно, вырабатываемая энергия может быть получена с марта по ноябрь.

Общие выводы:

1. Использование информационных технологий позволяет оценить целесообразность размещения солнечных и ветровых энергетических установок, оценить ожидаемые потоки энергии по месяцам года, а, следовательно, определить приоритетные потоки энергии, принципы управления и конструкции комбинированных солнечно-ветровых энергетических установок.
2. В Ростовской области наибольший поток ветровой энергии наблюдается с ноября по апрель, а наибольшая солнечная активность - с марта по ноябрь, следовательно, здесь целесообразно использовать комбинированные солнечно-ветровые энергетические установки для гарантированного автономного электроснабжения СМС.
3. Предложенный подход к использованию информационных ресурсов для выбора места размещения солнечных и ветровых энергетических установок может быть применен для любой точки планеты.

Литература:

1. Развитие электроэнергетики в России [Электронный ресурс] // Биофайл [сайт] URL: http://biofile.ru/geo/15479. (дата обращения 2.12.2014 г.)

2. Rudenko N.V., Sukiyazov A.G., Shokova Yu.A. Adaptive control efficiency enhancement for hybrid solar-wind energy farms // 7th International Scientific Conference Science and Society. Held by SCIEURO in London. 25-26 November 2014. P.43-50.

3. Руденко Н.В. [и др.] Энерго- и ресурсосбережение на основе использования комбинированной солнечно-ветровой энергетической установки с адаптивным управлением // Инновации, экология и ресурсосберегающие технологии (ИнЭРТ-2014) [Электронный ресурс]: труды XI международного научно-технического форума / ДГТУ; под ред. А.Д. Лукьянова — Ростов н/Д: ДГТУ, 2014. С. 394-399. Электрон, опт. диск (CD-ROM).

4. Руденко Н.В. [и др.] Применение информационных технологий для выбора места размещения солнечных и ветровых энергетических установок // Наука и образование в жизни

современного общества: сборник научных трудов по материалам Международной научно-практической конференции 30 декабря 2014 г.: в 12 частях. Часть 5. Тамбов: ООО «Консалтинговая компания Юком», 2015. С. 115-120

5. Ветрогенератор 5 КВт [Электронный ресурс] // Биофайл [сайт] URL: http://www.amteh.com/ (дата обращения 07.03.2015 г.)

6. Климатический справочник [Электронный ресурс] // Биофайл [сайт] URL:http://atlas-yakutia.ru/weather/spravochnik/wdsp/climate_sprav-wdsp_3173502142.php (дата обращения 07.03.2015 г.)

7. Солнечная энергия [Электронный ресурс] // Биофайл [сайт] URL: http://solnce-generator.ru/nedostatki-solnechnyx-batarej/ (дата обращения 07.03.2015 г.)

8. Свет-ДВ [Электронный ресурс] // Биофайл [сайт] URL: http://svetdv.ru/sun/price.shtml/ (дата обращения 07.03.2015 г.)

9. РИА наука [Электронный ресурс] // Биофайл [сайт] URL: http://ria.ru/science/20141113/1033215507.html#ixzz3MjTdXUYA/ (дата обращения 09.03.2015 г.)

В.В. Земляков, А.В. Еремеев

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПРОВЕДЕНИЯ ИЗМЕРЕНИЙ С ПРИМЕНЕНИЕМ СЕНСОРНОГО НАПОЛНЕНИЯ СОВРЕМЕННЫХ МОБИЛЬНЫХ УСТРОЙСТВ

Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: лабораторные установки, мобильные измерительные системы, Windows Phone, технология Sensor Fusion.

Реализовано программное обеспечение, имитирующее работу лабораторной установки для измерения коэффициента трения с помощью мобильного телефона.

V.V. Zemlyakov, A.V. Yeremeev

SOFTWARE DEVELOPMENT FOR THE MEASURMENT USING THE SENSOR FILLING MODERN MOBILE DEVICES

Southern Federal University, Rostov-on-Don, Russia

Key words: laboratory facilities, portable measurement system, Windows Phone, Sensor Fusing technology.

Implemented software that simulates laboratory apparatus for measuring the coefficient of friction by using mobile phone.

Мало кто в современном мире представляет жизнь без мобильных устройств. За последние пятнадцать лет они плотно внедрились в повседневность, став ее неотъемлемой частью. Мобильные телефоны стали незаменимыми и полезными помощниками как для деловых людей, так и для тех, чья работа никак не связана с переговорами. Мобильные устройства существенно отличаются от прежнего традиционного представления о персональных компьютерах, и все больше мобильных устройств на данный момент стали оснащаться различными датчиками. Это делает возможным использование мобильных телефонов и планшетных компьютеров в сфере образования в качестве измерительных установок.

Например, в устройствах, работающих под управлением операционной системы Windows Phone 8 основными датчиками, присутствующими практически в каждом мобильном устройстве, являются датчик освещенности, акселерометр и гироскоп [1]. Используя набор базовых датчиков можно построить программное обеспечение (ПО), которое позволит использовать мобильное устройство как лабораторную установку. Таким образом, для проведения лабораторных работ

студенту достаточно всего лишь иметь с собой смартфон, на котором предустановлено соответствующее ПО. Необходимость в дорогостоящем оборудовании для проведения лабораторных работ в такой ситуации исчезает.

Рассмотрим пример реализации лабораторной установки, моделирующей процесс скольжения тела по наклонной плоскости. По результатам моделирования студенту необходимо проанализировать зависимость коэффициента трения от угла наклона. Программный продукт был реализован на базе мобильной операционной системы Windows Phone 8.1 с использованием языка C# и платформы .NET Framework.

Пользовательский интерфейс приложения условно поделен на пять страниц.

MainPage – главная навигационная страница приложения. Из нее осуществляется переход к другим страницам приложения. Run – главная вычислительная страница. В ее пределах выполняются все вычислительные процедуры. Results – страница с результатами измерений. Переход на нее становится возможным только по окончанию измерительного процесса. Theory – информационная страница с описание лабораторной работы. About – информационная страница, содержащая контактные данные и описательную информацию о приложении.

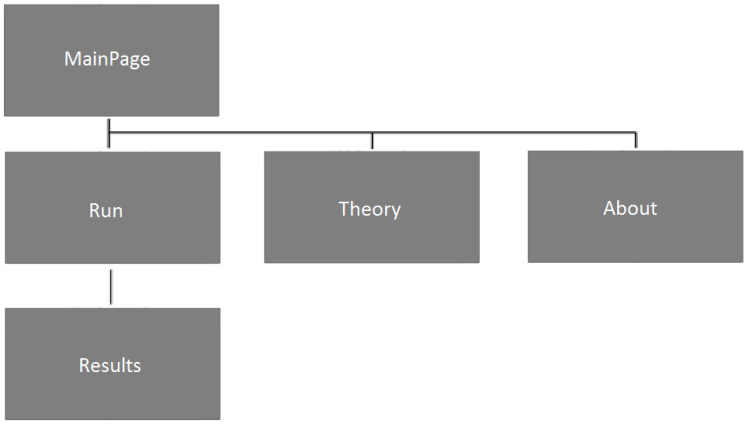


Рисунок 1. Граф страниц приложения, моделирующего лабораторную установку

Результатом каждого вычислительного цикла являются три значения: угол наклона плоскости α, коэффициент трения μ и время проведения опыта t.

Теоретически, угол наклона относительно плоскости можно было бы рассчитать, используя показания акселерометра напрямую. Однако, в операционных системах Windows 8 и Windows Phone 8, помимо физических датчиков (т.е. реальных сенсоров, находящихся на борту мобильного устройства), существуют, так называемые, «виртуальные датчики». Это программно реализованные датчики, показания которых основаны на комбинировании показаний нескольких «физических датчиков». Одним из примеров таких датчиков является «Инклинометр» [2].

Инклинометр (от лат. incline — наклоняю) — это прибор, предназначенный для измерения угла наклона относительно гравитационного поля Земли. Показания инклинометра рассчитываются на основе информации от акселерометра, гироскопа и магнитометра с помощью механизма под названием Sensor Fusion [2] (Рисунок 2). Если хотя бы одного из перечисленных трех физических сенсоров нет, инклинометр не будет доступен.

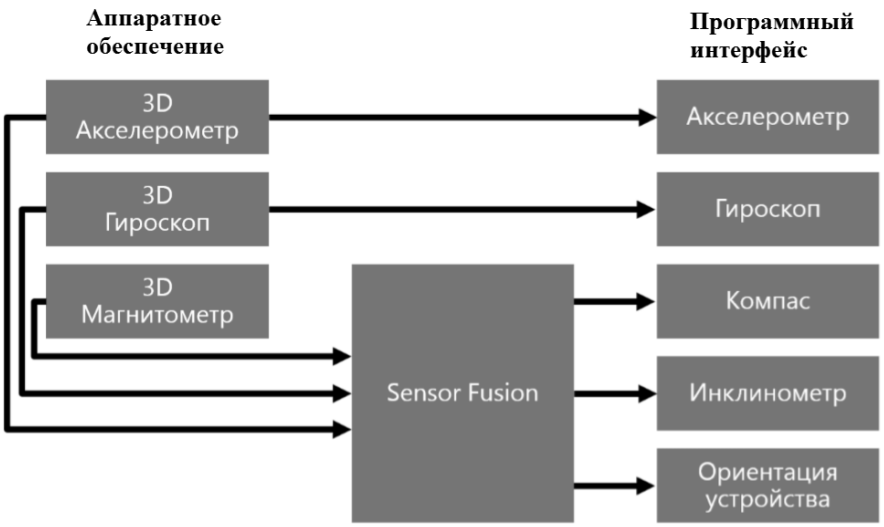


Рисунок 2. Механизм Sensor Fusion

Таким образом, расчет величины угла наклона сводится к запросу соответствующего параметра, с последующим получением значения его модуля:

$$\alpha = |\alpha_{Roll}|\,, \tag{1}$$

где α_{Roll} – значения параметра Roll инклинометра.

Расчет коэффициента трения производится на основе показаний акселерометра.

Уравнение движения тела по наклонной плоскости имеет вид:

$$ma = mg * \sin(\alpha) - F_{\text{тр}}, \tag{2}$$

где m – масса тела; a – ускорение вдоль наклонной плоскости; g – ускорение свободного падения; α – угол наклона плоскости; $F_{\text{тр}}$ – сила трения.

Силу трения можно представить, как:

$$F_{\text{тр}} = \mu * N, \tag{3}$$

где μ - коэффициент трения; N – реакция опоры.

Формула для вычисления реакции опоры имеет вид:

$$N = mg * \cos(\alpha). \tag{4}$$

Выполним подстановку и выразим коэффициент трения:

$$\mu = \frac{g*\sin(\alpha)-a}{g*\cos(\alpha)}. \tag{5}$$

Для вычисления коэффициента трения необходимо определить величину a, которая является результирующей векторов ускорений вдоль двух осей:

$$a = \sqrt{a_x^2 + a_z^2}, \tag{6}$$

где a_x – значение ускорения, полученное с акселерометра вдоль оси x (в плоскости телефона); a_z – значение ускорения, полученное с акселерометра вдоль оси z (перпендикулярно плоскости телефона).

Расчет времени проведения опыта сводится к программной фиксации начала опыта и его окончания:

$$t = t_{\text{н}} - t_{\text{о}}, \tag{7}$$

где $t_{\text{н}}$ – время начала опыта; $t_{\text{о}}$ – время окончания опыта.

На текущем этапе развития цифровой электроники обилие мобильных устройств, оснащенных разнообразными датчиками, открывают совершенно новое направление для построения портативных информационных измерительных систем. На данный момент на базе мобильных устройств можно как конструировать макеты лабораторных работ, так и сооружать полноценные мобильные системы сбора и обработки данных, функционирующих в реальном времени, таких как системы измерения уровня шума, бесконтактные амперметры и многие другие.

Литература:

1. Э. Троелсен Язык программирования C# 5.0 и платформа .NET Framework 4.5 // Вильямс. – 2013. – С. 231 - 455

2. Кичинский К., Пугачев С., Шериев А. Разработка приложений для Windows 8 на языке C# // ВХБ-Петербург. – 2013. – С. 275-288

Е.В. Еремеева

РАСЧЕТ ОПТИМАЛЬНОГО РАДИУСА СОТЫ СЕТИ UMTS ДЛЯ ГОРОДСКОГО РАЙОНА

Донецкий национальный технический университет, г. Донецк

Ключевые слова: модели распространения радиоволн, Уолфиш-Икегами, UMTS, радиус, сота, затухание, расчет.

В статье рассматривается проблемы проектирования мобильных сетей третьего поколения в условиях городской застройки. Проведен краткий сравнительный анализ таких моделей распространения радиоволн как модели Уолфиша-Икегами и Окамура-Хата. На примере Ворошиловского района г. Донецка (Украина) предложен один из возможных вариантов расчета оптимального радиуса соты на основе модели Уолфиша-Икегами, с учетом баланса мощностей на линиях “uplink” и “downlink”. Также дана рекомендация по оптимизации расположения базовых станций на основе полученного результата (радиуса).

E.V. Eremeeva

CALCULATION OF THE OPTIMAL CELL RADIUS UMTS NETWORK FOR URBAN AREA

Donetsk national technical University, Donetsk

Keywords: models of radiowave propagation, Walfish-Ikegami, UMTS, radius, cell, attenuation.

The article considers the problem of designing mobile networks of the third generation in urban conditions. Conducted a brief comparative analysis of such models of radio wave propagation, as models Wafish-Ikegami and Okamura-Hata. One of the possible variants of the calculation of the optimal cell radius in Voroshilovskiy district, Donetsk (Ukraine) based on the model of Walfish-Ikegami, with the balance of capacity on the lines of “uplink” and “downlink”. Also a recommendation for optimizing the location of base stations based on the received result (radius).

Развитие технологий способствует решению одной проблемы и параллельно возникновению другой. Так, например, развитие технологии строительства позволяет возводить многоэтажные комплексы (жилые дома, офисные здания). Это способствует решению проблемы жилья для населения и экономии места в городе. Однако, высокие здания являются препятствием для распространения радиоволн, что приводит к ухудшению связи и необходимости монтирования большего количества антенн. Последнее в свою очередь приводит к возрастанию стоимости связи. Задача проектирования сети связи усложняется из-за неравномерности высоты зданий, когда среди малоэтажных кварталов вырастают высотные здания. Здесь-то и возникает проблема неравномерной застройки.

Проектирование сети в условиях городской застройки - это трудоемкая задача. Здесь приходится учитывать ряд специфических факторов, таких как неравномерность рельефа, неравномерность застройки, наличие подвальных помещений (бары, подземные парковки), зеленые насаждения. Помимо этого необходимо также учитывать погодные условия, наличие достопримечательностей, а также электромагнитную обстановку, плотность населения и т.д. Чтобы учесть большинство вышеперечисленных проблем инженерами были предложены различные модели распространения радиоволн (Окамура-Хата, Уолфиш-Икегами, Ли, их модификации и т.п.)

В статье рассматривается возможность использования моделей распространения радиоволн для расчета оптимального радиуса сети третьего поколения в условиях городской застройки.

В качестве территории для проектирования был выбран Ворошиловский район города Донецка Донецкой области (Украина). С точки зрения проектирования имеются такие проблемы как: большое количество населения на сравнительно маленькой площади (приблизительно 95 000 человек на 10 км²), неравномерная застройка (от жилых пятиэтажек до современных офисных гигантов), хаотичное расположение зданий по району, наличие зеленых насаждений, хотя по сравнению со зданиями их процент очень мал. Также существенной проблемой является неравномерность рельефа: с востока на запад разница в высоте составляет 52 м, а с севера на юг – 44м.

В качестве основы для расчетов выбрана модель Уолфиша-Икегами [2], т.к. эта модель учитывает следующие параметры: высоту подъема базовой станции (антенны), высоту подъема мобильной станции, высоту близлежащих к базовой станции зданий, частоту, ориентацию улицы относительно направления прихода сигнала, расстояние между домами по ходу направления радиоволны, ширину улиц. Другой возможной моделью для расчетов могла быть выбрана модель Окамура-Хата [3], в которой, однако, используются только высоты подъема базовой станции (антенны), мобильной станций и загрождающего здания. В то же время модель Уолфиша-Икегами, в отличие от остальных моделей, позволяет учитывать возможность прихода волны в точку приема несколькими маршрутами с последующим сложением.

На основании анализа рельефа местности Ворошиловского района города Донецка было выбрано расположение трех базовых станций (БС) с координатами:

1. Высотное здание, проспект Панфилова (48°01'12,46" С, 37°47'15,85" В);
2. Высотное здание, улица Университетская (48°00'48,07" С, 37°47'52,62" В);
3. Гостиничный комплекс «Столичный», проспект Богдана-Хмельницкого (48°00'43,33" С, 37°48'18,08").

При выборе их месторасположения учитывались плотность и этажность застройки по плану генерального развития района, а также плотность населения района, рельеф.

Для начала с помощью модели Уолфиша-Икегами рассчитывается медианное затухание для каждой базовой станции. В результате расчета получены данные, представленные в таблице 1:

Таблица 1. Результаты расчета медианного затухания

	БС 1	БС 2	БС 3
L0,дБ	92,45	92,45	92,45

При расчете покрытия сети UMTS для городского района необходимо учитывать ограничения, которые влияют на радиус покрытия. Для линии “downlink” главным ограничением является мощность передатчика базовой станции, иногда значительно уменьшаемая за счет потерь в антенно-фидерном устройстве (АФУ). На линии “uplink” ограничением для увеличения радиуса соты является недостаточная чувствительность приемника. Следовательно, искомое решение должно учитывать сбалансированность мощности на линии “uplink” и “downlink” [1]

Для расчета мощностей линий воспользуемся выражением (1):

$$P_{inMS} = P_{outBTS} - V - L_{CBTS} + L_{FBTS} + G_A^{BTS} - L_p - I + G_A^{MS} - L_{CMS} \quad \text{дБ}, \qquad (1)$$

где P_{inMS} – мощность на входе мобильного терминала, дБмВт;

P_{outBTS} – максимальная мощность на выходе базовой станции, дБмВт.

V – регулирование мощности снижением ее уровня, дБ;

L_{CBTS} – потери в изоляторе, комбайнере, фильтре на базовой станции, дБ ;

L_{FBTS} – потери в фидере и соединителях на базовой станции, дБ;

G_A^{BTS} – коэффициент усиления антенн базовой станции, дБ;

L_p – потери на трассе downlink, дБ;

G_A^{MS} – коэффициент усиления мобильного терминала, дБi;

L_{CMS} – потери в изоляторе, комбайнере и фильтре в мобильной станции, дБ;

L_{FMS} – потери в фидере и соединителях в мобильном терминале, дБ;

I – запас на покрытие в зданиях (замирания и взаимные препятствия), дБ.

Из этой формулы получаем выражения для расчета потер на трассах “uplink” и “downlink” (2):

$$L_p = P_{inMS} - P_{outBTS} + V + L_{CBTS} - L_{FBTS} - G_A^{BTS} + I - G_A^{MS} + L_{CMS} \quad (2)$$

Полученные результаты представлены в таблице 2:

Таблица 2. Результаты расчета потерь на трассах “uplink” и “downlink”

L_p 1, дБ	-51,36
L_p 2, дБ	-17,55

В результате проведения расчета баланса мощности, было получено допустимое значение затухания сигнала на трассе, Подставив данное значение в формулу Уолфиша-Икегами, рассчитывается радиус соты по формуле (3):

$$d = 10^{L_b + L_p - 32{,}4 + 16{,}9 - k_a - (30 + k_f)\lg(f) + 10\lg(w) - 20\lg(h_r - h_2) - L_{cri} + 18\lg(1 + h_1 + h_r) + 9\lg(b)/(20 + k_f)} \quad (3)$$

При расчете радиуса соты зададимся следующими условиями:

Пусть Lrts+ Lmsd ≥ 0 и h1> hr, тогда Lbch=–18·lg(1+ h1- hr), а ka= 54. Тогда kf = –4+1.5·(f/925–1), kd = 18.

Затухание сигнала, обусловленное направлением прихода луча, максимальное при ϕ=55°, тогда потери, обусловленные ориентацией улиц относительно направления прихода сигнала, определяются по выражению Lcri = 4.0–0.114·(ϕ –55), 55°≤ ϕ ≤90°, дБ.

Таким образом, получаем следующую формулу (4) для расчета радиуса соты и полученный результат занесем в таблицу 3:

$$d = 10^{(L_b + L_p - 65{,}5 - (26 + 1{,}5(\frac{f}{925} - 1))\lg(f) + 10\lg(w) - 20\lg(h_r - h_2) + 18\lg(1 + h_1 + h_r) + 9\lg(b)/(16 + 1{,}5(\frac{f}{925} - 1)))/20} \quad (4)$$

Таблица 3. Результаты расчета

	БС 1	БС 2	БС 3
d, км	0,783	0,79307	0,68561

Для сети UMTS возможна расстановка базовых станций через 1-2 км, но из таблицы видно, что радиус соты для БС1 равен 793 м, для БС 2 – 793 м и для БС 3 – 685 м. Такой результат получен из-за того что сеть проектируется в городе и на нее «наложено» множество ограничений, которые учитывает модель Уолфиша-Икегами. Территориально базовые станции находятся недалеко друг от друга, однако подобная расстановка антенн компенсирует проблему высокой плотности населения и неравномерности рельефа и застройки.

В дальнейшем, используя радиус соты можно оптимизировать расположение базовых станций путем использования алгоритмов оптимизации, в частности генетические алгоритмы.

Литература:

1. Сундучков К. С. «Методика определения оптимальной топологии сети GSM для городского микрорайона» / К. С. Сундучков, М. А. Мальчук, Л. С. Кобзарь – Наукові записки УНДІЗ - 2008

2. В. А. Утц «Исследование потерь при распространении радиосигнала сотовой святи на основе статистиеских моделей» / В. А. Утц // Вестник Балтийского государственного университета им. Канта. – 2011. – вып. 5. – С. 44-49.

3. Нестеренко А. С. «Применение модели распространения волн Окамура-Хата» / Нестеренко А. С., Паслен В. В. // Международная научно-практическая конференция «Человек и космос» - 2009. Тези доповідей. – Дніпропетровськ: НЦАОМ им. А. М. Макарова, 2009.

Х.Н. Зайнидинов, Э.Ш. Назирова

ПАРАЛЛЕЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СТРУКТУРА НА ОСНОВЕ КУБИЧЕСКИХ БАЗИСНЫХ СПЛАЙНОВ

Ташкентский университет информационных технологии, г. Ташкент, Узбекистан

Ключевые слова: классические полиномы, алгоритм Горнера, параболические сплайны, B-сплайны, кубических сплайны.

В данной статье рассмотрена максимальная погрешность округления при аппроксимации сплайном второй степени приблизительно в четыре разе меньше, чем соответствующая погрешность при аппроксимации классическим полиномом второй степени, а также высокопроизводительные вычислительные структуры, основанные на применении таблично-алгоритмического метода обработки и базисной сплайн – аппроксимации, отличающиеся высоким быстродействием.

X.N. Zaynidinov, E.Sh. Nazirova

PARALLEL COMPUTING STRUCTURES ON THE BASIS OF CUBIC BASIC SPLINES

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: classical polynomials, Horner's algorithm, parabolic splines, B-splines, cubic splines.

This article describes the maximum rounding error in the approximation of second-degree spline approximately four raze smaller than the corresponding error in the approximation of classical polynomial of the second degree, as well as high-performance computing structures based on the use of table-algorithmic processing method and basic spline - approximation characterized by a high performance.

Традиционные таблично-полиномиальные методы аппроксимации сложных функциональных зависимостей имеют ограничения по точности, гладкости и не позволяют существенно распараллелить вычислительные структуры для реализации аппроксимации классическими полиномами по алгоритму Горнера [1-3]. Например, полином второй степени по алгоритму Горнера может быть представлен в виде:

$$P_2(x) = a_2x^2 + a_1x + a_0 = ((a_2x + a_1)x + a_0) \quad (1)$$

Использование для аппроксимации функций параболических базисных B-сплайнов позволяет улучшить свойства гладкости и локальности [5, 161].

Также как в случае полинома второй степени, классический полином третьей степени по схеме Горнера может быть представлен в виде:

$$P_3(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = (((a_3x + a_2)x + a_1)x + a_0) \quad (2)$$

Согласно формуле (2) значение интерполируемой функции в произвольной точке заданного интервала определяется значениями лишь m+1 слагаемых – парных произведений базисных функций на постоянные коэффициенты. Например, кубические *B*-сплайны требуют четырех базисных слагаемых.

Значение функции вычисляется по формуле

$$f(x) \cong S_3(x) = b_{-1}B_{-1}(x) + b_0B_0(x) + b_1B_1(x) + b_2B_2(x) \text{ при } x \in [0,1] \quad (3)$$

Остальные базисные сплайны на этом подинтервале равны нулю и, следовательно, в образовании суммы не участвуют.

Для вычисления *b*-коэффициентов существуют разные методы: интерполяционные и «точечные» формулы, сглаживающие сплайны, метод наименьших квадратов. Однако, для систем функционирующих в реальном масштабе времени следует использовать «точечные» формулы. Особенность этих методов заключается в независимости значения аппроксимирующего сплайна на данном участке от значений экспериментальной функции, удалённых от этого участка. Для кубических сплайнов также приведем «точечные» формулы в готовом виде:

1. *Трёхточечная формула*, в этом случае для вычисления коэффициента участвуют r-1, r и r+1 –ые значения функции

$$b_r = \frac{1}{6}(-f_{r-1} + 8f_r - f_{r+1}) \quad (4)$$

2. *Пятиточечная формула*, в этом случае для вычисления коэффициента участвуют r-2, r-1, r, r+1 и r+2 –ы значения функции

$$b_r = \frac{1}{36}(f_{r-2} - 10f_{r-1} + 54f_r - 10f_{r+1} + f_{r+2}) \quad (5)$$

здесь f_r сокращенная форма записи- $f_r(x)$.

Методическая погрешность интерполяции функции $f(x)$ кубическими базисными сплайнами определяется неравенством:

$$\varepsilon \le \frac{5}{384}h^4 \max\left|f^{IV}(x)\right| \quad (6)$$

для функции $f(x) = \ln(1+x)$, получим

$$\varepsilon \le \frac{5}{384 \cdot 1{,}0 \cdot 32^4} = 0{,}12 \cdot 10^{-7} \quad (7)$$

Для сравнения приведем значение погрешности интерполяции классическими кубическими полиномами Ньютона:

$$\varepsilon \le \frac{1}{24}h^4 \max\left|f^{IV}(x)\right| = \frac{1}{24 \cdot 32^4 \cdot 1{,}0} = 0{,}4 \cdot 10^{-7} \quad (8)$$

Как видно из (8), погрешность превышает величину, полученную в (7), более чем в три раза.

Структурная схема состоит из регистра аргумента, запоминающего устройства коэффициентов (ЗУК), запоминающего устройства (ЗУ) базисных функций и выходного сумматора-накопителя. накапливающих сумматоров. Для выборки различных четырех значений *B*-сплайнов с целью суммирования потребуются четыре подсекции, в каждой из которых должна храниться часть кривой *B*-сплайна, заданная на одном участке.

В случае параболических сплайнов, задание адреса группы из четырех значений базисных сплайнов требует лишь двух дополнительных двоичных разрядов, с помощью которых определяется, какому из четырех участков носителя [-2, 2] основного базисного сплайна принадлежат значения B_{-1}, B_0, B_1 и B_2 . Одно и тоже подслово адреса, задающее участок длиной h=1, может быть использовано для выборки значений базисных сплайнов в каждой из четырёх подсекций ПЗУ, которым можно присвоить следующие адреса:

11 для B_{-1} $x \in [-2, -1)$;
00 для B_0 $x \in [-1, 0)$;
01 для B_1 $x \in [0, 1)$;
10 для B_2 $x \in [1,2)$.

Для подтверждения справедливости вывода о приемлемости аппаратурных затрат в виде памяти и слабом увеличении их с возрастанием числа одновременно воспроизводимых в одном устройстве функций разобьем весь интервал задания произвольной многократно дифференцируемой функции $f(x)$ на участки при $n=2^p$, где p-целое число. Тогда, если двоичный код аргумента содержит l разрядов, то на один участок аппроксимации придется 2^{i-1} значений элементов таблицы базисного сплайна, а общий объем таблицы определяется по формуле:

$$Q=4\bullet 2^{l-1-p}=2^{l-p+1} \quad (9)$$

Ввиду четности базисного сплайна в памяти можно записать только половину таблицы, например для диапазона аргумента [0,2).

Если n=32, а l=16 двоичных разрядов, то $Q=2^{16}-2^5=2048$ слов может быть реализовано с помощью одной или двух микросхем. Емкость ЗУ коэффициентов при пересчете на одну функцию составит $n+2m+1$ слов.

Перестройка на новый вид функциональной зависимости осуществляется простым переключением коэффициентов на новую область ЗУ. При занесении базисных функций в ПЗУ алгоритм преобразования является, по существу, линейным. Параллельная структура может наращиваться в случае необходимости повышения степени базисного сплайна. Однако это приводит к усложнению вывода информации из памяти и увеличению числа умножителей.

Таким образом, основным достоинством структуры является высокое быстродействие, практически предельное для таблично-алгоритмических методов.

Литература:

1. Zaynidinov H.N., Jovliev S. Modeling Specialized Processor Signal Processing Based on Haar Wavelet. Proceedings of International Conference on IT Promotion in Asia 2011, September, 26-27, 2011, p. 314-318, Tashkent, Uzbekistan

2. Zaynidinov H., Bahramov S., Nishonboyev G. Modeling Specialized Processor Signal Processing Based on Hermit spline. Proceedings of International Conference on IT Promotion in Asia 2011, September, 26-27, 2011, p. 228-232, Tashkent, Uzbekistan.

А.П. Зверев, *И.П. Рыбалко, *Н.В. Болдырихин

ВЫБОР ПУТИ И РАСПРЕДЕЛЕНИЕ СИЛ, СРЕДСТВ И СИСТЕМ СВЯЗИ ПРИ СОВЕРШЕНИИ МАРША ДЛЯ УСТРАНЕНИЯ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ

Академия Гражданской Защиты МЧС России, г. Химки
*Северо - Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону

Ключевые слова: чрезвычайная ситуация, перераспределение ресурсов, принятие решения, спасательные формирования, модернизированный метод Хакими, контейнер с материально-техническими средствами.

Описана проблема принятия обоснованного решения на организацию марша для ликвидации чрезвычайной ситуации в условиях информационной неопределённости относительно кратчайших и оптимальных маршрутов движения колонн, а также времени получения со складов материально-технических средств и средств связи.

Для решения проблемы выбора маршрута движения предложено использовать модернизированный алгоритм Хакими и метод Севеджа. Повышение скорости получения материальных средств возможно за счёт созданных заранее запасов укомплектованных контейнеров, количество которых должно хватить для первой колонны спасателей.

A.P. Zverev, *I.P. Rybalko, *N.V. Boldyrikhin

THE CHOICE AND DISTRIBUTION OF FORCES, MEANS AND SYSTEMS OF COMMUNICATION WHEN MAKING STAIRS FOR EMERGENCY RELIEF

Civil defence Academy of EMERCOM of Russia, Khimki
*North - Caucasian branch of the Moscow technical University
communications and computer science, Rostov-on-don

Keywords: emergency, reallocation of resources, decision making, rescue, modernized method Hakimi, the container with the material and technical means.

Describes a problem making an informed decision on the organization of the March for liquidation of emergency situations in the conditions of information uncertainty about the shortest and best routes columns and time of receipt from the warehouse logistical and means of communication.

To solve the selection of routes proposed to use the modernized Hakimi algorithm and the method of Sewege. To increase the speed of money probably due to pre-stocked inventory of containers, the number of which should be enough for the first column of the rescuers.

В результате воздействия чрезвычайных обстоятельств, на значительных территориях сложится крайне сложная обстановка, характеризующаяся нарушением работы системы связи, негативными изменениями в качестве и доступности дорожной сети, трудностями в распределении имеющихся ресурсов, необходимых для ликвидации чрезвычайной ситуации (ЧС), что приведёт к увеличению времени прибытия спасательных формирований в зону ликвидации ЧС.

Существующая система реагирования на ЧС не в полной мере учитывает информационную не определенность, появляющуюся в связи с выше указанным. Из-за этого приобретает особое значение устойчивость управления, скорость принятия решения и время прибытия сил и средств в зону ликвидации ЧС (Lлчс). Таким образом, развитие теоретических основ принятия решения в условиях неопределенности и разработка методов прибытия спасательных формирований в зону ЧС в минимальные сроки, а также перераспределение сил и средств для проведения спасательной операции является актуальной задачей.

Решение выше указанной задачи (Lлчс) является сложной многофункциональной зависимостью, в общем виде её можно представить в виде (1).

$$Lлчс = f(Tп.р(Tп(Tк(Vс.д(Tм(I(x))))))) \quad (1)$$

В приведённой формуле (1) ликвидация последствий ЧС представлена параметрами:

Тп.р - времени принятия решения на ликвидацию чрезвычайной ситуации;

Тп - времени подготовки к маршу спасательных формирований для убытия в зону ликвидации последствий - время прибытия спасателей к местам, погрузки на транспорт для доставки формирований к месту ЧС;

Тк – время комплектования, которое включает время сбора необходимых материально-технических средств необходимых для устранения ЧС;

Vс.д - скорости движения колонн;

Тм – времени выполнения марша колонами;

I – изменения вызванные влиянием последствий чрезвычайных обстоятельств на время осуществления марша, проявляющиеся в изменении проходимости дорог и местности.

Проанализировав выявленные параметры можно выявить несколько общих составляющих для большинства из них.

Время принятия решения включает в себя время разработки плана ликвидации ЧС, который невозможно составить не имея, во-первых, точного маршрута движения колонн, а во-вторых, точного времени требуемого для комплектования материальными средствами.

Для решения первой проблемы штаб спасательной операции должен определиться со скоростью движения и маршрутом.

Скорость движения напрямую зависит от того, насколько сильно пострадало дорожное покрытие от воздействия ЧС.

Время выполнения марша зависит как от скорости движения, так и от выбранного маршрута движения. Оно определяется в соответствии с каким-либо критерием: оптимальный или кратчайший путь к месту ЧС.

Выбрать критерий можно получив и точно оценив последствия влияния воздействий ЧС на местность - I.

На данный момент, принятие решения о выборе критерия маршрута осуществляется на основе интуиции и знаний специалистов. Такой подход имеет недостаток - сильное влияние человеческого фактора. Для устранения этого фактора необходимо применение программных продуктов поддержки принятия решения командира.

Особенность такого программного средства является то, что выбор алгоритма метода принятия решения при сложной много функциональной зависимости не тривиальное решение. На основе проведённого анализа [1,2], было принято решение, что наиболее приемлемым методом является отыскание минимального пути прибытия в зону ЧС, на основе модернизированного метода Хакими [3], алгоритм которого был реализован в программном средстве «Расчёт временных характеристик прибытия спасательных формирований в зону ЧС, с учётом прохождения наиболее труднодоступных участков» [4]. Кроме того, программа реализует методику, основанную на методе Севеджа, для отыскания наиболее оптимальных путей в случае, когда спасательные формирования не имеют возможности прямого подъезда в зону ЧС интерфейс программного средства представлен на рисунке 1.

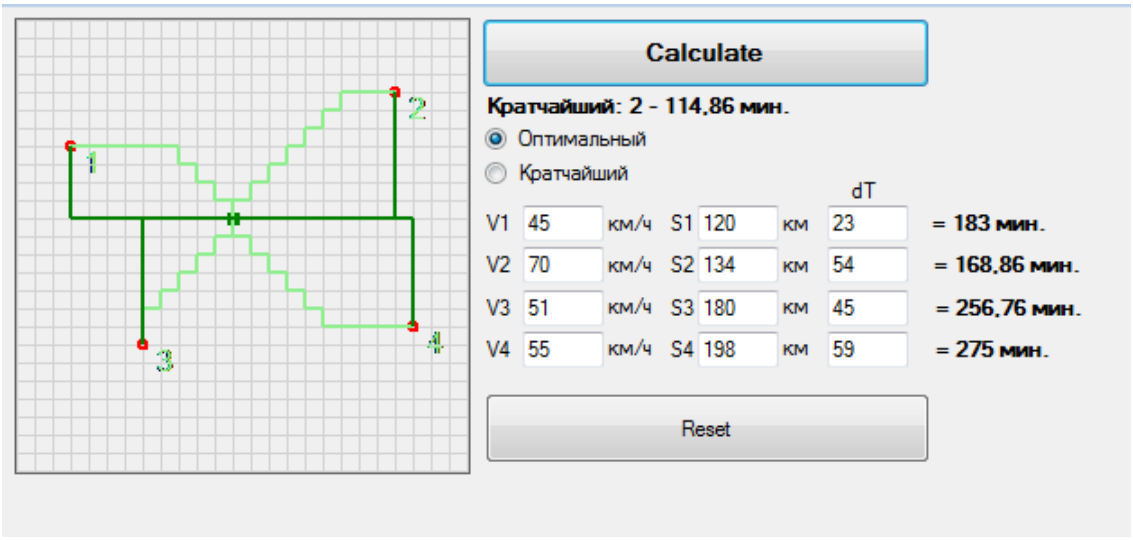


Рисунок 1. Интерфейс программного средства

На рисунке представлен расчёт пути для четырёх зон чрезвычайных ситуаций. Сетка на рисунке соответствует картографической сетке местности, прямые линии – государственной дорожной сети, а извилистые линии – кратчайшему пути из базы МЧС к месту ЧС.

Применение данной программы показало целесообразность её использования во время учений и тренировок.

Вторая составляющая принятия решения - время комплектования, она на сегодняшний момент, зависит от времени получения материальных средств со складов. Это мероприятие осложняется тем, что ручной электрический и шанцевый инструмент хранится на разных складах и, следовательно, выдаётся длительное время, последовательно.

Также для организации эффективной работы спасательной операции необходимо обеспечение средствами связи всех участников операции. Средства связи хранятся отдельно от инструментов, и требуется некоторое время для их проверки и получения.

Важно отметить, что параметры Тп и Тк однозначно взаимосвязаны, нет смысла в разрозненном прибытии колонн со специалистами и материальными средствами по отдельности в зону ЧС.

Устранить проблему длительного времени комплектования материально-техническими средствами и средствами связи можно создав контейнеры содержащие набор инструментов и средств связи. Набор должен содержать инструменты наиболее соответствующие типу ЧС (пожар,

наводнение и т.д.) и типовые средства связи. На базах хранения должно содержаться некоторое количество готовых для немедленной загрузки контейнеров. Их количество определяется исходя из вероятности возникновения типа ЧС в районе ответственности отряда МЧС и возможностей доставки первой колонной в зону ЧС, при этом необходимо учесть, что одновременно формируется, как правило, не одна колонна (рисунок 1).

Применение перспективного метода создания материальных и технических средств в виде укомплектованных контейнеров позволит точно расщитывать время комплектования – Тк, на основе специального программного средства. Это приведёт к уменьшению времени принятия решения на ликвидацию ЧС, что позволит снизить ущерб от него.

Литература:

1. Давыдов Э.Г. Исследование операций, - М.:, Наука, 1990.
2. Венцель Е.С. Исследование операций, - М.:, Наука, 1980.
3. Зверев А.П. Использование модифицированного метода Хакими в задачах перераспределения сил и средств в зоне чрезвычайных ситуаций. Инженерный вестник Дона, №4 (2014) http:// ivdon.ru.
4. Свидетельство о государственной регистрации программы для ЭВМ №2015610558 от 13 января 2015г.

И.В. Щербань, *Д.А. Знаменский, *В.А. Дорошкевич

ВЫДЕЛЕННЫЙ ДИСКРЕТНЫЙ ОПТИЧЕСКИЙ КАНАЛ ПЕРЕДАЧИ ДАННЫХ В ИНФРАКРАСНОМ ДИАПАЗОНЕ

Северо-Кавказский филиал Московского технического университета связи
и информатики, г.Ростов-на-Дону, Россия
*Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: волоконно-оптический канал, передача данных, информационно-измерительная система, аппаратная реализация, средства National Instruments.

Разработан и реализован волоконно-оптический канал передачи данных для информационно-измерительной системы. Схемотехническая реализация основана на аппаратных и программных средствах компании National Instruments.

I.V. Shcherban, *D.A. Znamensky, *V.A. Doroshkevich

EMITTED DISCRET OPTICAL CHANNEL FOR DATA TRANSMISSION IN THE INFRARED RANGE

The North Caucasian Branch of the Moscow Technical University
of Communications and Informatics, Rostov-on-Don, Russia
*Southern Federal University, Rostov-on-Don, Russia

Key words: optical fiber link, data transmission, information and measurement system, hardware realization, National Instruments hardware and software sets.

The optical fiber link has been developed and realized for data transmission to information and measurement system. Circuit implementation based on National Instruments hardware and software productsю

Для произвольной информационно - измерительной системы (ИИС) разработан выделенный дискретный оптический канал передачи данных. Отличительной особенностью канала является использование простых, имеющихся в свободной продаже неспециализированных

оптоэлектронных преобразователей, работающих в инфракрасном диапазоне с длиной волны 930 нм.

Выбор указанного окна прозрачности объясняется робастностью сигнала к засветкам и упрощением, соответственно, конструктивного исполнения преобразователей.

С целью обеспечения требуемой функциональности оптического канала передачи данных при низкой себестоимости комплектующих, а также вследствие того, что в составе подавляющего большинства ИИС используются средства аналого-цифрового преобразования, для схемотехнической реализации взяты аппаратные средства National Instruments (NI) [1, 2]. Программное обеспечение (ПО) канала передачи, соответственно, выполнено средствами LabVIEW [3].

Структурная схема приема и передачи сигнала по оптической линии связи представлена на рисунке 1.

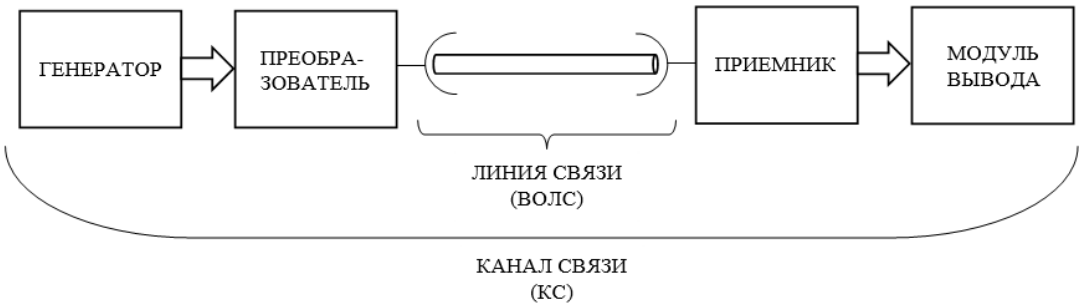


Рисунок 1. Общий вид канала передачи

В качестве генератора можно использовать любой таймер, счетчик, либо передатчик двоичной последовательности. Преобразованные электрические импульсы в световые подаются в ВОЛС и на приемном конце обратно преобразуются в электрические. В качестве модуля вывода используется аппаратные средства National Instruments.

Интеграция с аппаратурой NI упростила задачу синтеза функциональных блоков шифрации-дешифрации, модуляции, приема и передачи данных, а также аппаратную совместимость схем реализованного оптического канала.

Аппаратная схема оптоэлектронного преобразователя представлена на рисунке 2.

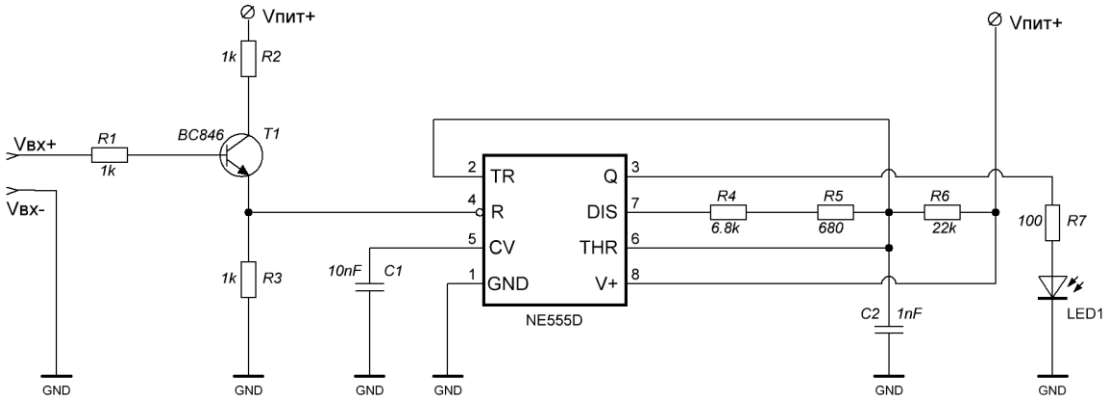


Рисунок 2. Принципиальная схема передатчика

Частотный генератор (таймер) NE555D с помощью резисторов настроен на частоту 36 КГц. При закрытом транзисторе на выход LED1 (инфракрасный светодиод) сигнал не подается. При открывании транзистора на вход RESET подается сигнал Uвх+ и частотный генератор с выхода Q передает сигнал на светодиод.

В качестве приемника инфракрасного излучения используется микросхема TSOP31236, работающая на той же частоте 36 КГц. Импульс на приеме формируется по изменению сигнала на приемном фотодиоде. При передаче используется метод расширения спектра [2] и, соответственно

один передаваемый импульс задается последовательностью импульсов. В используемой микросхеме эта последовательность может состоять из 15÷50 импульсов (рисунок 3).

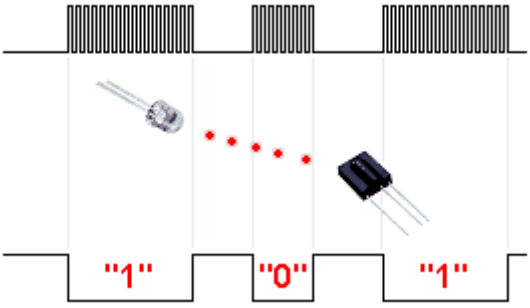


Рисунок 3. Модуляция сигнала

Параметры генератора выбраны следующим образом. Для задания логической единицы используется 30 импульсов с частотой следования 1,2 КГц, а для логического «0» – 15 импульсов с частотой 2,4 КГц. Скорость передачи данных при этом составляет 1,2 Кбит/с, что является приемлемым для многих промышленных ИИС [1, 4].

Известно, что затухание сигнала в инфракрасном спектре достаточно высокое и это ограничивает длину оптического канала передачи. В то же время, дальность передачи в разработанном канале без восстановления сигнала сравнима с дальностью современных проводных электрических каналов на базе интерфейсов RS-485, которая, как известно, не превышает 1,2 км.

Разработанный дискретный оптический канал передачи данных прост в реализации, построен на основе современной цифровой электронной базы и может быть использован в составе промышленных ИИС.

Литература:

1. Бутырин П.А., Васьковская Т.А., Каратаева В.В., Материкин С.В. Автоматизация физических исследований и эксперимента: компьютерные измерения и виртуальные приборы на основе LabVIEW. М.: ДМК-Пресс, 2005. 264с.

2. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием. – М.: Горячая линия – Телеком, 2009. 608 с.

3. Интернет-ресурсы National Instruments http://russia.ni.com/

4. Виглеб Г. Датчики. Устройство и применение. М.: Мир, 1998. 191 с.

И.В. Щербань, *Д.А. Знаменский, *С.А. Судаков

РЕШЕНИЕ ЗАДАЧИ ИДЕНТИФИКАЦИИ ХАРАКТЕРНЫХ ПАТТЕРНОВ БИОЭЛЕКТРИЧЕСКОЙ АКТИВНОСТИ ОБОНЯТЕЛЬНОГО НЕРВА ИЛИ ОБОНЯТЕЛЬНОЙ ЛУКОВИЦЫ КРЫСЫ

Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия
*Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: идентификация образа, распознавание, энергия сигнала, кепстральные признаки сигнала, пакет National Instruments LabView.

Исследованы и реализованы способы идентификации паттерна определенного типа внутри зашумленного сигнала, основанные на энергии и кепстральных признаках. Реализация методов производилась и успешно тестировалась на ЭЭГ грызунов в программном пакете NI LabView.

I.V. Shcherban, *D.A. Znamensky, *S.A. Sudakov

IDENTIFICATION PROBLEM'S SOLUTION OF SPECIFIC PATTERNS OF OLFACTORY NERVE BIOELECTRIC ACTIVITY OR RAT OLFACTORY BULB

The North Caucasian Branch of the Moscow Technical University
of Communications and Informatics, Rostov-on-Don, Russia
*Southern Federal University, Rostov-on-Don, Russia

Key words: pattern identification, recognition, signal energy, cepstral signal signs, National Instruments LabView software.

There are researched and realized methods of identification specific type patterns inside noisy input signal. Types are based on energy and cepstral signs. Realization of these methods produced and successfully tested on rodents EEG by NI LabView software.

Несмотря на актуальность вопросов, связанных с выяснением принципов организации нейронных систем, ответственных за билатеральное тактильное восприятие, а также способов кодирования пространственных параметров тактильных стимулов, исследованы они лишь в первом приближении. Изучение подобных вопросов осуществляется на животных с использованием специализированных программно-аппаратных комплексов [1-3].

В настоящее время в НИИ "Нейрокибернетики" Южного федерального университета реализован программно-аппаратный комплекс для изучения параметров импульсных и фокальных электрических ответов обонятельного нерва и обонятельной луковицы крысы на различные запахи. Известно, что макросматики, в том числе, крысы, рецепторные нейроны которых содержат тысячи различных рецепторных белков, обладают чрезвычайно высокой обонятельной чувствительностью. Целями работы являются, во-первых, обнаружение электрических ответов обонятельного нерва (обонятельной луковицы) крысы в составе снимаемого сигнала, и, во-вторых, идентификация специфических паттернов биоэлектрической активности обонятельного нерва и обонятельной луковицы крысы, соответствующих разным обонятельным раздражителям, разным запахам.

Исследования проводятся на белых беспородных крысах в условиях острого опыта – животное обездвижено и переведено на искусственное дыхание. Голова крысы фиксируется с помощью игольчатых головодержателей. Потенциалы с обонятельного участка коры головного мозга крысы регистрируются четырехканальными электродами. Интервалы опытных наблюдений равны одной минуте, где на 20-й секунде системой поддержания дыхания животного подаются различные запахи. Для увеличения информативности измерений регистрируются уровень дыхания животного и частота сердцебиения.

Основной проблемой в данном случае является проблема обнаружения и идентификации паттернов, соответствующих разным обонятельным раздражителям, в составе существенно зашумленного сигнала (рисунок 1) биоэлектрической активности обонятельного нерва или обонятельной луковицы крысы.

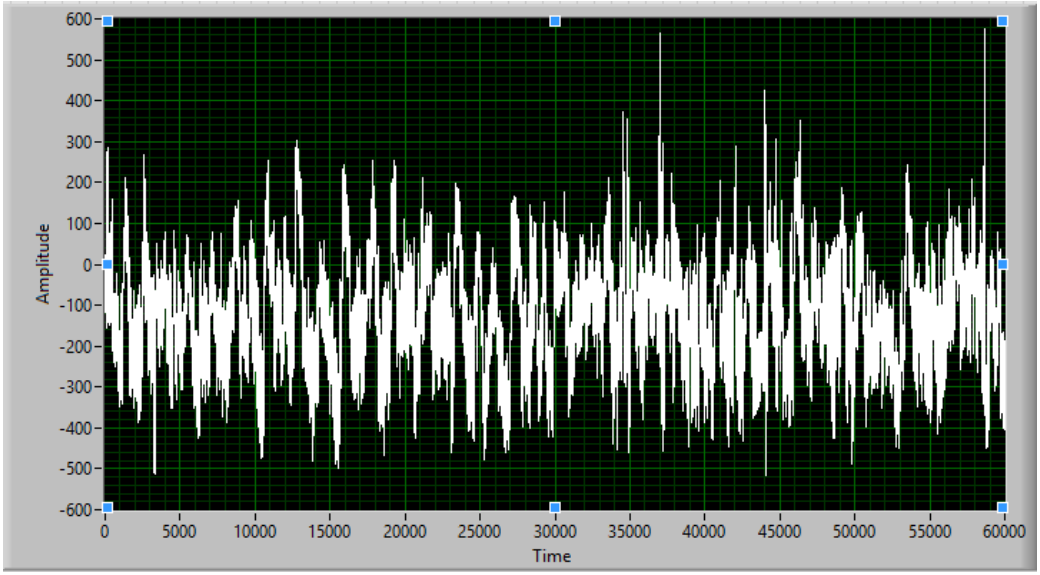


Рисунок 1. Сигнал биоэлектрической активности обонятельного нерва крысы

Проблема идентификации характерных осцилляторных паттернов электроэнцефалограммы (ЭЭГ) относится к числу актуальных задач современной нейрофизиологии. В настоящее время существуют различные методы, позволяющие решать подобные задачи с высокой степенью надежности [4]. Например, достаточно просто обнаруживаются характерные осцилляторные паттерны, такие как сонные веретена (SS) или пик-волновые разряды (SWD) [1,2,5]. В рассматриваемом же случае сложная частотно-временная организация паттернов, отражающих именно факты активности обонятельного нерва или обонятельной луковицы крысы, сосуществование близких по частоте ритмических компонент и существенная зашумленность сигнала обуславливают сложность процедур их выявления и идентификации.

Для идентификации в составе зашумленного сигнала биоэлектрической активности обонятельного нерва или обонятельной луковицы крысы паттернов, соответствующих целевым запахам, были выбраны метод отношения энергий сигналов и метод кепстральных коэффициентов [6].

В методе энергии паттерн идентифицируется на основе сравнения отношений между энергиями эталонного паттерна и паттерна, регистрируемого в бегущем относительно ряда измерений временном окне:

$$K = A_F / A_S , \quad (1)$$

где $K \in [0;1]$ – коэффициент соответствия; $A_F = \frac{1}{W_F}\sum_{i=0}^{N} S_i F_i$ и $A_S = \sqrt{W_S / W_F}$ – факторы, соответственно, исследуемого сигнала и образа искомого паттерна;

$W_S = \sum_{i=0}^{N} S_i^{\,2}$ – энергия дискретизированного (АИМ - амплитудно-импульсно модулированного) образа искомого паттерна; S_i – мгновенные значения амплитуд дискретизированного образа искомого паттерна; N – количество дискрет (отсчетов) АИМ-сигнала;

$W_F = \sum_{i=0}^{N} F_i^{\,2}$ – энергия исследуемого дискретизированного по времени (АИМ) сигнала; F_i – мгновенные значения амплитуд исследуемого входного АИМ-сигнала. По коэффициенту K определяется степень соответствия энергий образа искомого паттерна и временного окна входного исследуемого сигнала. Максимальному коэффициенту и соответствует искомая область в полном входном исследуемом сигнале.

Если рассматривать задачу в векторной области информационного пространства, то существует два вектора – вектор образа и вектор анализируемого паттерна. Таким образом, задача

сводится к определению наименьшего расстояния между векторами образа и снимаемых данных, а также установлением границы, выше которой система будет считать сигнал идентифицированным. Второе правило необходимо для уменьшения числа сравнений и, как следствие, служи сокращению количества действий программы.

Программа идентификации по методу энергий реализована средствами LabView. Программа сканирует данные во временном бегущем относительно ряда измерений окне. В ходе сканирования определяется длина вектора энергии анализируемого паттерна. Полученное значение сравнивается с длиной вектора энергии эталонного паттерна, характеризуемого воздействием эталонного запаха на обонятельную луковицу крысы. Определяется минимальное векторное расстояние для каждого входного паттерна. На выходе формируется массив из коэффициентов, где индекс максимального значения коэффициента и соответствует искомому паттерну. Соответствующий фрагмент блок-диаграммы представлен на рисунке 2.

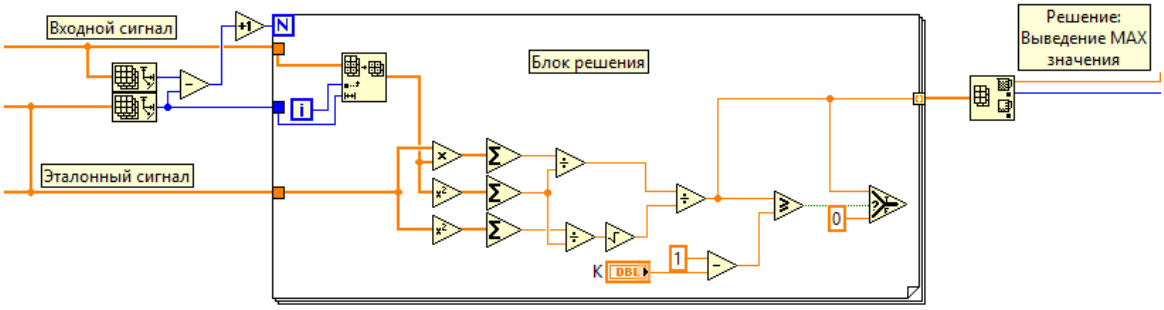


Рисунок 2. Блок-диаграмма идентификации по методу энергий

Недостатком метода сравнения энергий является тот факт, что невозможно записать в память ЭВМ уже готовые значения свойств сигналов, а необходимо содержать в памяти все элементы свойств дискретного сигнала образа. Если частота дискретизации сигнала достаточно высокая, то распознавание сигнала по энергии будет занимать значительное количество памяти ЭВМ.

Второй метод, фактически, основан на сравнении энергетических спектров входного паттерна и паттерна образа. Здесь наличествует возможность привести образ к конечному числу свойств, что уменьшает потребляемый объем памяти.

Входные данные делятся на фреймы произвольной длины. Их длина не должна быть слишком короткой, иначе возможна неверная идентификация. Деление на фреймы выполняется с "нахлестом", т.е., если первый фрейм имеет длину от 0 до 100 дискреты, то следующий будет не от 101, а, например, от 50-й дискреты и до 150-й. Таким образом повышается вероятность верного распознавания и уменьшается погрешность идентификации.

Далее каждый фрейм переносится в частотную область с помощью процедуры дискретного преобразования Фурье (FFT), после чего выбирается некоторый частотный диапазон, в котором находится искомый сигнал. Данный диапазон переносится в Mel-область, представляющую собой выделенный характерный частотный диапазон из общего частотного спектра сигнала [2].

Выбранная область делится на равные участки и, тем самым, определяются значения так называемых опорных точек. Полученные коэффициенты с помощью масштабирующего модуля согласуются с дискретным числом элементов каждого фрейма в частотной области. Например, если ширина спектра равна 16 КГц и при этом в него умещается 256 элементов, то на один элемент приходится 62,5 Гц. При делении полученных коэффициентов на это значение с округлением до целого получаются согласованные элементы будущего цифрового фильтра. Следующим этапом является синтез цифрового фильтра и наложение его на фрейм. АЧХ синтезированного цифрового mel-фильтра показана на рисунке 3.

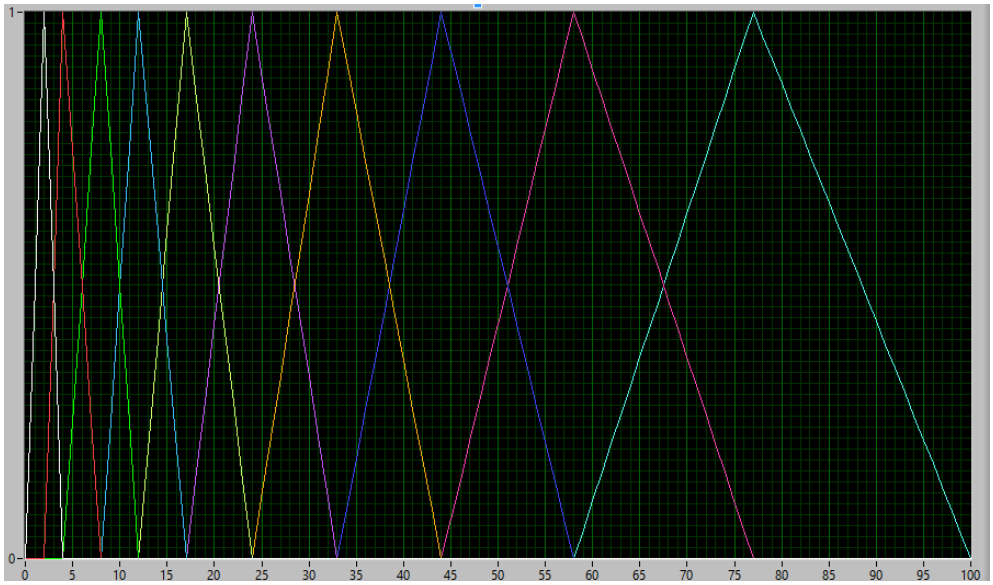


Рисунок 3. АЧХ десяти Mel-фильтров

После наложения фильтра для сжатия результатов и повышения значимости первичных коэффициентов к сигналу применяется процедура дискретного косинусного преобразования второго типа (DCT2). Анализируемый паттерн преобразуется в последовательность кепстральных коэффициентов (рисунок 4).

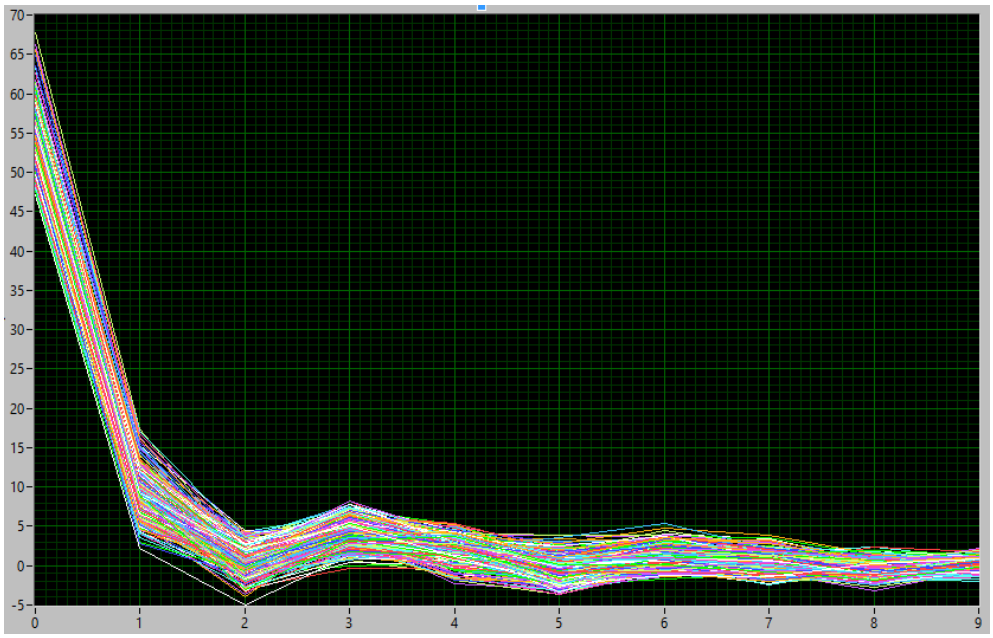


Рисунок 4. График Mel-кепстральных коэффициентов каждого фрейма

Данные коэффициенты можно вычислить единожды и хранить в памяти без необходимости повторных вычислений. Распознавание производится на основе поиска средних значений наименьших евклидовых расстояний между последовательностью кепстральных коэффициентов.

Программа идентификации по методу Mel-кепстральных коэффициентов реализована средствами LabView.

Использование второго метода оказалось более эффективным. Так, вероятность правильной идентификации характерных паттернов электроэнцефалограммы по второму методу была близка к единице, тогда как по первому методу не превышала 0,8.Однако, метод отношений энергии проще в реализации, так как для получения кепстральных признаков сигнала необходимо провести ряд ресурсоемких математических операций.

Литература:

1. Назимов А.И. и др. Распознавание осцилляторных паттернов на электроэнцефалограмме на основе адаптивного вейвлет-анализа // Вестник ТГУ. – 2013. – Т.18, № 4. – С. 1431-1434.

2. Трофимов А. Г., Скругин В. И. Адаптивный классификатор многомерных нестационарных сигналов на основе анализа динамических паттернов // Наука и образование. – 2010. – № 8. http://technomag.edu.ru/doc/151934.html

3. Сухов, А.Г., Бездудная, Т.Г., Медведев, Д.С. Особенности посттетанической модификации синаптической передачи в таламо-кортикальном входе соматосенсорной коры крыс // Журнал Высшей нервной деятельности. – 2003. – Т. 53, № 5. – С. 622-632.

4. Lewicki M. A review of methods for spike sorting: the detection and classification of neural potentials // Net. Com. Neu. Sys. – 1998. – V. 9. – P. R53-R78.

5. Скругин В.И. и др. Алгоритм классификации сигналов ЭЭГ на основе анализа в частотно-временной области // Сборник научных трудов XII Всероссийской научно-технической конференции "Нейроинформатика-2010". – М.: НИЯУ МИФИ, 2010. Т.1. С.266-276.

6. Отнес, Р. , Эноксон, Л. Прикладной анализ временных рядов. Основные методы. – М.: МИР, 1982. – 428 с.

А.В. Зуев

ФУНКЦИИ ПРОТОКОЛОВ MAC-УРОВНЯ ДЛЯ ДОСТУПА К КАНАЛЬНЫМ РЕСУРСАМ КОГНИТИВНЫХ СЕТЕЙ СВЯЗИ

Поволжский государственный университет телекоммуникаций и информатики

Ключевые слова: когнитивные сети, система радиосвязи с программируемыми параметрами, когнитивные радиосистемы, протокол управления звена данных, динамический доступ к радиочастотному спектру.

Когнитивные сети (CN) на основе программно-конфигурируемого радио SDR являются актуальной темой среди исследователей беспроводных сетей. Возможности CN и SDR позволяют идентифицировать временно свободные части радиочастотного спектра, которые ранее выделялись для использования только первичными пользователями. Динамический доступ является одним из главных требований, предъявляемых к передатчикам SDR, которые способны приспосабливаться к изменению количества и качества каналов связи, к резкому изменению количества абонентов в сети и к изменению качества услуг. Для этого необходимо исследовать свойства протоколов уровня звена данных и соответствующий варианты протоколов уровня звена данных.

A.V. Zuev

MAC PROTOCOL FUNCTIONS FOR THE ACCESS CHANNEL RESOURCE IN THE COGNITIVE COMMUNICATION NETWORKS

Povolzhskiy State University of Telecommunications and Informatics

Keywords: Cognitive networks CN, software defined radio SDR, cognitive radio systems CRS, media access control MAC, dynamic spectrum access DSA.

Cognitive Networks (CN) based on software-configurable radio SDR is in the focus among researchers wireless networks. Some opportunities of CN and SDR allow to identify temporarily free part of the radio spectrum which was previously allocated for using by primary users. Dynamic spectrum access is one of the main requirements for the SDR transmitters, which are able to adapt to changing number and quality of communication channels; to adapt to abrupt variation number of subscribers in the network and to services quality modification. Since it’s needful to investigate the features of the media access protocol for cognitive networks and an appropriate media access control (MAC) protocol options.

Введение.

Внедрение технологии радиосвязи с программируемыми параметрами software defined radio, SDR с использованием механизмов когнитивного управления в рамках технологии когнитивной системы радиосвязи представляет собой один из подходов для обеспечения более эффективного использования радиочастотного спектра, РЧС [1]. Пользователь может выбирать ту или иную радиосеть для получения требуемой услуги связи, используя мультистандартный терминал с несколькими программно-управляемыми радиоинтерфейсами.

Особенности когнитивных систем радиосвязи.

Когнитивная система радиосвязи КСР (cognitive radio systems, CRS) – технология, которая позволяет системе связи получать знания (данные) о своей операционной и географической среде функционирования, установленных политиках обслуживания пользователей радиочастотного спектра, своем внутреннем состоянии. Эта технология позволяет динамически и автономно корректировать операционные параметры и протоколы согласно заданным данным или параметрам, чтобы достигнуть предопределенных целей.

Когнитивное радио идентифицирует временно свободные части радиочастотного спектра и временно занимает эти т.н. называемые «белые пятна» («white spots») для приема и передачи информации, не создавая помех другим средствам в выбранном диапазоне [2]. Рабочая группа 1B МСЭ-R определила, что КСР не относится к службам радиосвязи и, следовательно, для КСР не выделяются полосы радиочастот. В настоящее время ведутся работы по нескольким стандартам КСР IEEE 802.11af, IEEE 802.16h, IEEE 802.22. –2009.

Система когнитивного радио может адаптировать характеристики SDR к радиосреде благодаря следующим когнитивным свойствам:

- возможность сбора информации SDR о свойствах окружающей радиосреды для выработки определенного решения об использовании РЧС;
- процесс распознавания свободных частот по сведения, которые предоставляются помощью когнитивного канала управления – пилот–канала (pilot-channel) или запрашиваются из централизованной базы данных защищаемых РЭС;
- способность автоматической реконфигурации аппаратно–программной части, в том числе автономной конфигурации [3].

В Российской Федерации с 2011 г. для создания когнитивной сети беспроводного широкополосного доступа выделена полоса частот 470–686 МГц с правом применения радиоэлектронных средств КСР только в опытной сети ФГУП НИИР. Выбор рабочих каналов осуществляется только при запросе вторичного РЭС к базе данных о защищаемых РЭС с информацией о доступных для работы частотных каналах, а при отсутствии связи вторичное РЭС должно прекратить излучение. Максимальная эффективная изотропно излучаемая мощность, ЭИИМ должна составлять для базовых станции 6 дБВт (4 Вт), а для персональных РЭС – 0 дБВт.

С учетом перечисленных особенностей, далее будут рассмотрены особенности использования радиочастотного спектра с помощью управления со стороны сети связи и особенности MAC-уровня когнитивных сетей связи.

Задача оптимального использования SDR канального ресурса.

В рамках КСР существующая модель управления спектром не может сделать временно неиспользуемый спектр доступным. Поэтому SDR предусматривает использование технологии динамического доступа к РЧС, DSA (dynamic spectrum access) и соответствующий режим управления РЧС [4].

С учетом применения DSA актуальной является задача выбор наилучшей радиосети для текущего обслуживания SDR. При этом со стороны оператора осуществляется управление запросами пользователей SDR на предоставление услуг [5]. Пусть в качестве цели управления доступом оператор связи стремится получить максимальный доход от использования своих канальных ресурсов с учетом ограничений пропускной способности узла доступа в сеть. Здесь важно учитывать коэффициент загруженности узла доступа, интенсивность запросов услуги, «вес» т.е. значимость каждого типа услуги (сервиса). Решения задачи оптимизации обусловлено ограничивающими коэффициентами для каждого типа услуги пользователя. Пусть эти коэффициенты доступны SDR. Учтем, что поиск оптимального решения по подключению к сети

учитывает значимость или «вес» сервиса j на узле доступа x, $c_{x,j}(t)$, который определяется по формуле 1:

$$c_{x,j}(t) = \frac{D_j \times \nu_{x,j}}{\sum_{j=1}^{J} D_j \times \nu_{x,j}}, \quad (1)$$

где D_j −стоимость тарифной единицы услуги j в момент времени t;

$\nu_{x,j}$ −количество тарифных единиц (минут, килобит), определяющие объём предоставленного сервиса j на узле доступа x в момент времени t.

В целом задача оптимизации в рамках стратегии выбора сети «за оператора связи» может быть выражена следующим общим выражением:

$$\max_{p^r_{\text{УД},1,1}..p^r_{\text{УД},k,j}} \sum_{k=1}^{K} \sum_{j=1}^{J} D_j \times \lambda^*_{k,j}(t) \times p^Y_{\text{УД},k,j}(t)\ , \quad (2)$$

где $\lambda^*_{k,j}(t)$ – оценочная интенсивность запросов на предоставление услуги j, поступивших от k-го пользователя (k-й группы пользователей) в момент времени t;

$p^r_{\text{УД},k,j}$– значение ограничивающего коэффициента узла доступа (УД) для сервиса j, который требуется предоставить k-му пользователю (k-й группе пользователей), с возможностью регулярного обновления значения $p^r_{\text{УД},K,J}$ через промежуток времени r.

Указанная постановка задачи в дальнейшем должна учитывать особенности когнитивных сетей. В КСР перечень доступных каналов является переменным параметром. Тогда при подключении к сети в целом возникает задача выбора наилучшего из возможных каналов. Для решения этой задачи на уровне оперативного управления в реальном времени используются протоколы уровня звена данных, MAC–протоколы (Media access control). Одновременно MAC–протоколы можно использовать для решения задачи распознавания частично или временного свободного РЧС.

С учетом сказанного, MAC–протокол КСР должен поддерживать следующие основные функции:

- контроль и предотвращение вмешательств в работу РЭС первичных пользователей радиоспектра;
- предотвращение коллизий доступа к каналу для вторичных пользователей радиочастотного спектра;
- реализацию процедуры выбора и занятия наилучшего из доступных, временно свободных, радиоканалов [6].

Протоколы MAC могут применяться в централизованной или распределенной архитектуре сетей КСР. В централизованной архитектуре есть главное устройство – базовая станция BS (Base Station), которая координируют доступ к РЧС для вторичного пользователя. В распределенных протоколах MAC такое деление отсутствует и каждое РЭС в определенный момент времени может выполнять как функции BS, так и функции обычного терминала.

Существует два вида MAC–протоколов: протоколы совместного и несовместного использования. По протоколам совместного использования вторичные пользователи работают сообща, чтобы максимизировать использование сети, увеличивая общую пропускную способность. Протоколы несовместного пользования позволяют каждому вторичному пользователю РЧС работать независимо от других, пытаясь улучшить лишь свою производительность [7].

По режиму доступа к РЧС в когнитивных сетях выделяют две категории с передачей подтверждения:

- в режиме без подтверждения вторичный пользователь получает доступ к спектру согласно времени простоя/отсутствия использования данной части радиоспектра;
- режим с подтверждением предполагает, что вторичные пользователи борются за возможность передачи по каналу, например, как в случае с множественным доступом с контролем несущей/с предотвращением коллизий CSMA/CA [8].

Все указанные особенности протоколов MAC–уровня будут учитываться в дальнейшем при исследовании эффективности использования каналов в когнитивных сетях следующего поколения.

Выводы.

Одной из наиболее привлекательных особенностей КСР является техническая возможность динамического доступа к РЧС и к различным радиосетям доступа в целом. Рассмотрена постановка задачи оптимизации как выбор для SDR наилучшего подключения (best connected) к одной из доступных сетей с последующим переходом к решению задачи выбора наилучшего канала данной сети на уровне звена данных с помощью когнитивного MAC–протокола.

Литература:

1. Tuttlebee, H.W. Software defined radio [Текст]/H.W.Tuttlebee –USA: John Wiley & Sons, Ltd., 2002 – 402 pages.

2. Zhang, Y. Cognitive radio networks: architectures, protocols, and standards [Текст]/ Edited by Zhang Yan, Zheng Jun, Hsiao-Hwa Chen.– UK.: CRC Press, 2010 – 525 pages.

3. Palicot, J. Radio engineering. From software to cognitive radio [Текст]/ J. Palicot. –USA.: John Wiley & Sons, Ltd., 2011. – 360 pages.

4. Burns, P. Software Defined Radio for 3G [Текст]/Burns Paul. – London: Artech House Inc., 2003 – 478 pages.

5. Гребешков А.Ю. Принятие решения по предоставлению услуги с помощью многофункционального абонентского терминала SDR в когнитивных сетях связи [Текст]// T-Comm. Телекоммуникации и транспорт. – 2011. – №7– С. 63–66.

6. Incel, O.D. MC-LMAC: a multi–channel MAC protocol for wireless sensor networks [Текст]: technical report of TR-CTIT-08-61/O.D. Incel, P.Jansen. – Netherlands: Mullender centre for telematics and information technology University of Twente. – 2008. – PP. 1381–3625.

7. Гребешков, А.Ю, Стандарты и возможности применения когнитивного радио[Текст]/ А.Ю. Гребешков, А.В. Зуев А//XXI Российск. научн. конф. проф.-преп. состава, научн. сотрудников и аспирантов ПГУТИ; тез. докл., Самара, 29–31 января 2014 г. – Самара: Изд-во ПГУТИ, 2014. – 1 с.

8. Nasipuri, A. A multichannel CSMA MAC Protocol for multihop wireless networks [Текст]/ A. Nasipuri, J. Zhuang, S. Dias//Wireless communications and networking international conference: proceedings, New Orleans (USA) September 21–24, 1999. – New Orleans, USA – PP. 1–6.

П.А. Александров, Р.Н. Калинин, И.А. Фокин

ОСОБЕННОСТИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЭНЕРГЕТИЧЕСКОГО РАСЧЁТА РАДИОЛИНИЙ БЛИЖНЕЙ КВ РАДИОСВЯЗИ, РАБОТАЮЩИХ ИОНОСФЕРНОЙ ВОЛНОЙ

Академия ФСО России г. Орел

Ключевые слова: радиосвязь, модель, мощность, чувствительность, радиотрасса, широта, долгота, рабочая частота, высота, время, число Вольфа, день, месяц.

Описана проблема установления устойчивой радиосвязи между объектами различных ведомств РФ, размещающихся на удалении от 40 до 500 км. Приведена математическая модель с помощью, которой возможна объективная оценка условий осуществления радиосвязи на радиолиниях ближней коротковолновой связи и принятие организационно-технических решений, позволяющих обеспечить качественную радиосвязь.

P.A. Alexandrov, R.N. Kalinin, I.A. Fokin

FEATURES OF MATHEMATICAL MODEL OF ENERGY CALCULATION OF RADIO LINES OF NEAR HF RADIO COMMUNICATION WORKING IONOSPHERIC WAVE

The Academy of Federal Guard Service of Russian Federation, Orel

Keywords: radio communication, model, power, sensitivity, radio track, width, longitude, working frequency, height, time, Wolf's number, day, month.

Described the problem of establishment of a steady radio communication between objects of various departments of the Russian Federation, which are placed at a distance from 40 to 500 km. The mathematical model is given with the help of which the objective assessment of conditions of implementation of a radio communication on radio lines of near short-wave communication is possible. Also on the basis of model it is possible to acceptance the organizational technical solutions allowing to provide a qualitative radio communication.

В последние годы, несмотря на огромные достижения в области спутниковых систем связи, во многих странах возрос интерес к КВ радиосвязи и поэтому небезосновательно считается, что этот вид радиосвязи приобретает второе дыхание.

Повышение интереса к КВ радиосвязи объясняется её преимуществами по сравнения с другими видами связи. Среди основных преимуществ отмечаются такие как: оперативность установления прямой связи на большие расстояния; простоту организации радиосвязи с подвижными объектами; возможность обеспечения связи через большие труднодоступные районы; высокую мобильность средств КВ радиосвязи, довольно простую восстанавливаемость связи в случае её нарушения и достаточно низкую стоимость одного канала на километр дальности связи. Особое значение КВ радиосвязь приобретает в чрезвычайных ситуациях, при организации и проведении аварийно-спасательных работ, координации действий различных организаций и служб в районах стихийных бедствий, а также в северных и приполярных районах, где иные средства связи по тем или иным причинам оказываются неэффективными.

Коротковолновая радиосвязь, как правило, используется для передачи информации на большие расстояния. При этом передача радиосигналов на радиотрассах большой протяженности основана на отражении сигналов декаметровых волн от слоев ионосферы с прижатым главным лепестком излучения антенны к горизонту. В то же время существует насущная необходимость установления связи внутри региона с ближайшими объектами, различных ведомств РФ, удалёнными на расстояния от 40 до 500 км. Для таких связей прижатый к горизонту максимум излучения антенны совсем не оптимален и даже вреден. Поэтому, как показано на рисунке 1, для таких корреспондентов предусматривается работа пространственной волной, падающей на ионосферный слой почти вертикально, создавая при этом значительную напряженность поля на небольших (десятки – сотни километров) расстояниях от передатчика.

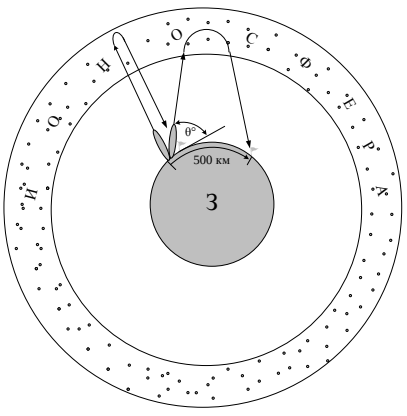


Рисунок 1. Условия распространения ЭМВ на радиолиниях ближней КВ радиосвязи

Особый интерес к радиолиниям ближней КВ радиосвязи возник сравнительно недавно, когда потребовалось устанавливать радиосвязь с некоторыми специфическими объектами радиосвязи. При этом обнаруживалось, что, несмотря на относительно небольшие расстояния (100–400 км), радиосвязь оказывалась либо низкого качества, либо отсутствовала вообще [1]. При этом, многолетняя практика эксплуатации радиолиний ближней КВ радиосвязи показывает, что перекрывать расстояние в 200–250 км всегда было достаточно тяжело.

Из теории распространения радиоволн известно, что ионизированные слои полностью характеризуются высотой максимума электронной концентрации h и максимальной частотой отражающейся от соответствующего слоя волны $f_{кр}$. При этом также известно, что при превышении частотой сигнала $f_с$ критической частоты $f_{кр}$, вертикально падающие волны перестают отражаться, но полого падающие волны еще отража ются. Следовательно, для ближней КВ радиосвязи пригодны только те волны, частоты которых ниже критической. Но в тоже время, теория гласит, что необходимо учитывать ещё и поглощение волн в ионосфере. Поглощение в ионосфере увеличивается с понижением частоты. Так, например, средние волны днем полностью поглощаются слоем D (h = 70 км), критическая частота которого недостаточна для их отражения, и поэтому волне приходится дважды его пронизывать, отражаясь от слоя E (h = 90...120 км).

Таим образом, с этой точки зрения, для уменьшения ослабления энергии электро-магнитной волны следует выбирать рабочую частоту радиолинии как можно ближе к $f_{кр}$, но немно го ниже ее, ориентируясь при этом на правильный выбор оптимальной рабочей частоты ($f_{орч}$).

Критические частоты слоя E и вышележащего слоя F (h = 200...350 км) очень сильно зависят от времени суток, времени года и солнечной активности. Все эти факторы определяют электронную концентрацию в слое, а, следовательно, и $f_{кр}$. Расчёты показывают, что рабочий диапазон частот для радиолиний ближней КВ радиосвязи чаще всего лежит в области 2...7 МГц, понижаясь ночью и возрастая днем. Для обеспечения эффективной связи на радиолиниях дальностью до 500 км необходимо использовать специальные антенны, способные формировать характеристику направленности с максимумом в вертикальной плоскости под углами возвышения от 60 до 90 градусов.

Кроме того, для обеспечения надежной круглосуточной радиосвязи, при любых изменениях состояния ионосферы, а также амплитудных и поляризационных замираниях, антенны на таких радиолиниях должны иметь, по возможности, высокий коэффициент усиления, работать в широком диапазоне частот и иметь преимущественно горизонтальную поляризацию ЭМВ. Поэтому совершенно очевидно, что радиосвязь ионосферными волнами для каждой конкретной радиолинии возможна лишь при условии правильного выбора рабочих частот и антенн, обладающих соответствующими направленными, диапазонными и энергетическими свойствами и характеристиками [2].

Авторами статьи разработана математическая модель энергетического расчёта радиолиний ближней КВ радиосвязи, позволяющая реализовать её в виде программного продукта, и на этой основе оперативно производить оценку условий осуществления радиосвязи. Математическая модель в полном формате представляет собой совокупность 50-ти аналитических выражений, учитывающих различные аспекты пространственно-временного распределения параметров ионосферы и их влияния на энергетику радиолиний.

Учитывая требования на ограничение объёма статьи, авторы не могут представить математическую модель в полном объёме, ограничившись лишь некоторыми её особенностями. В основу математической модели положено классическое аналитическое выражение, известное как уравнение радиопередачи [3], определяющее мощность сигнала на входе радиоприёмного устройства $P_{с,вт}$:

$$P_{с,вт} = P_1 \cdot \eta_{ф1} \cdot \eta_{ф2} \cdot G_1 \cdot G_2 \cdot \left(\lambda_в \cdot \frac{F_{(r)}}{4\pi r_л} \right)^2; \quad (1)$$

В свою очередь, степень ослабления энергии электромагнитной волны, при её прохождении через ионосферу, предлагается учесть с помощь формулы [3]:

$$F_{(r)} = 0.5 \cdot \exp\left(-\Gamma_{\Sigma}\right). \quad (2)$$

В данной формуле через коэффициент поглощения Γ_{Σ} учтены все нюансы ослабления энергии электромагнитной волны в ионосфере. Лучшие результаты по такому учёту дает ***метод Казанцева*** [4], ключевым элементом которого является критическая частота слоя *E* ионосферы:

$$f_0 E_{,\text{МГц}} = 0{,}6 + B \cdot C \text{ , где [6]} \tag{3}$$

$$B = 2{,}8 \cdot \sin(90 - \chi/1{,}26) + 0{,}009 \cdot W; \tag{4}$$

$$C = \exp\left[-2{,}1((\chi - \chi_{\min})/(113{,}5 - \chi_{\min}))^2 \right]; \tag{5}$$

$$\chi = \arccos\{A_1 + A_2 \cdot A_3\}; \tag{6}$$

$$\chi_{\min} = \arccos\{A_1 + A_2\}; \tag{7}$$

$$A_1 = \sin(\varphi_3) \cdot \sin[\delta_c \cdot \cos(30 \cdot n)]; \tag{8}$$

$$A_2 = \cos(\varphi_3) \cdot \cos[\delta_c \cdot \cos(30 \cdot n)]; \tag{9}$$

$$A_3 = \cos[15 \cdot (12 - t_{\text{мв}})]; \tag{10}$$

$$\varphi_3 = arctg[(tg(\varphi_2) \cdot \sin(\theta_3 - \theta_1) + tg(\varphi_1) \cdot \sin(\theta_2 - \theta_3))/\sin(\theta_2)] \tag{11}$$

$$\delta_c = 23{,}45^{\circ} \cdot \sin[0{,}99(d - 81)]; \tag{12}$$

$$d = [16 + (n-1) \cdot 30]; \tag{13}$$

$$t_{вс,ч} = \arccos\left[(\sin(\delta_c) \cdot \sin(\varphi_3) + 0{,}0145)/(\cos(\delta_c) \cdot \cos(\varphi_3))\right]/15; \tag{14}$$

$$t_{зс,ч} = 24 - t_{вс,ч}; \tag{15}$$

В приведённых соотношениях учтено:

- место положения радиостанций через их координаты $\varphi_{1,2}; \theta_{1,2}$;
- координата точки отражения φ_3;
- месяц года – n;
- день года – d;
- местное время $t_{мв}$, время восхода $t_{вс,ч}$ и захода $t_{зс,ч}$ Солнца, а также число Вольфа – W, учитывающее его активность, и угол склонения δ_c.

Предлагается математическая модель, с помощью которой процесс оценки условий осуществления радиосвязи можно, используя современные технологии и методы программирования, автоматизировать и тем самым значительно сократить время расчётов и их точность.

Кроме того, совокупность подобранных аналитических выражений математической модели позволяет проводить достаточно быстро и корректно исследования пространственно-временных, частотных и энергетических характеристик радиолиний, что в свою очередь, для

радиолиний ближней коротковолновой радиосвязи, даёт возможность своевременно, более объективно и реалистично осуществлять выбор и назначение рабочих частот.

Литература:

1. Поляков. В. Т. NVIS – техника ближней связи на КВ //Спецтехника и связь. 2009. № 1.

2. Бузов А. Л. Проектирование пассивных ретрансляторов для сетей ОВЧ радиовещание и подвижной радиосвязи: Учебное пособие для ВУЗов. М.: Радио и связь, 2005, 140 с.: ил.

3. Ерохин Г. А. и др. Антенно-фидерные устройства и распространение радиоволн. М.: Горячая линия – Телеком, 2007, 491 с.: ил.

4. Серков В. П. Распространение радиоволн и антенные устройства. – ВАС: ВАС, 1981, 468 с.: ил.

М.С. Корчагин, Е.Н. Сидоренко

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ ДЛЯ ДИСКРЕТНОГО ВЕЙВЛЕТ–ПРЕОБРАЗОВАНИЯ

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия

Ключевые слова: искусственные нейронные сети, нейрокомпьютеры, система остаточных классов, цифровая обработка сигнала, вейвлет анализ.

В статье рассматриваются вопросы цифровой обработки сигналов. Для увеличения скорости цифровой обработки сигналов все более актуальным становится применение нейросетевых процессоров, функционирующих в системе остаточных классов, что позволяет осуществлять параллельную обработку по нескольким каналам. Сочетание системы остаточных классов и нейронных сетей, которые дополняют друг друга, вызывает интерес по той причине, что легко реализовать принципы обменных операций между быстродействием, точностью и надежностью с целью создания отказоустойчивого сопроцессора вейвлет-анализа.

M.S. Korchagin, E.N. Sidorenko

APPLICATION OF ARTIFICIAL NEURAL NETWORKS AND SYSTEM OF RESIDUAL CLASSES FOR DISCRETE WAVELET TRANSFORM

Saint-Petersburg state University of telecommunications them. Professor M. A. Bonch-Bruevich,
St. Petersburg, Russia

Keywords: artificial neural network, neural computers, the system of residual classes, digital signal processing, wavelet analysis.

The article considers the issues of digital signal processing. To increase the speed of digital signal processing is becoming increasingly important application of neural network processors operating in the system of residual classes that enables parallel processing across multiple channels. The combination of the system of residual classes and neural networks, which complement each other, is of interest for the reason that easy to implement the principles of exchange transactions between performance, accuracy and reliability with the aim of creating a failover coprocessor wavelet analysis.

Повышение производительности и надежности компьютеров связывают с искусственными нейронными сетями (ИНС), являющимися основой нейрокомпьютеров (НК) [18].

Способность ИНС к обучению, самоорганизации и адаптации создает потенциальные предпосылки для создания нового класса вычислительных средств.

ИНС – это огромные параллельные взаимосвязанные сети простых элементов, которые предназначены для взаимодействия с объектами реального мира таким же образом, как взаимодействуют биологические нервные системы [3-5].

Методы распознавания образов можно разделить на два класса: контролируемые и неконтролируемые [1-2]. В контролируемых методах для каждой категории доступно определенное количество выборок, и эти выборки используются для тренировки классификатора. В случае неконтролируемых методов, обучающие выборки недоступны, и сеть обучается через распознавание сходства между входными векторами. Известны модели ИНС и алгоритмы для распознавания образов. К ним относятся: обучение обратного распространения, конкурентное обучение, обучение по Кохоннену, теория адаптивного резонанса, модели неокогнитрона, сети Хопфилда и Больцмана. Обучение обратного распространения относится к контролируемым типам, и сеть обучается при помощи обучающихся последовательностей [7].

Другим важным классом являются самоорганизующиеся нейросети. К ним относятся сети с алгоритмом конкурентного обучения [6]. Главный недостаток конкурентного обучения состоит в том, что сеть забывает свое раннее обучение из-за нового обучения и может установиться в неустойчивое состояние фальшивыми входными векторами. Для устранения этого недостатка разработана структура адаптивного резонанса, модель неокогнитрона, модель обучения по Кохонену. ИНС представляют модель параллельно-распределленной обработки. Функциональный синтез этих моделей заключается в установлении связи между входом и одним или более выходом. В ИНС узлы соединены друг с другом синаптическими связями, имеющими определенный вес. В процессе обучения изменяются синаптические веса, которые представляют знания, хранящиеся в сети. ИНС состоят из одного или нескольких слоев, каждый из которых состоит из нескольких узлов, на входы которых поступают входные векторы, которые могут представлять собой и вероятностные значения. Каждое возможное решение или результат представляется на выходе узла. ИНС – это система обработки информации, широко используемая в различных областях применения, причем, во всех этих областях, нейросети характеризуются соединением адаптивных алгоритмов и параллельно-распределенной обработки. Хотя ИНС и являются биологически мотивированы, их сходство с моделями мозга не является точным.

При сравнении человеческого мозга с современными компьютерами Фон Неймана [4-7], в плане обработки информации, можно заметить, что время переключения нейронов (несколько миллисекунд), примерно в миллион раз медленнее, чем время переключения элементов современного компьютера, но они имеют в тысячи раз большую соединяемость, чем современный компьютер. Однако необходимо отметить, что к ИНС применяются некоторые свойства, приобретаемые из биологических нейросетей, а именно:

1. Каждый нейрон действует независимо от всех остальных нейронов и его выход определяется только своим входом из соответствующих соединений.
2. Каждый нейрон располагает информацией, обеспечивающей только свои соединения.
3. Большое количество соединений обеспечивают многоразовое резервирование и обеспечивают распределенное представление информации.

Первые два свойства определяют параллельность обработки информации, третье – присущую нейросети отказоустойчивость.

Модель ИНС является связующей сетью с функциями обработки информации. Модели ИНС можно разделить на три категории в зависимости от соответствующих алгоритмов обучения: сети фиксированного веса, контролируемые и неконтролируемые. Сети фиксированного веса не требуют обучения, поэтому модели ИНС, способные к обучению, относятся либо к контролируемым, либо к неконтролируемым сетям.

Контролируемые сети обучения были господствующей тенденцией развития моделей ИНС. Так как примеры обучения состоят из множества пар образов обучения ввода-вывода, в неконтролируемом обучении существует "учитель", который в обучающей фазе "говорит" сети насколько хорошо она работает или какой режим является правильным. А в неконтролируемом обучении, так как набор обучения включает только образы ввода, сеть является автономной, то есть она смотрит только на представленные данные, ищет некоторые свойства набора данных и изучает их для того, чтобы отразить эти свойства в выводах.

Многим применениям также необходима высокая пропускная способность, особенно при обработке данных в реальном масштабе времени. Для этого необходимо развивать модели

параллельной ИНС так, чтобы параллелизм вычисления ИНС можно было легко реализовать. Модели параллельных ИНС должны удовлетворять следующим требованиям:

1. Функция каждого узла должна быть простой и выполнять постоянное действие;
2. Коммуникационная конфигурация должна быть простой и регулярной;
3. Передача данных между узлами должна быть параллельной и однообразной.

Несмотря на то, что каждый нейрон выполняет простую аналоговую обработку на низкой скорости, богатая связность между нейронами через синапсы представляет мощные вычислительные способности для большого количества данных. Известно, что большинство нейронных моделей, таких как сети обратного распространения, обладают свойством параллелизма. Некоторые модели подходят для параллельной обработки, например, иерархический персептрон и скрытая Марковская модель. Даже некоторые другие нейронные модели, такие как оригинальная модель Хопфилда, устройство Больцмана и метод отжига, могут стать параллелизуемыми после некоторой модификации оригинальных моделей. Кроме того, большинство нейронных алгоритмов включает в себя прежде всего повторяющиеся и регулярные операции. Их можно эффективно отобразить в параллельных структурах. В этой части развиты три вида моделей параллельных ИНС. Они представляются как:

- неконтролируемые модели обучения для нечеткой кластеризации;
- контролируемая модель обучения для классификации образов;
- модели нейронной сети для вычислений в конечных кольцах.

Нейронная сеть (НС) представляет собой высокопараллельную динамическую систему с топологией направленного графа [2-4], которая может получать выходную информацию посредством реакции ее состояния на входные воздействия. Узлами в НС называются процессорные элементы и направленные графы. Структура алгоритма обработки данных, также как и структура НС обладают естественным параллелизмом, что позволяет использовать НС в качестве формального аппарата описания алгоритмов криптографии. Кроме того, алгоритмы с ярко выраженным естественным параллелизмом, например, обработка сигналов, не используют режима обучения, вместе с тем органически вписываются в нейросетевой логический базис. С этой точки зрения алгоритмы модулярных вычислений соответствуют алгоритмам вычислений с помощью базовых процессорных элементов (искусственных нейронов). По этой причине схемы в СОК адекватны схемам на основе нейросетевого базиса. Искусственные нейронные сети и основные модулярные структуры представляют собой конвекционные устройства, полученные последовательным соединением между собой базовых элементов. Нейронные образования и модулярные образования будут послойно определены, если задан алгоритм соединения базовых элементов. Аппаратная реализация нейроподобных блоков, функционирующих в СОК, характерна и для нейроподобных образований, которые обладают максимальным естественным распараллеливанием и служат базой для разработки нового класса нейроподобных криптографических вычислительных структур.

Прогресс в создании и в будущем использовании нейрокомпьютеров не в малой степени зависит от решения двух проблем: проектирования вычислительных средств на новой схемотехнической базе и создание систем ЦОС на основе привлечения новых математических конструкций и концепции, в основе которых лежит массовый параллелизм [4, 6-7].

Аппаратная реализация нейроподобных блоков, функционирующих в системе остаточных классов, характерна и для нейроподобных образований, которые обладают максимальным естественным распараллеливанием и служат базой для разработки нового класса нейроподобных процессоров.

В настоящее время нейрокомпьютерная технология является одним из наиболее быстроразвивающихся разделов вычислительной техники [1-3]. Нейросетевые методы открывают широкие возможности для использования формального математического аппарата в различных сферах деятельности, ранее относящихся лишь к области человеческого интеллекта. Нейрокомпьютеры, построенные на базе нейронных сетей [2], являются перспективным направление развития вычислительной техники с массовым параллелизмом. Кроме того, при исследовании было установлено не только семантическое сходство математических моделей системы остаточных классов и нейронных сетей, но и единая их организация, что и определило перспективность разработки нейрокомпьютеров, функционирующих в системе остаточных классов. Параллельные вычислительные структуры являются идеальной основой для построения устойчивых к отказам вычислительных средств. Ключевую роль в процессе функционирования

таких вычислительных устройств играет способность сохранения работоспособного состояния за счет снижения в допустимых пределах каких-либо показателей качества при возникновении сбоев и отказов в системе. Достоинство данного подхода к выполнению процедур обеспечения отказоустойчивости реализуется в полной мере при перераспределении исходных данных между сохранившимися вычислительными ресурсами при деградации системы.

Сочетание системы остаточных классов и нейронных сетей, которые дополняют друг друга, вызывает интерес по той причине, что легко реализовать принципы обменных операций между быстродействием, точностью и надежностью с целью создания отказоустойчивого сопроцессора вейвлет-анализа [5].

Способность нейронных сетей к самообучению избавляет от необходимости использовать сложный математический аппарат. Благодаря своим способностям к самоорганизации и обучению, нейронные сети сейчас рассматриваются как перспективные средства для интеллектуальных систем, на основе которых появляется возможность создания принципиально новых приложений для ЦОС.

Литература:

1. Червяков Н.И., Головко А.Н., Кондрашов Ю.В., Лавриненко С.В. Метод и алгоритм основного деления модулярных чисел. СевКавГТУ, 2009 год – с. 124-128.

2. Червяков Н.И., Головко А.Н., Кондрашов Ю.В., Лавриненко С.В. Нейронная сеть для преобразования остаточного кода в позиционный с коррекцией ошибок. II Международная НТК – Невинномысск, 2009 год – С. 326-328.

3. Червяков Н.И., Кондрашов Ю.В. Модулярные вейвлет – преобразования и их применение к обработке сигналов. Самара, 2009 год – С. 12-14.

4. Червяков Н.И., Кондрашов А.В., Кондрашов Ю.В., Лавриненко А.В., Сляднев В.В. Взаимодействующие нейронные сети // XX Межвузовская научно-техническая конференция «Проблемы и перспективы развития инфотелекоммуникационных технологий в системах связи военного назначения»: – Сборник научных трудов – Ставрополь: СВИС РВ, 2008 – С. 13-14.

5. Сагдеев А.К., Груздев Д.А. Разработка и применение составных логистических функций для повышения скорости обучения вейвлет-нейронной сети // Наука и образование: проблемы и тенденции развития: материалы Международной научно-практической конференции (Уфа, 20-21 декабря 2013 г.):в 3-х ч. Часть II. – Уфа: РИЦ БашГУ, 2013. – 412 с. С. 129-135.

6. Сагдеев А.К., Новак А.В. Разработка нейросетевого вейвлет-фильтра // Наука и образование: проблемы и тенденции развития: материалы Международной научно-практической конференции (Уфа, 20-21 декабря 2013 г.):в 3-х ч. Часть II. – Уфа: РИЦ БашГУ, 2013. – 412 с. С. 204-210.

7. Сагдеев А.К., Сидоренко Е.Н. Анализ известных методов и алгоритмов дискретного вейвлет-преобразования // Наука и образование: проблемы и тенденции развития: материалы Международной научно-практической конференции (Уфа, 20-21 декабря 2013 г.):в 3-х ч. Часть II. – Уфа: РИЦ БашГУ, 2013. – 412 с. С. 227-233.

О.А. Лагунков, В.В. Шишкин

ТЕСТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНТЕРФЕЙСОВ МОДУЛЕЙ МЕЖБЛОЧНОЙ СВЯЗИ В АВИОНИКЕ ПО ТРЕБОВАНИЯМ НИЗКОГО УРОВНЯ

Ульяновский Государственный Технический Университет, г. Ульяновск, Россия

Ключевые слова: DO-178B, КТ-178B, тестирование программного обеспечения, аппаратные интерфейсы, ARINC, CAN, требования.

Описана проблема тестирования программного обеспечения, реализующего коммуникацию между авиационными блоками. К такому программному обеспечению предъявляются самые высокие требования по надежности, что усложняет процесс тестирования.

Тестирование проводится в несколько этапов и стоимость найденной ошибки постоянно возрастает. Приведены методические усовершенствования ранее представленного метода генерации модели тестируемого проекта, позволяющие сконцентрировать распределение найденных ошибок в первом этапе тестирования – тестировании по требованиям низкого уровня.

O.A. Lagunkov, V.V. Shishkin

LOW-LEVEL REQUIREMENTS SOFTWARE TESTING OF INTERFACES OF MODULES FOR INTERBLOCKS COMMUNICATION IN AVIONICS

Ulyanovsk State Technical University, Ulyanovsk, Russian Federation

Keywords: DO-178B, software testing, hardware interface, ARINC, CAN, requirements.

The problem in complexity emerges in testing software implementing communications of avionics blocks. This software must meet the highest requirements in terms of reliability. Testing performed in several stages and cost of error found constantly increasing. In this paper we deduced several methodical improvements of software model generation method. This improvements make possible to concentrate error distributing about first stage of testing – low-level requirements testing.

В процессе разработки бортовых систем возникает задача организации взаимодействия блоков. Такое взаимодействие обеспечивается с помощью стандартизированных протоколов, которые имеют аппаратно-программную реализацию, например CAN, ARINC-429, ARINC-629 и т.п. Жизненный цикл программного обеспечения бортовых систем в авионике регламентируется документом КТ-178В «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники», который является отечественным аналогом документа RTCA DO-178B «Software considerations in airborne systems and equipment sertification». Оригинальное руководство одобрено Федеральным управлением гражданской авиации США и рекомендовано к использованию Европейской организацией по обеспечению гражданской авиации. Одним из важнейших и трудоемких процессов разработки программного обеспечения для встраиваемых систем является тестирование и обеспечение покрытия кода. В данной работе рассматривается проблема невозможности подстройки тестового окружения для проверки на соответствие интерфейсной функции требованию низкого уровня.

Разработка программного обеспечения в соответствии с КТ-178В происходит в несколько этапов, декомпозирующих и дополняющих исходное техническое задание на требования системного уровня, высокого и низкого уровней. Последним этапом, предшествующим написанию исходного кода становится написание требований низкого уровня. Требование низкого уровня должно описывать то, что программное обеспечение должно делать или чего оно должно не делать. Требования низкого уровня, описание архитектуры, стандарты на кодирование и план разработки являются достаточными входными данными для начала процесса кодирования.[2] Следующим этапом жизненного цикла является верификация программного обеспечения, а самым трудоемким процессом верификации является тестирование.

Тестирование по требованиям низкого уровня должно показать соответствие программного обеспечение требованиям низкого уровня, а также показать отсутствие функций, не предусмотренных требованиями низкого уровня.[2,3] Первое условие проверяется за счет непосредственно процедуры тестирования, второе условие проверяется за счет обеспечения покрытия исходного кода. Критерий покрытия кода считается выполненным, если каждая строка исходного кода в процессе тестирования была выполнена хотя бы один раз. В рамках тестирования по требованиям низкого уровня используется метод генерации модели исходного кода, написанного на языке Си. Данный метод подразумевает использование функции исходного кода, как структурной единицы тестирования. В данном случае функция исходного кода является реализацией, требования низкого уровня – спецификацией. В идеальном случае стимулами для тестируемой функции являются входные параметры, а реакция выражается только через возвращаемое значение. Однако, объект тестирования погружен в среду или тестовое окружение, которое выражается ничем иным, как набором глобальных переменных, к которым функция имеет доступ. Глобальные переменные делятся на пересекающееся множества стимулов и реакций.[4]

Введем понятие *аппаратно-зависимый код* – это код, который может являться валидным, но при этом не может быть корректно скомпилирован и выполнен на хост-машине. Причиной может являться, например, обращение напрямую к регистрам микроконтроллера. Тестирование функций, содержащих аппаратно-зависимый код, выходит за рамки тестирования низкого уровня и относится к тестированию интеграции программного обеспечения и аппаратуры. Специфика программного обеспечения функций, реализующих межмодульные интерфейсы такова, что большая часть кода будет отнесена к тестированию интеграции программного обеспечения и аппаратуры. Такой подход существенно повышает затраты на тестирование, так как необходимо использование дополнительных инструментов для обеспечения анализа покрытия исходного кода. Также, возрастает стоимость обнаруженной ошибки, так как тестирование интеграции программного обеспечения и аппаратуры выполняется после тестирования низкого уровня и тестирования интеграции программного обеспечения. Целью исследования является сокращение объема тестирования на целевом вычислителе за счет вынесения максимально возможной части требований низкого уровня в тестирование на хост-машине.

Основной задачей тестирования низкого уровня является проверка правильности работы *логики и алгоритмов* кода, при этом, процесс тестирования интеграции программного обеспечения и аппаратуры подразумевает проверку специфику выполнения кода в среде целевого вычислителя, а именно – отсутствие переполнения стека, валидное время счета, корректная обработка прерываний и т.п.[5]

В качестве предмета рассмотрения аппаратно-зависимого кода выступила кодовая база ОАО «Ульяновское Конструкторское Бюро Приборостроения», которое занимается разработкой блоков авионики, в том числе в соответствии с КТ-178В. В результате рассмотрения исходного кода интерфейсных модулей блоков различного назначения был выявлен основной маркер аппаратно-зависимого кода – использование прямых адресов регистров и портов. При тестировании на хост-машине невозможно гарантировать, что конкретные адреса памяти могут быть доступны для использования в процессе тестирования.

Вторым маркером аппаратно-зависимого кода является алгоритм, в котором покрытие классов эквивалентности выходных данных является возможным только при запуске на целевом вычислителе. Примером такого кода является цикл, внутри которого массив заполняется побайтово из одного и того же байтового регистра без использования дополнительных функций.

В третью категорию попадает исходный код, который может быть заменен на эквивалентный аппаратно-независимый, также соответствующий требованиям низкого уровня. Примером является реализация сложения четырехбайтного адреса регистра и байтного подадреса с помощью дизъюнкции, что имеет место, если целевой вычислитель обеспечивает распределение памяти кратное 0x00. Однако при компиляции и запуске на хосте невозможно гарантировать кратность адреса массива 0x00.

Рассмотрим механизмы, позволяющие расширить область действия тестирования по требованиям низкого уровня.

Метод генерации модели исходного кода содержит процедуру заполнения шаблона тестового примера. Также метод реализует механизм заглушек функций исходного кода, который используется в двух случаях. Первый случай – это вызов из тестируемой функции другой функции, которая описана в другом компоненте того же проекта. В этом случае из спецификации известна ожидаемая реакция сторонней функции. Вместо сторонней функции будет подставлена заглушка, которая будет возвращать необходимую реакцию, что делает функцию неотличимой от оригинальной в рамках конкретного теста. Второй случай – функция, которая вызывается из тестируемой и взаимодействует со средой. В таком случае может быть эффективно заменить вызываемую функцию на заглушку, если вызываемая функция уже покрыта тестами[1].

Вторым механизмом является работа с указателями. Если одним из стимулов или реакций тестируемой функции является указатель, то в процессе составления тестового примера этому указателю в качестве значения может быть присвоен адрес пользовательской переменной определенного типа. При этом поддерживается многоуровневая система указателей.

Третий механизм реализуется через подмену используемых файлов исходного кода. При обеспечении целостности модуля тестируемой функции данные других модулей могут быть существенно упрощены или заменены для проведения корректного тестирования по требованиям низкого уровня. Требования, касающиеся взаимодействия модулей выносятся в отдельный вид тестирования – тестирование интеграции программного обеспечения.

Используя указанные механизмы, реализованные в методе генерации модели исходного кода, легко устраняется первый маркер аппаратно-зависимого кода. Очевидно, что регистры в рамках тестирования алгоритмов могут быть корректно заменены указателями на переменные с разрядностью не меньшей, чем у регистра. Для реализации такой замены необходимым и достаточным будет внесение дополнительного ограничения на использования адресов в стандарты кодирования предприятия, а именно требования о хранении любых значений константных адресов в отдельном заголовочном файле проекта. При тестировании такой файл будет заменен на аналогичный файл, где переменным будет вместо константного адреса присвоен тип *указатель*. При генерации модели исходного кода, в ходе анализа потока данных такие указатели будут опознаны, как стимулы или реакции и вынесены в шаблоны тестовых примеров.

Второй маркер может быть также устранен, однако для этого требуется введение дополнительных ограничений на этап проектирования. В данном случае при разделении интерфейсного и функционального кода понижается количество аппаратно-зависимого кода за счет возможности использования заглушек на интерфейсные функции. Другими словами, вынесение *любого* взаимодействия с аппаратурой в отдельные функции делает исходную функцию аппаратно-независимой, при создании заглушек на код, вынесенный в отдельные функции. Под интерфейсной функцией здесь подразумевается функция, которая содержит линейный код без операторов ветвления, которая обращается к аппаратной части компонента. В зависимости от сложности проекта целесообразным может быть внесение в стандарт на кодирование обособления всех таких интерфейсных функций в отдельный модуль.

Также становится возможным тестирование по требованиям низкого уровня большей части таких интерфейсных функций при корректной формулировке самих требований. Следует отметить, что аппаратная часть блока проходит отдельный процесс тестирования, показывающий корректную работу ячеек памяти, регистров, портов и т.п. Таким образом, проверка того, что в определенный регистр могут быть записаны данные, выполняется за рамками верификации программного обеспечения. Тестирование программного обеспечения должно показать, что интерфейсная функция обращается по корректному адресу. Это может быть проверено в процессе тестирования по требованиям низкого уровня с помощью следующего ряда формальных рассуждений. Если функция должна записывать значение в регистр, адрес которого хранится в переменной, то достаточно проверить, берет ли функция адрес регистра из корректной переменной и хранит ли эта переменная корректный адрес. Первое утверждение проверяется с помощью механизма работы с указателями, второе же утверждение требует внесения в архитектуру дополнительной функции, дающей доступ к чтению исходных переменных, хранящих адреса в заголовочных файлах. Для прозрачности проведения такого тестирования необходимо соответствующим образом разрабатывать требования низкого уровня.

Третья категория аппаратно-зависимого кода устраняется на стадии рассмотрения кода и не требует составления общих методик.

Вынесение большого количества тестируемого кода в процесс тестирования интеграции программного и аппаратного обеспечения увеличивает издержки на процесс тестирования. Это особенно актуально для интерфейсных модулей, реализующих взаимодействие между блоками, так как такие модули для конкретного протокола будут являться типовыми. Рассмотренная в работе методика позволяет максимально использовать метод генерации модели исходного кода в модулях, отвечающих за взаимодействие между блоками. Тестирование интерфейсных функций в рамках тестирования по требованиям низкого уровня уменьшает стоимость ошибок за счет раннего обнаружения. Покрытие всех требований низкого уровня в рамках тестирования на хост-машине позволяет демонстрировать покрытие кода уже на первом этапе тестирования, что также уменьшает стоимость ошибок проектирования.

Литература:

1. Kondratiev S.A., Lagunkov O.A., Shishkin V.V., Automatic Test Cases Generation Method for Embedded Systems Software. International Congress on Information Technologies-2012 (ICIT-2012): Proceedings of Abstracts. – Saratov : SSTU, 2012.

2. КТ-178. Квалификационные требования. Требования к программному обеспечению бортовой аппаратуры и систем сертификации авиационной техники. — Межгосударственный авиационный комитет, Авиационный регистр, 1996.

3. RTCA/DO-178B. Software considerations in airborne system and equipment certification – RTCAInc, 1992.

4. Шишкин В.В., Черкашин С.В. Автоматизированная система создания диагностического обеспечения комплексных систем электронной индикации и сигнализации летательных аппаратов. Датчики и системы. Москва: 2007, N12 (103). с. 39-42.

5. Шишкин В.В., Черкашин С.В. Автоматизация проектирования диагностического обеспечения и диагностирования авиационных бортовых информационных систем. УлГТУ, Ульяновск, 2010.

Д.М. Лебеденко, Н.Н. Чернышев

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

Донецкий национальный технический университет, г.Донецк, Украина

Ключевые слова: программа SAP, методы автоматизации, аналитическая отчетность, решение по оптимизации, финансовая деятельность, управление, предприятие.

В настоящие время существует острая необходимость организации системы автоматизированного финансового учета с целью обеспечения анализа эффективности деятельности предприятия и совершенствования процесса принятия стратегических управленческих решений …

D.M. Lebedenko, N.N. Chernyshev

INFORMATION TECHNOLOGY APPLICATIONS FOR AUTOMATING THE PROCESS ENTERPRISE MANAGEMENT

Donetsk National Technical University, Donetsk, Ukraine

Keywords: program SAP, automation methods, analytical reporting, decision optimization, finance, management, enterprise.

Now exist an acute necessity to organize automatic financial accounting system to ensure the efficiency analysis of the enterprise management and improve the process of making strategic management decisions ...

Актуальность.

В современных условиях функционирования предприятий существует необходимость организации системы управленческого учета с целью обеспечения объективного анализа эффективности деятельности предприятия, и в свою очередь, совершенствования процесса принятия стратегических управленческих решений. Для этого требуется разработка отдельных механизмов, с помощью которых производится формирование аналитической отчетности и которые упрощают процесс обобщения и обработки большого массива данных. Важную роль в решении этой проблемы должна выполнить методика построения бизнес процессов при формировании аналитической отчетности, а также обеспечение ее полноты, оперативности и достоверности [1].

Основное внимание направлено на создание алгоритмов и решений по оптимизации существующих форм отчетности. В работе учитывается опыт введенных программ по филиалу управления магистральными газопроводами «Донбастрансгаз» (г. Донецк).

Цель.

Усовершенствование существующих бизнес решений методам автоматизации при составлении аналитической отчетности в финансовых отделах предприятия.

Для достижения цели необходимо решить следующие задачи:

1. Исключить двойное введение данных отделами и службами при создании « Служебных записок на перечисление средств»;
2. Свести финансовый, плановый и договорной учет в единую систему учета для формирования единой информационной базы данных;
3. Разработать механизмы построения отчетности из существующих признаков и показателей;
4. Обеспечить синхронизацию между разными модулями в части восстановления и дополнение информации при сравнении унифицированных однородных признаков;
5. Повысить достоверность информации что составляется;
6. Сократить время на формирование финансовой отчетности;
7. Предоставить возможность формирования отчетности с необходимой степенью детализации и критериям (например, в разрезе статей финансового плана, центров финансовой ответственности, структурных подразделов, контрагентов, договоров и дат возникновение задолженности, а также в разрезе необходимого периода: день, месяц, квартал, год).

Постановка проблемы.

При проведении масштабной реконструкции ГТС важную роль играет оптимальное и своевременное распределение финансовых ресурсов компании. Для этого требуется наличие достоверной оперативной финансовой информации, на основании которой принимаются правильные управленческие решения.

При составлении финансовой отчетности важной составляющей является скоординированная работа финансового, договорного, планово-экономического отделов и бухгалтерии предприятия. Выходом из ситуации является создание единой информационной базы данных, которая отражает реквизиты, составляющие части и признаки первичных и платежных документов, их взаимосвязь, с целью общего доступа финансового, договорного, бухгалтерского и планово-экономического отделов. Ввод данных должен осуществляться сотрудниками инициирующих отделов в единую информационную базу данных. Необходимые данные должны автоматически отображаться во всех отчетных формах каждого отдела. Данная конструкция позволит обеспечить устранение механических ошибок, возникающих в последствии дублирующего ввода первичных данных в систему, и получить единую унифицированную базу данных для составления различной отчетности.

Создание аналитической отчетности из единой базы данных системы SAP с учетом взаимоотношений между модулями

ДК «Укртрансгаз» - это крупная производственная компания, которая охватывает всю территорию Украины. Внедрение единого программного комплекса SAP для компании ДК «Укртрансгаза» в будущем обеспечит работу 16 функциональных направлений (в том числе: финансовый и налоговый учет, управление и учет материальных потоков, учет основных средств, управление технологическим процессом, затратами, качеством, ремонтами, бюджетами, доходами, проектами, капитальными инвестициями). Система SAP является одной из лучших систем в мире, позволяет объединить такое количество функциональных направлений. Внедрение основных модулей программы осуществляется высокими темпами в сжатые сроки. Центр внедрения полноценно не учел все бизнес процессы многоуровневой системы компании, тем самым не решив важную задачу - составление корпоративной отчетности без дублирования данных.

Количество созданных отчетов центром внедрения полноценно не удовлетворяют пользователей программы, а иногда вводят в заблуждение, заставляя дублировать ввод данных для проверки, выгружая их из программы SAP в Excel для анализа и составления корпоративных отчетов. Для упрощения механизма составления аналитических отчетов для руководства рекомендуется предоставить уполномоченным работникам филиала разрешение на использование штатных аналитических возможностей в системе SAP - Business Explorer Analyzer.

SAP Business Explorer Analyzer - это интегрированная программа в Microsoft Office, обеспечивает возможность самостоятельного создания отчетов. Она позволяет:

- использовать широкий набор формул расчетов коммерческих показателей и показателей времени с целью нахождения, сравнения и прогнозирования бизнес-факторов в Excel (рисунок 1);
- приводить глубинный анализ бизнес-процессов, изучать тенденции, резко отвергают ключевые показатели и все это без помощи администратора базы данных;

– создавать интерактивные презентации Powerpoint с встроенными способами аналитики (рисунок 2 и 3);
– обмениваться аналитической информацией с коллегами; обновлять данные отчета в режиме онлайн;
– быстро анализировать большие объемы данных в SAP Netweaver BW с ускорением In Memory.

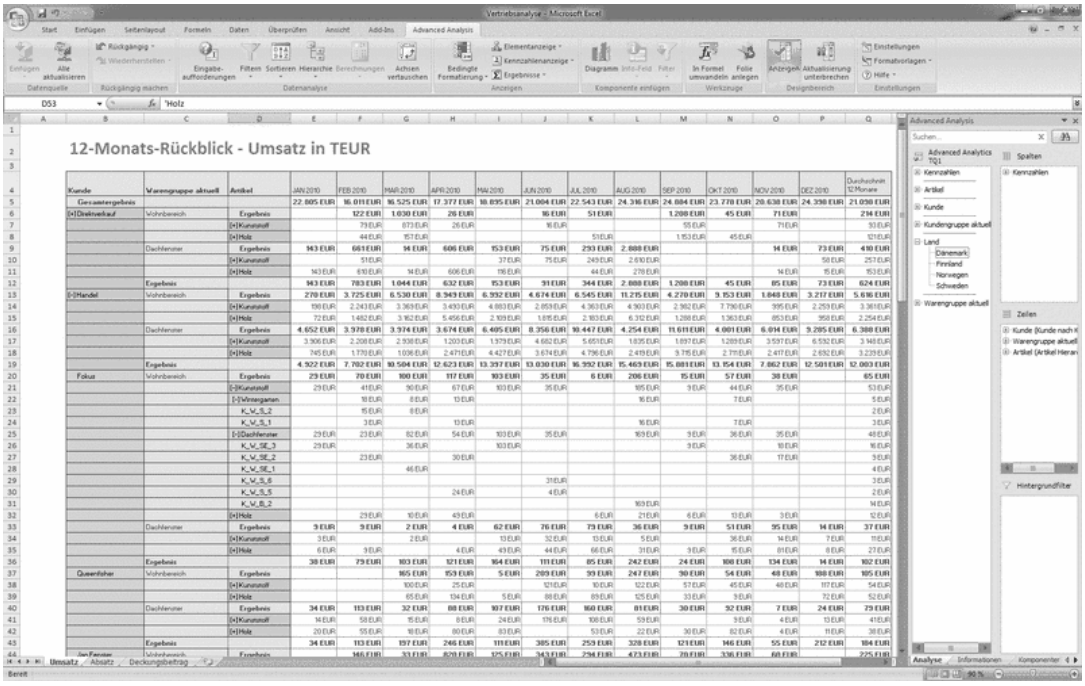


Рисунок 1. Пример плоского отчета сделанного при помощи SAP Bex Analyzer

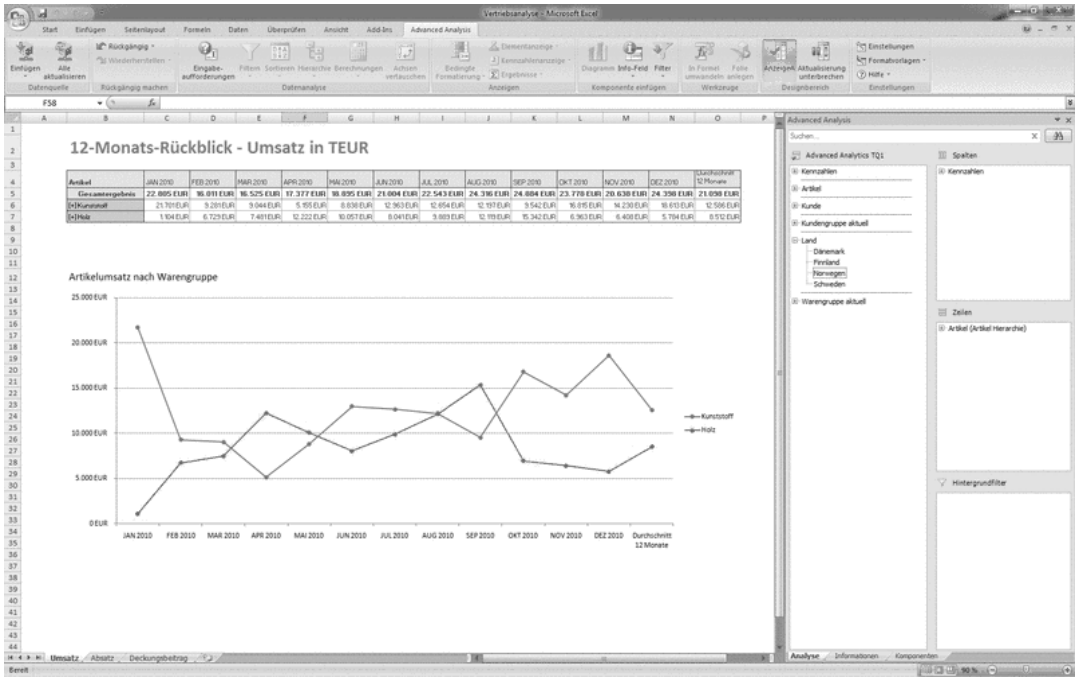


Рисунок 2. Отчет с использованием диаграмм сделанного в SAP Bex Analyzer

Модуль Analyzer интегрирован в Excel - это инструмент, предоставляющий уникальные аналитические возможности, включая возможность одновременного просмотра данных из нескольких источников, который интуитивно понятны и просты в использовании. Например, можно использовать в одном отчете дани по финансовой деятельности модулю FM, служебной

записке по ТОРА заказам модулю PM, информации по договорам/тендерам модулю MM и другим модулям.

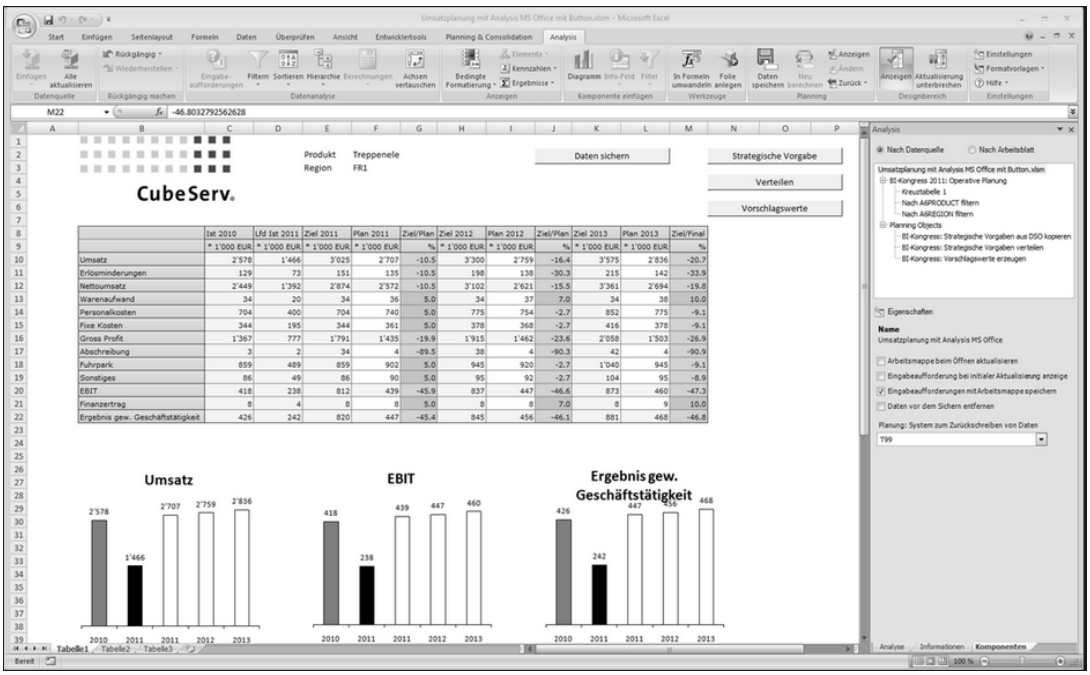


Рисунок 3. Пример аналитического отчета сделанного в SAP Bex Analyzer

Использованные методы позволили повысить уровень квалификации сотрудников, открывши перед ними новые технические возможности и методы в формировании нестандартных аналитических отчетов. Данные методы позволили подготовить их к внедрению новых форм отчетности при помощи программы SAP ERP.

Выводы.

1. В данной работе изложенные алгоритмы работы, которые были введены в аппарате УМГ «Донбастрансгаз» и его структурных подразделах, и имеют рекомендованный характер при внедрении программы SAP ERP.

2. Внедрение рекомендованного SAP Business Explorer Analyzer позволит самостоятельно пользователям программы формировать необходимые аналитические отчеты без применения специалистов центра внедрения программы SAP и отдела информационных технологий. Данная возможность позволит перераспределить функциональную нагрузку на систему SAP ERP и уменьшить нагрузку на работников центра внедрения программы SAP централизуя их внимание на совершенствование управления бизнес процессами.

Литература:

1. Программное обеспечение и решения SAP. Режим доступа: http://www.sap.com/cis/pc/bp/erp.html

2. Цисарь И.Ф. Компьютерное моделирование экономики / И.Ф. Цисарь, В.Г. Нейман. – М. - «Диалог-МИФИ», 2002.-304 с.

3. Фещенко О. Информационное и методическое обеспечения анализа состояния государственных предприятий Украины / О. Фещенко // Рынок ценных бумаг Украины. - 2009. - №1-2. - С. 49-61.

4. Шумило О.Ю. Пути усовершенствования проведения анализа на предприятии / О.Ю. Шумило // Экономика. Финансы. Право. - 2009. - №3. - С.25-28.

М.П. Лялина

НАДЕЖНОСТЬ КАНАЛА СВЯЗИ

Московский технический университет связи и информатики, г. Москва

Ключевые слова: компактная рамочная антенна, надежность радиосвязи, повышение надежности радиосвязи, антенная решетка, магнитнодиэлектрическая стенка.

Описана проблема обеспечения повышения надежности радиосвязи в коротковолновом диапазоне. Приведена модель антенны, при помощи которой возможно улучшение надежности радиосвязи. Уникальным является магнитнодиэлектрическая стенка между антенными системами, предназначенная для повышения развязки между антенными системами.

M.P. Lyalina

THE RELIABILITY OF THE COMMUNICATION CHANNEL

Moscow Technical University of Communications and Informatics, Moscow

Keywords: compact antenna system, reliability of radio communication, antenna array, dielectric-magnetic wall.

Described the problem of improving the reliability of radio communication in the short range. A model of the antenna, with which you can improve the reliability of radio communications. Unique is magnetic-dielectric wall between the antenna systems designed to improve isolation between antenna systems.

Статистические вопросы радиотехники стали активно внедряться в теорию и практику радиосвязи в начале 60-х гг., когда статистическая радиофизика стала одним из наиболее внедряемых предметов в системе высшей школы.

Действительно, надежность канала коротковолновой радиосвязи порядка 10-2 перестал удовлетворять потребителей и появилась насущная необходимость повысить надежность канала с 10-2 до 10-4, 10-6, 10-8, а в 1960-х годах — до 10-11, 10-12. Резкое повышение надежности канала было достигнуто за счет строенного приема и внедрения систем с переспросом. Так как наиболее надежной системой связи была телеграфная связь, то в качестве качественной характеристики надежности связи было принято отношение неверно принятых знаков к общему числу переданных знаков.

При дальнейшем развитии радиосвязи проявилась потребность в более глубоком определении статистических характеристик, относящихся к качеству связи, поэтому появился термин «устойчивость радиосвязи». Устойчивость функционирования сети электросвязи определена ГОСТом [5] и обозначает способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов. На сети электросвязи могут воздействовать как внешние, так и внутренние дестабилизирующие факторы. Поэтому устойчивость сети электорсвязи можно представить в виде суммы свойств надежности и живучести. Надежность определена ГОСТом так: свойство сети электросвязи сохранять способность выполнять требуемые функции в условиях воздействия внутренних дестабилизирующих факторов.

В значительной мере, вопросы, связанные с надежностью радиосвязи, определяются качеством работы антенны. Вопросы обработки сигнала достигли достаточно высокого уровня, поэтому в значительной мере качество приема сигнала можно повысить антенной, т.к. антенны не до конца изучены и, как следствие, использованы не все ее возможности.

Антенны можно использовать для повышения качества сигнала. Для этого применяется поляризационно разнесенный прием. Две антенны используют также для повышения пропускной способности канала.

Рассмотрим антенны с поляризационно разнесенным приемом. В таком случае, для приема лучей с разной поляризацией используют две системы антенн.

Обязательным условием применения любого разнесенного приема - в точке приема сигналы должны быть независимы. Если условие выполнено, то максимальные и минимальные значения амплитуд сигналов с наибольшей вероятностью не совпадут. Благодаря этому уменьшается динамический диапазон изменений амплитуды результирующего сигнала и, следовательно, повышается среднее отношение сигнал/помеха по сравнению с одиночным (неразнесенным) приемом.

Компактная рамочная антенная система с поляризационным разнесением для мобильных телефонов, роутеров и других подобных систем мобильной связи, предложенная Белянским В.Б. и Аникиным К.В., способна повысить надежность радиосвязи. Система представляет собой две решетки рамок прямоугольной формы, скомпонованных перпендикулярно плоскому экрану и ограниченных в пространстве полупрозрачным (магнитным) экраном в форме прямоугольного параллелепипеда, разделенного по диагонали плоским экраном на две области, в каждой из которых и расположены решетки со взаимоперпендикуляными рамками. Рамки имеют одинаковую ширину и одинаковое расстояние между ними.

Антенная система с поляризационным разнесением имеет размеры 10x10x0,5 мм3, работает на частотах в области 6 МГц с относительной рабочей частотной полосой частот 5 – 10 % (рисунок 1). Если выполнить размеры антенных систем, подчиняющимися логопериодическому закону, то рабочую полосу частот можно сделать существенно более широкой. Кроме того, если снабдить каждую рамку конденсатором, снижающим ее резонансную частоту, то можно также существенно снизить габариты антенны. Антенные системы, имеющие различные поляризации, разделены магнитной стенкой с $\varepsilon r \neq 1$, $\mu r \neq 1$. Поляризационные экраны могут существенно изменить характер ближнего поля системы, почти не меняя поле в дальней стенке. Стенки предназначены для повышения развязки между антенными системами.

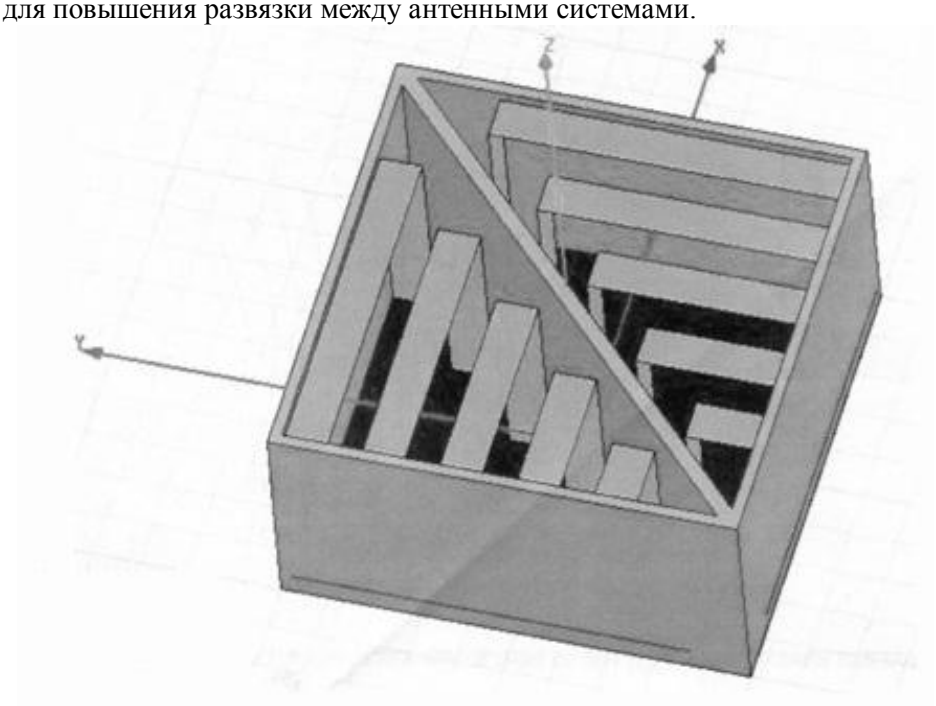


Рисунок 1. Антенная система, состоящая из двух рамочных систем с двумя ортогональными поляризациями. Используются полупрозрачные (магнитные) экраны/

Исследование зависимости степени развязки между антенными системами в зависимости от параметров стенки выполнены с участием Лялиной М.П. и Аникина К.В. с помощью точного электродинамического расчета. Результаты расчета представлены на рисунке 2 и рисунке 3. Показано, что при заданной толщине стенки 0,1 мм имеется оптимальные значения диэлектрической и магнитной проницаемости стенок, при которых коэффициент развязки антенных систем максимален.

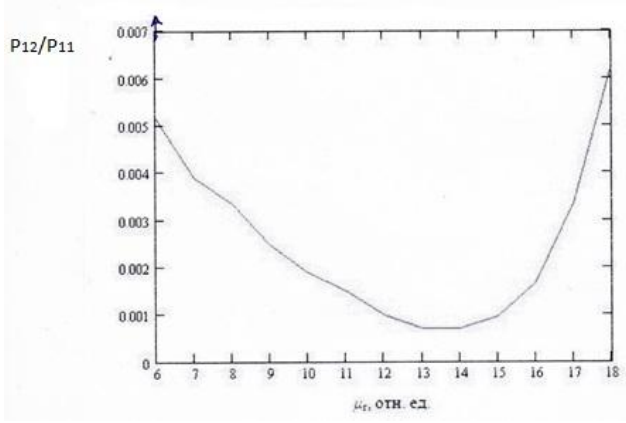


Рисунок 2. Зависимость коэффициента развязки по мощности $|\xi|^2$ от относительной магнитной проницаемости μ_r экранов

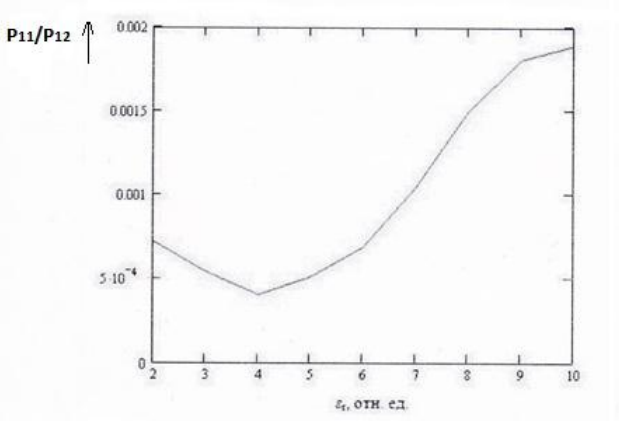


Рисунок 3. Зависимость коэффициента развязки от магнитной и диэлектрической проницаемости стенки

Литература:

1. Войтович Н.Н., Каценеленбаум Б.З., Коршунова Е.Н. и др. Электродинамика антенн с полупрозрачными поверхностями: методы конструктивного синтеза. Под. ред. Б.З.Каценеленбаума и А.Н.Сивова. М.: Наука, 1989г.

2. Аникин К.В., Белянский В.Б. Компактная рамочная антенная система разнесенного приема. Т – Comm, №8, 2011г., стр. 15 – 18.

3. Аникин К.В., Белянский В.Б. Компактная рамочная антенная система разнесенного приема. Антенны. Выпуск 1 (176), 2012г., стр. 9 – 16.

4. Банков С.Е., Курушин А.А. Электродинамика и техника СВЧ для пользователей САПР. М., ИРЭ РАН, http://www.cplire.ru/rus/library/276c

5. В.В.Миркин. К истории Советской радиосвязи и радиовещания в 1945 — 1965гг. Вестник Томского государственного университета. История. 2013. №1 (21)

6. ГОСТ 53111 – 2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки

А.В. Ляхов, В.П. Пашинцев, Н.Г. Касьяненко

АНАЛИЗ СРЕДНЕКВАДРАТИЧЕСКОЙ ПОГРЕШНОСТИ ОПРЕДЕЛЕНИЯ ИНТЕНСИВНОСТИ МЕЛКОМАСШТАБНЫХ НЕОДНОРОДНОСТЕЙ ИОНОСФЕРЫ НА БАЗЕ ДВУХЧАСТОТНОГО ПРИЕМНИКА СИГНАЛОВ GPS/ГЛОНАСС

Северо-Кавказский федеральный университет, Ставрополь, Россия

Ключевые слова: среднеквадратическая погрешность, интенсивность мелкомасштабных неоднородностей ионосферы, двухчастотный приемник сигналов GPS/ГЛОНАСС.

Получены аналитические выражения, позволяющие исследовать среднеквадратическую погрешность определения интенсивности мелкомасштабных неоднородностей искусственных ионосферных образований на базе двухчастотного приемника сигналов GPS/ГЛОНАСС.

A.V. Lyakhov, V.P. Pashintsev, N.G. Kas'yanenko

ANALYSIS OF ROOT MEAN SQUARE ERROR OF FINDING THE INTENSITY OF SMALL-SCALE INHOMOGENEITIES OF ARTIFICIAL IONOSPHERIC FORMATIONS, USING A TWO-FREQUENCY GPS / GLONASS SIGNAL RECEIVER

North-Caucasus Federal University, Stavropol, Russia

Keywords: root-mean-square error, the intensity of small-scale ionospheric formations, double-frequency GPS/GLONASS signal receiver.

In a result obtained the analytical expressions, allowing to research the root mean square error of finding the intensity of small-scale inhomogeneities of artificial ionospheric formations, using a two-frequency GPS / GLONASS signal receiver.

Известно [1–3], что радионагрев ионосферы мощным коротковолновым излучением приводит к возникновению в локальной области искусственного ионосферного образования (ИИО), содержащего вытянутых вдоль геомагнитного поля неоднородности электронной концентрации (ЭК), и сопровождается возрастанием интенсивности ее мелкомасштабных неоднородностей (ММН). Количественно эта интенсивность характеризуется отношением [4]:

$$\beta\left(\sigma_{\Delta I},\langle I_m\rangle,h_э,l_s\alpha\right)=\frac{\sigma_{\Delta I}}{\langle I_m\rangle}\sqrt{\frac{h_э\operatorname{cosec}(\alpha)}{\sqrt{\pi}l_s}}\,, \tag{1}$$

где $\sigma_{\Delta I}$ – среднеквадратическое отклонение (СКО) флуктуаций ΔI полного электронного содержание (ПЭС) в ионосфере, эл/м^2; $\langle I_m\rangle$ – максимальное среднее значение ЭК в ионосфере на высоте $h = h_{\text{m}}$ максимума ее ионизации, эл/м^2; $h_э$ – эквивалентная толщина ионосферы ($h_э \approx 5\cdot10^5$ м); l_s – характерный (средний) размер мелкомасштабных ионосферных неоднородностей ($l_s \sim$ 400 м); α – угол наклона трассы распространения радиоволн (РРВ) относительно горизонта ($\alpha \geq 30^\circ$).

Как было показано в [4], выражение (1) позволяет реализовать способ не только обнаружения, но и пеленгации ИИО на основе измерения интенсивности ионосферных неоднородностей с помощью двухчастотного приемника сигналов GPS/ГЛОНАСС. При этом правило принятия решения об обнаружении ИИО принимает вид:

$$\beta(\alpha_n)\geq\beta_{\text{пор}}, \tag{2}$$

где $\beta_{\text{пор}}$ – некоторое пороговое значение интенсивности неоднородностей ионосферы.

В работе [4] показано, что на практике при выборе порогового значения $\beta_{\text{пор}}$ необходимо учесть, что в нормальной ионосфере интенсивность неоднородностей мала и составляет β = 0,1…1% [4], а в условиях ИИО ионосферы она может заметно возрастать до β = 1…20%. Поэтому значение порогового уровня целесообразно выбирать из условия: $\beta_{\text{пор}} = 1$% или $\beta_{\text{пор}} = 0,01$.

Так как пороговое значение уровня интенсивности ММН ионосферы представляет достаточно малую величину, то актуальной задачей является оценка точности, с которой может быть определен этот параметр. Кроме того, как следует из (1), оценка интенсивности ионосферных неоднородностей производится не непосредственно, а косвенно посредством предварительного определения параметров: $\sigma_{\Delta I}$, $\langle I_m\rangle$, $h_э$, l_s, α.

Полагаем известной область G в пространстве переменных $\sigma_{\Delta I}$, $\langle I_m\rangle$, $h_э$,. Требуется на основе соотношения (1) оценить, как изменяется среднеквадратическая погрешность определения интенсивности ММН ионосферы при изменении угла α наклона трассы РРВ относительно горизонта в интервале углов $30^\circ \leq \alpha \leq 90^\circ$.

Из теории ошибок известно, что квадрат среднеквадратической погрешности функции общего вида $u = f\left(x,y,z,\ldots\right)$ равен сумме квадратов произведений частных производных по каждой переменной, умноженных на их среднеквадратические погрешности

$$\sigma_u^2=\left(\frac{\partial f}{\partial x}\right)^2\sigma_x^2+\left(\frac{\partial f}{\partial y}\right)^2\sigma_y^2+\left(\frac{\partial f}{\partial z}\right)^2\sigma_z^2\ldots\,, \tag{3}$$

С учетом (3) среднеквадратическая погрешность функции (1) принимает вид:

$$\sigma_\beta = \sqrt{\left(\frac{\partial\beta}{\sigma_{\Delta I}}\right)^2 \sigma^2_{\sigma_{\Delta I}} + \left(\frac{\partial\beta}{\partial\langle I_m\rangle}\right)^2 \sigma^2_{\langle I_m\rangle} + \left(\frac{\partial\beta}{\partial h_э}\right)^2 \sigma^2_{h_э} + \left(\frac{\partial\beta}{\partial l_s}\right)^2 \sigma^2_{l_s} + \left(\frac{\partial\beta}{\partial\alpha}\right)^2 \sigma^2_\alpha}, \quad (4)$$

где $\sigma^2_{\sigma_{\Delta I}}$ – квадрат среднеквадратического отклонения СКО флуктуаций ΔI полного электронного содержания (ПЭС) в ионосфере; $\sigma^2_{\langle I_m\rangle}$ – квадрат среднеквадратического отклонения максимального среднего значения ЭК в ионосфере на высоте $h = h_m$ максимума ее ионизации; $\sigma^2_{h_э}$ – квадрат среднеквадратического отклонения определения эквивалентной толщины ионосферы; $\sigma^2_{l_s}$ – квадрат среднеквадратического отклонения определения характерного (среднего) размера мелкомасштабных ионосферных неоднородностей; σ^2_α – квадрат среднеквадратического отклонения определения угла наклона трассы распространения радиоволн (РРВ) относительно горизонта.

Выполнив дифференцирование (1) по аргументам $\sigma_{\Delta I}$, $\langle I_m\rangle$, $h_э$, l_s, α, получим следующие выражения для частных производных по каждой переменной:

$$\frac{\partial\beta}{\sigma_{\Delta I}} = \frac{1}{\langle I_m\rangle}\sqrt{\frac{h_э \operatorname{cosec}(\alpha)}{\sqrt{\pi} l_s}}, \quad (5)$$

$$\frac{\partial\beta}{\partial\langle I_m\rangle} = -\frac{\sigma_{\Delta I}}{\langle I_m\rangle^2}\sqrt{\frac{h_э \operatorname{cosec}(\alpha)}{\sqrt{\pi} l_s}}, \quad (6)$$

$$\frac{\partial\beta}{\partial h_э} = \frac{\sigma_{\Delta I}\operatorname{cosec}(\alpha)}{2\sqrt{\pi} l_s \langle I_m\rangle\sqrt{\frac{h_э \operatorname{cosec}(\alpha)}{\sqrt{\pi} l_s}}}, \quad (7)$$

$$\frac{\partial\beta}{\partial l_s} = -\frac{\sigma_{\Delta I} h_э \operatorname{cosec}(\alpha)}{2\sqrt{\pi} l_s^2 \langle I_m\rangle\sqrt{\frac{h_э \operatorname{cosec}(\alpha)}{\sqrt{\pi} l_s}}}, \quad (8)$$

$$\frac{\partial\beta}{\partial\alpha} = -\frac{\sigma_{\Delta I} h_э \operatorname{cosec}(\alpha)^2 \cos(\alpha)}{2\sqrt{\pi} l_s \langle I_m\rangle\sqrt{\frac{h_э \operatorname{cosec}(\alpha)}{\sqrt{\pi} l_s}}}, \quad (9)$$

Для дальнейших расчетов примем: $\sigma_{\Delta I} = 0,005$ эл/м^2, $\langle I_m\rangle = 20$ эл/м^2, $h_э = 5\cdot 10^5$ м, $l_s = 400$ м, $\sigma_{\sigma_{\Delta I}} = 0,0005$ эл/м^2, $\sigma_{\langle I_m\rangle} = 0,1$ эл/м^2, $\sigma_{h_э} = 1000$ м, $\sigma_{l_s} = 10$ м, $\sigma_\alpha = 0,5^\circ$.

Результаты расчетов среднеквадратической погрешности определения интенсивности ММН ионосферы по формуле (4) при изменении угла α наклона трассы РРВ относительно горизонта в интервале углов $30^\circ \le \alpha \le 90^\circ$ представлены в форме графика на рисунке 1.

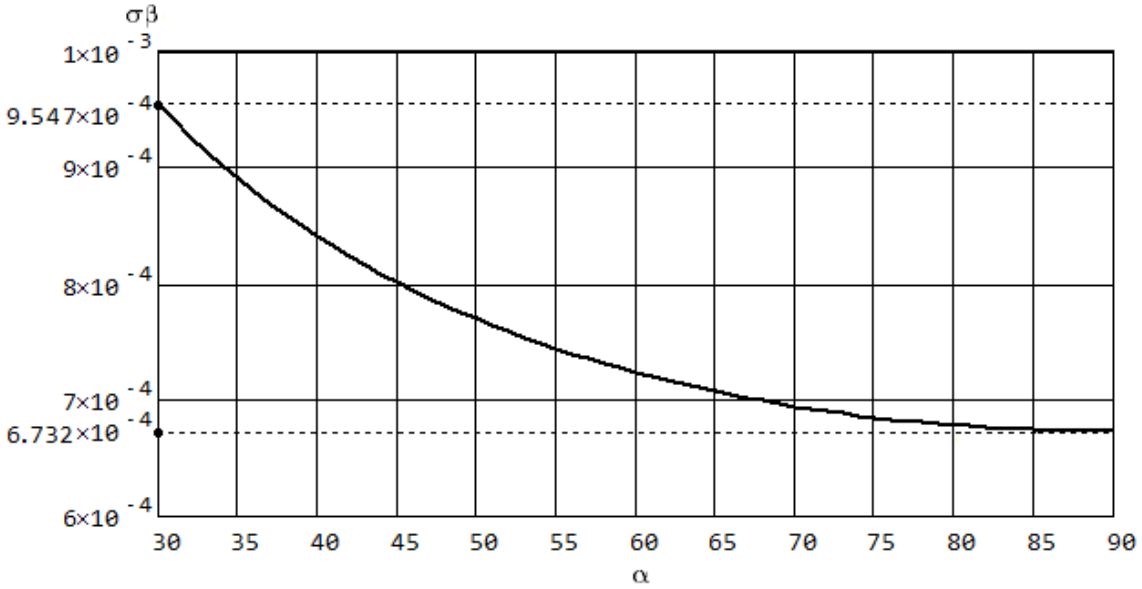


Рисунок 1. График изменения среднеквадратической погрешности определения интенсивности ММН ионосферы при изменении угла α наклона трассы РРВ относительно горизонта в интервале углов $30^\circ \le \alpha \le 90^\circ$

Из анализа графика на рисунке 1 можно сделать следующие выводы:

1. При изменении угла α наклона трассы РРВ относительно горизонта в интервале углов $30^\circ \le \alpha \le 90^\circ$ среднеквадратическая погрешность определения интенсивности ММН ионосферы монотонно убывает в интервале от $9,547 \times 10^{-4}$ до $6,732 \times 10^{-4}$;
2. Для уменьшения среднеквадратической погрешности определения интенсивности ММН ионосферы с помощью двухчастотного приемника сигналов GPS/ГЛОНАСС необходимо использовать трассы РРВ, имеющие угол места относительно горизонта близкий к зенитному.

Практическая значимость полученных результатов состоит в том, что они позволяют обосновать требования, которым должны удовлетворять среднеквадратические погрешности параметров, входящих в правую часть формулы (1), при заданных ограничениях на среднеквадратическую погрешность расчета значения интенсивности мелкомасштабных неоднородностей ионосферы, что и составит предмет дальнейших исследований.

Литература:

1. Лобанов Б.С. Исследование возможности создания в ионосфере объемных образований, эффективно взаимодействующих с электромагнитным излучением в сверхширокоm диапазоне частот // Теория и техника радиосвязи, 2009, №3, с. 16-24.

2. Афраймович Э.Л., Перевалова Н.П. GPS – мониторинг верхней атмосферы Земли. – Иркутск, 2006 – 480с.

3. Пашинцев В. П., Коваль С.А., Стрекозов В. И., Бессмертный М. Ю. Обнаружение искусственных ионосферных образований с помощью спутниковых радионавигационных систем / В. П. Пашинцев, С.А. Коваль, В. И. Стрекозов, М. Ю. Бессмертный // Теория и техника радиосвязи, 201 3, Т.48, №1, с. 112-117.

4. Ляхов А.В., Пашинцев В.П., Касьяненко Н.Г. Обнаружение и пеленгация искусственных ионосферных образований на базе спутниковых систем GPS/ГЛОНАСС // Инфокоммуникационные технологии в науке, производстве и образовании: шестая международная научно-техническая конференция. – Ставрополь, Северо-Кавказский федеральный университет, 2014, с. 162-167.

Е.А. Волгарев, И.А. Малкова, Н.И. Ильиных

ТЕРМОДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ МАТЕРИАЛОВ ЭЛЕКТРОННОЙ ТЕХНИКИ

Уральский технический институт связи и информатики (филиал) федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге, Россия

Ключевые слова: полупроводниковые материалы, галлий, сурьма, алюминий, индий, термодинамическое моделирование, расплав, свойства.

В настоящей работе с использованием методики термодинамического моделирования и программного комплекса TERRA проведено исследование равновесного состава и термодинамических характеристик бинарных расплавов Ga-Sb, Al-Sb, In-Sb в широком интервале температур и составов. Построены концентрационные зависимости содержания активностей компонентов, парциальных и интегральных характеристик смешения расплавов. Показано, что для всех исследованных расплавов наблюдаются большие отрицательные отклонения от закона Рауля. Этот факт обусловлен наличием ассоциатов и свидетельствует о сильном взаимодействии между компонентами расплава.

E.A. Volgarev, I.A. Malkova, N.I. Ilinykh

THERMODYNAMIC MODELING OF ELECTRONICS MATERIALS

Federal State Budget Institution of Higher Professional Education «Siberian State University of Telecommunications and Informatics» Ural Technical Institute of Communications and Informatics (Branch), Yekaterinburg, Russia

Keywords: semiconductor materials, gallium, antimony, aluminum, indium, thermodynamic modeling, melt, properties.

At the presented paper the investigation of equilibrium composition and thermodynamic characteristics of binary Ga-Sb, Al-Sb and In-Sb melts was carried out in a wide range of temperatures and compositions using the thermodynamic modeling method and TERRA software.

The concentration dependencies of composition, activities of components, integral and partial excess characteristics of melt were constructed. It was shown, that the big negative deviation from Raol's low take place for all of investigated systems. This fact is caused by the presence of associates and justify, that strong interaction between particles takes place.

Современная электронная техника развивается таким образом, что в сферу активного использования вовлекаются все более сложные полупроводниковые материалы. Наибольший научный и практический интерес представляют бинарные соединения типа $A^{III}B^{V}$, $A^{II}B^{VI}$ $A^{IV}B^{IV}$, которые в настоящее время являются важнейшими материалами полупроводниковой электроники. В настоящее время трудно представить разработку и исследование процессов получения полупроводниковых полифункциональных структур сложного состава и строения без предварительного термодинамического рассмотрения. Термодинамические исследования являются основой технологии управляемого синтеза полупроводниковых и других материалов электронной техники для создания на их базе электронных структур. Таким образом, проведение термодинамических исследований является ***актуальной*** задачей. Наряду с задачей получения материалов для микроэлектроники и изучения их характеристик ***актуальной*** является также задача исследования поведения этих материалов в экстремальных условиях, в частности, в агрессивных средах, при высоких или, наоборот, криогенных температурах, повышенных давлениях и т.д. Поэтому ***целью*** настоящей работы является исследование равновесного состава и термодинамических характеристик бинарных расплавов Ga-Sb, Al-Sb, In-Sb в широком интервале температур и составов.

Исследование выполнено с использованием методов термодинамического моделирования (ТМ), программного комплекса TERRA, модели идеальных растворов (ИР) и модели идеальных растворов продуктов взаимодействия (ИРПВ) [1 - 3] в исходной среде аргона при общем давлении 10^5 Па. Исследовалась область температур и составов, соответствующая жидкому состоянию согласно [4]: система AlSb: T = 1300 – 1700 К, системы Ga-Sb, In-Sb: T = 1000 - 1600 К, $0 \le x_{Ga(In,\ Al)} \le 1$, где $x_{Ga(In,\ Al)}$ - исходное содержание галлия (индия, алюминия) в расплаве (мол. доли). При моделировании учитывались термодинамические функции следующих элементов и соединений: газообразных Ga, Sb, In, Al, Sb_2, Sb_3, Sb_4, In, Al, Al_2, Ar^+, Ga^+, In^+, Al^+ и конденсированных Ga, Sb, Al, In, InSb, AlSb и GaSb.

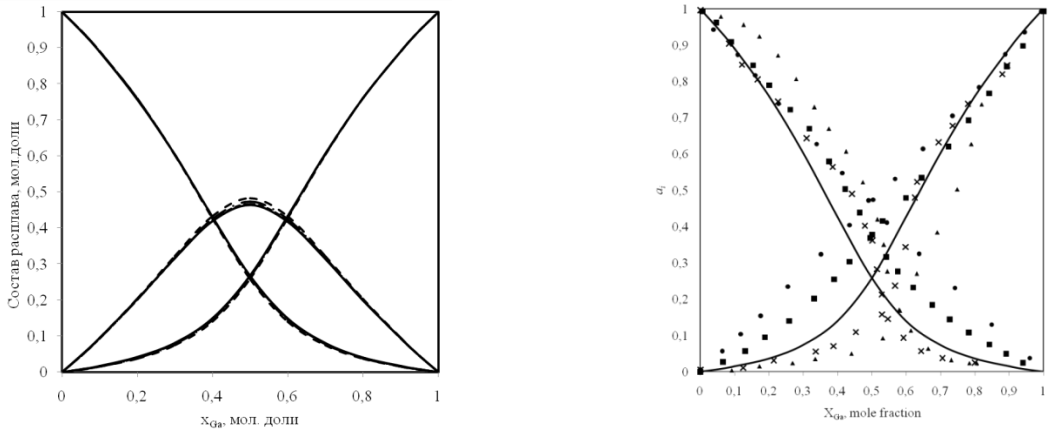
Построены концентрационные зависимости содержания компонентов расплавов, активностей компонентов при различных температурах. Установлено, что во всех исследованных расплавах наблюдаются отрицательные отклонения от закона Рауля, что обусловлено наличием ассоциатов. Максимальные концентрации ассоциатов в расплавах наблюдаются при эквимольных соотношениях элементов, характерных для образования соединений в соответствии с диаграммами состояния [4]. На рисунке 1-а представлены концентрационные зависимости содержания компонентов расплавов Ga-Sb при различных температурах. Аналогичные зависимости наблюдаются для расплавов Al-Sb и In-Sb. На рисунке 1-б представлены концентрационные зависимости активностей компонентов (a_i) расплавов Ga-Sb по результатам настоящей работы и авторов [5 - 8]. Сравнение значений a_i, полученных в настоящей работе, с литературными данными показывает, что для системы Ga-Sb существует достаточно хорошее согласование a_{Sb} в области концентраций галлия 0-0.5, a_{Ga} - в области концентраций 0.5-1.0 [5, 6] и удовлетворительное согласование с данными авторов [7, 8]. Для системы Al–Sb наблюдается очень хорошее согласование a_{Sb} с литературными данными [10-15] в области концентраций алюминия 0 - 0.5, a_{Al} - в области концентраций 0.5 - 1.0. Для активностей компонентов расплавов In-Sb наблюдается хорошее согласование a_{Sb} с литературными данными [5, 18 - 21] в области концентраций алюминия 0-0.5, a_{In} - в области концентраций 0.5-1.0.

Рассчитаны концентрационные зависимости избыточных интегральных энтропий, энтальпий и энегий Гиббса расплавов Ga-Sb, Al-Sb, In-Sb при различных температурах. Установлено, что все эти зависимости являются немонотонными с экстремумами при эквимольном содержании компонентов расплавов.

На рисунке 2 в качестве примера представлены зависимости интегральных характеристик для расплава Ga-Sb. Как видно из рисунка 2, значения ΔH_{int}, полученные в настоящей работе, достаточно хорошо согласуются с литературными данными [6, 9]. Что же касается ΔG_{int}, имеется наших результатов с литературными данными. Возможно, это связано с особенностями проведения экспериментов и расчетов различными авторами.

Сравнение результатов, полученных в настоящей работе, с литературными данными показывает, что наблюдается достаточно хорошее согласование значений ΔH_{int} для расплавов Al-Sb с данными [13, 16] и удовлетворительное – с данными [10, 15, 16]; для расплавов In –Sb наблюдается качественное согласование с данными [5, 21 - 22]. Значения ΔG_{int} для расплавов Al-Sb качественно согласуются с литературными данными [10, 13-15], для расплавов In-Sb – с данными [5]. Следует отметить, что численные значения ΔG_{int}, рассчитанные в настоящей работе и представленные различными авторами, отличаются.

Таким образом, можно сделать **вывод**, что модель идеальных растворов продуктов взаимодействия адекватно описывает термодинамические характеристики расплавов Ga-Sb, Al-Sb, In-Sb.



а б

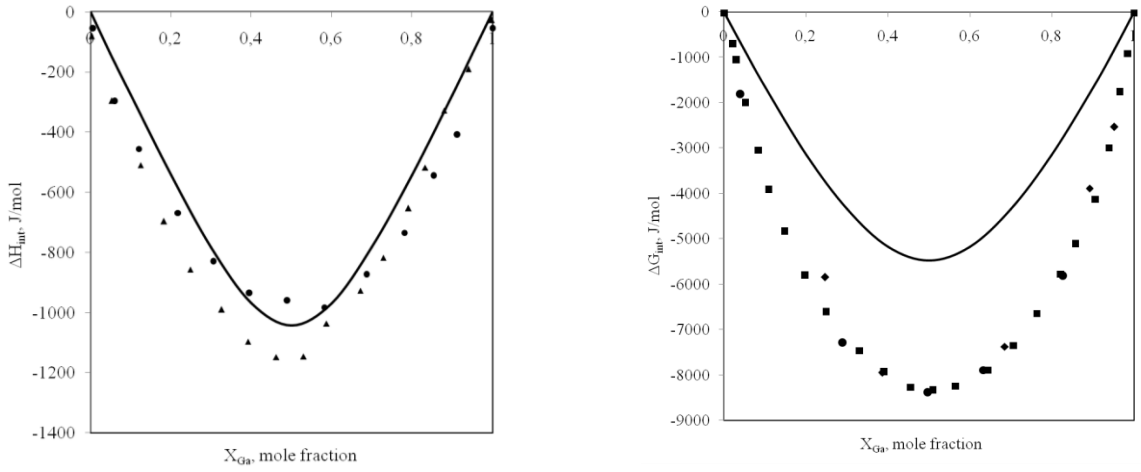
Рисунок 1. Концентрационные зависимости содержания компонентов и активностей компонентов расплавов Ga-Sb при различных температурах:

а)– – – наши расчеты при Т = 1000 К; – · – – наши расчеты при Т = 1200 К; - - - – наши расчеты при Т = 1400 К; —— – наши расчеты при Т = 1600 К.

б) ■ – данные работы [5] при Т = 1003 К; ● – данные работы [6] при Т = 1003 К; × – данные работы [7] при Т = 988 К; ▲– данные работы [8] при Т=1023 К; сплошная линия – наши расчеты при Т = 1000 К.

Сравнение результатов термодинамического моделирования с известными экспериментальными и теоретическими данными показывает, что наблюдается хорошее качественное и количественное согласование значений активностей компонентов и некие расхождения в результатах для избыточных интегральных характеристик расплавов. Возможно, это связано с особенностями проведения экспериментов и расчетов различными авторами.

Полученная информация позволяет прогнозировать свойства изделий из различных материалов, открывает дополнительные возможности для управления процессом получения и формирования продукта с определенными качественными показателями.



а б

Рисунок 2. Концентрационные зависимости избыточных характеристик расплавов Ga-Sb.

а) Избыточные интегральные энтальпии: ● – данные работы [6]; ▲ – данные работы [9]; сплошная линия – наши расчеты при Т = 1000 К.

б) Избыточные интегральные энергии Гиббса: ■ – данные работы [5] при Т = 1003 К; ● – данные работы [5] при Т = 1003 К; ♦ – данные работы [5] при Т = 1003 К; сплошная линия – наши расчеты при Т = 1000 К;

Литература:

1. Синярев Г.Б., Ватолин Н.А., Трусов Б.Г., Моисеев Г.К. Применение ЭВМ для термодинамических расчетов металлургических процессов. - М.: Наука, 1983. - 263 с.

2. Ватолин Н.А., Моисеев Г.К., Трусов Б.Г. Термодинамическое моделирование в высокотемпературных неорганических системах. - М.: Металлургия, 1994. - 353 с.

3. Трусов Б.Г. Программная система моделирования фазовых и химических равновесий при высоких температурах // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение, 2012. С.240-249.

4. Massalski T.B. Binary Alloy Phase Diagrams. - American Society for Metals. Metals Park. Ohio, 1986, V. 1, 1987. V.2. - 2224 p.

5. T. J. Anderson. Thermodynamics of solid and liquid group III-V ALLOYS. Ph. D. thesis, Lawrence Berkeley Laboratory, 1980, 292 p.

6. A. Yazawa, T. Kawashima, and K. Itagaki. Measurements of Heats of Mixing in Liquid Antimony Binary Alloys // J. Japan Inst. Metals, Vol. 32, No. 12, 1968, p. 1288-1293

7. Яценко С.П., Данилин В.Н. К вопросу о связи термодинамических свойств и вязкости жидких сплавов /В сб.: Теплофизические свойства жидкостей. М.: Наука, 1970, с.120-124.

8. L.N. Gerasimenko, I.V. Kirichenko, L.N. Lozhkin, and A.G. Morachevskii, Zashichitn. Metal. i Oksidnye Pokrytia, Korrozyz Metal. i Issled. v Obl. Electrokhim., Akad. Nauk SSSR, Otd. Obshch. i Tekhn. Khim., Sb. Statei (1965) p. 236.

9. B. Predel and D.W. Stein. Beitrag zur kenntnis der thermodynamischen Eigenschaften des systems Gallium-Antimon // Less-Common Metals, Vol. 24, Is. 4, 1971, p. 391- 403.

10. M. Paliwal. Thermodynamic modeling of the Mg-Al-Bi and Mg-Al-Sb systems, 2009, 106 p.

11. B. Predel and U. Schallner. Thermodynamische untersuchung der systeme aluminium-antimon und aluminium-gold // Materials Science and Engineering Vol. 5, Is. 4, 1970, p. 210-219

12. A. Zajaczkowski, and J. Botor. Thermodynamics of the Al-Sb System Determined by Vapour Pressure Measurements // Z. Metallkd., Vol. 86, Is. 9, 1995, p. 590-596.

13. C.A. Coughanowr, U.R. Kattner and T.J. Anderson. Assessment of the Al-Sb system // Calphad Vol. 14, Is. 2, 1990, p. 193-202.

14. K. Yamaguchi, M. Yoshizawa, Y. Takeda, K. Kameda and K. Itagaki. Measurement of Thermodynamic Properties of Al-Sb System by Calorimeters // Mater. Trans. JIM Vol. 36 No. 3, 1995, p. 432 - 437.

15. T. Balakumar and M. Medraj, Thermodynamic modeling of the Mg-Al-Sb system // Calphad Vol. 29, Is. 1, 2005, p. 24-36.

16. C. Girard, J.M. Miane, J. Riou, R. Baret and J.P. Bros. Enthalpy of formation of Al-Sb and Al-Ga-Sb liquid alloys // Less-Common Met. Vol. 128, 1987, p. 101–115.

17. C. Klančnik, J. Medved. Thermodynamic investigation of the Al-Sb-Zn system // Materials and technology, Vol. 45, No. 4, 2011, p. 317-323.

18. Terpilowski J., Zaleska E., Gawel W. Characterystyka termodynamiczna ukladu stalego tal-tellur. // Roczniki Chemii. 1965. V.39. p.1367-1375.

19. H. Hoshino, Y. Nakamura, M. Shimoji, and K. Niwa. Thermo dynamic Properties of Indium-Antimony and Indium-Bismuth Liquid Alloys // Berichte der Bunsengesellschaft für physikalische Chemie, Vol. 69, Is. 2, 1965, p. 114-118.

20. D. Chatterji and J. V. Smith. The Activity of In in Liquid In-Sb Alloys // Journal of The Electrochemical Society Vol. 120 No. 6, 1973, p.770.

21. D. Chatterji and R. W. Vest. Thermodynamic Properties Of The System Indium-Oxygen // Journal of the American Ceramic Society, Vol. 55, Is. 11, 1972, p. 575-578.

22. A.A. Vecher, E.I. Voronova, L.A. Mechkovskii, and A.S. Skoropanov. Determination of the enthalpy of mixing in the Ga-In-Sb and Bi-Sn-Sb systems by differential thermal analysis //Russ. Phys. Chem., 48, 584 (1974).

23. Wittig F.E., Gehring E. Die Mischungswärmen des Antimons mit B-Metallen: II. Die Systeme mit Indium und Thallium // Berichte der Bunsengesellschaft für physikalische Chemie, Vol. 71, Is. 1, 1967, p. 29-34.

С.А. Мамлин, Э.Л. Портнов

РАСЧЕТ НАДЕЖНОСТИ ПОДВОДНОЙ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ ВДОЛЬ ПОБЕРЕЖЬЯ КРАСНОДАРСКОГО КРАЯ ОТ ПОРТА «КАВКАЗ» ДО СЕЛА ВЕСЕЛОЕ

Московский технический университет связи и информатики, г. Москва

Ключевые слова: подводная волоконно-оптическая линия связи, расчёт надежности, коэффициент готовности.

Подводные линии связи играют большую роль в телекоммуникационном мире, ведь по ним осуществляется сообщение между странами и континентами, разделенными морями и океанами. Сейчас в мире существует очень много подводных волоконно-оптических линий передачи, которые проложены по дну морей и океанов, и благодаря которым многие из нас могут позвонить или передать электронное письмо на другой континент.

В докладе рассмотрен расчет надежности, подводной волоконно-оптической линии связи вдоль побережья Краснодарского края «порт «Кавказ» - г. Анапа - г. Новороссийск, п. Мысхако - г. Геленджик - п. Архипо-Осиповка г. Геленджик - п. Джубга, Туапсинский район - п. Новомихайловский, Туапсинский район - г. Туапсе - п. Лазаревское, г. Сочи - п. Головинка, г. Сочи - г. Сочи - с. Веселое, г. Сочи».

S.A. Mamlin, E.L. Portnov

RELIABILITY CALCULATION OF UNDERWATER FIBER-OPTIC LINE ALONG KRASNODAR REGION SHORE FROM THE PORT «CAVKAZ» TO THE VILLAGE VESELOE

Moscow Technical University of Communications and Informatics, Moscow

Keyword: underwater fiber-optic communication line, reliability calculation, availability factor.

Underwater communication lines are very important in the telecommunication world, because it is communication between countries and continents, separated by seas and oceans. Now in the world there are a lot of underwater fiber-optic transmission lines, which are laid on the bottom of seas and oceans, and by which many of us can call or send an email to another continent.

The report considers the reliability calculation, underwater fiber-optic line along Krasnodar region shore "port "Cavkaz", Anapa, Novorossiysk, s. Myskhako, Gelendzhik - s. Arkhipo-Osipovka, Gelendzhik - s. Dzhubga, Tuapse district - s. Novomikhailovskoye, Tuapse district, Tuapse - s. Lazarev, Sochi - s. Golovinka, , Sochi, Sochi – s. Veseloe, Sochi."

Подводные линии связи играют большую роль в телекоммуникационном мире, ведь по ним осуществляется сообщение между странами и континентами, разделенными морями и океанами. Сейчас в мире существует очень много подводных волоконно-оптических линий передачи, которые проложены по дну морей и океанов, и благодаря которым многие из нас могут позвонить или передать электронное письмо на другой континент.

В Черном море предполагалось реализовать проект по строительству подводной волоконно-оптической линии связи вдоль побережья Краснодарского края, которая должна была стать резервной линией для проложенных на суше волоконно-оптических линий связи, а также обеспечить высокую пропускную способность для существующего и предполагаемого траффика. К сожалению, по ряду причин данный проект по строительству подводной линии связи не был реализован, тем не менее он не упущен из вида связистами и ждет своего часа…

Проект предусматривал строительство подводной волоконно-оптической линии связи методом «гирлянды» и должен был иметь точки вывода кабеля на берег в 12-ти населенных пунктах:

- порт «Кавказ»;
- г. Анапа;
- г. Новороссийск, п. Мысхако;

– г. Геленджик;
– п. Архипо-Осиповка г. Геленджик;
– п. Джубга, Туапсинский район;
– п. Новомихайловский, Туапсинский район;
– г. Туапсе;
– п. Лазаревское, г. Сочи;
– п. Головинка, г. Сочи;
– г. Сочи;
– с. Веселое, г. Сочи».

Расстояния участков «гирлянды» и длин подводного волоконно-оптического кабеля (ПВОК) приведены в Таблице 1.

Таблица 1. Расстояния участков «гирлянды» волоконно-оптической линии связи

	Участок «гирлянды»	Расстояние, км	Длина ПВОК, км
1	Порт-Кавказ –г.Анапа	100,04	105,042
2	г.Анапа – п.Мысхако	70,63	74,1615
3	п.Мысхако – г.Геленджик	28,65	30,0825
4	г.Геленджик – п.Архипо-Осиповка	54,85	57,5925
5	п.Архипо-Осиповка – п.Джубга	19,02	19,971
6	п.Джубга – п.Н.Михайловка	14,63	15,3615
7	п.Н.Михайловка – г.Туапсе	28,62	30,051
8	г.Туапсе – п.Лазаревское	36,30	38,115
9	п.Лазаревское – п.Головинка	18,07	18,9735
10	п.Головинка – г. Сочи	33,43	35,1015
11	г.Сочи – с.Веселое	38,16	40,068

Общая длина трассы ПВОЛС составляет 442,40 км, расчетная длина ВОК составляет 464,52 км.

Рассмотрим расчет надежности, предполагаемой подводной волоконно-оптической линии связи вдоль побережья Краснодарского края.

Проектируемая ПВОЛС состоит из последовательно соединенных элементов (мультиплексоров оптических кроссов, ВОК, разветвительных муфт), каждый из которых характеризуется своими параметрами надежности, и отказы в первом приближении происходят независимо.

Интенсивность отказов магистрали проектируемой транспортной сети в общем виде определяется как сумма интенсивностей отказов пассивного и активного оборудования, соединительных и разделительных элементов и ВОК:

$$\lambda = \lambda_{\text{ос}} \times Q_{\text{ос}} + \lambda_{\text{оп}} \times Q_{\text{оп}} + \lambda_{\text{окр}} \times Q_{\text{окр}} + \lambda_{\text{вок}} \times L \quad (1)$$

где: $\lambda_{\text{ос}}, \lambda_{\text{оп}}, \lambda_{\text{окр}}$– интенсивности отказов оптических соединений строительных длин, оптических приборов, оптических кроссов и разделительных муфт;

$Q_{\text{ос}}$ – количество оптических соединений;

$Q_{\text{оп}}$ – количество оптических приборов;

$Q_{\text{окр}}$ – количество оптических кроссов и разделительных муфт;

$\lambda_{\text{вок}}$ – интенсивность отказов одного километра оптического кабеля;

L – протяженность оптической трассы.

Средний поток отказов за счет внешних повреждений на 100 км ВОК в год (по статистике повреждений из опыта эксплуатации на магистральной первичной сети) равен $\Lambda_{\text{к}} = 0{,}34$, что соответствует интенсивности отказов ОК за 1 час на длине трассы ВОЛП L км равной:

$$\lambda_{\text{вок}} = \Lambda_{\text{к}} \cdot L/8700 \cdot 100 \quad (2)$$

Для рассматриваемой магистрали $\lambda_{\text{вок}} = 5{,}045\times10^{-7}$ час$^{-1}$, что дает величину интенсивности отказов на 1км ВОК $\lambda_{\text{вок}} = 3{,}881\times10^{-7}$. Интенсивности отказов пассивных оптических элементов полагаются равными 0,1 интенсивности отказов на 1 км ВОК. Согласно данным изготовителя рассматриваемого при разработки данного проекта оборудования, наработка на отказ аппаратуры OLT, ONT равна 10 годам или 87600 часов, откуда интенсивность отказов будет равна $\lambda = 10^{-7}$.

Значения необходимых для расчетов показателей магистрали проектируемой транспортной сети магистрали приведены в таблице 2.

Таблица 2. Параметры интенсивности отказов оборудования.

Наименование элемента	Активное оборудование	Пассивное оборудование	ВОК
λ, 1/ч	$1\times\cdot10^{-7}$	$0{,}388\times10^{-7}$	$3{,}881\times10^{-7}$ (на 1км)

Для рассматриваемой в расчете магистрали величина интенсивности отказов составит:

$$\lambda = 0{,}388\times10^{-7}\times132 + 10^{-7}\times12 + 0{,}388\times10^{-7}\times33 + 3{,}881\times10^{-7}\times515{,}986 = 1942{,}2846\times10^{-7}\ \frac{1}{\text{ч}}$$

Средняя наработка на отказ (среднее время безотказной работы), T_0, час составит:

$$T_0 = t_{\text{ср}} = \frac{1}{1942{,}2846\times10^{-7}} = 0{,}0005148\times10^{-7} = 5{,}148\times10^{3}\ ч$$

Рассчитаем коэффициент готовности. Предварительно найдем среднее время восстановления работоспособности магистрали по формуле:

$$t_{\text{в}} = \frac{1}{\lambda}\left(\lambda_{\text{ос}}\times t_{\text{в.ос}}\times Q_{\text{ос}} + \lambda_{\text{оп}}\times t_{\text{в.оп}}\times Q_{\text{оп}}\times\lambda_{\text{ом}}\times t_{\text{в.ом}}\times Q_{\text{ом}} + \lambda_{\text{окр}}\times t_{\text{в.окр}}\times Q_{\text{окр}} + \lambda_{\text{каб}}\times t_{\text{вкаб}}\times L\right) \quad (3)$$

Где $t_{\text{в.ос}}, t_{\text{в.оп}}, t_{\text{в.ом}}, t_{\text{в.окр}}, t_{\text{вкаб}}$ - время восстановления соответственно оптических соединений (оптических муфт), оптических приборов, оптических кроссов и оптического кабеля.

$$t_{\text{в}} = \frac{1}{0{,}0005148\times10^{-7}}(0{,}388\times10^{-7}\times8\times0{,}25 + 10^{-7}\times2\times0{,}5 + 0{,}388\times10^{-7}\times3\times0{,}25\times 0{,}388\times10^{-7}\times2\times0{,}15 + 3{,}881\times10^{-7}\times0{,}556\times3{,}5) = 1{,}1424\ ч$$

Коэффициент готовности:

$$K_{\text{г}} = \frac{10{,}8674\times10^{5}}{10{,}8674\times10^{5} + 1{,}1424} = 0б9999989$$

Полученные результаты подтверждают высокую надежность подводной волоконно-оптической линии связи.

Вероятность безотказной работы в течение суток: $t_1 = 24$ часа

$$P(t) = e^{-10{,}2018\times10^{-7}\times24} = 0{,}999975$$

В течение месяца: $t_2 = 720$ часов:

$$P(t) = e^{-10{,}2018\times10^{-7}\times720} = 0{,}999266$$

В течение года: $t_3 = 8760$ часов:

$$P(t) = e^{-10,2018\times10^{-7}\times8760} = 0,991106$$

Таким образом, расчеты подтверждают правильность выбранных проектных решений по реализации проекта строительства подводной волоконно-оптической линии связи вдоль побережья Краснодарского края.

Литература:

1. Стратегия социально экономического развития Краснодарского края до 2020 г.
2. Гулевич Д.С. Сети связи следующего поколения. – М.: Интернет-Университет информационных технологий, 2009.
3. Алексеев Е.Б., Гордиенко В.Н., Крухмалев В.В., и др. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей. – М.: Горячая линия - Телеком, 2008.
4. «Руководством по строительству линейных сооружений местных сетей связи», 1995 г.
5. Фокин В.Г. Оптические системы передачи и транспортные сети. — М.: Эко-Трендз, 2008.

Э.Х. Мариносян, Э.Л. Портнов

О ПРИМЕНЕНИИ КЛАССИЧЕСКОГО СОЛИТОНА В ТЕЛЕКОММУНИКАЦИЯХ

Московский технический университет связи и информатики, г. Москва

Ключевые слова: классический солитон, гиперболический секанс, уширение импульса, дисперсионная длина, нелинейная длина, период солитона.

Классические солитоны способны распространяться в оптическом волокне на несколько тысяч километров с сохранением своей начальной формы. Для обеспечения формирования классического солитона необходимо иметь решение уравнения Шредингера. Благодаря такому решению, при определенных параметрах, можно определить «взаимозачет» дисперсии групповых скоростей (ДГС) и фазовой самомодуляции (ФСМ). Общее решение уравнения Шредингера [1] показывает существование фундаментального классического солитона и солитонов N-го порядка. Фундаментальный классический солитон соответствует солитону 1-го порядка и по своей форме соответствует форме гиперболического секанса. Порядок N определяет относительное влияние эффектов дисперсии групповых скоростей и фазовой самомодуляции на эволюцию импульсов в волоконном световоде. Если $N\sim1$, то и дисперсия групповых скоростей, и фазовая самомодуляция играют одинаково важную роль в процессе эволюции импульса.

В докладе рассмотрены основные параметры классического солитона, часть из которых не отражены в ряде работ и имеют важное значение.

E.Kh. Marinosyan, E.L. Portnov

ON THE APPLICATION OF CLASSICAL SOLITON IN TELECOMMUNICATIONS

Moscow Technical University of Communications and Informatics, Moscow

Keyword: classical soliton, hyperbolic secant, pulse broadening, dispersion length, nonlinear length, soliton period.

Classical solitons can propagate in the optical fiber for several thousand kilometers preserving its initial shape. To ensure the formation of the classical soliton must have a solution Schrodinger equation. Thanks to this solution, under certain parameters, it is possible to determine the "offsetting" the group velocity dispersion (GVD) and self-phase modulation (SPM). The general solution of the Schrödinger equation [1] shows the existence of a fundamental classical soliton and soliton N-th order. Fundamental classical soliton soliton corresponds to the 1st order and in its shape conforms to the shape of a hyperbolic secant. N specifies the order of the relative influence of the effects of group-velocity dispersion and self-

phase modulation on the evolution of the pulse in an optical fiber. If N ~ 1, then the group velocity dispersion and self-phase modulation play an equally important role in the evolution of the pulse.

The report describes the main parameters of the classical soliton, some of which are not reflected in a number of studies and are important.

Классические солитоны способны распространятся в оптическом волокне на несколько тысяч километров с сохранением своей начальной формы. Если два солитона сталкиваются, то они способны восстанавливать параметры движения и свою амплитуду. Классические солитоны двигаются нелинейно в сильных электромагнитных полях. За счет того, что у одномодового оптического волокна очень малый диаметр сердцевины (до 10 мкм), плотность мощности очень высокая. Из-за этого, при использовании источников излучения малой мощности (несколько мВт), образуются сильные электромагнитные поля. Нелинейные эффекты так же могут проявляться, если в системах используется спектральное уплотнение каналов (различные WDM), мощные усилители, а также в системах с мощными лазерными источниками. Для обеспечения формирования классического солитона необходимо иметь решение уравнения Шредингера. Благодаря такому решению, при определенных параметрах, можно определить «взаимозачет» дисперсии групповых скоростей (ДГС) и фазовой самомодуляции (ФСМ). Общее решение уравнения Шредингера [1] показывает существование фундаментального классического солитона и солитонов N-го порядка. Фундаментальный классический солитон соответствует солитону 1-го порядка и по своей форме соответствует форме гиперболического секанса.

Для укороченных импульсов (длительность $T_0 < 100$ пс) дисперсионная длина L_D становится соизмеримой с нелинейной длиной L_{NL}, и в этом случае необходимо рассмотреть совместное действие эффектов дисперсии групповых скоростей и фазовой самомодуляции. Именно, когда действует эффекты ДГС и ФСМ в области аномальной дисперсии ($\beta_2 < 0$) возможно существование оптических солитонов.

Физический смысл N показывает, что целые величины N связаны с порядком солитона. N определяет относительное влияние эффектов ДГС и ФСМ на эволюцию импульсов в волоконном световоде. Если $N \sim 1$, то и ДГС, и ФСМ играют одинаково важную роль в процессе эволюции импульса.

$$N^2 = \frac{2 \cdot \gamma \cdot P_0 \cdot T_0^2}{|\beta_2|} \quad (1)$$

Дисперсионная длина L_D определяется из выражения [1-4]:

$$L_D = \frac{T_0^2}{|\beta_2|} \quad (2)$$

Значение пиковой мощности фундаментального классического солитона P_1 определяется из формулы (при подстановке $N = 1$) [2]:

$$P_1 \approx \frac{3{,}11 \cdot |\beta_2|}{\gamma \cdot T_{FWHM}^2} \quad (3)$$

где T_{FWHM} – длительность импульса на высоте $1/2$ по интенсивности.

Используя определение $\zeta = z/L_D$ [1], запишем период солитона [1]:

$$z_0 = 0{,}322 \frac{\pi \cdot T_{FWHM}^2}{2 \cdot |\beta_2|} \quad (4)$$

$$B \approx \frac{0{,}88}{q_0 \cdot T_{FWHM}} \quad (5)$$

Распространение солитонов становится неустойчивым при передаче на расстояние $L \approx 8 \cdot z_0$. Свяжем L со скоростью передачи информации соотношением [3]:

$$L \leq \frac{3 \cdot \pi}{3 \cdot q_0^2 \cdot |\beta_2| \cdot B^2} \quad (6)$$

где q_0 – относительное расстояние между солитонами.

Если использовать оптическое волокно со смещенной дисперсией и использовать значение $q_0 = 10$, то произведение $B^2 \cdot L$ ограничено величиной [1]:

$$B^2 \cdot L \leq 1 \cdot 10^4, \frac{\text{Гбит}}{\text{с}^2} \cdot \text{км} \quad (7)$$

Защищенность в электрическом канале находится через -фактор:

$$A_{\text{з.э}} = 20 \cdot \lg(Q_0^4) \quad (8)$$

Для RZ в оптическом канале -фактор находится по формуле:

$$Q_0 = \frac{T_\delta}{2 \cdot \sqrt{|\beta_2| \cdot l}} \quad (9)$$

где:
l – длина участка, км
β_2 – дисперсия групповых скоростей

Определим рекомендованные параметры. Дисперсионная длина будет равна:

$$L_D = \frac{T_{1/2}^2}{2{,}77 \cdot \beta_2} \quad (10)$$

Длительность конечного гауссовского импульса можно рассчитать по формуле:

$$T_1 = T_0 + \sqrt{1 + \left(\frac{z}{l_d \cdot d_m^2}\right)^2} \quad (11)$$

Длительность солитона вычисляется по формуле:

$$\theta_1^2 = \theta_0^2 + \frac{1}{2} \cdot \left(\frac{L}{L_D}\right)^2 \quad (12)$$

где $\theta_0^2 = \frac{\pi^2 \cdot T_0^2}{6}$

Подставим (13) в (12) и получим:

$$\theta_1^2 = \frac{\pi^2 \cdot T_0^2}{6} + \frac{1}{2} \cdot \left(\frac{L}{L_D}\right)^2 \quad (13)$$

Потери на хроматическую дисперсию можно рассчитать по формуле:

$b_{\text{уш}} = 10 \cdot \lg(\sqrt{1 + \left(\frac{8 \cdot \beta_2 \cdot B^2 \cdot L}{d_m^2}\right)^2}$ – для узкополосных источников (14)

$b_c = 10 \cdot \lg(\sqrt{1 + \left(\frac{6 \cdot \beta_2 \cdot L}{\pi^2 \cdot T_0^2 \cdot d_m^2}\right)^2}$ – для солитона (15)

Полученные параметры подтверждают значительные отличия параметров классического солитона от параметров гауссовского импульса.

Литература:
1. Agrawal G.P. Nonlinear Fiber Optics, Academic Press, 2013. – 631 p.
2. Кившарь Ю.С., Агравал Г.П. Оптические солитоны: от световодов к фотонным кристаллам / Пер. с англ. - М.: Физматлит, 2005. – 648 с.
3. Слепов Н.Н. Современные технологии цифровых оптоволоконных сетей связи. – М.: Радио и связь, 2000. – 468 с.
4. Фриман Р. Волоконно-оптические системы связи / Пер. с англ. - М.: Техносфера, 2003. 440 с.

Э.Х. Мариносян, Э.Л. Портнов

СРАВНЕНИЕ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ С РАДИОЧАСТОТНЫМИ СИСТЕМАМИ

Московский технический университет связи и информатики, г. Москва

Ключевые слова: оптическое волокно, радиочастотные системы, дисперсия, нелинейность, коэффициент битовых ошибок.

Емкость проводных систем постоянно увеличивалась со дня их создания от нескольких бит в секунду до систем со скоростью терабит в секунду в настоящее время и это не предел. С читается, что емкость транспортных систем удваивается каждые два года. Такая динамика развития стала возможной с 70-х годов прошлого века, начиная с введения светоизлучающих диодов и многомодового оптического кварцевого волокна с одноканальной емкостью 45-90 Мбит/с с передачей на 10 км. К середине 80-х годов одномодовое волокно и инжекционные лазеры позволили передавать скорости от 565 Мбит/с до 2,5 Гбит/с через расстояние до 100 км без регенерации. Несмотря на многие преимущества, привнесенные электронной обработкой сигналов и цифровой технологии коммуникации, нужно отметить, что оптическая волоконная сеть существенно отличается от радиочастотных каналов связи и фундаментально, и технологически. Оптическое волокно – среда передачи, позволяющая передавать огромное количество информации: весь радиочастотный спектр 3кГц-200ГГц может быть легко передан по одному волокну.

В работе обобщены некоторые основные отличия между оптическими и радиочастотными каналами и дана оценка их совместного использования на телекоммуникационной сети.

E.Kh. Marinosyan, E.L. Portnov

COMPARISON OF FIBER-OPTIC LINES FROM THE RF SYSTEMS

Moscow Technical University of Communications and Informatics, Moscow

Keyword: optical fiber, radio frequency systems, dispersion, nonlinearity, the ratio of bit errors.

The capacity of transmission systems has increased steadily since their creation from a few bits per second to speed terabits per second in real time and this is not the limit. With reads that the capacity of transport systems doubles every two years. This dynamic development has become possible with the 70-ies of the last century, starting with the introduction of light-emitting diodes and multimode optical quartz fiber with a single channel capacity 45-90 Mbps with 10 km. To mid 80-ies of the single-mode fiber and injection lasers made it possible to convey the speed of 565 Mbit/s to 2.5 Gbit/s over a distance of 100 km without regeneration. Despite the many advantages brought by the electronic signal processing and digital communications, it should be noted that the optical fiber network is significantly different

from the radio frequency communication channels and fundamentally and technologically. Optical fiber is a transmission medium that can transfer a huge amount of information: the entire radio frequency spectrum 3 kHz-200GHz can be easily transmitted over a single fiber.

In the work summarized some of the main differences between optical and radio channels and assess their joint use in a telecommunication network.

Емкость телекоммуникационных систем постоянно увеличивалась со дня их создания от нескольких бит в секунду до систем со скоростью терабит в секунду в настоящее время и это не предел. Считается, что емкость транспортных систем удваивается каждые два года. Такое революционное решение стало возможным при создании новых оптических устройств при полном переходе к оптическим транспортным системам. Такая динамика развития стала возможной с 70-х годов прошлого века, начиная с введения светоизлучающих диодов и многомодового оптического кварцевого волокна с одноканальной емкостью 45-90 Мбит/с с передачей на 10 км. К середине 80-х годов одномодовое волокно и инжекционные лазеры позволили передавать скорости от 565 Мбит/с до 2,5 Гбит/с через расстояние до 100 км без регенерации.

После замены коаксиальных кабельных систем оптическими были внедрены оптические эрбиевые усилители в 90-ые годы прошлого века, что значительно отодвинуло устройства электронной регенерации на значительное расстояние и импульсная дисперсия и лазерный чирп становится ограничивающим фактором. Это привело к развитию коммутационных систем на местных центральных офисах и объединением групп местных станций в несколько сотен тысяч до одного миллиона абонентов, которые обслуживаются кросс-коннект коммутаторами в больших офисах. Аналогичная ситуация существует в сетях передачи данных с маршрутизаторами – Интернет Протоколами, обслуживающими средние, базовые и оконечные соответствующие сети. Магистральные сети базируются на передаче голоса и данных и пользуются поддержкой конечных пользователей. Одним из основных показателей транспортной сети является размер транспортной емкости к требованию средней или максимальной, которая диктует высокую степень ресурса сети среди конечных пользователей.

При канальной символьной скорости от 40 до 100 Гбод возможности электронной компенсации все еще ограничены низкой сложностью структур электронных и оптических устройств. В этой области представляют основной интерес *форматы модуляции* и *линейное кодирование*. Они используются, чтобы минимизировать линейные и нелинейные ухудшения оптоволоконной передачи, а также достигнуть высокой спектральной эффективности в сетях с оптической маршрутизацией. При скорости 40 Гбит/с FEC (упреждающая коррекция ошибки) – стандартная функция коммерчески развернутых оптических транспортных систем становится эффективной.

Несмотря на многие преимущества, привнесенные электронной обработкой сигналов и цифровой технологии коммуникации, нужно отметить, что оптическая волоконная сеть существенно отличается от радиочастотных каналов связи и фундаментально, и технологически. Оптическое волокно – среда передачи, позволяющая передавать огромное количество информации: весь радиочастотный спектр 3кГц-200ГГц может быть легко передан по одному волокну.

Некоторые основные отличия между оптическими и радиочастотными каналами обобщены в таблице 1.

Самое важное фундаментальное различие между оптической и радиочастотной связью заключается в присутствии нелинейных искажений в оптическом волоконном канале связи. Высокое поперечное ограничение оптического сигнального поля в сердцевине волокна с эффективным сечением от 20 до 110 мм^2 является причиной того, что интенсивность света достигает или превышает мегаватт/см^2. При таких высоких оптических интенсивностях показатель преломления оптоволокна реагирует на присутствие оптических сигналов в виде оптического эффекта Керра и вызванные сигналом изменения показателя преломления переходят в изменения фазы оптических сигналов. На расстояниях с оптическим усилением, достигающих многих сотен или даже несколько тысяч километров, эти вращения фазы вместе с дисперсией волокна приводят к различным волновым искажениям, которые увеличиваются с мощностью сигнала.

Таблица 1. Сравнение оптических и радиочастотных систем коммуникации

	Оптическая связь	**Радиочастотная связь**
Фундаментальные		
Шум	Квантовый	Тепловой
Помехи	Многолучевость, перекрестные помехи WDM	Многопутевые, многопользовательские
Канал	Нелинейность оптоволокна + дисперсия	Линейный канал, замирание
Динамика канала	~кГц (постоянная, для ~10^7 битов)	~кГц (постоянная, для ~10^1…10^3 битов)
Технологические		
Электрическая полоса пропускания	~60 ГГц – ограничена технологией (полоса пропускания/несущая от 10^{-4} до 10^{-6})	Ограничена регулированием спектра (полоса пропускания/несущая от 10^{-2} до 10^{-4})
Обнаружение	Преимущественно квадратичное	Преимущественно когерентная (I/Q) демодуляция
Цифровая обработка	Довольно простая компенсация и FEC	Экстенсивно используется, комплексная
Показатель мощности на информационный бит	Довольно низкий	Очень высокий

Как следствие и как абсолютный контраст с классическими радиочастотными системами, пропускная способность оптического канала связи достигает максимума при определенном уровне мощности сигнала, который обеспечивает оптимальный компромисс между шумом оптического усилителя (усиленной спонтанной эмиссией, ASE) и нелинейностью Керра в волокне. Как пример, на рисунке 1 (a) показана измеренная частота ошибок в битах (BER) как функция начальной мощности сигнала для различных форматов оптической модуляции при передаче через более чем 1980 км по стандартному одномодовому оптоволокну (SSMF).

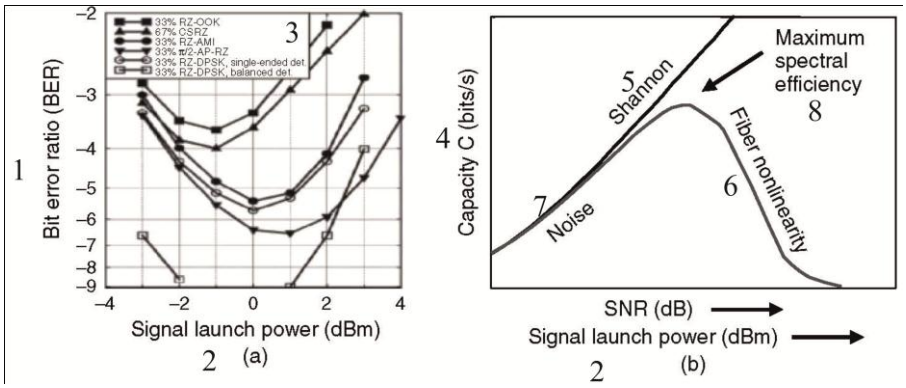


Рисунок 1. (a). Измеренная BER в зависимости от выходной мощности сигнала для различных оптических форматов модуляции; (b) Схематическое представление пропускной способности волоконного канала связи в зависимости от полученного SNR.

Рисунок показывает компромисс между характеристикой, обусловленной ASE, при низкой мощности входного сигнала и характеристикой, обусловленной нелинейностью волокна, при высокой мощности, отмечены различные оптимальные характеристики при оптимальной входной мощности для конкретных форматов. На рисунке 1 (b) схематично показано поведение *пропускной способности* волоконного канала как функции полученного отношения сигнал-шум (SNR) Вследствие квантово-механических нижних ограничений шума оптического усилителя SNR может только увеличиваться при более высокой начальной мощности сигнала, что в конечном счете приводит к нелинейным искажениям сигнала. Отметим, что, работая с оптимальной

производительностью, *каждая* система оптоволоконной связи показывает признаки нелинейного искажения сигнала.

Оба случая показывают максимальную производительность при определенном уровне мощности сигнала, представляя оптимальный компромисс между шумом оптического усилителя и нелинейностью Керра волокна: 1 – частота ошибок в битах (BER); 2 – входная мощность сигнала (дБм); 3 – несимметричное обнаружение, симметричное обнаружение; 4 – пропускная способность С (бит/с); 5 – Шеннон; 6 – нелинейность волокна; 7 – шум; 8 – максимальная спектральная эффективность. Второе главное различие между оптическими и радиочастотными системами коммуникации как с фундаментальными, так и с технологическими последствиями, – высокая *абсолютная полоса пропускания* оптических коммуникационных сигналов. В общем случае и как доказано историческим развитием оптических систем максимально возможная битовая скорость в канале всегда приводила к самой низкой стоимости, занимаемой площади и потребляемой мощности в расчете на передачу одного информационного бит из конца в конец сети каждый раз, когда основополагающие технологии достигали достаточной зрелости. Поэтому оптические системы коммуникации всегда поднимали ограничения, свойственные высокоскоростным электронным и оптикоэлектронным компонентам, вплоть до систем передачи на скорости 100 Гбит/с, которые представляют в настоящее время предельные возможности электронных мультиплексирования и демультиплексирования. Абсолютная полоса пропускания на канал оставляет немного места для реализации сложных алгоритмов обработки сигналов, включая когерентное обнаружение с цифровым захватом фазы ("интрадинное" обнаружение). Вместе с тем, те преимущества, которое имеет оптическое волокно перед медными (симметричными и коаксиальными) кабелями позволяет в будущем полностью его использовать на всех участках сети, и только радиочастотная связь будет участвовать в общей сетевой технологии.

Несомненно, преимущества оптических волоконно-оптических линий имеют важное значение при протяженных трассах, больших и малых сетях, тогда, как радиочастотная связь оптимальна при малых расстояниях непосредственно для абонентов. Сочетание волоконно-оптических и радиочастотных технологий позволяет оптимально их объединить и использовать в едином формате.

Литература:

1. Иванов А.Б. Волоконная оптика: компоненты, системы передачи, измерения. – М.: САЙРУС СИСТЕМС, 1999. – 671 с.

2. Портнов Э. Л. Оптические кабели и пассивные компоненты волоконно-оптических линий связи. – М.: Горячая линия-Телеком, 2007. – 464 с.

3. Листвин А.В., Листвин В.Н. Оптические волокна для линий связи. –М.: ВЭЛКОМ, 2003. – 288 с.

4. Волоконно-оптическая техника: современное состояние и перспективы. изд. 2-е, перераб. и доп.\под ред. С.А. Дмитриева, Н.Н. Слепова. М.: ООО «Волоконно-оптическая техника». – 2005. – 576 с.

5. Портнов Э.Л. Принципы построения первичных сетей и оптические кабельные линии связи. М.: Горячая линия-Телеком, 2009. – 544с.

А.М. Межуев, Е.В. Коновальчук, А.Н. Роза

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА ЦИФРОВЫХ РАДИОСЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», г. Воронеж, Россия

Ключевые слова: оценка эффективности, цифровые радиосети, имитационное моделирование, информационная мощность, потери, коэффициент полезного действия.

В работе предложен метод оценки информационной эффективности цифровых радиосетей с детерминированными структурами, представляющий собой комбинацию аналитического и имитационного моделирования. Оценка производится основе обобщенных параметров – информационная мощность и к.п.д. сети в смысле передачи информации, с учетом ограничения на временную задержку. Применение данного подхода позволяет сочетать в себе достоинства имитационных и аналитических моделей, а также определить практические рекомендации для выбора структуры цифровой радиосети в зависимости от интенсивности входного информационного трафика.

A.M. Mezhuev, E.V. Konovalchuk, A.N. Roza

ESTIMATION OF EFFICIENCY OF AN INFORMATION EXCHANGE OF DIGITAL RADIO NETWORKS WITH USAGE OF A SIMULATION MODELING

Military educational centre of science of Air Forces “Air Force Academy of a name prof. N.E. Zhukovski and Y.A. Gagarin”, Voronezh, Russia

Keywords: an estimation of efficiency, digital radio networks, imitative simulation analysis, information power, losses, efficiency.

In operation the method of an estimation of information efficiency of digital radio networks with the determined structures representing a combination analytical and a simulation modeling is offered. The estimation is made to the basis of generalized parameters - information power and efficiency of a network in sense of an information communication, with allowance for limitings on a time delay. The application of the given approach allows to combine in itself virtues of imitative and analytical models, and also to define the practical guidelines for choice of structure of a digital radio network depending on intensity of input information traffic.

Проведенный анализ публикаций, посвященных задачам анализа, синтеза и оценки информационной эффективности телекоммуникационных систем и информационно-вычислительных сетей, в том числе цифровых радиосетей (ЦРС), свидетельствует, что для их решения в настоящее время в равной степени используются аналитические модели и средства имитационного моделирования [1; 2].

Аналитические модели применяются для проведения глубокого анализа, математического описания и обобщения результатов. С их помощью наиболее полное исследование возможно провести лишь в том случае, когда удается построить в явном виде зависимости, связывающие искомые величины с параметрами сети и начальными условиями ее существования, поэтому, как правило, такие решения можно получить лишь для простых систем.

В то же время имитационное моделирование используется при исследовании сетей, сложность которых изменяется в широких пределах. При этом с усложнением исследуемой системы не обнаруживается столь резкого роста сложности создания и применения имитационных моделей, как это бывает при использовании аналитического моделирования. Вместе с тем в процессе создания имитационных моделей разработчики сталкиваются с проблемами, связанными с трудностями формального описания функциональных зависимостей основных сетевых параметров, а при переходе к исследованию новой сети требуется создание абсолютно новой имитационной модели.

Таким образом, использование при моделировании ЦРС со сложными структурами метода, сочетающего в себе достоинства имитационного и аналитического моделирования, является актуальной задачей и имеет важное научное, а также практическое значение.

Для имитационного моделирования работы ЦРС предлагается использовать специальный пакет моделирования дискретных систем GPSS/PC. Построенные на его основе модели дают возможность одновременно наблюдать не только процесс прохождения пакетов по сети, но и изменение величин очередей в обслуживающих приборах, время занятости устройств, данные регистрирующих таблиц.

В этом случае для моделирования используется теория систем массового обслуживания (СМО). ЦРС представляется в сети массового обслуживания (СеМО), описывающей и отражающей основные характеристики исследуемых топологий, и является сетью смешанного

типа, которая содержит в себе элементы замкнутых и разомкнутых СМО. Причем заданное в качестве исходных данных значение допустимого времени нахождения сообщений в сети $\grave{O}_{äîï}$ позволяет отслеживать потери просроченных пакетов и осуществлять управление интенсивностью входного информационного потока.

Модель ЦРС, описываемая СеМО, включает в себя следующие основные элементы:

- входные и транзитные узлы коммутации (УК), обеспечивающие доставку внешнего потока сообщений до УК адресата;
- выходные УК, осуществляющие выдачу информации оконечным пользователям и управление входным потоком, исходя из заданного ограничения по временной задержке $\grave{O}_{äîï}$ (таким образом учитываются потери пакетов при информационном обмене);
- каналы связи (КС) или обслуживающие приборы, имеющие ограничение по пропускной способности.

На рисунке 1 в качестве примера представлена модель ЦРС со структурой «звезда» в виде совокупности взаимосвязанных элементов замкнутых и разомкнутых СМО.

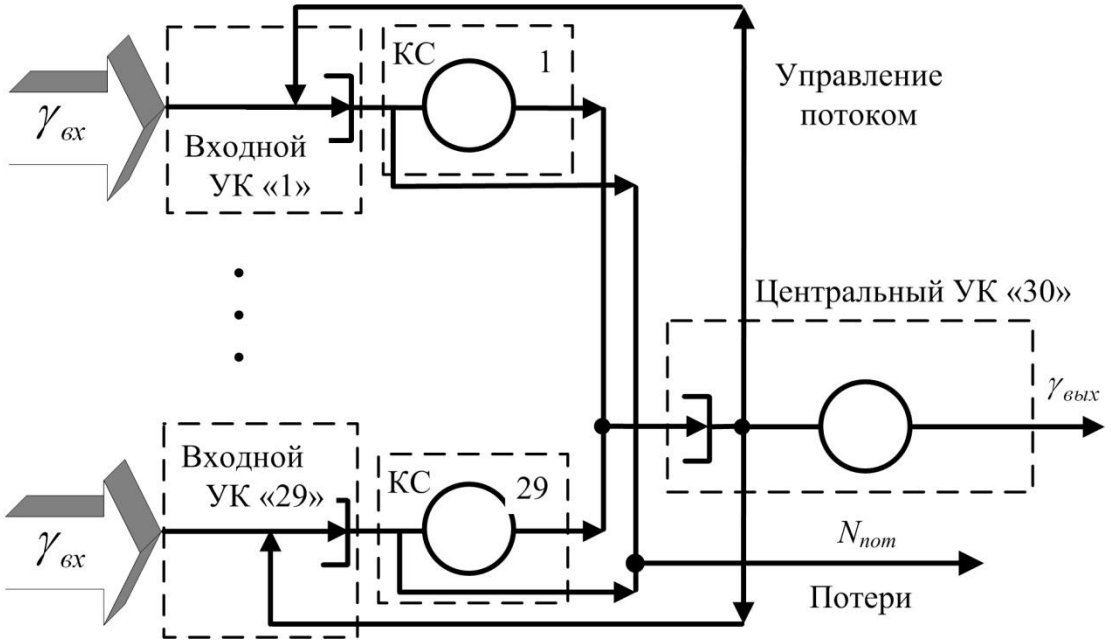


Рисунок 1. Модель СеМО для ЦРС с топологией «звезда»

В качестве математического метода при моделировании выбран метод статистических испытаний. При этом основная задача моделирования состояла в учете наиболее важных характеристик ЦРС, таких как (рисунок 2):

- число пакетов $N_{îáù}$, находящихся в системе при заданном ограничении по временной задержке $\grave{O}_{äîï}$;
- производительность сети G в условиях изменения входной нагрузки и с учетом ограничения по пропускной способности каналов;
- число потерь $N_{ïîò}$, возникающих в ЦРС вследствие переполнения очередей, а также реализации процедуры управления входным и транзитным трафиком (их влияние на эффективность информационного обмена в ЦРС учитывается с помощью коэффициента потерь $\hat{E}_{ïîò}$).

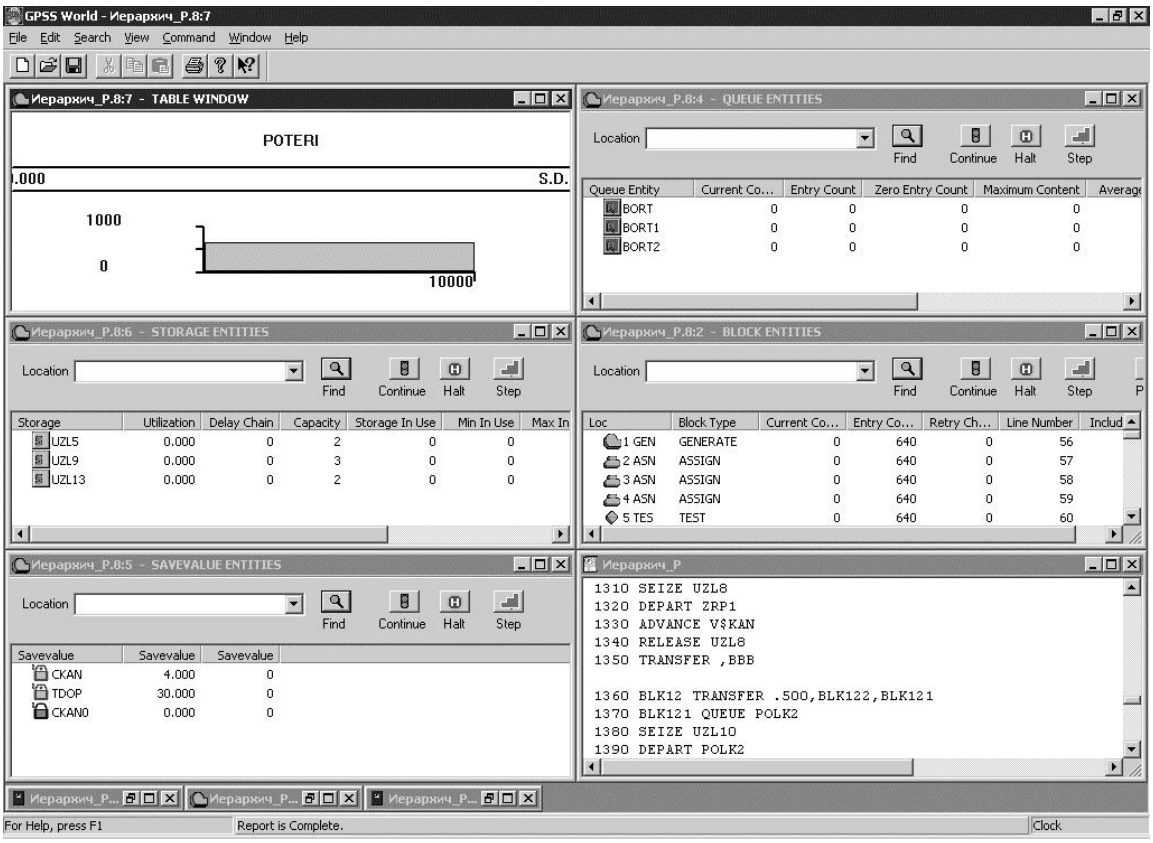


Рисунок 2. Окна программы GPSS/PC регистрирующие основные параметры модели ЦРС

Наличие перечисленных параметров ЦРС позволяет оценить эффективность информационного обмена в сети с помощью обобщенного показателя информационной мощности, значением к.п.д. в смысле передачи информации [3, 4].

Выражение для информационной мощности ЦРС, отражающей реальные возможности сети по передаче информации, с учетом потерь при заданном ограничении на временную задержку $\grave{O}_{\ddot{a}\hat{i}\ddot{i}}$ принимает вид

$$P_{\ddot{O}\dot{D}\tilde{N}} = \hat{E}_{\ddot{i}\hat{i}\grave{o}}\ N_{\hat{i}\acute{a}\grave{u}}\ G\big|_{T_{\ddot{a}\hat{i}\ddot{i}}}, \qquad (1)$$

где $\hat{E}_{\ddot{i}\hat{i}\grave{o}} = 1 - \dfrac{N_{\ddot{i}\hat{i}\grave{o}}}{N_{\hat{i}\acute{a}\grave{u}}}$ – коэффициент потерь, характеризующий долю потерянных пакетов от общего их числа прошедших через сеть за интервал времени моделирования и показывающий снижение значения к.п.д. сети вследствие этих причин; G – производительность ЦРС, которая определяется значением выходного потока $\gamma_{\hat{a}\hat{u}\tilde{o}}$ и ограничивается величинами пропускных способностей каналов выходных УК $\mu_{i\,\hat{a}\hat{u}\tilde{o}}$.

На основании известного представления ЦРС в виде совокупности отдельных одноканальных систем (ОС), полная информационная мощность, определяющая предельные возможности сети по передаче информации, в рассматриваемой имитационной модели определяется выражением

$$P_{\ddot{i}\tilde{n}\ddot{e}\acute{i}} = \sum_{i=1}^{k} P_i = \sum_{i=1}^{k} N_{i\,\hat{i}\acute{a}\grave{u}} \cdot \mu_i\big|_{T_{\ddot{a}\hat{i}\ddot{i}}}, \qquad (2)$$

где k – число ОС из которых состоит ЦРС; P_i – информационная мощность *i*-той ОС; $N_{i\,\hat{i}\acute{a}\grave{u}} = N_{i\,\ddot{a}\hat{i}\ddot{i}} + N_{i\,\hat{i}\acute{a}\tilde{n}\ddot{e}}$ – допустимое суммарное количество пакетов в ней, при заданном

ограничении на временную задержку пакетов $\grave{O}_{äîï}$ и ее производительности μ_i; $N_{i\,îáñë} = \mu_i$ – число пакетов, уходящих в единицу модельного времени на обслуживание в КС.

Тогда эффективность информационного обмена в ЦРС можно оценить значением к.п.д. в смысле передачи информации, как отношение представленных выше мощностей

$$\eta_{ÖÐÑ} = \frac{Ð_{ÖÐÑ}}{Ð_{ïîëí}}. \qquad (3)$$

В результате использования параметра к.п.д. в смысле передачи информации появляется возможность оценить степень близости ЦРС к ее предельным возможностям по информационному обмену, а использование имитационного моделирования позволяет непосредственно наблюдать процессы функционирования сети с одновременной регистрацией всех необходимых текущих и усредненных за период моделирования результатов в специально создаваемых таблицах. Все это приводит к значительному упрощению аналитических расчетов и сокращению временных затрат, свойственных аналитическим моделям при определении основных параметров и характеристик ЦРС. Наличие необходимой статистики, полученной в имитационной модели, сводит дальнейший процесс оценки информационной эффективности ЦРС к элементарным операциям, выполняемым средствами аналитического моделирования. В результате чего, реализуются основные достоинства указанных выше подходов к моделированию сложных ЦРС.

На основе представленного метода комбинирующего средства имитационного и аналитического моделирования были проведены исследования информационной эффективности ЦРС с топологиями «звезда» и иерархическая типа «дерево» для 30 УК. Полученные результаты показывают, что в условиях малых информационных нагрузок более эффективно работает ЦРС с топологией «звезда», что может объясняться меньшим количеством ретрансляций при информационном обмене. При увеличении входного трафика значительно лучшие результаты дает ЦРС с иерархической структурой. При этом данная сеть более устойчива к дальнейшим изменениям потоковой обстановки, тогда как в ЦРС типа «звезда» начинают сказываться значительные перегрузки в центральном УК.

В качестве общего вывода по проведенным исследованиям можно отметить, что для эффективной работы ЦРС необходимо обеспечение баланса между обеспечением максимального использования скоростных возможностей КС и временным хранением информации в УК с учетом заданного ограничения на временную задержку. На основе детального анализа условий передачи и хранения информации могут быть даны практические рекомендации по использованию топологий ЦРС в зависимости от интенсивности входной нагрузки.

Литература:

1. Захаров Г.П. Методы исследования сетей передачи данных. – М.: Радио и связь, 1982, 208 с.

2. Шварц М. Сети связи: протоколы, моделирование и анализ: Пер. с англ. – М.: Наука. Гл. ред. физ-мат. лит., 1992. Ч. 1, 336 с.

3. Межуев А.М. Тензорные методы в теории оценки информационной эффективности и анализа элементов цифровых радиосетей (монография). – Тамбов: Интеграция, 2008, 262 с.

4. Патент №247928, МПК7 H04L29/00 Способ оценки информационной эффективности системы связи / А.М. Межуев, И.И. Пасечников, А.В. Пономарев, Д.Л. Стуров (РФ). №2011151376/08. Заявл. 15.12.2011; опубл. 20.03.13. Бюл. № 8.

А.М. Межуев, Д.А. Смирнов, В.В. Харченко, А.И. Родзевич

СПОСОБЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В ЦИФРОВЫХ РАДИОСЕТЯХ ПРИ ИЗМЕНЕНИЯХ ВХОДНОГО ТРАФИКА

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», г. Воронеж, Россия

Ключевые слова: оценка, эффективность, информационный обмен, радиосеть, трафик, изменение, интенсивность, адаптация, топология, информационная мощность, тензорная методология.

В статье представлены способы оценки эффективности информационного обмена в цифровых радиосетях с заданной структурой с использованием обобщенного параметра – коэффициента полезного действия в смысле передачи информации. Разработан программный продукт, обеспечивающий получение зависимости коэффициента полезного действия от изменения входной нагрузки, а также расчет значений «полосы пропускания» цифровых радиосетей по трафику и временной задержке. Получен алгоритм оперативной смены информационной топологии сети, в условиях резких изменений входного потока и воздействия на систему связи средств радиоэлектронной борьбы противника.

A.M. Mezhuev, D.A. Smirnov, V.V. Kharchenko, A.I. Rodzevic

MODES OF AN ESTIMATION OF EFFICIENCY OF AN INFORMATION EXCHANGE IN DIGITAL RADIO NETWORKS AT VARIATIONS INPUT TRAFFIC

Military educational centre of science of Air Forces “Air Force Academy of a name prof. N.E. Zhukovski and Y.A. Gagarin”, Voronezh, Russia

Keywords: an estimation, efficiency, information exchange, radio network, traffic, variation, intensity, adapting, topology, information power, tensor methodology.

In paper the modes of an estimation of efficiency of an information exchange in digital radio networks with given structure with usage of the generalized parameter - efficiency in sense of an information communication represented. The software product providing deriving of dependence of an efficiency from variation of an input termination, and also calculation of values of "passband" ЦРС on traffic and time delay is designed. The algorithm of operating change of information topology of a network, in conditions of leaps of an input stream and action on a communication system of a means electronic warfare activity of the opponent is obtained.

За последние десятилетия в области передачи информации бурное развитие получили беспроводные цифровые радиосети (ЦРС). Такой качественный скачок был достигнут благодаря: повсеместной автоматизации систем связи и управления, высокой мобильности абонентов, бурному развитию беспроводных сетевых служб локальных, территориальных и даже глобальных сетей.

Тем не менее, процесс развития ЦРС сталкивается с рядом трудностей и решением ряда сложных задач к их числу можно отнести: резкое изменение интенсивности входной информационной нагрузки, значительное усложнение структуры сетей и расширения спектра услуг предоставляемых пользователям. Решение первой задачи является наиболее актуальным, так как оно не может быть достигнуто простым увеличением пропускной способности каналов связи (КС). Это приводит к работе ЦРС в режиме с промежуточным хранением информации в узлах коммутации (УК), для которого свойственны потери из-за ограничения на временную задержку пакетов. С учетом высокой гибкости ЦРС задача наращивания существующей сети путем введения в ее состав новых элементов решается довольно просто, т.к. беспроводная технология позволяет создавать практически любые структуры сетей на больших территориях [1, 2].

Вследствие всего выше сказанного, задача оценки информационной эффективности ЦРС в условиях изменения входного трафика и количества УК сети с учетом ограничения на временную задержку сообщений актуальна и имеет важное практическое значение.

Актуальность исследований определяется также соответствием решаемой задачи Федеральной и ведомственной целевым комплексным программам «По поэтапному переводу сети связи Вооруженных Сил Российской Федерации на цифровое телекоммуникационное оборудование».

Анализ существующих методов оценки информационной эффективности ЦРС, показал, что они имеют следующие недостатки: отражают только скоростные характеристики передачи информации (скорость передачи, коэффициент использования канала, производительность, временная задержка); не учитывают свойство временного хранения информации в условиях высокой информационной нагрузки в БЗУ; не позволяют оценить степень близости систем к оптимальным условиям информационного обмена (нет обобщенного параметра для однозначной оценки); не пригодны для сравнения сетей в различных условиях функционирования (при одинаковой производительности сетей невозможно сказать, какая из них более эффективно использует свои возможности по передаче информации); не могут быть использованы для практических рекомендаций и работы процедур, направленных на повышение качества работы сетей.

Данная работа посвящена решению задачи оценки эффективности информационного обмена в ЦРС с заданными структурами при высокой входной нагрузке с использованием обобщенного параметра – информационной мощности, отражающей, как скоростные возможности сети, характеризуемые задержкой при передаче информации и интенсивностью выходного потока, так и свойство хранения информации, определяемое числом сообщений, находящихся на хранении в буферных запоминающих устройствах (БЗУ) УК. При этом для анализа и определения основных параметров ЦРС предлагается использовать метод, основанный на тензорной методологии, который в процессе расчета одновременно учитывает структуру сети и протекающие в ней процессы.

Цель работы – объективная оценка возможностей ЦРС по передаче информации и определение условий её оптимального функционирования исходя из значения входной информационной нагрузки.

Информационная мощность ЦРС $P_{ЦРС}$ определяется допустимым числом сообщений V, которые могут находиться в сети с учетом ограничения по временной задержке и заданной производительности сети G, ограничивающейся пропускными способности КС в условиях высокой информационной нагрузки.

Тогда выражение для информационной мощности на основе аналогий с параметрами электрических цепей имеет вид:

$$P_{ÖÐÑ} = [I_{âõ}][R_t][I_{âûõ}] = VG \mid_{T_{äîï}} \quad (1)$$

Использование данного параметра для известной модели ЦРС в виде совокупности несвязанных ОС позволяет ввести понятие полной информационной мощности, характеризующей предельные возможности сети по передаче информации

$$P_{полн} = \sum_{i=1}^{M} P_i = \sum_{i=1}^{M} V_i \; {}^{вых}\gamma^i = V_i \; {}^{вых}\gamma^i \mid_{T_{доп}} \quad (2)$$

где i – условный номер ОС; P_i – мощность i-той ОС, V_i и ${}^{вых}\gamma^i$ – соответственно суммарное состояние, определяемое транзитными и внешними (поступающими от пользователей) сообщениями, и информационный поток на выходе (производительность) i-той ОС.

Для определения степени близости ЦРС к ее предельным возможностям по передаче информации используется параметр – коэффициент полезного действия (к.п.д.) в смысле информационного обмена, как отношение рассмотренных выше мощностей (отношение «реальной» мощности ЦРС к «идеальной»)[3].

$$\eta_{ÖÐÑ} = \frac{P_{ÖÐÑ}}{P_{ïîëí}} \quad (3)$$

Проведение цикла последовательных измерений к.п.д. передачи информации η позволяет определять интервал входного трафика $[\gamma_{âõ\,ïð\,1}, \gamma_{âõ\,ïð\,2}]$, в пределах которого система связи

функционирует с требуемой эффективностью информационного обмена, исходя из заданного порогового значения обобщенного параметра $\eta_{\text{ïîð}}$ и получить новый оценочный параметр полоса пропускания ЦРС по входному трафику на заданном уровне

$$\Ï_{\gamma(\eta_{\text{ïîð}})} = \gamma_{\text{âõ ïîð 2}} - \gamma_{\text{âõ ïîð 1}}. \quad (4)$$

Подобный параметр может быть получен и во временной области, если рассматривать зависимость к.п.д. в смысле передачи информации от величины временной задержки $\Ò$, т.о. также определяется полоса пропускания ЦРС по временной задержке на заданном уровне $\eta_{\text{ïîð}}$

$$\Ï_{\Ò(\eta_{\text{ïîð}})} = \Ò_{\text{ïîð 2}} - \Ò_{\text{ïîð 1}}. \quad (5)$$

На основе вычисления параметра коэффициента полезного действия разработан программный продукт, который позволяет: моделировать основные процессы, происходящие в ЦРС с заданными структурами при передаче информации; отображать зависимость к.п.д. сети от изменения входной нагрузки; определять оптимальные условия функционирования ЦРС. На рисунке 1 представлен интерфейс программы, производящей расчет эффективности информационного обмена в ЦРС со структурами типа «звезда» при различном количестве УК.

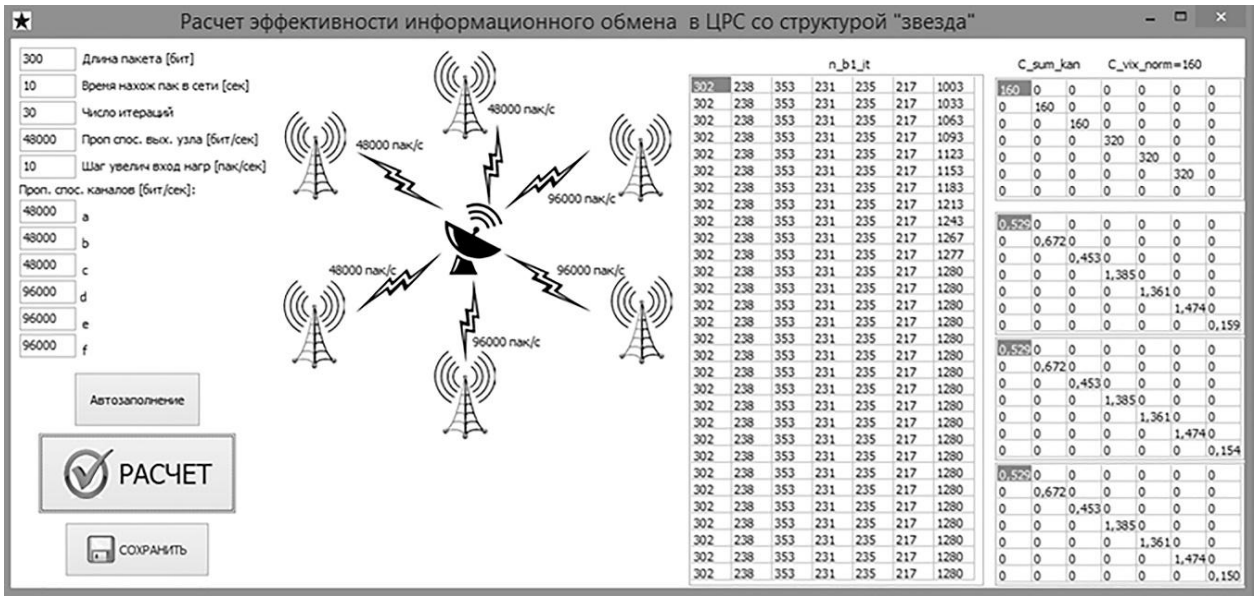


Рисунок 1. Интерфейс программы для оценки информационной эффективности ЦРС

На основе баз данных по оценке эффективности информационного обмена при изменении входного трафика для различных вариантов топологий ЦРС может быть реализована процедура оперативной смены логической (информационной) топологии сети без потери управления войсками в условиях резких изменений интенсивности входной нагрузки и воздействия на систему связи средств РЭБ противник. На рисунке 2 представлен алгоритм смены логической топологии сети.

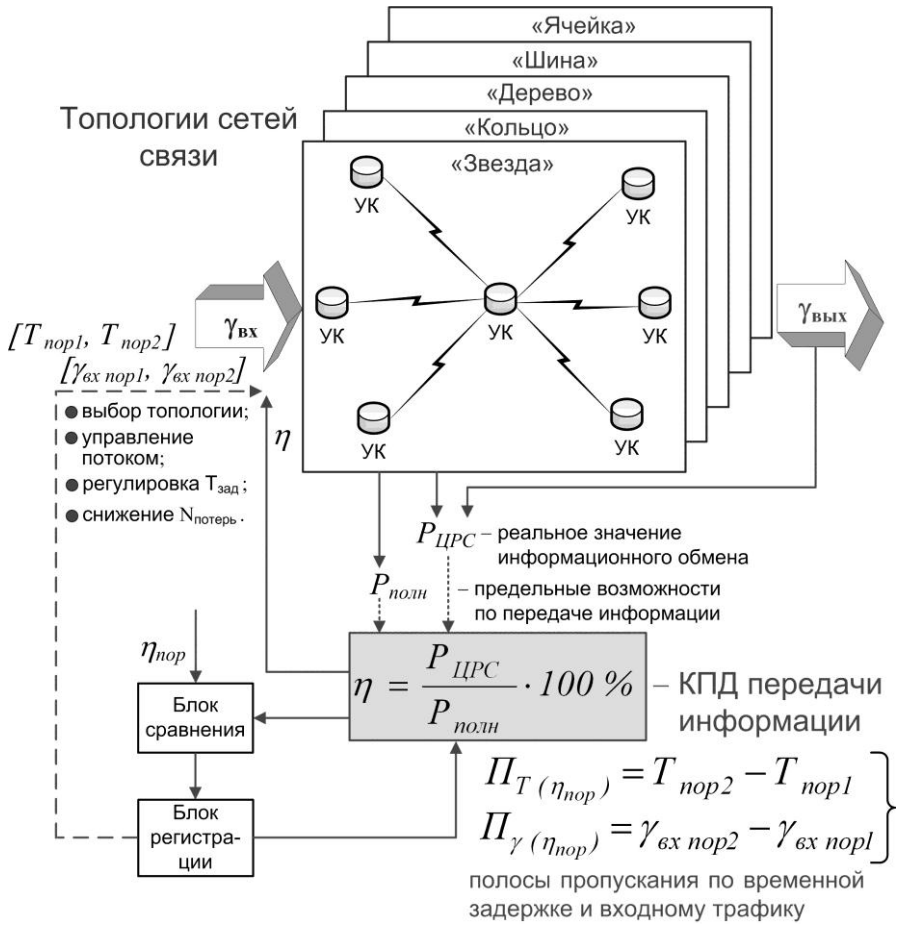


Рисунок 2. Алгоритм оперативной смены логической (информационной) топологии сети

Из вышеизложенного можно сделать выводы, что разработанные способы оценки эффективности информационного обмена в ЦРС: учитывают свойство временного хранения информации в сети; обобщенный параметр - к.п.д. в смысле передачи информации, позволяет оценить степень близости ЦРС к предельным возможностям по информационному обмену; с использованием параметров полосы пропускания ЦРС по входному трафику $Ï_{\gamma(\eta_{пор})}$ и временной задержке $Ï_{Ò(\eta_{пор})}$ могут быть сформулированы практические рекомендации для обеспечения заданного качества информационного обмена в сети и для работы процедур, направленных на повышение информационной эффективности сетей (управление входным потоком, регулировка ограничения на временную задержку, маршрутизация и смена топологии); разрабатываемые методы и алгоритмы являются универсальными для сравнения информационной эффективности ЦРС с разными структурами, функционирующих в различных условиях информационного обмена; моделирование в работы ЦРС на основе тензорной методологии позволит реализовать алгоритмы структурной и алгоритмической адаптации сетей в условиях изменения входной информационной нагрузки.

Литература:

1. Головин О.В., Чистяков Н.И., Шварц В., Хардон Агиляр И. Радиосвязь. – М.: Горячая линия-Телеком, 2001. с. 28.

2. Шаров А.Н., Степанец В.А., Комашинский В.И. Сети радиосвязи с пакетной передачей информации. СПб.: ВАС им. С.М. Буденного, 1994. 216 с.

3. Межуев А.М. Тензорные методы в теории оценки информационной эффективности и анализа элементов цифровых радиосетей (монография). – Тамбов: Интеграция, 2008, 262 с.

О.Ю. Миронов

ОБЕСПЕЧЕНИЕ ГАРАНТИРОВАННОГО ОБСЛУЖИВАНИЯ ПОТОКОВ ДАННЫХ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ ПРОМЫШЛЕННОГО НАЗНАЧЕНИЯ

Академия ФСО России, г. Орел, Россия

Ключевые слова: мультисервисные сети связи, технологическое управление, качество обслуживания, транспортная сеть коммутации пакетов, технология, архитектура, алгоритм, оптимизация, нагрузка, трафик, блоки данных.

Описана проблема обеспечения гарантированного обслуживания потоков данных в мультисервисных сетях связи промышленного назначения и возможность достижения прогресса в области управления трафиком путем построения системы управления доступом (СУД) потоков данных с учетом эффекта группирования потоков. Приведен рассчет пропускной способности, необходимой для изолированного обслуживания *n* потоков, и выделяемая пропускная способность для групповой системы из этих *n* потоков. Проанализирована "эффективность группирования" как разница между изолированной и групповой системами в отношении выделяемой суммарной скорости обслуживания для *n* потоков.

O.J. Mironov

SOFTWARE GUARANTEED SERVICE DATA FLOWS IN MULTISERVICE NETWORKS OF INDUSTRIAL PURPOSE

Academy FSO Russia, Orel, Russia

Keywords: multi-network communications, process control, quality of service, packet transport network, technology, architecture, algorithm optimization, load, traffic data blocks.

Described the problem of providing guaranteed service data flows in multiservice communication networks for industrial use and the ability to make progress in the field of traffic management by building access control system (AMS) data flows, taking into account the effect of grouping flows. An calculation capacity necessary for the maintenance of isolated n streams and allocates the bandwidth to the group of n of these streams. Analyzed the "efficiency of the grouping" as the difference between the isolated and group systems in relation to the total service rate allocated for the flow.

Основной целью функционирования мультисервисных сетей связи (МСС) промышленного назначения (ПН) является передача информации в виде команд технологического управления (ТУ), а также инфокоммуникационное обеспечение потребителей (должностных лиц) с соблюдением требований по обеспечению гарантий качества обслуживания (КО). Перспективная транспортная инфраструктура корпорации или распределенного хозяйствующего субъекта, обеспечивающая передачу потоков данных МСС ПН, реализует, как правило, технологию *MPLS* (*Multi Protocol Label Switching*). Одним из условий эффективного функционирования МСС ПН является оптимизация взаимодействия алгоритмов двух архитектур [1, 2] – интегрированных и дифференцированных услуг для обеспечения гарантированного качества обслуживания (ГКО) команд ТУ и потоков блоков данных пользователей МСС ПН.

В настоящее время опыта применения технологии *MPLS* для реализации МСС ПН еще не достаточно. Необеспечение ГКО передачи команд ТУ может привести к нарушению производства, что обуславливает финансовые потери предприятия.

В общем случае задача гарантированного обслуживания команд ТУ и потоков данных решается выделением требуемого объема ресурсов каждому изолированному соединению в сети. В реальных сетях вид кривой поступления входящего потока данных обусловлен алгоритмами формирования трафика "*дырявого ведра*, "*ведра жетонов*" [1, 2] и их модификаций. На рисунке 1 показаны функции поступления и обслуживания нагрузки для потока *TSpec* (*TSpec* - спецификация трафика, описывается параметрами, характеризующими модель функционирования "ведро жетонов"), иллюстрирующие порядок расчета параметров, характеризующих обеспечение ГКО на

наихудший случай. Здесь r_i - средняя скорость поступления нагрузки, b_i - максимальный размер пачки, p_i – пиковая скорость поступления нагрузки (в байтах/сек), L_i – максимальный размер пакета (в байтах), *W(t)* - кривая обслуживания.

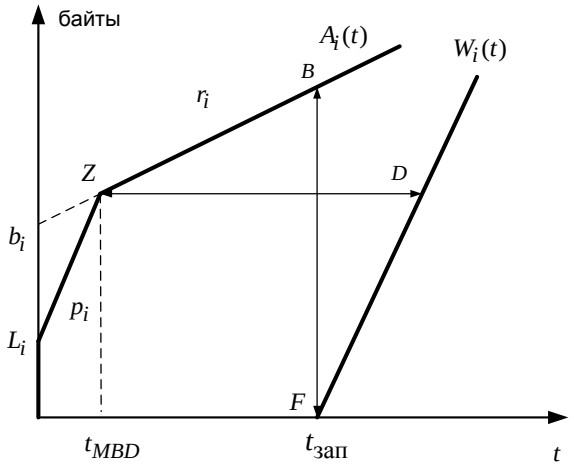


Рисунок 1. Графическое представление области ГКО для потока с заданными параметрами трафика *TSpec*

Исходя из подхода, изложенного в RFC 2212 [6], на основе известных кривых поступления и обслуживания становится возможным рассчитать значения управляющих параметров обслуживающей системы, определяемых на рисунке 1 положением прямой ZD как верхней границы суммарной задержки пакета в системе из K узлов $t_{\max}$ потоков и условии, что $p_i > r_i$:

$$t_{\max} = \begin{cases} \dfrac{(b_i - L)(p_i - R_i)}{R(p_i - r_i)} + \dfrac{L + \Delta_{C\sum}}{R_i} + \Delta_{D\sum} & \text{при } p_i \geq R_i \geq r_i \\ \dfrac{L + \Delta_{C\sum}}{R_i} + \Delta_{D\sum} & \text{при } R_i \geq p_i \geq r_i \end{cases}, \quad (1)$$

где $L_{\max} = \max(L_1, \ldots L_n)$ для всех n, допущенных к обслуживанию.

Здесь $t_{\max}$ имеет физический смысл гарантированного значения времени задержки и может быть обеспеченно при резервировании пропускной способности R_i (в байтах/сек) в каждом УК для обслуживания. Значение $t_{\max}$ в свою очередь зависит от значения выделяемой обслуживаемому потоку полосы пропускания R_i. Основой функционирования узла доступа к ТСКП при управлении доступом потоков данных является оценивание требуемых ресурсов сети для вновь поступающего потока. При этом пропускная способность сети, выделяемая потоку, является важнейшим из ресурсов сети. Расчет выделяемых ресурсов производится для системы из K узлов относительно пиковых и средних скоростей потока данных:

$$R_i = \begin{cases} \dfrac{p_i \dfrac{b_i - L_i}{p_i - r_i} + L_i + \Delta_{C\sum}}{t_{\max} + \dfrac{b_i - L_i}{p_i - r_i} - \Delta_{D\sum}}, & \text{при } p_i \geq R_i \geq r_i \\ \dfrac{L_i + \Delta_{C\sum}}{t_{\max} - \Delta_{D\sum}}, & \text{при } R_i \geq p_i \geq r_i \end{cases}, \quad p_i > r_i \quad . \quad (2)$$

В первом случае R_i превышает поступающую пиковую нагрузки, а во втором меньше пикового и не превышает среднюю скорость поступления нагрузки.

Одной из выявленных особенностей функционирования узла доступа к ТСКП с управлением ресурсами при изолированном обслуживании потоков данных является переоценка требуемых ресурсов, в некоторых случаях в разы превышающая достаточные значения. Такое явление называют "заброс трафика" [3]. Переоценка рассчитываемых ресурсов связана с параметрами, характеризующими пачечность трафика и не правильным выбором величины глубины "ведра жетонов". Кроме отмеченного недостатка модель управления доступом при изолированном обслуживании потоков данных в узлах доступа к ТСКП не может быть масштабируема на магистральные сети из-за потенциально большого количества обслуживаемых потоков.

Прогресса в области управления трафиком можно добиться путем построения системы управления доступом (СУД) потоков данных с учетом эффекта группирования потоков. Группированный поток, обрабатываемый при передаче мультисервисного трафика в ТСКП, обслуживается по классу наивысшего требования к уровню обслуживания входящего в него потока. Согласно концепции характеризации трафика групповых потоков, представленной в RFC 2216 [4], для аналитического описания группированного потока, поступающего с выходного порта узла доступа (маршрутизатора) в ТСКП, сумма *n* потоков, специфицированных как *TSpec*, описывает суммарную кривую поступления (СКП) следующим образом:

$$A_{\text{СКП}}(t) = \sum_{i=1}^{n}(r_i, b_i, p_i, L_i) = (\sum_{i=1}^{n} r_i, \sum_{i=1}^{n} b_i, \sum_{i=1}^{n} p_i, \max(L_i)) \quad , \qquad (3)$$

где $\max(L_i) = L_{mtu}$. (L_{mtu} - размер блока данных максимальной длины из всех обслуживаемых потоков).

При этом групповой поток обслуживается в маршрутизаторах зоны агрегации ТСКП как изолированное соединение с дисциплиной обслуживания *FIFO* в отдельно зарезервированном буфере. Ошибки возникают только в узле агрегации при передаче и узле сегрегации при приеме группированного потока, т.е. в узлах коммутации на границе сегментов *DiffServ* и *IntServ*.

Для упрощенной модели источника, использующей одиночные "ведра жетонов", при описании изолированных потоков типа *CBR* (нагрузка, которая на выходе характеризуется как "с постоянной скоростью передачи"), поступающих на узел *IntServ* от множества источников с $lb_i(r_i, b_i)$ и $t_{\max i}$, и общая пропускная способность, необходимая для изолированного обслуживания *n* потоков, может быть рассчитана как:

$$R_{lb}^{\text{Из}}(n) = \sum_{i=1}^{n} \frac{b_i + \Delta_{C\sum}}{t_{\max i} - \Delta_{D\sum}} \qquad (4)$$

где $t_{\max}$ – требуемое значение задержки пакетов "из конца в конец", в узлах коммутации, функционирующих в архитектуре *IntServ*, Δ_C – параметр, учитывающий ошибку, зависящую от скорости передачи и определяющую размер задержки пакета, проходящего "из конца в конец", Δ_D – ошибка, зависящая от дисперсии времени прохождения пакета некоторого потока через конкретный узел коммутации

Тогда с учетом выражения (2), для групповой системы из этих *n* потоков, выделяемая пропускная способность [4]:

$$R_{lb}^{\text{СКП}}(n) = \frac{\sum_{i=1}^{n} b_i + \Delta_{C\sum}}{\min t_{\max i} - \Delta_{D\sum}} \quad . \qquad (5)$$

Следует заметить, что за счет накопления ошибок планирования в узлах коммутации на всем протяжении маршрута передачи $R_{lb}^{\text{Из}}(n) \le R_{lb}^{\text{СКП}}(n)$.

Разница между изолированной и групповой системами в отношении выделяемой суммарной скорости обслуживания для n потоков есть "эффективность группирования" $GE_{Lb}(n)$, т.е.

$$GE_{Lb}(n) = R_{Lb}^{\text{Из}}(n) - R_{Lb}^{\text{СКП}}(n). \quad (6)$$

Продолжая вычисления для n потоков, характеризуемых кривой поступления от контроллера "дырявое ведро" с одинаковым значением требуемого времени задержки (объективно завышенной для некоторых потоков) можно получить следующее уравнение:

$$GE_{Lb}(n) = \sum_{i=1}^{n} \frac{b_i + \Delta_{C\sum}}{t_{\max} - \Delta_{D\sum}} - \frac{\sum_{i=1}^{n} b_i + \Delta_{C\sum}}{\min t_{\max i} - \Delta_{D\sum}} = \frac{(n-1)\Delta_{C\sum}}{\min t_{\max i} - \Delta_{D\sum}}. \quad (7)$$

Его анализ показывает, что независимо от зарезервированной скорости для однородных в отношении задержки потоков имеется выигрыш. При этом выигрыш будет наибольшим, если отдельные потоки имеют низкие требования к полосе пропускания и одинаковые требования к КО[4]. Кроме того следует отметить, что *GE* возрастает с увеличением таких параметров как: b, $\Delta_{C\sum}$ и $\Delta_{D\sum}$ и, в свою очередь, снижается вместе с увеличением требований по задержке – $t_{\max}$.

Таким образом, обслуживание группированного потока в сети позволяет при обеспечении заданного КО снизить объемы используемой пропускной способности каналов связи и буферного пространства портов УК. Это осуществляется за счет однократного учета появления ошибок планирования для всех потоков группы, в то время как для изолированного обслуживания потоков эти ошибочные члены должны учитываться по отдельности для каждого потока и УК [5].

Литература:

1. Turner, J.S. New directions in communications (or which way to the information age) / J.S. Turner. – IEEE Communication Magazine, vol. 24, issue 10, October 1986, pp.8–15.
2. Terms and Definitions related to Telephony Engineering. – Rec. E. 600. – 1995. – 242c.
3. Кутненко, В.В. Разработка и анализ распределенных систем интерактивной мультимедиа и графики в глобальных сетях :дис. канд. техн. наук: 05.13.13 / Кутненко Василий Васильевич. – М., 2004. – 186 с.
4. Shenker, S. General Characterization Parameters for Integrated Service Network Elements / J. Wroczlawski // September1997. RFC 2216.
5. Schmitt, J. On the Aggregation of Deterministic Service Flows. / M. Karsten, R. Steinmetz // In Proceedings of the Seventh IEEE/IFIP International Workshop on Quality of Service (IWQoS'99), London, UK. IEEE/IFIP, June 1999.
6. Chenker, S. Specification of Guaranteed Quality of Service / C. Patridge, R. Guerin. – RFC 2212, September 1997.

И.А. Молоковский, В.А. Прысь

АНАЛИЗ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ ДЛЯ УСЛОВИЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН В ОГРАНИЧЕННОМ ПРОСТРАНСТВЕ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

ГВУЗ «Донецкий национальный технический университет», г. Донецк

Ключевые слова: беспроводные технологии, Wi-Fi, ZigBee, NanoNet

Рассмотрен выбор беспроводных технологий в ограниченном пространстве в промышленных предприятиях. Учтены критерии: дальность распространения сигналов, мощность

излучения, скорость передачи, возможность работы в условиях ограниченного пространства, помехоустойчивость. Предложено использовать технологию NanoNet, которая имеет высокую скорость передачи до 2 Мб/с, дальность действия до 900 м и возможность работы приемников и передатчиков с малой мощностью, что позволяет проектировать сеть для предприятий с взрывоопасным технологическим циклом.

I.A. Molokovskiy, V.A. Prys

ANALYSIS OF WIRELESS TECHNOLOGY FOR RADIO PROPAGATION CONDITIONS IN THE CONFINED SPACE OF THE INDUSTRIAL ENTERPRISES

State Higher Education Establishment “Donetsk National Technical University”, Donetsk

Keywords: wireless technology, Wi-Fi, ZigBee, NanoNet

The problem of wireless communications was analyzed. The complex technological communication was considered and defined its advantages and disadvantages. NanoNet is chosen technology. This technology has a high transfer rate of up to 2 Mb / s, range up to 900 m.

Рост механизации производственных процессов в промышленных предприятиях чаще выдвигало на передний план проблему создания беспроводной локальной связи между персоналом. Важным условием предоставления связи – общение между всеми работниками, возможность в любой момент связаться с центральным диспетчером через голосовую связь или короткие сообщения. Поэтому для улучшения способов связи можно использовать беспроводную радиосвязь, не требующую больших затрат для расширения сети и которой может пользоваться каждый работник, имеющий приемник, независимо от своего места расположения. Однако условия распространения электромагнитных волн в промышленных предприятиях с ограниченным пространством по сравнению со свободным менее благоприятные. Надежная радиосвязь возможна обычно лишь в пределах видимости. Затухание и отражение радиоволн каменным углем, боковыми породами и креплением, металлом, стенами и фасадами сильно ограничивают дальность действия радиосвязи.

Беспроводные локальные сети занимают ведущее место. Сегодня они могут предоставлять подключение в местах, где прокладка проводной сети невозможна или затруднена. Для осуществления связи в ограниченном пространстве в промышленных предприятиях беспроводные сети должны предоставлять постоянный мониторинг места нахождения оборудования и персонала в цехах, а также отслеживать информации о состоянии производственных процессов, которые помогут избежать аварийных ситуаций и сократить до минимума затраты, осуществлять связь работников между собой и с центральным диспетчером. Именно для этого в статье рассмотрен вопрос внедрения новых технологий в промышленных телекоммуникационных сетях.

Современные беспроводные сети позволяют абоненту работать и предоставляют доступ к нужной информации, где бы не находилась точка доступа. Персонал, имеющий абонентский комплект не привязывается к определенной проводной сети или к рабочей станции, которая постоянно находится в сети. Беспроводные сети предусматривают возможность передвижения по участку покрытия без разрыва связи с подключением [1,2].

Все беспроводные сети поддерживают два режима: режим инфраструктуры (подключение через точку доступа) и режим ad-hoc (настройка работы без использования точки доступа), что позволяет добавлять новых пользователей в любое время и устанавливать дополнительные узлы [3].

Каждый рабочий, который имеет переносной абонентский комплект, может добавляться в сеть без ухудшения работы сети. В случае перегрузки сети трафиком, необходимо увеличивать зону покрытия. Увеличить зону покрытия возможно при добавлении точек доступа, что приведет к уменьшению времени отклика сети на запрос абонента.

Персонал промышленного предприятия может перемещаться между точками доступа без разрыва соединения с сетью благодаря использованию роуминга. Роуминг происходит за счет обмена между точками доступа полезной информацией.

Существующие беспроводные сети строго отвечают стандартам, что позволяет взаимодействовать беспроводными сетями между собой. Для анализа таких сетей в ограниченном

пространстве в промышленных предприятиях, нужно ознакомиться с существующими сетями промышленных инфокоммуникаций.

Под ограниченным пространством в промышленности подразумевается рабочее помещение в замкнутом виде, которое имеет вход и выход по разные стороны соответствующего сооружения. Площадь такого пространства измеряется от метров до километров. Необходимостью является покрытие всей площади сетью.

Для проектирования промышленной сети проведем анализ существующих беспроводных технологий, которые нашли свое применение во всех отраслях промышленности. Промышленные сети обеспечивают уменьшение экономических затрат на ресурсы и оборудование. Промышленные беспроводные сети могут быть созданы на технологиях: Wi-Fi (IEEE 802.11x), ZigBee (IEEE 802.15.4) и Nanonet (IEEE 802.15.4a).

Технология Wi-Fi, или RadioEthernet IEEE 802.11 – первый беспроводной промышленный стандарт работающий в на ограниченном пространстве. Подключенные абонентов имеют равноправные права на пользование ресурсом передачи данных в общем канале. На сегодняшний день существует 4 версии этого стандарта – IEEE 802.11(a,b,g,n). Промышленной телекоммуникации используется только два стандарта 802.11b и 802.11g, работающие на частоте 2,4 ГГц со скоростью передачи данных 11 Мбит/с и 54 Мбит/с соответственно. Покрытие одной точки доступа в закрытом пространстве может достигать от 10 до 100 м. На дальность действия сети влияет выбор соответствующего оборудования и антенны.

Многие пользователи думают, что промышленный Wi-Fi соответствует домашнему, но такое мнение является ошибочным. Для проектирования промышленной сети на основе Wi-Fi технологии, необходимо сначала провести множество расчетов и исследований таких как:

- дополнительных помехи и излучений (например, СВЧ-излучения);
- существующие препятствия на затухание радиоволн (например, стены, двери, металлоконструкции, изгибы помещения).

Сравнивая промышленный Wi-Fi с другими беспроводными технологиями, можно сказать, что для его создания необходимы большие затраты с экономической стороны, т.к. его оборудование дороже, энергопотребление выше, которое достигает 50мВт, а так же он имеет ограниченный радиус действия. Кроме недостатков в этой технологии есть и свои преимущества в скорость передачи до 54 Мбит/с.

Технология ZigBee – стандарт IEEE 802.15.4 нашел широкое применение в системах сбора информации, управления, мониторинга и отслеживания перемещения. Основное свое применение приобрел в промышленных предприятиях. Основные достоинства – низкое энергопотребление, надежность в передаче и защите информации, совместимость с иным оборудование других технологий.

Сети ZigBee способны самостоятельно образовывать и восстанавливать сеть за счет программного обеспечения. Сеть может увеличивать свой радиус действия при поломке соседнего датчика или искать другие пути передачи информации. Сети ZigBee способны, как и сети Wi-Fi, предоставлять доступ нескольким абонентам одновременно.

Протокол ZigBee работает на частоте 2,4 ГГц со скоростью передачи 250 кбит/с. Диапазон 2,4 ГГц разделен на 11 - 26 частотных каналов по 5 МГц каждый. Дальность связи этой технологии зависит от мощности передатчика и чувствительности приемника. Передатчик с мощность 1мВт образует дальность связи в ограниченном пространстве 10 м, а с мощностью 10мВт – до 80 м и с учетом прямой видимости дальность связи может увеличиваться до 1 км [4]. Так же дальность можно увеличить с помощью установки специальных антенн.

Достоинства ZigBee-сетей – малое энергопотребление и возможность работы от двух батарей размерами AA, низкая стоимость обслуживания и малогабаритность, легкость развертывания и настройки, возможность подключения большого числа датчиков. Недостатки – малая скорость передачи информации.

Технология NanoNet. Новая технология беспроводных сетей, которая получила свое применение в системах мониторинга и управления. Работает эта технология на частоте 2,4 ГГц со скоростью передачи информации до 2 Мбит/с.

Технология основана на использовании линейно-частотной модуляции, что позволяет увеличить ширину спектра тем самым повышать помехоустойчивость системы. Увеличение ширины спектра приводит к размытию мощности сигнала и при воздействии помех искажается только часть сигнала. На принимающей стороне сигнал восстанавливается в приемнике.

Использование широкого спектра технологией до 64 МГц, повышает надежность передачи информации и позволяет передавать информацию на высоких скоростях, по сравнению с сетями ZigBee.

Технология способна использоваться в тех местах, где радиуса действия технологии ZigBee не достаточно, а Wi-Fi сеть неспособна работать из-за высокого энергопотребления. Сеть NanoNet охватывает радиус действия сети до 900 м, что уменьшает количество точек доступа в промышленном помещении.

Приемопередатчики NanoNet имеют встроенный контроллер, что позволяет поддерживать несколько методов доступа к спектру. Мощность передачи сигнала колеблется в пределах от 1 мкВт до 6,3 мВт, что позволяет обеспечивать нужную зону покрытия сети. Основным преимуществом такой технологии является обеспечение большого радиуса действия и защищенность передаваемой информации.

Сравнивая все три технологии можно сказать, что каждая из технологий имеет свои достоинства и недостатки. Основными критерием выбора нужной топологии для создания беспроводной сети в промышленном предприятии с ограниченным пространством являются: – высокая помехоустойчивость; – большой радиус действия; – малые затраты на оборудование; – экономия в энергопотреблении; – высокая скорость передачи информации.

Основываясь на выше перечисленных критериях, можно сказать, что наиболее подходящей является технология NanoNet. Технология имеет широкий спектр, что увеличивает помехоустойчивость, высокую скорость передачи до 2 Мбит/с, дальность действия сети достигает 900 м, а так же малая мощность передатчика составляет 1 мкВт, что позволяет использовать такую технологию в помещениях со взрывоопасными веществами [5].

Для проектирования инфокоммуникационной сети с использование беспроводных технологий необходимо так же рассчитать информационную модель.

Информационная модель сети строится исходя из организационной структуры и взаимовоздействия между компонентами сети. Информационная модель сети представлена на рисунке 1.

Пользователи проектированной сети условно разделены на 2 категории:

- персонал промышленного предприятия;
- администратор (диспетчер).

Инфокоммуникационная сеть предоставляет следующие виды услуг:

1. Телефония;
2. SMS- оповещение;
3. Передача данных от датчика;
4. Местоположение;
5. Управление процессом;
6. Сигнализация.

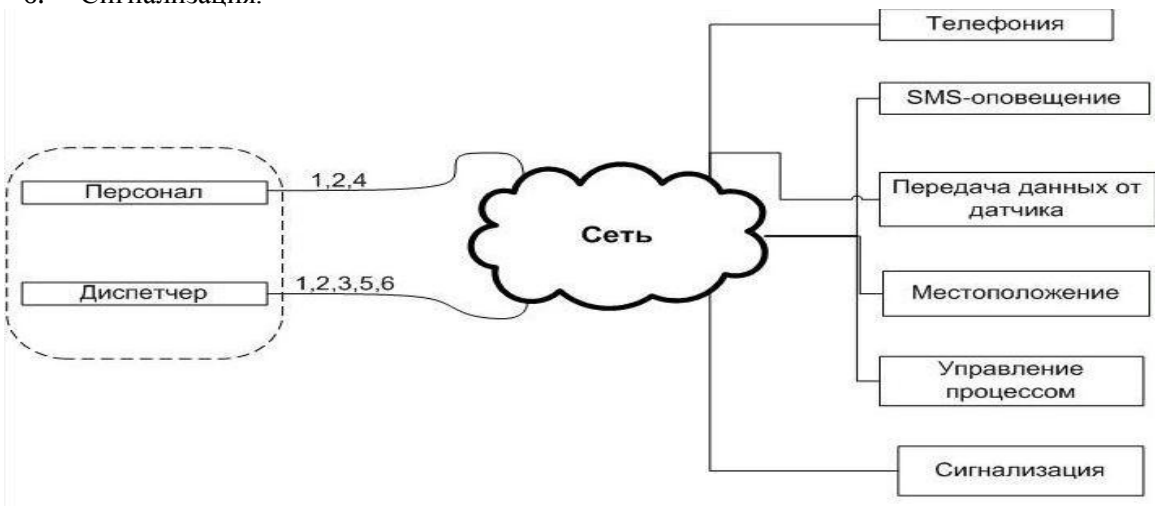


Рисунок 1. Информационная модель сети

Рассмотрев существующие технологии можно сказать, что с целью удовлетворения условий выбора технологии для промышленного предприятия с ограниченным пространством

подходит технология NanoNet. Она имеет высокую скорость передачи, дальность действия, помехоустойчивость и возможность работы приемников и передатчиков с малой мощностью, что позволяет устанавливать такие датчики определения местоположения и возможность использования их во взрывоопасных помещениях.

Литература:

1. Молоковский И.А. Исследование особенностей проектирования систем связи с использованием излучающего кабеля [Текст]/ И.А. Молоковский // Наукові праці Донецького інституту залізничного транспорту Української державної академії залізничного транспорту. – Донецьк, 2013. – Випуск 36. – С. 90-96.
2. Молоковский И.А. Исследование возможности передачи информации с помощью беспроводных технологий в телекоммуникационных сетях промышленных предприятий [Текст]/ Молоковский И.А. // Сборник научных трудов Донецкого национального технического университета, серия: «Вычислительная техника и автоматизация-2010». Донецк, 2010 р. – Выпуск 19 (171). – С. 77-82.
3. Беспроводное оборудование/ [Электронный ресурс] – Режим доступа: http://www.dlink.ru/ru/faq/112/790.html, свободный. – Название с экрана.
4. Беспроводные локальные сети/ [Электронный ресурс]: Промышленные сети и интерфейсы. – Электрон. дан. - Энциклопедия АУП ПТ. – Режим доступа: http://bookasutp.ru/Chapter2_11_1.aspx, свободный. – Название с экрана.
5. Nanotron: Технология NanoNET// [Электронный ресурс] - Режим доступа: http://efo.ru/cgi-bin/go?2490 , свободный. – Название на экране.

И.А. Калмыков, Д.О. Науменко

ОБОБЩЕНИЕ МЕТОДОВ ПЕРЕВОДА В КОД ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ ИЗ ПОЗИЦИОННОГО КОДА

Северо-Кавказский федеральный университет, г. Ставрополь

Ключевые слова: криптографическая система, модуляционный код, полиномиальноя системы вычетов, ортогональные преобразования сигналов.

В статье рассмотрены методы, используемые для ускорения работы блока криптографической системы, способной выполнять прямое преобразование в модулярный код, с использованием полиномиальной системы классов вычетов и с помощью которой возможна организация ортогональных преобразований сигналов в расширенных полях Галуа $GF(p^v)$. Исполнение данных методов позволяет разрабатывать высокоскоростные преобразователи кодов.

I.A. Kalmykov, D.O. Naumenko

GENERALIZATION OF THE TRANSLATION INTO THE CODE POLINOMIANOY SYSTEM OF RESIDUE CLASSES OF THE POSITION CODE

North-Caucasian Federal University, Stavropol

Keywords: cryptographic system, the modulation code, polinomialnoya deduction system, orthogonal transformation signals.

In the state the methods used for the acceleration of the block cryptographic system that can perform direct conversion to modular code using a polynomial system of residue classes and by means of which can be arranged orthogonal transformation signals in extended Galois fields GF (pv). Execution of these methods allows us to develop high-speed converters codes.

Основным достоинством полиномиальной системы классов вычетов (ПСКВ) является легкость модульных вычислений, благодаря чему можно повысить скорость вычислительных устройств цифровой обработки сигналов.

Для выполнения вычислений с использованием ПСКВ надлежит выполнить преобразование из позиционного кода в модулярный и обратно.

Как выглядит операнда в позиционном счислении показано ниже:

$$Y(x) = y_r x^r + y_{r-1} x^{r-1} + \cdots + y_1 x + y^0 \quad (1)$$

где y_j – элементы поля GF(2); *j = 0, … , r.*

Для перевода в непозиционную систему счисления из позиционной, определенную взаимно простыми основаниями $p_1(x), p_2(x), \ldots, p_n(x)$, надлежит делить на модули $p_i(x)$, *i* = 1, 2, …, *n.* Уравнение остатка $\beta_i(x)$ в этом случае выглядит как показано ниже:

$$\beta_i(x) = Y(x) - [Y(x)/p_i(x)]p_i(x) \quad (2)$$

где $[Y(x)/p_i(x)]$- наименьшее целое от деления $Y(x)$ на основание $p_i(x)$, i = 1, 2, …, n.

Таким образом, цель данной статьи - обобщение методов перевода в коды системы классов вычета из позиционного кода и выбор наиболее высокоперспективных из них.

Перечисленные выше методы можно разделить на три существенные группы. В первой группе за основу взят метод уменьшения разрядности числа, не имеющий операции деления.

Метод основан на следующем принципе: вычисление остатка реализуется при помощи итерационного алгоритма. Для этого надлежит определить остатки от деления на p_i степеней основания, которые дадут набор чисел C_i, i = 1, 2, …, r. Если остаток от деления степени основания C_i больше 1/2 модуля p_i, то значение C_i надлежит взять число, дополняющее до значения p_i, со знаком минус. Значения C_i можно знать до вычисления, и они являются константами для выбранной системы счисления. Количество разрядов C_i задается разрядностью исходного числа *Y.*

Далее выполняется произведение цифр исходного числа на соответствующие числа C_i, полученная сумма вычисляется

$$Y_i = Y_k \cdot C_k + \cdots + Y_1 \cdot C_1 + Y_0 \cdot C_0 < Y_k \cdot S^k + \cdots + Y_1 \cdot S^1 + Y_0 \quad (3)$$

По значению Y_i можно выявить остаток от деления числа *Y* на p_i. Если количество разрядов Y_i больше, чем p_i, то цифры числа Y_i снова умножить на числа C_i, причем полученная сумма будет $Y_2 < Y_i$.

По значению Y_2 возможно узнать остаток от деления числа Y на p_i. Это выполняется, пока не вычислим число Y_i, разрядностью меньшей или равной разрядности p_i. По данному числу и вычисляется остаток от деления числа Y на p_i.

Несмотря на простоту исполнения, вышеуказанный метод преобразования чисел по модулю, основанных по принципу рекуррентной редукции, сильно уменьшают область приложения модулярной арифметики.

Вторая группа - методы, обеспечивающие пространственное распределение вычислительного процесса – перехода из позиционной системы счисления в ПСКВ. Исключение обратных связей в нейронных сетях (НС) допускает устранение вышеперечисленных недостатков и реализует обработку исходных данных на сети прямого распространения. В нынешнее время существует математическая модель НС, реализующей прямое преобразование позиционного двоичного кода в код классов вычетов, на основе сети прямого распространения.

Итеративный алгоритм преобразования Y по модулю p будет выглядеть следующим образом:

$$Y(l+1) = \sum_{i=0}^{ord\,Y(l)} \left|2^i\right|_P^+ \cdot \left|\left[\frac{Y(l)}{2^i}\right]\right|_2^+ \quad (4)$$

где l=0, 1, 2,… - число итераций. Исключение обратных связей в НС увеличивает скорость обработки данных, потому что в такой сети одновременно исполняется несколько отсчетов и в каждом такте работы сети на входе формируются обработанные данные.

Третья группа выполняет различные варианты метода непосредственного суммирования.

Переход реализуется следующим образом:

$$\beta_i \equiv Y\,(x) mod\; p_i(x) = \sum_{l=0}^{k} y_l(x) \cdot x^l mod\; p_i(x) \quad (5)$$

где *i*=1, 2,…, *n*.

Для определения $Y\,(x)$ в системе классов вычетов с основаниями $p_1(x), p_2(x), \ldots, p_n(x)$.

Нужно вычислить в этой системе значения $y_l(x) \cdot x^l \bmod p_i(x)$. Тогда остаток по модулю $p_i(x)$ определяется

$$\beta_i(x) = \left|\sum_{l=0}^{k} \left(y_l^i \cdot x^l\right) mod\;\; p_i(x)\right|_2^+ \quad (6)$$

где $y_l^i = y_l(x) \bmod p_i(x))$, *i* = 1, 2, …, *n*.

В соответствии с (6), перевод Y (x) из ПСС в НСС сводится к суммированию по модулю два $\left(y_l^i \cdot x^l\right) mod\;\; p_i(x)$ в соответствии с заданным полиномом Y (x).

Таким образом, очевидно, что модификация и реализация метода непосредственного суммирования для ПСКВ позволяет разрабатывать более быстрые кодирующие устройства.

Литература:

1. Элементы компьютерной математики и нейроноинформатики /Червяков Н.И., Калмыков И. А., Галкина В.А., Щелкунова Ю.О., Шилов А.А.. - М.:

2. Червяков, Н.И., Калмыков, И.А., Щелкунова, Ю.О., Бережной, В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований сигналов в расширенных полях Галуа // Нейрокомпьютеры: разработка и примене-

3. Калмыков, И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/под ред. Н.И. Червякова – М.:ФИЗМАТЛИТ, 2005. – 276 с.

Г.М. Нашвандова, *З.Т. Хакимов, М.М. Хасанов

АНАЛИТИЧЕСКИЙ ОБЗОР РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В УЗБЕКИСТАНЕ

Ташкентский государственный технический университет, г. Ташкент, Узбекистан
*Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: мультимедиа, технология Wi-Fi, широкополосный доступ, волоконно-оптические линии связи, портал, интерактивные услуги, информационно-библиотечный центр, электронное правительство, электронная почта.

Приведён аналитический обзор развития информационно-коммуникационных технологий в Республике Узбекистан по итогам 2014 года. Анализированы развитие телекоммуникационной инфраструктуры связи с широкополосным доступом, развитие и внедрение современных информационно-коммуникационных технологий в системе «Электронное правительство». Описан анализ развития почтовой связи с использованием информационно-коммуникационных технологий для учета выплаты пенсий, пособий и др. денежных услуг. Рассмотрена подготовка и переподготовка кадров в области информационно-коммуникационных технологий на уровне международных стандартов.

G.M. Nashvandova, *Z.T. Xakimov, M.M. Xasanov

ANALYTICAL REVIEW OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN UZBEKISTAN

Tashkent State Technical University, Tashkent, Uzbekistan *Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: media, technology Wi-Fi, broadband, fiber-optic communication lines, portal, online services, information and library center, e-government, e-mail.

The analytical overview of the development of information and communication technologies in the Republic of Uzbekistan by the end of 2014. Analyzed the development of telecommunications infrastructure in communication with the broadband access, the development and introduction of modern information and communication technologies in the system of "Electronic government". Describes the analysis of the development of postal services using information and communication technologies to account for the payment of pensions, allowances and other monetary services. Reviewed the training and retraining in the field of information and communication technologies on the level of international standards.

Внедрение современных информационно-коммуникационных технологий – необходимое условие для развития любого государства. Узбекистан, идущий по пути демократических реформ и развития рыночной экономики, не является исключением.

Стратегия развития информационно-коммуникационных технологий в стране реализуется в соответствии с Комплексной программой развития Национальной информационно-коммуникационной системы Республики Узбекистан, рассчитанной на 2013–2020 годы. Данная программа утверждена Постановлением Президента Республики Узбекистан Ислама Каримова от 27 июня 2013 года «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан».

На заседании Кабинета Министров Республики Узбекистан, посвященном итогам социально-экономического развития республики в 2013 году и основным приоритетам экономической программы на 2014 год, перед Государственным комитетом связи, информатизации и телекоммуникационных технологий были поставлены задачи по своевременному выполнению мер и реализации проектов, определенных в Комплексной программе развития Национальной информационно-коммуникационной системы [1].

Основой для развития информационно-коммуникационных технологий является телекоммуникационная инфраструктура. За счет принимаемых мер в этом направлении на сегодняшний день уже достигнуты следующие результаты:

Развитие телекоммуникационной инфраструктуры. Нынешний этап развития телекоммуникационных технологий, сетей и инфраструктуры связи страны ведется путем расширения сетей фиксированного и мобильного широкополосного доступа, расширение центров коммутации передачи данных и голосового трафика, модернизации и расширения магистральных телекоммуникационных сетей, а также создания инфраструктуры для развития мультимедийных услуг.

На сегодняшний день общая скорость пользования международными информационными сетями возросла на 42,3% по сравнению с началом 2014 года и составила 15,5 Гбит/с.

Осуществлено строительство более 2000 км волоконно-оптических линий связи для широкополосного доступа по современным технологиям на участках «Бузатау-Кунград», «Гузар-

Байсун», «Денау-Узун-Шаргун», «Жаслик-Каракалпакия», «Муйнак-Кибла-Устюрт», «Узун-граница Таджикистана» с предоставлением конвергентных услуг, таких как видеотелефония, интернет-телевидение, высокоскоростной Интернет, просмотр HDTV-каналов и другие. Количество портов, установленных для оказания услуг фиксированного широкополосного доступа к сети Интернет, доведено до 640 тыс., а количество используемых портов возросло на 135,1%.

В целях экстренного реагирования на запросы пользователей по информационно-коммуникационным услугам во всех регионах страны были созданы 13 колл-центров в рамках проекта внедрения Единого центра обслуживания вызовов АК «Узбектелеком», а также для нужд государственных органов и хозяйствующих субъектов. Эти меры служат повышению качества оказываемых телефонных и интернет-услуг на более высокий уровень.

Ведется постепенная модернизация местных телефонных сетей на основе технологий следующего поколения. В течение текущего года по всей республике были запущены в эксплуатацию 26 единиц современного коммутационного оборудования, что значительно увеличивает емкость телефонных номеров.

Согласно Постановлению главы государства «О мерах по реализации инвестиционных проектов развития и модернизации телекоммуникационной сети Республики Узбекистан с участием Государственного банка развития Китая» от 2 декабря 2014 года осуществляются проекты по развитию телекоммуникационной инфраструктуры на общую сумму 117,6 млн. долларов США, в т. ч. за счет кредитных средств, выделенных Государственным банком развития Китая (КНР) на сумму 100,0 млн. долларов США. Эти проекты нацелены на расширение пропускной способности магистральных сетей передачи данных: по международному направлению — в 10 раз (до 100 Гбит/сек), до областных центров — в 4 раза (до 40 Гбит/сек) и райцентров — в 10 раз (до 10 Гбит/сек).

Реализуется программа развития сетей широкополосного доступа по технологии Wi-Fi в Республике Узбекистан на период 2014-2015 годы, направленная на создание возможности определить стратегические направления развития инфраструктуры беспроводных сетей широкополосного доступа по технологии Wi-Fi. Целью этой Программы является создание в каждом регионе республике, в том числе в аэропортах, вокзалах, в местах частого пребывания туристов, парках, торговых центрах и других общественных местах широкополосного беспроводного доступа по технологии Wi-Fi.

Продолжается работа по внедрению современных телекоммуникационных технологий в сферу телевидения согласно Постановлению Президента страны «О Государственной программе по техническому и технологическому переходу на цифровое телевещание в Республике Узбекистан». В рамках Программы переход на цифровое телевизионное вещание в нашей стране осуществляется в два этапа: первый охватывает 2013-2015 годы, второй — 2016-2017 годы [2].

Параллельно, развивая телекоммуникационную инфраструктуру страны, ведется работа по внедрению современных ИКТ путем создания информационных систем и информационных ресурсов, которые должны действовать в телекоммуникационных сетях.

Развитие и внедрение современных ИКТ.

Большое значение в этом направлении придается развитию системы «Электронное правительство». Успешно функционируют отдельные элементы данной системы, в частности:

С целью дальнейшего развития системы «Электронное правительство» утвержден Государственный заказ на реализацию проектов по внедрению и развитию информационно-коммуникационных технологий, в соответствии с которым ведется работа по реализации приоритетных проектов в сфере электронного правительства, в частности по созданию комплекса информационных систем «Предприниматель», формированию базы данных физических и юридических лиц, созданию Национальной географической информационной системы и др.

С 1 января 2014 года все бюджетные организации Республики Узбекистан осуществляют бухгалтерский учет и отчетность в единой системе «УзАСБО», которая позволила автоматизировать весь цикл бухгалтерского учета.

Значимыми темпами развивается Единый портал интерактивных государственных услуг, созданный в соответствии с Государственной программой «Год благополучия и процветания», утвержденной Постановлением Президента Республики Узбекистан от 14 февраля 2013 года №ПП-1920, посредством которого гражданам и предпринимателям оказано в общей сложности более 96 тыс. электронных услуг. Колл-центр Единого портала обработал более 40 тыс. вызовов. На сегодняшний день на портале доступно 230 интерактивных услуг.

На сегодняшний день зарегистрировано 226 государственных информационных ресурсов и 297 информационных систем государственных органов, которые используются как для автоматизации деятельности самих организаций, так и для оказания электронных услуг населению и субъектам предпринимательства.

Почти все образовательные учреждения страны подключены к образовательной сети ZiyoNET, что позволило создать единое образовательное пространство информационного взаимодействия. Быстрыми темпами набирает популярность запущенная в этом году новая версия образовательного портала сети ZiyoNET, реализованная в рамках выполнения Государственной программы молодежной политики в Республике Узбекистан (справочно: портал ZiyoNET функционирует с 2005 года) [3].

Продолжается техническое оснащение информационно-библиотечных центров (ИБЦ) страны. В 2014 году ИБЦ Кашкадарьинской, Наманганской, Сырдарьинской областей и г. Ташкента оснащены новым современным оборудованием в комплекте которого компьютеры, высокопроизводительные поточные сканеры, источники бесперебойного питания, резательное оборудование, переплетное оборудование.

Сегодня, на новом этапе развития информационно-библиотечной отрасли республики и в рамках данного проекта у наших информационно-библиотечных центров появилась реальная возможность установить взаимодействие и сотрудничество на новом уровне, позволяющем сделать его более эффективным, плодотворным и взаимовыгодным.

Особое внимание уделяется развитию отечественного рынка программных продуктов. В рамках реализации мер по дальнейшему усилению стимулирования отечественных разработчиков программного обеспечения создан Национальный реестр разработчиков программного обеспечения, в который уже включены 69 отечественные компании, в отечественном каталоге разработчиков программных продуктов software.uz размещены сведения о 1 600 отечественных программных продуктах [4].

Развитие почтовой связи с использованием ИКТ. В 2014 году с целью сокращения сроков перевозки почтовых отправлений обеспечен автомобильный транспорт в количестве 114 ед. которые используется на 483 маршрутах.

В октябре прошлого года АО «Узбекистон почтаси» подключилось к системе «PRIME», позволяющая повысить качества почтовых услуг путем организации быстрого и эффективного поиска международных посылок по поступившим рекламациям, налаживания электронного обмена данными с зарубежными почтовыми администрациями через международную систему «IBIS».

Одним из основных приоритетов АО «Узбекистон почтаси» является модернизация сети почтовой связи, развитие и внедрение новых видов услуг на базе ИКТ. В АО «Узбекистан почтаси» создана корпоративная сеть, на базе которой функционируют автоматизированные системы: электронных денежных переводов; гибридных денежных переводов; приема платежей; учета выплаты пенсий и пособий; мониторинга прохождения регистрируемых почтовых отправлений и др.

Ведется пилотный проект в г. Ташкенте и Ташкентской области автоматизированной системы приема подписки, оформления и обработки заказов на периодические издания с возможностью осуществления электронной подписки через Интернет [2].

Подготовка и переподготовка кадров. В целях улучшения системы подготовки высококвалифицированных специалистов в области ИКТ на уровне международных стандартов для отраслей и сфер экономики республики Ташкентский университет информационных технологий начал обучение по таким новым направлениям, как компьютерный инжиниринг, программный инжиниринг, телекоммуникационные технологии, телевизионные технологии, а также экономика и менеджмент в сфере ИКТ.

Также в этом году согласно Постановлению Президента страны в университете были открыты два новых направления магистратуры: управление системой «Электронное правительство», информатизация и библиотековедение. Эти новые направления открыты, исходя из растущей потребности на специалистов этих сфер, особенно с учетом развития системы «Электронное правительство» в стране [1].

Эффективность развития информационно-коммуникационной системы необходимо дополнять повышением уровня знаний по ИКТ специалистов различных сфер деятельности. В этих целях в этом году при ТУИТ был учрежден учебный центр электронного правительства, где

налажено обучение руководителей и сотрудников государственных и хозяйствующих органов и местных органов управления. На сегодняшний день обучение прошли более 16 тыс. сотрудников 63 учреждений.

В соответствии с Постановлением Президента Республики Узбекистан от 26 марта 2013 года №ПП-1942 года «О мерах по дальнейшему совершенствованию системы подготовки кадров в области информационно-коммуникационных технологий» в течение 2014 года более 60 молодых и перспективных преподавателей ТУИТ и его филиалов прошли обучение на курсах в Южной Корее и Германии. Это будет способствовать обеспечению качественной, на уровне международных стандартов, подготовки и повышения квалификации высококвалифицированных специалистов в сфере информационно-коммуникационных технологий.

Подводя итоги, можно отметить, что стратегия развития Национальной информационно-коммуникационной системы Республики Узбекистан, осуществляемая по всем направлениям развития информационно-коммуникационных технологий, демонстрирует положительную тенденцию.

Литература:

1. http://uzbekistan.uz/uz/resources.
2. http://uza.uz/ru/tech.
3. http://ziyonet.uz/ru.
4. http://software.uz/?AspxAutoDetectCookieSupport=1 .

А.В. Лемешко, Е.С. Невзорова

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ИЕРАРХИЧЕСКО-КООРДИНАЦИОННОЙ МАРШРУТИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Харьковский национальный университет радиоэлектроники, г. Харьков, Украина

Ключевые слова: принцип координации, количество итераций, иерархическая маршрутизация, потоковая модель маршрутизации.

Исследован метод двухуровневой маршрутизации на основе принципа целевой координации. Определены факторы, влияющие на количество координирующих итераций. Показана зависимость количества координирующих итераций от загруженности сети. Предложен метод уменьшения количества итераций за счет изменения маршрутной метрики каналов связи. Использование предложенного метода позволяет повысить масштабируемость маршрутных решений в телекоммуникационной сети, сократить количество итераций при реализации иерархической маршрутизации, тем самым сократить объемы служебного трафика в сети.

A.V. Lemeshko, E.S. Nevzorova

THE INCREASING EFFICIENCY OF AN IMPLEMENTATION OF HIERARCHICAL ROUTING WITH COORDINATION IN TELECOMMUNICATION NETWORK

Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

Keywords: coordination method, number of iterations, hierarchical routing, flow model of routing.

The two-level routing method based on the coordination principle has been investigated. The factors that influence on the number of coordinating iterations were determined. The dependence of the number of iterations on transmitted packet flows rate was shown. A method to reduce the number of iterations by changing the routing metric of links was proposed. Using the proposed method can both improve the scalability of routing decisions in the telecommunication network and reduce the number of

iterations in the implementation of hierarchical routing, and thus reduce the volume of service traffic on the network.

На сегодняшний день стремительно развиваются телекоммуникации в направлении парадигмы сетей нового поколения. При этом важными остаются вопросы, связанные с обеспечением качества обслуживания в телекоммуникационных сетях (ТКС) и повышению масштабируемости подобных решений. Поэтому на первое место выходит проблема разработки и использования адекватных моделей и эффективных методов иерархической маршрутизации в ТКС, основанных на теории иерархических многоуровневых систем [1,2].

В этой связи пусть структура ТКС описывается с помощью графа $G=(M,E)$, где M – множество вершин, моделирующее маршрутизаторы, а E – множество дуг, моделирующее каналы связи сети. Все множество M можно разбить на два подмножества: $M^+=\left\{M_r^+, r=\overline{1,m^+}\right\}$ – подмножество приграничных маршрутизаторов, где m^+ – количество приграничных маршрутизаторов; $M^-=\left\{M_j^-,\ j=\overline{1,m^-}\right\}$ – подмножество транзитных маршрутизаторов, где m^- – их общее число. Каждому каналу связи $(i,j)\in E$ соответствует пропускная способность φ_{ij}. Для каждого узла-источника в ТКС в качестве искомых выступают переменные $x_{ij}^{k_r}$, равные доле интенсивности k_r-го потока пакетов, передаваемого по каналу (i,j); k_r – поток пакетов, поступающий в сеть через r-й приграничный маршрутизатор; λ^{k_r} – интенсивность k_r-го потока.

С целью предотвращения потерь пакетов на маршрутизаторах и в сети в целом необходимо обеспечить выполнение условия сохранения потока:

$$\begin{cases} \sum\limits_{j:(i,j)\in E} x_{ij}^{k_r} - \sum\limits_{j:(j,i)\in E} x_{ji}^{k_r} = 1, \ \textit{если i-й маршрутизатор - узел-отправитель;} \\ \sum\limits_{j:(i,j)\in E} x_{ij}^{k_r} - \sum\limits_{j:(j,i)\in E} x_{ji}^{k_r} = 0, \ \textit{если i-й маршрутизатор - транзитный узел;} \\ \sum\limits_{j:(i,j)\in E} x_{ij}^{k_r} - \sum\limits_{j:(j,i)\in E} x_{ji}^{k_r} = -1, \ \textit{если i-й маршрутизатор - узел-получатель.} \end{cases} \quad (1)$$

Система уравнений (1) должна выполняться для каждого потока пакетов. Кроме того, с целью предотвращения перегрузки каналов связи важно выполнить условия:

$$\sum_{r\in M^+}\sum_{k_r\in K}\lambda^{k_r}x_{ij}^{k_r}\le\varphi_{ij}. \quad (2)$$

Стоит учесть, что при децентрализованном расчёте маршрутных переменных на каждом отдельно взятом узле-источнике условия (2) в явном виде учесть не представляется возможным, т.к. каждый маршрутизатор определяет путь передачи потока пакетов без информации о результатах расчёта другого источника. В связи с этим условие условия (2) запишем в следующем виде:

$$\sum_{k_r\in K_r}\lambda^{k_r}x_{ij}^{k_r}\le\varphi_{ij}-\sum_{\substack{s\in M^+\\ s\ne r}}\sum_{k_s\in K_s}\lambda^{k_s}x_{ij}^{k_s}. \quad (3)$$

С целью реализации многопутевой маршрутизации на маршрутные переменные накладываются ограничения вида:

$$0\le x_{ij}^{k_r}\le 1. \quad (4)$$

В векторно-матричной форме условия (1) и (3) представляются в следующем виде:

$$A_r\vec{x}_r=\vec{a}_r, \quad (5)$$

$$B_r\vec{x}_r \le \sum_{\substack{s\in M^+\\ s\ne r}} C_{rs}\vec{x}_s, \tag{6}$$

где $\vec{x}_r$ – вектор, координатами которого являются искомые переменные $x_{ij}^{k_r}$.

В ходе расчёта вектора искомых переменных $\vec{x}_r$ в качестве критерия оптимальности получаемых решений выбран минимум следующей целевой функции:

$$F = \sum_{r\in M^+} \vec{x}_r^t H_r \vec{x}_r, \tag{7}$$

где H_r – диагональная матрица весовых коэффициентов, координаты которой являются метрикой каналов связи, $[\cdot]^t$ - операция транспонирования вектора (матрицы).

Для решения сформулированной оптимизационной задачи использован принцип целевой координации [2-4]. Тогда, переходя к задаче на безусловный экстремум, необходимо максимизировать лагранжиан. По множителям Лагранжа:

$$\min_x F = \max_\mu L,$$

$$L = \sum_{r\in M^+} \vec{x}_r^t H_r \vec{x}_r + \sum_{r\in M^+} \mu_r^t (B_r\vec{x}_r - \sum_{\substack{s\in M^+\\ s\ne r}} C_{rs}\vec{x}_s). \tag{8}$$

В рамках данного принципа лагранжиан (8) представим в виде:

$$L = \sum_{r\in M^+} \vec{x}_r^t H_r \vec{x}_r + \sum_{r\in M^+} \mu_r^t (B_r\vec{x}_r) - \sum_{r\in M^+} \mu_r^t \sum_{\substack{s\in M^+\\ s\ne r}} C_{rs}\vec{x}_s. \tag{9}$$

В рамках двухуровневой иерархии решений предположим, что μ_r для нижнего уровня (уровня приграничных маршрутизаторов) являются фиксированными, т.е. значение множителя Лагранжа определяется на верхнем уровне. Тогда выражение (9) примет вид:

$$L = \sum_{r\in M^+} L_r,$$

$$L_r = \vec{x}_r^t H_r \vec{x}_r + \mu_r^t (B_r\vec{x}_r) - \sum_{\substack{s\in M^+\\ s\ne r}} \mu_s^t C_{rs}\vec{x}_s \tag{10}$$

.

Таким образом, лагранжиан (10) приобретают сепарабельную форму, а общая проблема маршрутизации оказалась декомпозицированной на ряд маршрутных задач (по числу приграничных маршрутизаторов). Решение задачи по минимизации выражения (10) определяет нижний уровень расчётов. Основной задачей верхнего уровня является координация решений полученных на нижнем уровне с целью недопущения перегрузки каналов связи сети (3). На верхнем уровне осуществляется модификация вектора множителей Лагранжа в ходе выполнения следующей градиентной процедуры:

$$\mu_r(\alpha+1) = \mu_r(\alpha) + \nabla\mu_r, \tag{11}$$

где α – номер итерации, $\nabla\mu_r$ – градиент функции рассчитывается исходя из получаемых на нижнем уровне результатов решения задач маршрутизации на каждом узле-отправителе:

$$\nabla\mu_r(x)\Big|_{x=x^*} = B_r\vec{x}_s^* - \sum_{\substack{s\in M^+\\ s\ne r}} C_{rs}\vec{x}_s^*. \tag{12}$$

Исследование сходимости процедуры (11), (12) для примера рассмотрено для структуры сети, представленной на рис. 1. Сеть состояла из 6 маршрутизаторов и 9 каналов связи. На каналах связи показана их пропускная способность (1/с). В ходе исследования была установлена зависимость количества итераций (11) от интенсивности потоков пакетов. Число потоков для

наглядности было выбрано двум. Первый поток пакетов передавался от первого маршрутизатора к третьему, а второй поток – от пятого к третьему. Максимальная интенсивность потоков от каждого источника составляла 200 1/с, т.к. при интенсивностях выше 200 1/с от каждого источника наблюдалась перегрузка каналов связи.

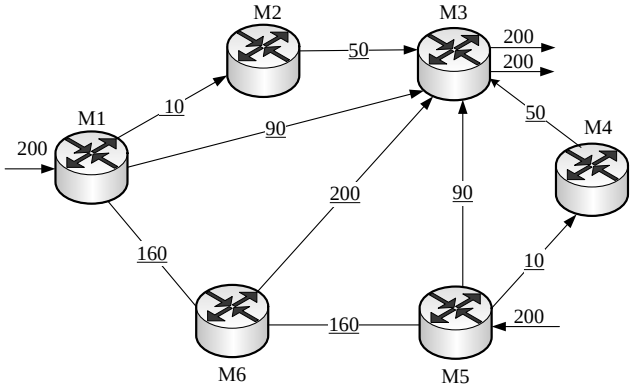


Рисунок 1. Структура исследуемой сети

Из табл. 1 видно, что с ростом интенсивностей потоков увеличивается и количество координирующих итераций, то есть замедляется сходимость метода иерархическо-координационной маршрутизации (8)-(12). Максимальное количество итераций равнялось 13 и наблюдалось при интенсивностях в 200 1/с для каждого потока. В ходе исследований установлено, что причина роста числа координирующих итераций – это перегрузка удалённых по количеству переприемов от узлов отправителя или получателя каналов связи.

Таблица 1. Результаты сравнительного анализа сходимости метода

№ расчета	Интенсивность первого потока пакетов, 1/с	Интенсивность второго потока пакетов, 1/с	Количество итераций в методе (8)-(12)	Количество итераций при использовании (13)
1	20	20	1	1
2	40	20	1	1
…	…	…	…	…
10	200	20	3	2
…	…	…	…	…
57	140	180	7	2
58	140	200	8	2
…	…	…	…	…
92	200	40	3	2
…	…	…	…	…
98	200	160	9	2
99	200	180	12	2
100	200	200	13	2

В этой связи в работе предлагается для каждого потока пакетов обеспечить увеличение метрики использования им каналов связи пропорционально удалённости этих каналов (по числу узлов) до соответствующего узла-отправителя или получателя. Поэтому для каждого потока для модификации метрик предлагаются следующие выражения:

$$M_i^* = M_i^n + q \cdot p_i, \qquad p_i = \mathbf{min}(hop_i^s, hop_i^d) - 1, \tag{13}$$

где M_i^n – метрика i-го канала связи, формирующаяся тем или другим протоколом маршрутизации; q – коэффициент изменения метрики ($q > 0$); hop_i^s – минимальное количество

узлов между узлом-отправителем и i-м каналом связи; hop_i^d – минимальное количество узлов между узлом-отправителем и i-м каналом связи.

Используя выражение (13) в рамках метода иерархической маршрутизации на основе принципа целевой координации, была также получена зависимость количества итераций от интенсивностей входящих потоков пакетов (табл. 1). Таким образом, после проведенных исследований можно сделать вывод, что модификация метрики удаленных каналов (13) значительно повлияла на количественный результат сходимости координационной процедуры, а именно – удалось сократить число итераций в среднем от 1,5 до 5 раз в зависимости от интенсивностей передаваемых потоков пакетов.

Литература:

1. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Издательство "Мир", 1973, 344 с.

2. Лемешко А.В., Ахмад М. Хайлан. Многоуровневое управление трафиком в сети MPLS–TE DiffServ на основе координационного принципа прогнозирования взаимодействий [Электронный ресурс] // Проблеми телекомунікацій, 2010, № 1 (1), с. 35-44. Режим доступа:http://pt.journal.kh.ua/2010/1/1/101_lemeshko_traffic.pdf.

3. Lemeshko O., Ahmad M. Hailan, Ali S. Ali. A flow-based model of two-level routing in multiservice network // Proceedings of the international conference «Modern Problems of Radio Engineering, Telecommunications and Computer Science». – Lviv-Slavsko, 2010, p. 225.

4. Невзорова Е.С. Ахмед К. Хасан, Бильчук В.А. Анализ метода двухуровневой маршрутизации на основе принципа целевой координации // Труды Северо-Кавказского филиала Московского Технического университета связи и информатики: Часть I, СКФ МТУСИ «ИНФОКОМ - 2014», 2014, с. 289-293.

А.Н. Павлов, С.А. Новичков

ВЛИЯНИЕ БИОИНФОРМАЦИОННОГО СОСТОЯНИЯ ВОДЫ НА ПРОЦЕССЫ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Московский технический университет связи и информатики, Москва, Россия

Ключевые слова: воздействие электромагнитного излучения, продольная электромагнитная волна, составляющие воды, кислотная вода, отличия поперечной от продольной ЭМВ, ИК спектр поглощения.

Аннотация: Исследуются явления, возникающие в процессе воздействия на водную среду электромагнитного излучения (ЭМИ). Показана особенность такого воздействия, процесс образования продольной электромагнитной волны (ПЭМВ), а также отличие ее свойств от поперечной ЭМВ, в частности, преобладания токов смещения, образуемый в воде, как в диэлектрике, над токами проводимости. Описаны обнаруженные в результате эксперимента пики «оптического пропускания» на частотах 170 МГц и 270 МГц и соответствующие им кластерные состояния водной среды. Описаны полученные в результате исследования различия между откликами на воздействие ЭМИ на кислотную и щелочную составляющие воды. Показана определяющая роль кислотной составляющей на процессы жизнедеятельности. Описан процесс, при котором возможно изменение pH в сторону увеличения, а также получен опытный результат: при воздействии ЭМИ на частоте 170 МГц в течении 60 минут, достигнуто изменение pH исходной воды с 6.4 до 7.3. Выдвинута гипотеза о возможности использования полученных результатов на процессы жизнедеятельности.

A.N. Pavlov, S.A. Novichkov

THE INFLUENCE OF WATER ON THE STATE OF BIOINFORMATIC PROCESSES OF LIFE

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: electromagnetic radiation of longitudinal electromagnetic waves that make up the water, acidic water, the differences of the longitudinal transverse electromagnetic wave, infrared absorption spectrum.

Abstract: The phenomena occurring during the impact on the aquatic environment of electromagnetic radiation (EMR). The show features such impacts, the formation of longitudinal electromagnetic waves (LEMW), as well as the contrast of its properties from the transverse electromagnetic wave, in particular, the prevalence of bias currents formed in the water as a dielectric over the conduction currents. Describes a result of an experiment revealed peaks "optical transmittance" at frequencies of 170 MHz and 270 MHz and the corresponding cluster of the aquatic environment. Describes the resulting study the differences between the responses to the effects of EMR on acid and alkaline components of the water. The determining role of the acid component in the processes of life. Describes the process by which you can change the pH upward, and the experimental results obtained under the influence of EMI at a frequency of 170 MHz for 60 minutes, achieved initial water pH change from 6.4 to 7.3. The hypothesis about the possibility of using the results obtained in the processes of life.

Известно, что основой функционирования живых систем является водно-белково-нуклеиновый комплекс, определяющий жизнедеятельность клеток. При этом наиболее слабым звеном в этом комплексе является водная составляющая, в отличии от более стабильных в энергетическом плане белковой и нуклеиновой компоненты [1].

Изучая детали изменения состояния водной составляющей можно проследить динамику процессов жизнедеятельности биообъектов. Поскольку молекулы воды обладают большим дипольным моментом (1,9Д), то они при взаимодействии образуют связанные структуры (кластеры), способные поглощать и излучать электромагнитные излучения (ЭМИ), выполняя при этом роль биоинформационного генератора слабоинтенсивного ЭМИ. Этот генератор имеет широкополосный спектр, поскольку источником излучений являются многочисленные кластерные образования, претерпевающие постоянные изменения в результате флуктуаций внешних факторов (температуры, электромагнитных полей и т.д.), то есть в спектре электромагнитного отклика водной среды можно обнаружить сигнал практически любой частоты [2].

Все кластерные перестройки обязаны структуре молекулы воды, в которой при взаимодействии ковалентных и водородных связей между атомами кислорода и водорода может происходить миграция протона (H^+), приводящая к его делокализации, что, в итоге, может привести к реструктуризации конкретного кластера [3]. В результате изменения энергетики кластера увеличивается вероятность межкластерного взаимодействия при внешнем воздействии, приводящего к изменению электромагнитных характеристик воды, что является первичным механизмом в сложной цепи биологических процессов в любом биообъекте [4].

Перспективным подходом к изучению механизмов изменения состояния водных кластеров являются воздействия «высокочастотных» ЭМП в замкнутом объёме, например, кварцевой ампуле («оптическом волноводе»). В процессе распространения ЭМП в «волноводе» создаётся продольная электромагнитная волна (ПЭМВ) в которой преобладает мода Е- типа, исследуемая нами [5].

Специфика энергетического действия ПЭМВ отличается от общепринятого представления, связанного с пропорциональностью действия внешней энергии электромагнитного излучения его частоте (поперечные ЭМВ).

В данном случае ситуация иная, поскольку в водной среде, где в разном соотношении присутствуют одновременно свободные и связанные заряды, определяющим является не частота излучения, а число квантов ($E = n \cdot \hbar\Omega$). То есть в процессах кластерного преобразования вода рассматривается как преимущественно диэлектрическая среда со связанными зарядами, поэтому, в результате внешнего электромагнитного воздействия, токи смещения преобладают над токами

проводимости. С другой стороны, носителями токов проводимости являются продукты диссоциации воды, свободные ионы кислорода, электроны и т.д. Поэтому процесс кластерной перестройки является сложным взаимосвязанным процессом влияния токов смещения и токов проводимости на эффекты поляризации, ответственных за новое кластерное состояние.

Для кластерной перестройки величины фиксируемых токов смещения и токов проводимости являются объективно значимыми параметрами. Численная оценка токов может осуществляться при выделении отдельных кластеров определённой формы и размеров с привлечением различных методов оценок, подробно рассмотренных в [6]. В настоящее время существует экспериментальный метод измерения токов проводимости в различных тканях человека в диапазоне частот 1…200 МГц при напряжённости внешнего электромагнитного поля – порядка десятков кВ/м [7]. Однако эта методика с позиций резонансного отклика водосодержащих биологических тканей на воздействие ЭМИ не отработана и практического применения не нашла.

В работе исследуемыми объектами являлась вода, подготовленная различными способами. Эксперимент проводился в кварцевой трубке, диаметром 25 мм и длиной 400 мм, с вмонтированными медными электродами, осуществляющими контакт с водой. Мощность входного сигнала составляла 250 мВт.

Ранее в [5] при изучении АЧХ воды нами обнаружены два характерных пика оптического пропускания, присущие различным кластерным состояниям на частотах 170 МГц и 270 МГц.

Первое состояние отличается строгой структурированностью кластеров, характеризуемое пиком «оптического пропускания» с частотой 170 МГц. Основным свойством этого излучения является то, что выдержка воды при комнатной температуре в течении часа на частоте 170 МГц [9] привела к существенному искажению ИК спектра поглощения, а именно, обнаружены изменения валентных колебаний (О-Н-молекул λ=2,9мкм.), деформационных мод (Н-О-Н-молекул λ=6мкм.) и вибрационных колебаний молекул H_2O λ=14мкм, что свидетельствует о предпосылках кластерных перестроек.

Второе состояние (пик на частоте 270 МГц) представляет кластеры, характеризуемые малоустойчивыми молекулярными связями, которые сравнительно легко разрушаются при малейших внешних воздействиях ЭМИ или температуры.

Помимо двух обнаруженных, различия кластерных состояний вероятно значительно многообразнее, о чём свидетельствуют многочисленные аномалии электромагнитного пропускания (промежуточные пики оптического пропускания) в исследуемом частотном диапазоне.

В общем случае электрохимические реакции, приводящие к образованию новых кластеров, изменяющих систему межмолекулярных взаимодействий, нельзя рассматривать без участия роли свободных токов. Носителями которых являются растворённый кислород, свободные гидроксильные группы, водород, азот и т.д. Эти носители токов особенно явно будут проявлять себя после электролиза при получении кислотной и щелочной составляющих.

В нашем случае изучались АЧХ воды с различным pH при воздействии ЭМИ в частотном диапазоне 1...150 МГц, в котором проявлялись стабильные по частотному расположению пики «оптического пропускания». Разложение на кислотную и щелочную составляющие производилось с помощью электролизёра «Ива–1». В результате электролиза исходной воды с pH=7,3 получалась вода с pH=2.9 (кислотная) и с pH=11,2 (щелочная). Полученные АЧХ системы с кислотной и щелочной водой, показанные на рис.1, существенно отличаются как по частотному расположению пиков «оптического пропускания», так и по амплитуде пропущенного сигнала, что свидетельствует о различных условиях реструктуризации кластеров. В [9] и [10] установлено, что щелочная вода, в отличии от кислотной, имеет пониженное содержание кислорода и азота, повышенную концентрацию водорода и свободных гидроксильных групп, меньшую электропроводность. Эти свойства щелочной воды могут свидетельствовать о том, что её кластеры более инертны к изменениям при внешнем воздействии, по сравнению с кластерами кислотной воды, что подтверждается идентичностью характера АЧХ щелочной (рис.1) и исходной воды (рис 2).

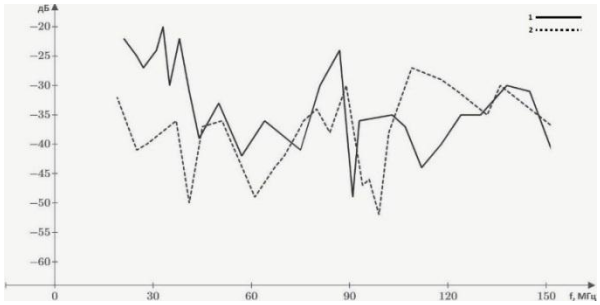


Рисунок 1. АЧХ системы с щелочной (1) и кислотной (2) составляющими воды, полученные в результате электролиза

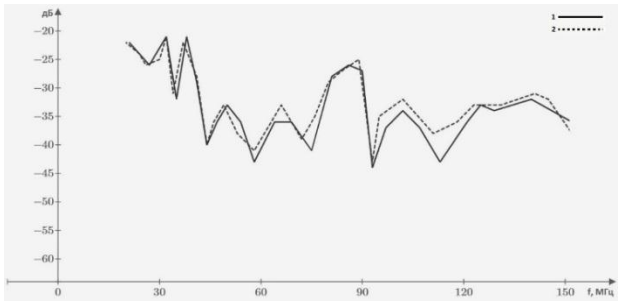


Рисунок 2. АЧХ системы с исходной водой (2) и водой после смешивания кислотной и щелочной составляющих (1)

На рис. 2 приведены АЧХ исходной воды, полученной до электролиза, (1) и АЧХ той же воды спустя 2 часа после последующего смешивания кислотной и щелочной составляющих (2).

Сравнение зависимостей 1 и 2 (рис.2) указывает на практически неизменный характер АЧХ, что является доказательством сохранения некоторой кластерной «памяти» исходной воды (с pH=7,3) через сутки после разложения её на две различные по кластерному составу составляющие (с pH=2,9 и pH=11,2).

Из приведенных АЧХ следует, что структурные изменения состояния воды в большей степени определяются кислотной составляющей, которая в исходной воде носит скрытый характер и в явном виде себя не проявляет. Однако именно это обстоятельство является определяющим в жизнедеятельности, поскольку глубинный механизм обезвоживания организма начинается с изменения кислотной составляющей, что в итоге приводит к различным заболеваниям, старению и смерти.

На основе этого можно предположить, что решить проблему приостановки (или торможения) «закисления» конкретного водного кластера можно при резонансном электромагнитном воздействии на его структуру. Для этого необходимо подавить функционирование основных составляющих кислотной компоненты с одновременным сдвигом в сторону «раскрепощения» компонент щелочной составляющей. Такое перераспределение не противоречит законам сохранения, поскольку все компоненты присутствуют изначально в исходном состоянии воды, а в результате воздействия требуется лишь их структурно перераспределить, при этом энергетика системы в целом не должна изменится.

В частности, нами было обнаружено, что при воздействии ЭМИ с частотой 170 МГц на водную среду длительное время возможно изменение pH в сторону увеличения (в одном из экспериментов при воздействии ЭМИ на данной частоте в течении 60 минут pH водной среды изменился с 6.4 до 7.3, что также было подтверждено в [11]). Факт увеличения pH путём электромагнитного воздействия крайне интересен и важен, что указывает на необходимость проведения дальнейших исследований в этом направлении с целью увеличения полноценной продолжительности жизни человека.

Литература:

1. Линг Г. Физическая теория живой клетки. Незамеченная революция. // СПб.: Наука. 2008, 375 с.

2. Бецкий О. В., Козьмин А. С., Файкин В. В., Ярёменко Ю. Г. Анализ биофизических механизмов воздействия низкоинтенсивных электромагнитных волн в крайне высокочастотном и терагерцовом диапазоне частот // Биомедицинская радиоэлектроника. 2014. №5, с. 29-37.

3. Бецкий О. В. Вода и электромагнитные волны // Биомедицинская радиоэлектроника. 1998. №2, с. 3-6.

4. Fesenko E. E. Geletyuk V. I. Kasachenko V. N. Chemeris N. K. Prelinainary microwave irradiation of water solution changes their channel-modifying activity // FEBS Letters. 1995. V.366. P. 49-52.

5. Павлов А. Н., Новичков С. А., Ломакова Е. М., Морозова Н. В. Изменение состояния водной составляющей жидких сред при воздействии электромагнитного излучения в УКВ диапазоне // Электромагнитные волны и электронные системы. 2014 №12 с .68-71.

6. Готовский М. Ю., Перов С. Ю., Белая О. В. Анализ возможностей методов теоретической дозиметрии в оценке биологического действия и терапевтического применения низкочастотных электромагнитных полей // Биомедицинская радиоэлектроника 2014. №12 с.12-16.

7. Hagmann M. J., Babij T. M. Noninvasive measurement of current in the human body for electromagnetic dosimetry // IEEE Trans Biomed Eng.1993.V.40 №5 p.418-423.

8. Павлов А. Н. Ермолаев Ю. М. Биоинформационная экология // М.: ИРИАС, 2011—144С.

9.Хан В. А., Власов В. А., Мышкин В. Ф., Ижойкин Д. А., Рахимжанова Л. А. Исследование влияния электромагнитных полей на структуру и свойства воды // Научный журнал КубГАУ №8 (07), 2012 с 1-13.

10.Прилуцкий В. И., Бахир В. М. Электроактивированная вода. Аномальные свойства, механизм биологического действия // М.; ВНИИИМТ АО, Экран, 1997. с.228.

11. Бессонова А. П., Стась И. Е. Влияние высокочастотного электромагнитного поля на физико–химические свойства воды и её спектральные характеристики // Ползуновский вестник, 2008. №3 с.305-309.

Д.Л. Осия

МОДЕЛЬ ИЕРАРХИЧЕСКОЙ СЕТИ ДОСТУПА С ПОВТОРНЫМИ ВЫЗОВАМИ

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: модель иерархической сети доступа, влияние поведения пользователя, анализируемый поток заявок, итерационный метод Гаусса-Зейделя.

Построена математическая модель иерархической сети доступа, в которой учитывается влияние поведения пользователя на процесс формирования входного потока заявок. Абонент, получив отказ в обслуживании из-за недостаточности ресурса передачи информации хотя бы в одной из соединительных линий, составляющих маршрут движения анализируемого потока заявок, с определенной вероятностью повторяет вызов через случайный промежуток времени. Для расчета характеристик обслуживания поступающих заявок предлагается использовать итерационный метод Гаусса-Зейделя решения системы уравнений статистического равновесия исследуемой модели иерархической сети доступа.

D.L. Osiya

HIERARCHICAL MODEL OF NETWORK ACCESS WITH REPEATED CALLS

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: model of hierarchical access network , the impact of user behavior , analyzed the flow of applications , iterative Gauss-Seidel method.

A mathematical model of a hierarchical network access, which takes into account the influence of user behavior on the formation of the input stream applications. Subscriber receiving a denial of service due to lack of transmission resource information in at least one of the connecting lines that make up the route of the analyte flow applications, with a certain probability, recalls after a random interval. To calculate the characteristics of the service incoming requests are encouraged to use the iterative Gauss-Seidel method for solving the equations of statistical equilibrium model under investigation hierarchical access network.

Введение.

В настоящее время большинство операторов при планировании мультисервисных сетей и их фрагментов используют методики, в которых заложены избыточные требования к ресурсу передачи информации. Связано это в основном с низкими ценами на канальные ресурсы и ошибками в оценке объёма услуг передачи данных. Стоимость сети доступа, по разным

исследованиям, составляет 20-30 процентов в общей структуре затрат, требуемых для создания местной телекоммуникационной системы. Развитие услуг связи меняет подход к построению сетей доступа. Они должны поддерживать все виды телекоммуникационных услуг (речь, данные, видеоинформация), обладать высокой надежностью, гарантировать требуемое качество передачи сигналов.

Для разработки эффективных методик оценки величины канального ресурса сетей доступа, в которых учитываются топология, особенности предоставления абонентам действующих и перспективных коммуникационных сервисов, а также поведение абонента после получения отказа в обслуживании необходимо построение соответствующих математических моделей. Иерархическая сеть доступа часто используется для концентрации информационных потоков, поступающих от абонентов. Для ее топологии характерно следующее свойство: узлы и связи между ними образуют неориентированный ациклический граф, не содержащий замкнутых путей, позволяющий соединить единственным образом пару любых узлов. В теории графов такие сети называются древовидными. Пример иерархической сети показан на рисунке 1. Для практических приложений большое значение имеет анализ моделей иерархических сетей доступа с учетом влияния повторения заблокированной заявки.

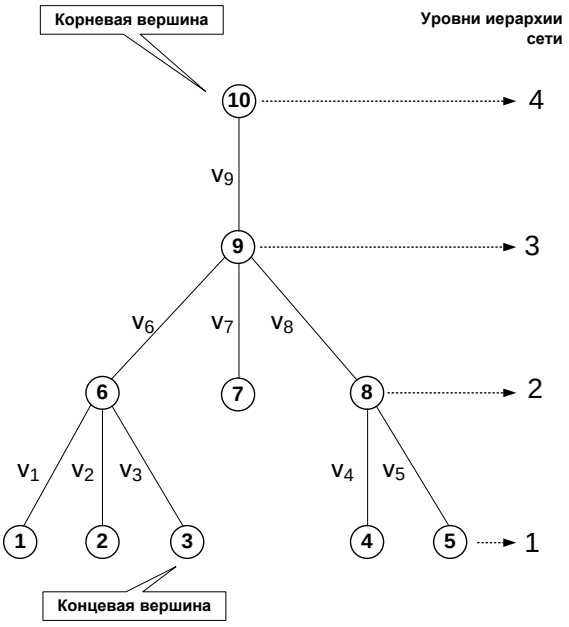


Рисунок 1. Иерархическая сеть доступа

Описание модели.

Далее будем считать, что рассматриваемая модель иерархической сети доступа имеет нумерацию линий и узлов, использованную на рисунке 1. Сеть имеет следующие особенности, обусловленные ее определением: число узлов сети на единицу больше, чем J — число линий; каждый узел сети, за исключением (J +1)-го, имеет одну исходящую линию; все узлы сети, за исключением концевых, имеют одну или несколько входящих линий; все маршруты передачи информации начинаются в одном из концевых узлов и заканчиваются в корневом узле; максимальное число узлов в маршруте определяет число уровней иерархии сети. В построенной модели иерархической сети доступа имеется n потоков заявок на передачу трафика от одного из концевых узлов до корневого узла. Поток заявок с номером k, характеризуется интенсивностью поступления заявок λ_k, средним временем обслуживания заявки $\frac{1}{\mu_k}$, числом канальных единиц, необходимых для обслуживания одной заявки b_k и маршрутом передачи трафика R_k. Обозначим через $a_k = \frac{\lambda_k}{\mu_k}$ интенсивность поступления заявок в эрлангах.

Поступившая заявка *k*-го потока принимается к обслуживанию, когда во всех линиях маршрута следования трафика имеются не менее b_k свободных канальных единиц. Если таковых нет, то заявка получает отказ. Пусть: H_k — вероятность повторения заявки из-за нехватки канального ресурса в маршруте следования трафика, $\frac{1}{\nu_k}$ — средняя длительность промежутка времени между последовательными повторными заявками одного абонента, $k = 1, 2, \ldots, n$. Будем полагать, что это время имеет экспоненциальное распределение с соответствующим параметром. Топология сети задаётся маршрутной матрицей R, которая определяет множество N_j номеров потоков заявок, использующих *j*-ую линию, $j = 1, 2, \ldots, J$, и множество R_k номеров линий, составляющих маршрут движения трафика, относящегося к обслуживанию *k*-ой заявки, $k = 1, 2, \ldots, n$. Определение структуры маршрутной матрицы приведено в [2]. Любой входной поток заявок представляет собой сумму пуассоновского потока первичных заявок и потока повторных заявок, вызванных негативной реакцией абонентов сети на отказ в попытке установить соединение. Схема иерархической сети доступа с учетом повторных вызовов показана на рисунке 2.

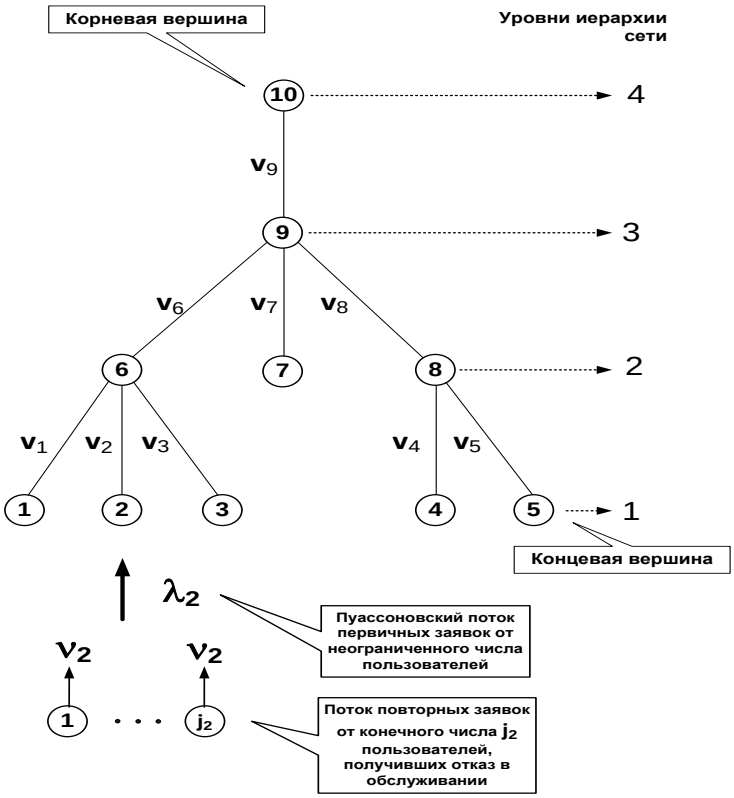


Рисунок 2. Схема функционирования модели иерархической сети доступа с учетом повторных вызовов

Область использования модели — расчёт пропускной способности линий связи в условиях перегрузки. Дополнительными показателями качества работы системы связи в условиях перегрузки являются: среднее число повторных попыток соединения на одну первичную, среднее число отказов на одно установленное соединение, доля повторных заявок в общем потоке заявок, поступающих на обслуживание. Эти и другие характеристики могут быть найдены, если известны значения стационарных состояний модели $\rho(j_1,\ldots,j_n,i_1,\ldots,i_n)$, где значения j_k, $k = 1, 2, \ldots, n$, изменяются в интервале $[0,\infty)$, а значения $i_1,\ldots,i_n$ в совокупности удовлетворяют неравенству

$$\sum_{k \in N_j} b_k i_k \le v_j \quad , \quad j = 1, 2, ..., J .$$

Для оценки вероятностных характеристик модели, основанный на использовании вероятностей стационарных состояний модели, можно использовать итерационный метод Гаусса-Зейделя решения системы уравнений равновесия.

Заключение.

Разработана модель иерархической сети доступа с учетом влияния поведения пользователя на процесс формирования входного потока заявок. Для расчета характеристик обслуживания поступающих заявок предлагается использовать итерационный метод Гаусса-Зейделя. Модель может быть использована при решении задач планирования пропускной способности иерархической сети доступа.

Литература:

1. Алексеев Е.Б. Оптические сети доступа: учебное пособие –М: ИПК МТУСИ 2005. -140с

2. Степанов С.Н. Основы телетрафика мультисервисных сетей—М.: Эко-Трендз, 2010.

3. Степанов С.Н., Осия Д.Л. Алгоритм оценки показателей обслуживания заявок в иерархических сетях доступа - Т-СОММ. Телекоммуникации и транспорт. - 2012. -№7. - С.193-195.

4. Степанов С.Н., Осия Д.Л. Приближённый метод оценки показателей обслуживания заявок в иерархических сетях доступа с учетом влияния поведения пользователя //Т-СОММ. Телекоммуникации и транспорт. — 2014. — N 8. — С.93-96.

Е.Д. Пронина, В.Б. Белянский

МАЛОГАБАРИТНЫЕ ПЕРЕДАЮЩИЕ АНТЕННЫ ДЛИННОВОЛНОВОГО ДИАПАЗОНА ЦИФРОВОГО СТАНДАРТА РАДИОВЕЩАНИЯ

Московский технический университет связи и информатики, г. Москва

Ключевые слова: длинноволновый диапазон, логопериодическая антенна, квазилогопериодическая антенна, предел Чу-Харрингтона, КСВ, частотно-расширяющие цепи (ЧРЦ).

Исследовалась возможность реализации DRM длинноволнового диапазона радиовещания на переходной период и разработка концептуальной модели радиовещательной антенны длинноволнового диапазона с расширенной полосой частот. Рассматривалась возможность уменьшение габаритов антенны при помощи преодоления предела Чу-Харрингтона, а так же использования частотно-зависимых изоляторов (ЧЗИ). Так же рассчитывались габариты антенны и необходимое количество вибраторов антенны для обеспечения требуемой полосы частот.

E.D. Pronina, V.B. Belyanskii

MINIATURE TRANSMITTING ANTENNAS LONG WAVELENGTH DIGITAL BROADCASTING STANDARD

Moscow Technical University of Communications and Informatics, Moscow

Keywords: long-wavelength range, log-periodic antenna, limit Chu-Harrington, SWR, frequency-expanding circuits.

Investigated feasibility of long wavelength DRM broadcasting on the transition period and the development of a conceptual model of the broadcasting antenna longwave range with extended bandwidth. The possibility to reduce the size of the antenna by means of overcoming the limit of the Chu-

Harrington, as well as the use of frequency-dependent insulators. As the dimensions of the antenna are calculated and the required number of dipoles of the antenna to ensure the required bandwidth.

В статье «Расширение полосы согласования передающих вещательных антенных систем диапазона ДВ для работы в режиме DRM» журнала T-Comm #1-2013 Вармамовым О.В. было предложено использование частотно-расширяющих цепей (ЧРЦ) для расширения диапазона. [1]

Однако, на частотах выше 300 кГц и при высотах антенны менее 257м при помощи ЧРЦ реализовать радиовещательную антенну невозможно. Поэтому нами предлагается для этих случаев использовать антенну мачту как конструкцию, которая поддерживает полотна антенн, близких к логопериодическим антеннам. Прототипом для разрабатываемой антенны служит антенна типа ШАРРТ -257,5 (антенна с регулируемым распределением тока).

Использование диапазона ДВ для радиовещания экономичнее примерно в 5 раз из-за малого затухания волны, чем СВ диапазон, и соответствует УКВ диапазону. Следует так же упомянуть, что зона покрытия одного передатчика свыше 400 км в радиусе, и при использовании всего 30 передатчиков вещание может вестись по всей территории России. Поэтому поиск решений для использования ДВ вещания стандарта *DRM* является более чем актуальным.

К основным техническим показателям разрабатываемой антенны квазилогопериодического типа относятся: полоса частот, КСВ, добротность, волновое сопротивление, сопротивление излучения вибратора и ДН в горизонтальной плоскости. К конструкторским показателям устройства относятся: высота основной мачты (218м), высота мачт крепления леера или оттяжек (50м), длина леера (120м) и длина оттяжек (74м).

Проектируемая антенна состоит из 3 полотен, антенн, близких к логопериодическим. Понятно, что часть площади полотна антенны над изоляторами не используется, поэтому для увеличения длины всех активных вибраторов, что приведет к увеличению сопротивления излучения, уменьшения добротности антенны, и расширению рабочей полосы частот, предлагается использовать площадь полотна вплоть до леера. Таким образом фактически будет использоваться не логопериодическая антенна, а квазилогопериодическая антенна, предложенная в середине прошлого века. [1]

Если рабочий диапазон частот является очень большим, то антенна должна быть только логопериодической, если широкий диапазон частот не требуется (в нашем случае для *DRM*), то вполне возможно отклонение от принципа электродинамического подобия, что в нашем случае приведет к уменьшению необходимого числа вибраторов при заданной полосе частот. При проектировании, мачта модернизируемой антенны используются как опорная для трех квазилогопериодических полотен. Высота мачты в нашем случае равна 218 метров. Легко рассчитать, что при длине плеч вибраторов $l \leq 218$ метров все вибраторы будут нерезонансными. Следовательно, антенна будет неработоспособной. Для достижения резонанса каждый вибратор снабжается дополнительным конденсатором, приводящим систему в резонанс на заданной частоте в рабочем диапазоне частот fв=177кГц, fн=143кГц, f0=160кГц.

В модернизируемой антенне расстояние от центральной мачты до мачты крепления 120 метров. Если длина полотен менее 76 метров, то площадь занимаемой антенны совершенно не меняется. Однако, габариты площади, предоставленной для размещения антенны, позволяет увеличить длины квизилогопериодической антенны до 120 метров, что облегчает реализацию заданной полосы частот и, как показывают расчеты, приводит к уменьшению необходимого числа вибраторов. Остается открытым вопрос реализации антенной системы описанного типа, при заданных ее габаритах.

Для увеличения значения КСВ в фидере, а так же для уменьшения пределов входного сопротивления вибратора в рабочем диапазоне, используют симметричные вибраторы, которые обладают пониженным волновым сопротивлением. Кроме того, снижение волнового сопротивления повышает его электрическую прочность. В данной антенне используется вибраторы С.И. Наденко. Условно данный вибратор обозначается ВГД. Его волновое сопротивление может быть определено по формуле $W_{wav} = 120\left(ln\left(\frac{h}{a_{ekviv}}\right) - 2{,}25\right)$, где a_{ekviv} – эквивалентный радиус вибратора, т. е. радиус вибратора, выполненного из сплошной трубы и имеющего такое же волновое сопротивление, как и данный вибратор.

Подставим наши значения в формулу:

R=0,5 м – радиус цилиндрической поверхности вибратора,

n=6 – число проводов вибратора,
r=0,003 м – радиус одного вибратора,

$$a_{ekviv} = R\sqrt[n]{\frac{nr}{R}} = 0{,}287 \text{ м} \quad (1)$$

И получим, что эквивалентный радиус нашего цилиндра равен 0.287м, следовательно, диаметр одного вибратора около полуметра. Из этого следует, что вибраторы необходимо располагать на расстоянии полтора метра. Расстояние от основной мачты до мачт крепления леера H=120м. Следовательно, количество вибраторов, необходимое для обеспечения достаточной полосы пропускания, которое можно разместить, будет равно:

$$\frac{H}{1{,}5} = 80 \text{ шт.} \quad (2)$$

Однако, количество вибраторов, обеспечивающее нужную полосу пропускания, может быть меньше 80 штук. Поэтому, далее в расчетах будем использовать количество вибраторов равное 78. При этом леер натянут по формуле цепной линии. Цепной линией называется плоская кривая, форма которой соответствует однородной гибкой нерастяжимой тяжелой нити, закрепленной в обоих концах и провисающей под действием силы тяжести.

Требования к КСВ.

Антенны диапазонов ДВ и СВ вместе с элементами настройки и согласования обычно образуют систему, аналогичную резонансному контуру. Цифровой стандарт *DRM* требует КСВ<1,05 [2], т.е. хорошее согласование с нагрузкой во всей полосе частот передаваемого сигнала. На данный момент традиционные методы не могут обеспечить требуемые значения для КСВ в антенных системах ДВ диапазона и, частично, в СВ диапазоне, поэтому антенные системы данных диапазонов не могут быть согласованы до нужных значений. Для устранения этой проблемы предложено использовать частотно-расширительные цепи (ЧРЦ). Эти цепи основаны на классе цепей с постоянным резистивным сопротивлением, они позволяют работать на узкополосных антеннах в диапазонах ДВ и СВ в режиме *DRM.*

Расчетные соотношения для предела Чу-Харрингтона.

$$\frac{2\pi a}{\lambda} = b\sqrt[3]{\frac{1}{2\pi}\frac{\chi^3-1}{\chi^3}\left|\ln\frac{1}{\rho}\right|}, \quad (3)$$

где $\chi = \frac{f_в}{f_н}$, fв=177кГц, fн=143кГц, f0=160кГц, λн=2097м,

КСВ=1,05; $\rho = \frac{КВС-1}{КВС+1} = 0{,}0243$; $|\ln\rho| = 3{,}714$; b=1 – коэфф. пропорциональности

$\frac{a}{\lambda_н} = \frac{0{,}6537}{2\pi}$, a- высота антенны в длинах волн.

$hmin = a\lambda_н$, высота антенны в метрах.

$hmin = 218м.$

Так же следует, что если бы у логопериодической антенны элементы решетки не были бы связаны между собой, то антенну можно было бы сделать сколь угодно маленькой со сколь угодно широкой полосой частот. Так как у нас элементы связаны между собой, то последовательно с удлиняющим дросселем можно включить частотно-зависимый изолятор (ЧЗИ), в качестве которого можно использовать длинную линию с плавающей точкой отсечки с большим входным сопротивлением. Эквивалентной схемой такой длинной линии являются ленточные двухполюсники.

Серьезным недостатком такой антенны является необходимость расчета индуктивности дросселя, обеспечивающего резонанс на необходимой частоте ля каждого вибратора антенного полотна. Если расчет одного вибратора требует времени t=1мс, то на полный расчет потребуется около трех лет, что, естественно, совершенно неприемлемо. Задачу можно резко упростить, если заменить в данном случае квазилогопериодическую антенну логопериодической антенной. В этом случае достаточно рассчитать индуктивность удлиняющего дросселя только один раз. Кроме того, величину индуктивности этого дросселя приближенно можно рассчитать аналитически. Легко понять, что при использовании леера для подвеса вибраторов длина логопериодической антенны будет неприемлемо малой. Устранить этот недостаток можно, используя для подвески антенного полотна выносную стрелу (рис 1)

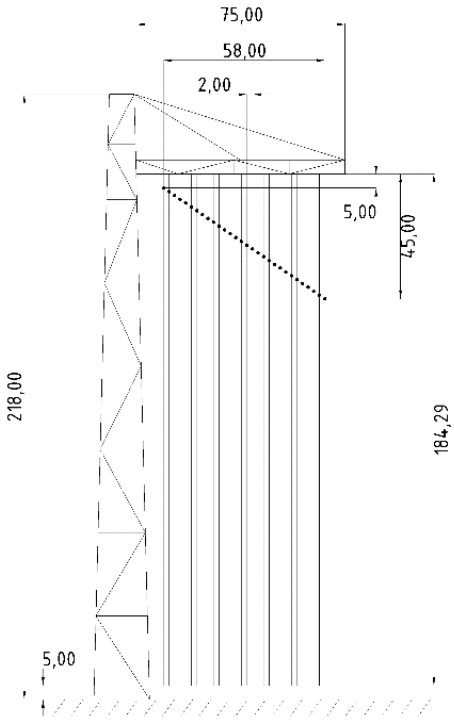


Рисунок 1. Логопериодическая антенна с выносной стрелой.

Вывод: Проиллюстрирована возможность преодоления предела Чу-Харрингтона на основе принципа использования распределенного согласования. Показано, что использование логопериодических антенн уменьшенных размеров и частотно-зависимых изоляторов позволяет получить требуемую полосу частот в 34 кГц при использовании типовых мачтовых устройств, существующих в данное время.

Литература:

1. Варламов О.В., Горегляд В.Д. Расширение полосы согласования передающих вещательных антенных систем диапазона ДВ для работы в режиме DRM. – T-Comm, №1, 2013.

2. Варламов О.В. Разработка алгоритма и программных средств проектирования антенно-согласующих цепей цифровых радиовещательных передатчиков стандарта DRM. – T-Comm, №2, 2013.

3. Пиминов Ю.В., Белянский Б.В. Длинные линии с плавающей точкой отсечки. //Тезисы доклада на НТК МТУСИ 2004.

4. Белянский В.Б. Возможно ли преодолеть предел Чу-Харрингтона? – T-Comm, №8, 2013.

Н.С. Резников

КОНЦЕПЦИЯ ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА И БЕЗОПАСНОСТИ ПОТЕНЦИАЛЬНО-ОПАСНЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ SKYLINK

Московский технический университет связи и информатики
Северо-Кавказский филиал, г. Ростов-на-Дону, Россия

Ключевые слова: системы мониторинга, безопасность, SkyLINK

Описана концепция построения комплексной многоступенчатой системы мониторинга и безопасности потенциально опасных объектов муниципального и регионального уровней с

использованием технологии SkyLINK. Предлагаемые концептуальные решения позволят создать систему мониторинга нового поколения, соответствующую европейским стандартам и обеспечивающую мониторинг радиационных, химических, метеорологических, и др. параметров окружающей среды, в соответствии с санитарно-гигиеническими экологическими радиационными нормативами РФ……

N.S. Reznikov

CREATION CONCEPT OF SYSTEM OF MONITORING AND SAFETY OF POTENTIALLY DANGEROUS OBJECTS WITH SKYLINK TECHNOLOGY USE

Moscow technical university of communication and informatics
North Caucasian branch, Rostov-on-Don, Russia

Keywords: monitoring, security, SkyLINK

The article describes the concept of creation of complex multistage system of monitoring and safety of potentially dangerous objects of municipal and regional levels with SkyLINK technology use. Proposed conceptual solutions will allow to create a monitoring system of the new generation, conforming to the European standards and providing monitoring of radiation, chemical, meteorological and other parameters of environment, according to sanitary and hygienic ecological radiation standards of the Russian Federation…

В целях обеспечения безопасной эксплуатации опасных производственных объектов на территории Российской Федерации Правительство Российской Федерации постановило принять предложение Федерального горного и промышленного надзора России, согласованное с Министерством промышленности, науки и технологий Российской Федерации, Министерством экономического развития и торговли Российской Федерации, Министерством юстиции Российской Федерации и другими заинтересованными федеральными органами исполнительной власти, об организации работы по развитию и внедрению системы контроля, позволяющего осуществлять экспертизу промышленной безопасности и проводить техническое диагностирование без нарушения пригодности к дальнейшему применению и эксплуатации проверяемых технических устройств, оборудования и сооружений (неразрушающий контроль), для принятия решения о продлении срока их безопасной эксплуатации на опасных производственных объектах (определение остаточного ресурса) на территории Российской Федерации.

В целях реализации Постановления Правительства РФ от 28.03.2001г. №241 «О мерах по обеспечению промышленной безопасности опасных производственных объектов на территории Российской Федерации» (с изменениями на 4 февраля 2011 года) данной статьей предлагаются концептуальные решения, позволяющие создать систему мониторинга нового поколения соответствующую европейским стандартам и обеспечивающую мониторинг радиационных, химических, метеорологических, и других параметров окружающей среды, в соответствии с санитарно-гигиеническими, экологическими, радиационными нормативами РФ.

Реализация представляемой системы мониторинга и безопасности на базе предлагаемых далее концептуальных решений с использованием системы SkyLINK, предполагается на территории Ростовской области и позволяет объединить на единой технической платформе с минимальными затратами и в короткое время обеспечить создание единой системы мониторинга и безопасности объекта, города, региона, а в последующим возможно и страны.

Основу построения системы мониторинга будут составлять размещенные в регионе - на территории потенциально-опасных предприятий, в их санитарно-защитных зонах и в зонах наблюдения, а также в любых представляющих интерес местах - измерители и датчики, контролирующие вредные выбросы, а также метеорологические и сейсмические станции, датчики уровня вод и прочее.

Система мониторинга и безопасности региона позволит организовать в реальном масштабе времени мониторинг всех потенциально-опасных объектов региона.

Для передачи информации, по радиоканалу малой мощности на большие расстояния, до 100 км, без затрат на кабели и их прокладку используются приемные антенны на телевышках

передающих центров, которые позволяют обеспечить комплексный мониторинг (радиационный, химический, метео, пожарный, контроль параметров физической защиты объектов на больших и труднодоступных территориях, мониторинг потенциально опасных объектов – зданий и сооружений, плотин, мостов, ж/д, аэропорты и прочее) на базе единой технической платформы SkyLINK.

Предлагаемые решения построения систем мониторинга и безопасности региона на базе технологии SkyLINK охватывает следующие аспекты комплексного мониторинга:

1. **Объектовый уровень** – автоматизированные измерительные системы производственно-экологического мониторинга (АИСПЭМ) потенциально-опасных химических и радиационных объектов и их сопряжение с ЕДДС МО и ЦУКС регионального уровня.
2. **Региональный уровень** – системы мониторинга опасных объектов - СМОО (удаленные пожароопасные объекты, водомерные посты на гидротехнических сооружениях и естественных водоемах, посты сейсмического мониторинга, независимый (в интересах структур МЧС) мониторинг опасных химических и радиационных предприятий, расположенных в радиусе 100 км от региональных ЕДДС.
3. **Мобильный уровень** – система мобильного мониторинга (СММ) параметров окружающей среды для дооснащения мобильных комплексов химической и радиационной разведки МЧС (зона мониторинга – 5км от мобильного комплекса, автоматическая передача информации о параметрах окружающей среды в зоне проведения работ по ликвидации ЧС в радиусе до 100км по цепочке ДДС областного центра – ЕДДС.

Объектовый уровень.

Объектовая автоматизированная измерительная система производственно-экологического мониторинга (АИСПЭМ) предназначена для непрерывного контроля превышения ПДК вредных химических и радиоактивных веществ на рабочих местах, на территории промышленной площадки потенциально-опасного предприятия, в санитарно-защитной зоне, в зоне наблюдения и обеспечивает:

- измерение параметров химической и радиационной обстановки с чувствительностью, позволяющей регистрировать ее изменение на уровне ПДК, МДА и радиационного фона;
- оперативное обнаружение аварийных ситуаций;
- оценку мощности и динамики газо-аэрозольного выброса в точках контроля и его распространение;
- измерение и регистрацию метеорологических параметров в местах наблюдения;
- сбор, обработку и отображение данных о санитарно-гигиенической, радиационной и экологической обстановке на АРМах дежурно-диспетчерской службы (ДДС) объекта;
- отображение прогнозируемой и фактической санитарно-гигиенической и радиационной обстановки на электронных картах предприятия, ЗН и СЗЗ на планах местности с доступом к этим данным посредством интернет-технологий через локальную сеть предприятия, Интернет и мобильный коммуникатор;
- передача данных в ЕДДС муниципального образования и далее в государственные органы для выполнения функции оповещения и информирования населения, в органы местного самоуправления.

Данные посты контроля имеют автономное электропитание и комплект измерительных средств, позволяющий измерять параметры химической и радиационной обстановки (с учетом опасных компонентов технологических процессов конкретного объекта) в условиях его нормального функционирования и аварийных (чрезвычайных) ситуациях. Наличие автономных постов мониторинга, совместно с информацией от объектовой системы АИСПЭМ или при ее отсутствии позволяет:

- повысить информативность сообщения об аварии, поступающем из ДДС;
- исключить «человеческий фактор» замалчивания факта возникновения аварийной ситуации или тенденций, предшествующих ее возникновению;

- автоматически осуществлять оперативное обнаружение и регистрацию ЧС на достаточном или избыточном уровне реагирования;
- осуществлять передачу минимально - достаточного объема информации о ЧС на объекте в комплексную многоступенчатую систему мониторинга по цепочке:
- осуществлять (через ЕДДС) оповещение соответствующих аварийных служб в соответствии с алгоритмами реагирования.

Информация от автономных постов мониторинга может считываться также расчетами мобильных комплексов МЧС с использованием приемных устройств ShortLINK–приемник из состава СММ.

В случае отсутствия объектовых систем мониторинга данные посты включаются в региональную систему мониторинга окружающей среды в структуре МЧС.

Региональный уровень.

Система мониторинга опасных объектов (СМОО) внедряется на региональном уровне, является составной частью комплексной многоступенчатой системы мониторинга и безопасности и предназначена для:

- сбора информации от приемно-контрольных приборов систем пожарной и охранной сигнализации объектов, не имеющих прямого канала связи с ДДС (школы, больницы, госучреждения, места массового скопления людей в радиусе до 100 км от областного центра);
- сбора информации от водомерных постов потенциально-опасных гидротехнических сооружений и естественных водоемов;
- сбора информации от сейсмических датчиков (постов контроля сейсмической активности природного и техногенного происхождения);
- сбор информации от пунктов контроля транспортных средств, обеспечивающих контроля перемещения радиоактивных веществ и ядерных (делящихся) материалов;
- сбор информации местоположения и состояния химически опасных, радиоактивных веществ и ядерных (делящихся) материалов в процессе транспортировки;
- приема информации от СММ мобильных комплексов МЧС из зон защитных мероприятий и зон оперативных мероприятий по ликвидации ЧС;
- приема информации от автономных постов объектовых систем мониторинга в радиусе до 100 км;
- предоставления полученной информации персоналу ДДС в удобном для оперативного реагирования виде:
- формирование информации для системы оповещения ДДС в соответствии с разработанными сценариями.
- обеспечение доступа к информации от ЕДДС, ЦУКС областного центра и ЦУКС ПУРЦ по специальным каналам связи и Интернет;
- защита информации от несанкционированного доступа;

В рамках развертывания системы мониторинга и безопасности опасных объектов региона ответственные лица и руководители предприятий и подразделений МЧС обеспечиваются мобильными коммуникаторами, на которых отображается текущая ситуация на контролируемых объектах в соответствие с зоной ответственности. Степень детализации представляемой информации: регион, область, опасный объект, характеристика ситуации на объекте.

Система мобильного мониторинга.

Система мобильного мониторинга (СММ) устанавливается на мобильный комплекс МЧС и предназначена для организации временного мониторинга зоны оперативных мероприятий по ликвидации ЧС (в радиусе до 5 км от места расположения мобильного комплекса), разведки и оперативного определения степени опасности очагов радиоактивного, химического заражения путем считывания информации от автономных датчиков контроля химических и радиационных параметров опасного производственного объекта, защиты населения и мобильной группы персонала МЧС, находящегося в зоне заражения, автоматической передачи параметров мониторинга в ДДС (в радиусе до 100 км).

В зависимости от характера аварии (радиационная, химическая или комбинированная) и метеообстановки (направления ветра) вокруг очага, устанавливаются соответствующие датчики контроля, информация с которых по каналу ShortLINK передается на мобильный комплекс и отображается на экране автоматизированного рабочего места (АРМ) начальника мобильной

группы, расположенного в салоне автомобиля. Расстояние от автомобиля до датчиков не должно превышать 5 км.

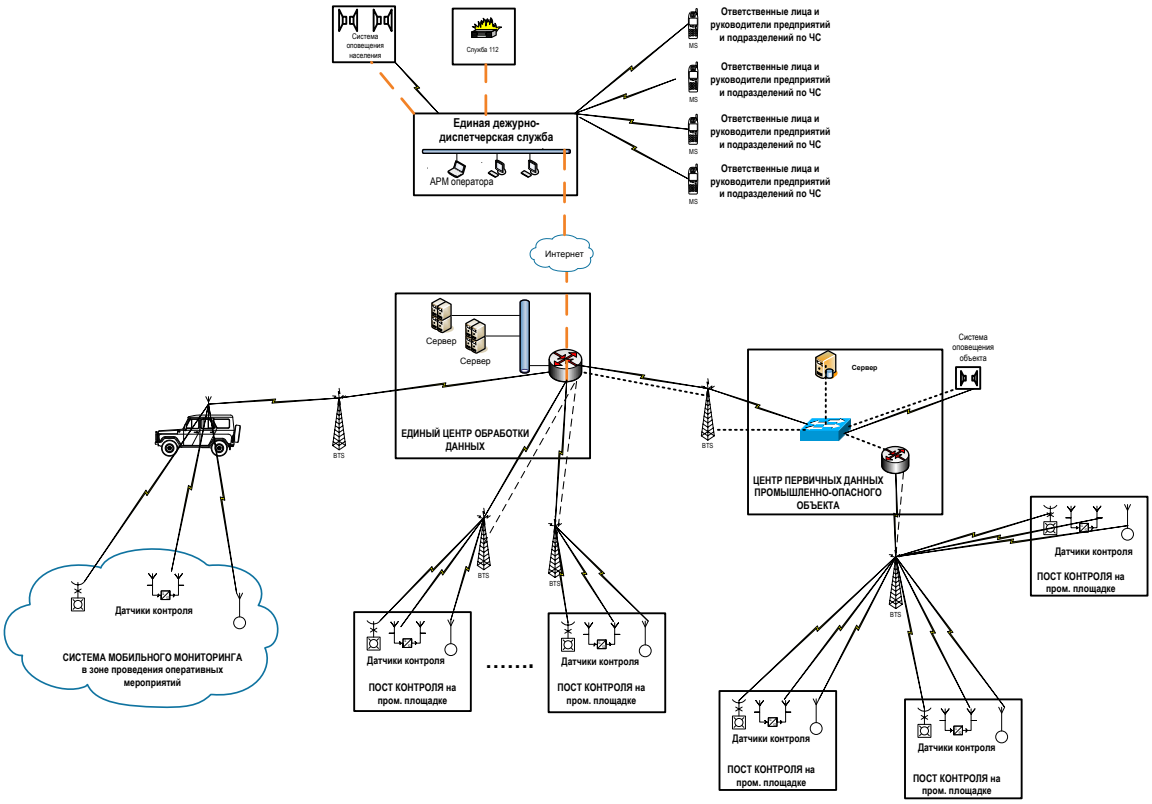


Рисунок 1. Структурная схема системы мониторинга и безопасности потенциально-опасных объектов с использованием технологии SkyLINK.

<u>Сеть SkyLINK включает в себя следующие компоненты:</u>

- Передатчик SkyLINK, который подключается к сенсорному датчику или прибору;
- Внешние компоненты приемника: антенна, опора, понижающий преобразователь;
- Внутренние компоненты приемника: заземление, стойка приемного устройства (включает аналоговую секцию, цифровую секцию и СБЭ (система бесперебойного электроснабжения).

Центр первичных данных (ЦПД) это компьютер-сервер высокой надежности с базой данных MS SQL и программным обеспечением по управлению данными DataEXPERT.

На ЦДП установлены устройства звукового и визуального оповещения о сигналах тревоги, а также система удаленного оповещения (при помощи SMS, FAX).

Данные поступающие от датчиков контроля до единой диспетчерской службы обычно имеют несколько категорий и к каждой из них предъявляются требования по времени доведения и достоверности информации. Этот вид трафика может обладать значительными пульсациями.

Пропускная способность канала связи $V_{канала}$ от датчиков контроля поста контроля на промышленной площади до BTS определяется следующим образом:

$V_{канала}$=q* к*L = 20*2*4=2,6 Кбит/сек, где

q – кол-во датчиков на пром. площадке;

к – кол-во сообщений в единицу времени;

L – объем передаваемой информации, байт.

Из приведенного расчета следует, что возможно использовать радиоканал сотовой подвижной радиотелефонной связи стандарта IMT-MC-450 или GSM скоростью 9,6 Кбит/сек.

Н.С. Резников

ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА СТРОИТЕЛЬСТВА БАЗОВОЙ СТАНЦИИ СОТОВОЙ СЕТИ

Московский технический университет связи и информатики
Северо-Кавказский филиал, г. Ростов-на-Дону, Россия

Ключевые слова: БС, сотовая связь, ТЭО, инвестиционный проект.

Описана процедура изучения экономической выгодности, анализ и расчет экономических показателей создаваемого инвестиционного проекта. Целью проекта является строительство базовой станции сотовой связи стандарта IMT-MC-450. Предлагаемые концептуальные решения позволят дать характеристику выбора территориального и географического положения действующего и предполагаемого строительства базовой станции, а так же описывается техническая и экономическая сторона обоснования строительства базовой станции сотовой связи. При этом финансовая часть ТЭО содержит информацию об источниках финансирования и сроки погашения задолженности, сроки окупаемости и необходимость строительства…

N.S. Reznikov

FEASIBILITY STUDY OF CONSTRUCTION PROJECT OF CELLULAR NETWORK BASE STATION

Moscow technical university of communication and informatics
North Caucasian branch, Rostov-on-Don, Russia

Keywords: BS, cellular communications, feasibility studies, investment project.

The article describes the procedure of economic advantage studying, the analysis and calculation of economic indicators of the investment project under construction. The purpose of the project is construction of a cellular communication base station of the IMT-MC-450 standard. Proposed conceptual solutions allow to characterize the choice of a territorial and geographical position of construction, actual and planned, of a base station. The technical and economic aspects of justification of construction of a cellular communication base station are also described. As well the financial part of the feasibility report contains information on sources of financing and debt maturity dates, payback periods and need of construction….

В современных бизнес-процессах технико-экономическое обоснование прочно вошли в лексикон терминов предпринимателей и экономистов. В материале делается попытка осветить вопросы основные аспекты технико-экономического обоснования строительства базовой станции сотовой связи.

Необходимо отметить, что если порядок составления и структуры бизнес-плана четко прописаны в организации, то при составлении ТЭО можно найти несколько различных вариантов написания, которые различаются в зависимости от рассматриваемых проблем.

При проведении исследования в области маркетинга, задачей которого являлось выявление предпочтений потребителей на рынке услуг связи, была выявлена, в том числе и потребность в написании технико-экономического обоснования строительства базовых станций сотовой связи.

При составлении ТЭО допускается следящая последовательность тематических частей:

- исходные данные, информация о секторе рынка;
- существующие возможности действующего бизнеса предприятия;
- общая информация о строительстве базовой станции;
- капитальные затраты предполагаемые для достижения поставленной цели;
- эксплуатационные затраты при реализации проекта;
- производственный план;
- финансовая политика и финансовая составляющая проекта.

В общем, в ТЭО приводится описание отрасли, в которой работает предприятие, и дается обоснование выбора территориального и географического положения действующих и

планируемых базовых станций. Здесь необходимым является описание и обоснование цен. При этом финансовая часть ТЭО содержит информацию об источниках финансирования и сроки погашения задолженности, сроки окупаемости объекта.

Немаловажной частью ТЭО является техническая сторона вопроса описываемая в ТЭО. Предлагаемый вариант раскрытия технической составляющей технико-экономического обоснования строительства базовой станции сети связи стандарта IMT-MC-450 (CDMA-450) приведен ниже:

1.Технические характеристики проекта

1.1. Технические данные объекта

Таблица 1. Технические данные объекта:

Номер БС	**Адрес размещения БС (размещение аппаратной)**	**Координаты БС**		**подвеса антенны БС от поверхности**	**главного лепестка излучения**	**Тип антенны**	**выходе передатчика**
		град., мин., сек.	**град., мин., сек.**				
БС-214м	г. Ростов-на-Дону, ул. Войкова, 136. (контейнер на земле, АФУ на башне Билайн)	47°11'42.87"С	39°39'28.25"В	26	40/-2 155/-2 275/-2	К741 516	20 Вт

1.2. Общий вид БС-214м «Ростов-Войкова»:

Рисунок 1. Общий вид БС

1.3. Схема размещения АФУ БС:

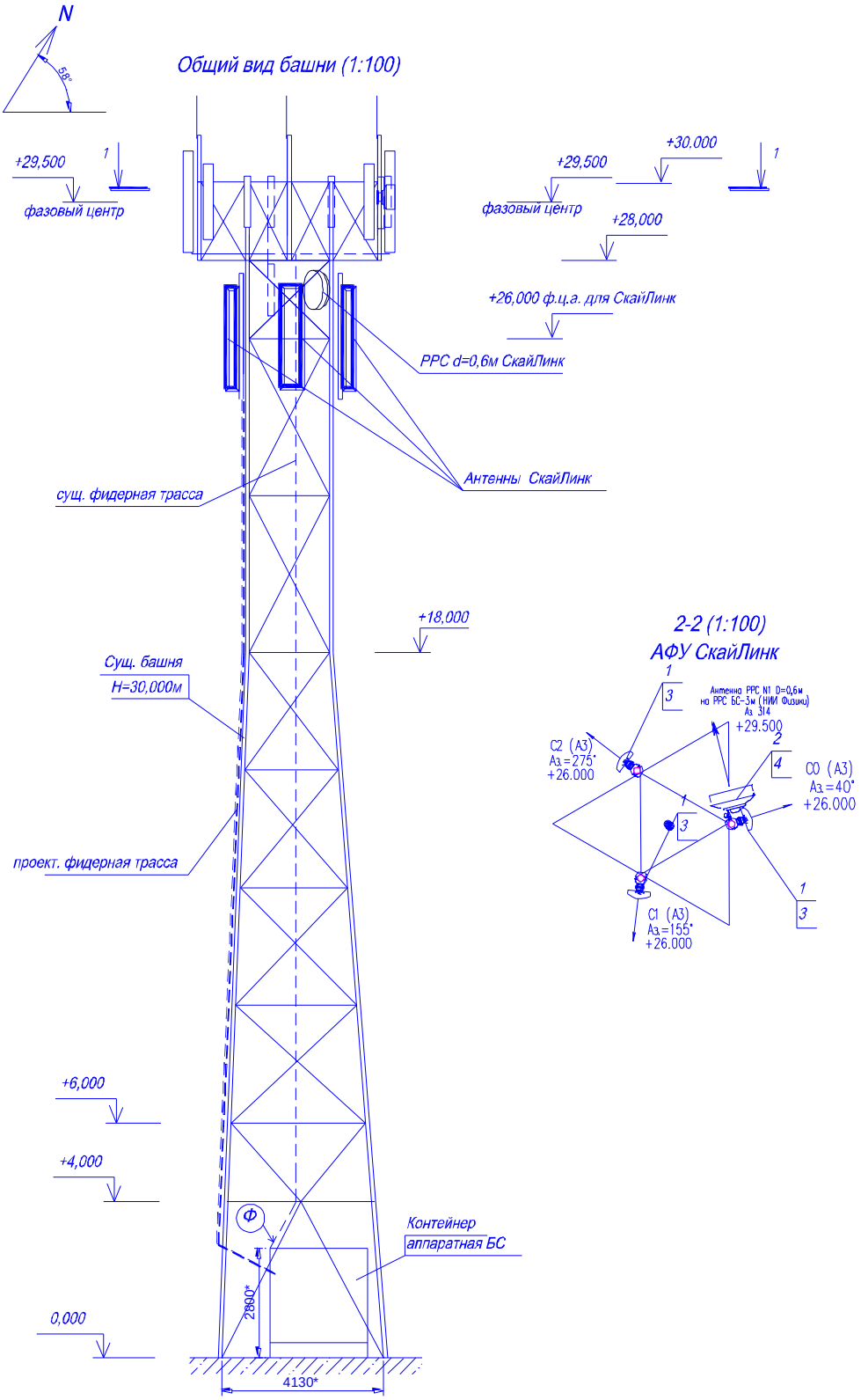


Рисунок 2. Схема размещения АФУ БС

1.4. Обоснование установки БС-214м:

- Разгрузка БС-205м; БС-3м; БС-23м.
- Покрытие «темной» зоны по ул. Портовая, Всесоюзная, Войкова, Циалковского.
- Улучшение качества связи в ниже ул. Портовая и исключение возникающих претензий на качество связи от абонентов.

Таблица 2. Нагрузка по ПД окружающих БС в месте предполагаемого размещения БС за январь 2011г.:

БС205м	
объем трафика за месяц, тыс. МБ	528,39
средний за ЧНН процент загруженных слотов, %	97,59%
максимальное количество активных абонентов, чел.	125
БС23м	
объем трафика за месяц, тыс. МБ	410,27
средний за ЧНН процент загруженных слотов, %	95,44%
максимальное количество активных абонентов, чел.	105
БС3м	
объем трафика за месяц, тыс. МБ	437, 61
средний за ЧНН процент загруженных слотов, %	96,67%
максимальное количество активных абонентов, чел.	115

1.5. Результаты расчетного радиопокрытия в районе предполагаемого расположения БС, выполняемое на программном комплексе ONEPLAN RPLS (ONEGA RPLS) планирования и оптимизации сетей подвижной радиосвязи:

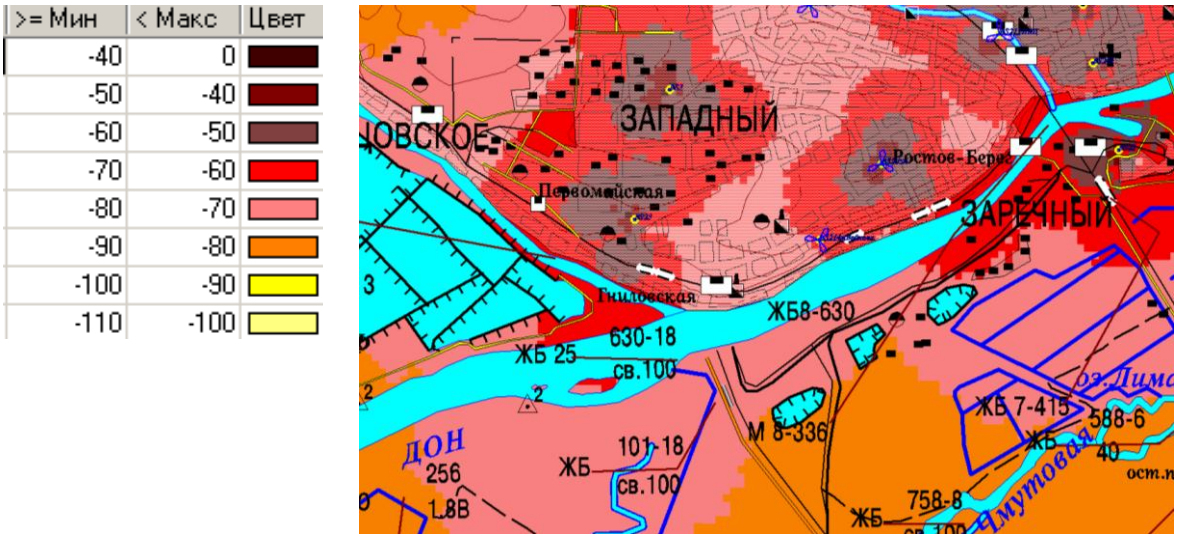


Рисунок 3. Существующее расчетное радиопокрытие в г. Ростове-на-Дону в месте размещения БС-214м.

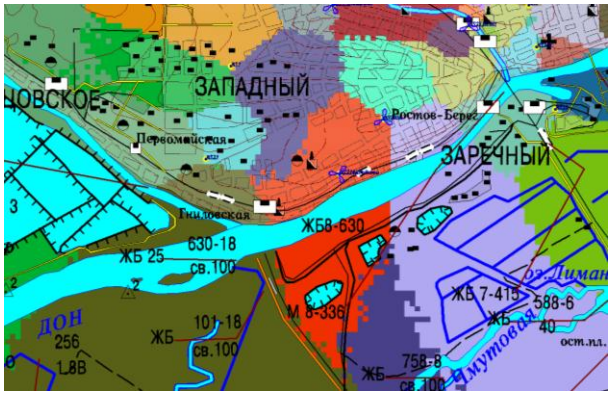


Рисунок 4. Существующая расчетная карта границ секторов

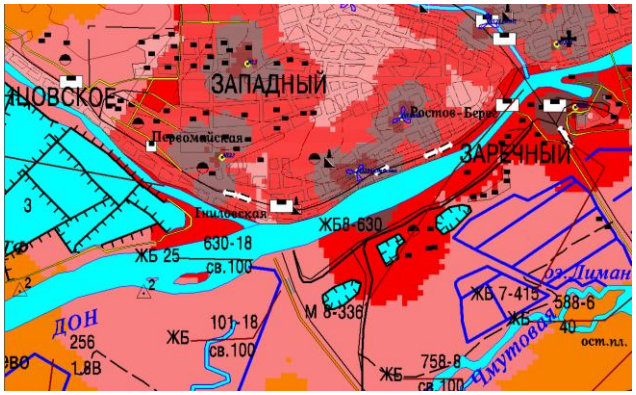


Рисунок 5. Планируемое расчетное радиопокрытие при включенной БС-214м

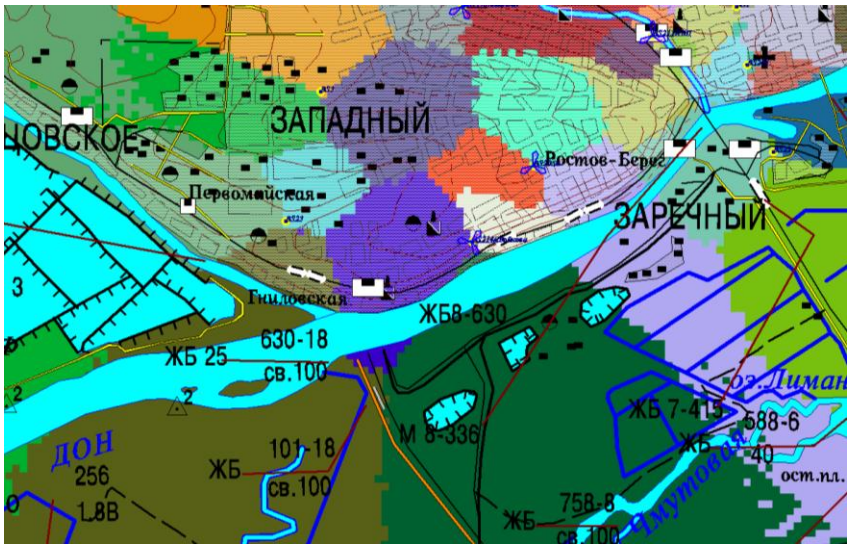


Рисунок 6. Планируемая расчетная карта границ секторов при включении БС-214м

1.6. Технические особенности, касающиеся строительства объекта:

В предполагаемом месте установки новой БС монтаж АФУ будет производится на существующей АМС, что позволит минимизировать затраты на строительство БС.

Операционные затраты могут быть снижены путем строительства собственной транспортной сети, при этом мы экономим на аренде каналов в среднем 15 000 руб./мес., что было учтено при расчете бюджета проекта.

Такая структура ТЭО может и не являться единственно правильной и может изменяться в зависимости от конкретного проекта. Так же, она может быть расширена для больших и сложных бизнес проектов, например для разработки системного проекта строительства сети сотовой подвижной радиотелефонной связи.

Р.И. Русанов, В.Д. Кутакова,
Л.Н. Харченко, Н.В. Руденко, В.В. Евстафьев

ИСПОЛЬЗОВАНИЕ СОЛНЕЧНОЙ ЭНЕРГИИ ДЛЯ РЕЗЕРВНОГО ЭЛЕКТРОСНАБЖЕНИЯ БАЗОВЫХ СТАНЦИЙ СОТОВОЙ СВЯЗИ

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: альтернативная энергетика, электроснабжение базовых станций сотовой связи, солнечные батареи, фотоэлектрические элементы.

Рассмотрены возможности применения альтернативной энергетики для резервного электроснабжения базовых станций сотовой связи, строящихся в труднодоступных районах и не имеющих надежного централизованного электроснабжения. Рассмотрен пример использования для указанных целей компанией «Мегафон» солнечных батарей. Выполнен анализа опыта проектирования и эксплуатации систем электропитания базовых станций на основе солнечных батарей. Сформулированы основные принципы эксплуатации таких систем: принцип замещения, а также принцип использования программных и аппаратных методов оптимизации энергопотребления.

R.I. Rusanov, V.D. Kutakova,
L.N. Kharchenko, N.V. Rudenko, V.V. Evstafyev

USE OF SOLAR ENERGY FOR THE RESERVE POWER SUPPLY OF BASE STATIONS OF CELLULAR COMMUNICATION

Don State Technical University, Rostov-on-Don, Russia

Keywords: alternative power engineering, power supply of base stations of cellular communication, solar batteries, photo-electric elements.

Possibilities of application of alternative power engineering for reserve power supply of the base stations of cellular communication which are under construction in the remote areas which don't have the reliable centralized power supply are considered. Use example for the specified purposes is reviewed by the "Megafon" company of solar batteries. It is executed the analysis of experience of design and operation of power supply systems of base stations on the basis of solar batteries. The basic principles of operation of such systems are formulated: principle of replacement, and also principle of use of program and hardware methods of optimization of energy consumption.

Постановка задачи. Использование альтернативных источников энергии для электропитания базовых станций систем сотовой связи в России имеет большие перспективы. Это обусловлено наличием значительных ресурсов энергии ветра и солнца, а также большого количества труднодоступных регионов, где облуживание и питание этих станций представляет серьезную проблему. Введение в эксплуатацию подобных базовых станций обеспечит более обширное покрытие.

Анализ технических решений. Использовать альтернативную электроэнергетику и получить выгоду, возможно, но только при правильной оценке возможностей региона. Требуется проведение масштабных исследований, которые позволяют определить, какое именно оборудование будет оптимально для использования именно в этом месте. Эти исследования включают анализ рельефа местности, параметров ветров, солнечной активности [1, с.43].

Одним из примеров использования альтернативной энергетики является базовая станция компании «Мегафон» расположенная в 30 км от Махачкалы на горе Таш-Баш на высоте более 600 м над уровнем моря, введенная в эксплуатацию в 2006 году и оборудованная солнечными батареями в 2014. Необходимость использования солнечных батарей возникла из-за нестабильности централизованного электроснабжения, что пагубно влияло на состояние аккумуляторов [2; 3, с.114]. Разработанная система электропитания состоит из панелей с фотоэлектрическими элементами, контроллера солнечной батареи, гибридной электропитающей установки, аккумуляторных батарей.

На объекте функционирует 42 солнечные панели, каждая с 72 фотоэлементами. Общая площадь панелей составляет 53 кв. м, они способны генерировать до 5 кВт. Система работает по принципу замещения, т.е. днем, когда достаточно света оборудование питается от солнечных батарей, ночью или при отсутствии солнечного света - от стационарной сети при ее отключении от аккумуляторов. Так достигается уменьшения циклов заряда-разряда батарей, что положительно сказывается на их сроке службы [2; 3, с.115].

Анализа опыта проектирования и эксплуатации систем электропитания базовых станций на основе солнечных батарей можно сделать **следующие выводы.**

1. При проектировании систем электропитания базовых станций на основе солнечных батарей целесообразно рассчитать площадь и угол наклона солнечных панелей в зависимости от географических координат объекта, мощности солнечного излучения с учётом круглогодичного использования, а также максимальной и средней требуемой мощности нагрузки.
2. Использование современных аккумуляторов позволяет свести к минимуму негативное воздействие нестабильности потока энергии от солнечных батарей в течение суток и года. Это позволяет обеспечить автономную работу базовой станции длительное время.
3. Для повышения эффективности использования солнечных батарей базовых станций систем сотовой связи целесообразно использовать программные и аппаратные методы оптимизации энергопотребления. Например, систему динамического энергосбережения, которая позволяет отключать неиспользуемые модули базовой станции, что позволяет добиться снижения энергопотребления на 10-20% в зависимости от условий эксплуатации [4].
4. Использование подобных систем экономически выгодно, так как обеспечивает энергосбережение и повышает надежность электроснабжения ответственных потребителей, однако использование таких установок не позволяет полностью отказаться от централизованного электроснабжения, а даёт возможность его резервирования.

Литература:

1. Rudenko N.V., Sukiyazov A.G., Shokova Yu.A. Adaptive control efficiency enhancement for hybrid solar-wind energy farms // 7th International Scientific Conference Science and Society. Held by SCIEURO in London. 25-26 November 2014. P.43-50.

2. Базовая станция на солнечных батареях [Электронный ресурс]: — URL: http://habrahabr.ru/company/megafon/blog/241365 (дата обращения 06.03.2015)

3. Руденко Н.В. [и др.]. Использование альтернативных источников энергии для резервного электроснабжения базовых станций систем сотовой связи. Наука и образование в жизни современного общества: сборник научных трудов по материалам Международной научно-практической конференции 30 декабря 2014 г.: в 12 частях. Часть 5. Тамбов: ООО«Консалтинговая компания Юком», 2015. С. 114-115

4. Энергосберегающие технологии на практике [Электронный ресурс]: — URL: http://habrahabr.ru/company/beeline/blog/154423/ (дата обращения 06.03.2015)

А.Б. Саркисов

МИНИМИЗАЦИЯ СХЕМНЫХ ЗАТРАТ НА РЕАЛИЗАЦИЮ МОДУЛЬНЫХ ОПЕРАЦИЙ В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

Северо-Кавказский Федеральный Университет, г. Ставрополь, Россия

Ключевые слова: полиномиальная система классов вычетов, спецпроцессоры цифровой обработки сигналов, модульные операции в ПСКВ, минимизация схемных затрат, поля Галуа $GF(p)$, математическая модель ортогональных преобразований сигналов.

Рассмотрена математическая модель ортогональных преобразований. В ходе статьи было выявлено, что главным недостатком являются схемные затраты на реализацию модульных операций. Чтобы минимизировать схемные затраты, применяется ПСКВ, которые в свою очередь помогают добиться минимизации схемных затрат на реализацию модульных операций в полиномиальной системе классов вычетов.

A.B. Sarkisov

MINIMIZATION OF CIRCUIT COSTS FOR IMPLEMENTING MODULAR OPERATIONS IN POLYNOMIAL SYSTEM OF RESIDUE CLASSES

North-Caucasian Federal University, Stavropol, Russia

Keywords: polynomial system of residue classes, special digital signal processors, modular operations polynomial system of residue classes, minimizing circuit costs, Galois field, mathematical model of orthogonal transformations signals.

A mathematical model of orthogonal transformations. In the article, it was found that the main disadvantage is the cost of circuit implementation of modular operations. To minimize circuit costs polynomial system of residue classes used, which in turn help to achieve minimize circuit costs of the modular operations in polynomial system of residue classes.

В настоящее время одним из популярных методов цифровой обработки сигналов, является математическая модель ортогональных преобразований сигналов, реализуемых в полях Галуа. С помощью данной модели возможно довольно легко повысить точность вычислений за счет использования всего лишь одного вычислительного тракта. Главным недостатком данной системы является повышенная точность результата, которая достигается с помощью использования поля $GF(p)$ с большим значением характеристики p. Результатом данного недостатка является увеличение схемных затрат на реализацию арифметической операции по модулю p.

Устранить данный недостаток позволит полиномиальная система классов вычетов(ПСКВ), которая позволяет повысить эффективность ортогональных преобразований в полях Галуа $GF(p^v)$. В работах [1,2], повышение эффективности ортогональных преобразований достигается за счет скорости обработки сигналов.

Применение ПСКВ позволяет не только повысить производительность спецпроцессора(СП) ЦОС, но и достичь минимизацию схемных затрат на реализацию модульных операций. Данная минимизация схемных затрат достигается за счет использования непозиционной системы в вычислительных системах ЦОС, которые позволяют снизить объем вычислений и использовать многомерную обработку сигналов.

Проведя вычисления в расширенном поле Галуа $GF(p^v)$, получается, что зная все элементы этого поля, можно определить минимальные многочлены, к которым относятся неприводимые полиномы над $GF(p)$, корнями которых являются некоторые выбранные элементы расширенного поля $GF(p^v)$. Согласно работе [3], минимальные многочлены $p_i(z)$

представляют собой нормированные многочлены наименьшей степени с коэффициентами из $GF(p)$, неприводимые над этим полем.

Можно эффективно находить многочлен элемента в конечном поле, если учитывать свойства корней минимальных многочленов, а так же используя условие, что $\beta,\beta^q,..,\beta^{q^{n-1}}$, при этом эти многочлены будут делителем двучлена. Равенство $z^{p^v-1}-1=\prod_{j=1}^{p^v-1}(z-\beta^j)$ $z^{p^v-1}+1=\prod_{j\in J}p_j(z)$ можно представить в виде .

Исходя из выше описанного можно сделать вывод, что существует возможность организации вычислений в расширенных поля Галуа $GF(p^v)$, которая базируется на изоморфизме китайской теоремы об остатках (КТО). Если в качестве оснований новой алгебраической системы выбрать минимальные многочлены $p_i(z)$ поля $GF(p^v)$, то любой полином $A(z)$, удовлетворяющий условию, $ordA(z)<ordP_{пол}$, где $P_{пол}=\prod_{i=1}^{n}p_i(z)=z^{p^v-1}-1$ можно представить в виде *n*-мерного вектора

$$A(z)=(\alpha_1(z),\ \alpha_2(z),\ \dots,\ \alpha_n(z)), \tag{1}$$

где $\alpha_i(z)=rest(\frac{A(z)}{p_i(z)}),\ i=1,2,...,n$.

Такое представление является однозначным, т.е. зная значение остатков ПСКВ, можно осуществить обратный переход к полиномиальному позиционному виду.

Пусть степень минимального многочлена $p_i(z),\ i=1,...,n$, равна $ordp_i-m_i$. Значения остатков операнда $A(z)$ представляется в виде полиномиальной записи:

$$\alpha_i(z)=\lambda^i_{m_i-1}z^{m_{i-1}}+\lambda^i_{m_i-2}z^{m_{i-2}}+...+\lambda^i_1z^1+\lambda_0, \tag{2}$$

где λ^i_j - элемент поля Галуа $GF(p)$.

Для второго операнда $B(z)$ получается:

$$\beta_i(z)=\gamma^i_{m_i-1}z^{m_{i-1}}+\gamma^i_{m_i-2}z^{m_{i-2}}+...+\gamma^i_1z^1+\gamma_0, \tag{3}$$

Требуется произвести операцию сложения для полиномов $A(z)=(\alpha_1(z),\ \alpha_2(z),\ \dots,\ \alpha_n(z))$ и $B(z)=(\beta_1(z),\ \beta_2(z),\ \dots,\ \beta_n(z))$, представленных в ПСКВ:

$$|A(z)+B(z)|^+_{p(z)}=\left(|\alpha_1(z)+\beta_1(z)|^+_{p_1(z)},...,|\alpha_n(z)+\beta_n(z)|^+_{p_n(z)}\right)=$$

$$\left(\lambda^1_0\oplus\gamma^1_0,\sum_i(\lambda^2_{m_2-i}\oplus\gamma^2_{m_2-i})z^i,\sum_j(\lambda^3_{m_2-j}\oplus\gamma^3_{m_2-j})z^j,...,\sum_w(\lambda^n_{m_2-w}\oplus\gamma^n_{m_2-w})z^w\right), \tag{4}$$

где $\oplus$ –операция суммирования по модулю p.

Произведем операцию вычитания, используя те же самые полиномы:

$$|A(z)-B(z)|^+_{p(z)}=\left(|\alpha_1(z)-\beta_1(z)|^+_{p_1(z)},...,|\alpha_n(z)-\beta_n(z)|^+_{p_n(z)}\right)=$$

$$\left(\lambda^1_0\circ\gamma^1_0,\sum_i(\lambda^2_{m_2-i}\circ\gamma^2_{m_2-i})z^i,\sum_j(\lambda^3_{m_2-j}\circ\gamma^3_{m_2-j})z^j,...,\sum_w(\lambda^n_{m_2-w}\circ\gamma^n_{m_2-w})z^w\right), \tag{5}$$

где $\circ$ – операция вычитания (обратная операция суммирования) по модулю p.

Полученные подмножества в выражениях (4) и (5) по основаниям $p_i(z),\ i=1,...,n$ ПСКВ образуют циклическую группу сложения, которая содержит конечное число элементов. Операции

сложения и вычитания производятся по модулю p, так как данные подмножества образуют аддитивную циклическую группу.

В связи с тем, что минимальные многочлены образуют кольцо, то третей модульной операцией должна быть операция мультипликативная. Так как дистрибутивность операции умножения операндов над кольцом на элементы этого кольца относительно операции сложения, получается:

$$\left|A(z)\bullet B(z)\right|_{p(z)}^{+}=\left(\left|\alpha_1(z)\bullet\beta_1(z)\right|_{p_1(z)}^{+},...,\left|\alpha_n(z)\bullet\beta_n(z)\right|_{p_n(z)}^{+}\right)=$$
$$\left(\lambda_0^1\gamma_0^1,\ \sum_{l=0}^{2m_2-2}q_{2m_2-2-l}^2 z^{2m_2-2-l},...,\ \sum_{j=0}^{2m_n-2}q_{2m_n-2-j}^n z^{2m_n-2-j}\right), \quad (6)$$

где $q_s^i=\sum_{k=0}^{s}\lambda_k^i\gamma_{s-k}^i$ - линейная свертка; $s=0,...,2m_i-2; i=0,...,n$.

Проведя вычисления, показанные выше, можно сделать вывод, что выполнение операции умножения в расширенном поле Галуа $GF(p^v)$ согласно

$$A(z)B(z)=\left(\sum_{k,l\geq 0}a_k b_l z^{k+1}\right)\bmod P_{пол}(z), \quad (7)$$

сводится к умножению соответствующих остатков по основаниям ПСКВ с последующим суммированием по модулю характеристики поля.

Согласно выражениям (4) – (6), мы имеем, что данные операции базируются на модулярных операциях свертки и суммирования по модулю характеристики поля. Исходя из полученных результатов, можно сделать вывод, что очевидна актуальность разработки алгоритмов реализации этих операций.

Согласно патенту [6], известен умножитель по модулю, который содержит умножитель, n сумматоров, n инверторов, (n-1) умножителей на константу, где n– размер умножителя, мультиплексор, два выхода для подачи двоичных кодов умножаемых чисел, вход для подачи двоичного кода модуля p, выход.

Значительные схемные (аппаратные) затраты, на реализацию данного устройства, является недостатком. Снижение аппаратных затрат на выполнение операции умножения по модулю, является основной задачей данной статьи.

При умножении по модулю $p(z)=z^4+z+1$, двух операндов $A(z)$ и $B(z)$, степени которых удовлетворяют условию:

$$\deg A(z)<\deg p(z)$$
$$begB(z)<\deg p(z) \quad (8)$$

Могут быть получены результаты, которые являются элементами поля Галуа $GF(2^4)$.

Рассмотрим ситуацию когда одновременно подаётся единичный сигнал на разряды 1 и z^3 второго операнда $B(z)$, при условии, что $A(z)=z$, то результат будет следующий:

$$A(z)B(z)\bmod z^4+z+1=(z(z^3+1))\bmod z^4+z+1=(z^4+z)\bmod z^4+z+1=1.$$

Результат, был получен с помощью сложения результатов двух произведений по модулю два:

$$z*1\bmod z^4+z+1+z*z^3\bmod z^4+z+1=z+z+1=1.$$

Значит, чтобы решить данную проблему необходимо использовать двухвходовой сумматор по модулю два, на входы которого подаются сигналы с 1 и z^3 второго операнда $B(z)$. Выход этого сумматора по модулю два подключается на второй вход элемента И, на первый вход которого поступает сигнал в разряде z первого операнда $A(z)$.

Согласно проведенных вычислений, для осуществления снижения аппаратных затрат, позволяющих выполнять операцию умножения по модулю, необходимо введение 16

двухвходовых элементов n, 6 двухвходовых сумматоров по модулю два, 4 четырехвходовых сумматоров по модулю два.

Используя модульные операции в ПСКВ, можно добиться минимизации схемных и временных затрат.

Литература:

1. Калмыков, И.А. Применение систолических ортогональных преобразований в полиномиальной системе классов вычетов для повышения эффективности цифровой обработки сигналов / И.А. Калмыков, А.В. Зиновьев, Д.Н. Резеньков, В.Р. Гахов // Инфокоммуникационные технологии. №3 – 2010;

2. Калмыков, И.А. Технология цифровой обработки сигналов с использованием модулярного полиномиального кода / И.А. Калмыков, А.Б. Саркисов, А.В. Макарова // Известия Южного федерального университета. Технические науки. №12 – 2013;

3. Саркисов, А.Б. Математические основы построения живучих спецпроцессоров цифровой обработки сигналов, функционирующих в полиномиальной системе классов вычетов /А.Б. Саркисов, Е.М. Яковлева, И.А. Калмыков // Актуальные проблемы современной науки. II Международная научно-техническая конференция. В трех томах. Выпуск 2. Том 3 – г.Ставрополь –2013;

4. Калмыков, И.А. Структура организации параллельного спецпроцессора цифровой обработки сигналов, использующего модулярные коды / И.А. Калмыков, М.И. Калмыков // Теория и техника радиосвязи. №2 – 2014;

5. Калмыков, И.А. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров / И.А. Калмыков, Д.Н. Резеньков, Д.В. Горденко, А.Б. Саркисов // ООО «Издательско-информационный центр «Фабула»». – г. Ставрополь – 2014 г.

6. Петренко, В.И. Умножитель по модулю. [Текст] / В.И. Петренко, Ю.В. Кузьминов /Патент России №2299461 C1 МПК G06F7/523, G06F7/72, 2007.

А.В. Лемешко, М.В. Семеняка, А.В. Симоненко

МОДЕЛЬ АКТИВНОГО УПРАВЛЕНИЯ ОЧЕРЕДЯМИ НА МАРШРУТИЗАТОРАХ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Харьковский национальный университет радиоэлектроники

Ключевые слова: модель, очередь, маршрутизатор, перегрузка, поток, пакеты.

Предложена модель активного управления очередями на маршрутизаторах телекоммуникационной сети. Новизна модели состоит в обеспечении согласованного решения задач по распределению поступающих потоков между отдельными очередями сетевого узла (Congestion Management); выделению пропускной способности интерфейса для каждой из очередей (Resource Allocation) и превентивному ограничению интенсивности поступающих на интерфейс потоков пакетов (Congestion Avoidance). В рамках предложенной модели сформулирована оптимизационная задача нелинейного программирования с квадратичной целевой функцией и нелинейными ограничениями.

A.V. Lemeshko, M.V. Semenyaka, A.V. Simonenko

ACTIVE QUEUE MANAGEMENT MODEL ON THE TELECOMMUNICATION NETWORK ROUTERS

Kharkiv National University of Radio Electronics

Keywords: model, queue, router, overload, flow, packets.

A model of the active queue management on the telecommunication network routers proposed. The novelty of the model is providing a consistent solution of congestion management problems of incoming flows distribution between the individual queues on the network node; resource allocation of interface throughput for each queue, and congestion avoidance preventive restriction of arriving packet flows intensity at the interface. Within the framework of the proposed model it was formulated a nonlinear programming optimization problem with quadratic objective function and nonlinear constraints.

Технологические средства обслуживания очередей, представленные механизмами FIFO, Priority Queues, Custom Queues, Weighted Fair Queue и др., имеют ряд недостатков, среди которых преобладающими являются статичность настроек, проявляющаяся в необходимости вмешательства администратора при конфигурировании механизма; неспособность к адаптации под изменения в состоянии интерфейса и сети в целом; несогласованность получаемых решений с другими средствами управления очередями, например, механизмами предотвращения перегрузок Random Early Detection (RED) и Weighted Random Early Detection (WRED), что способно нивелировать достоинства как первой, так и второй группы решений [1, 2]. Поэтому актуальным видится направление исследований, связанное с разработкой новых моделей и методов активного управления очередями, которые могли быть положены в основу соответствующих управляющих механизмов на маршрутизаторах телекоммуникационной сети.

В этой связи в данной работе предлагается потоковая модель активного управления очередями, в рамках которой обеспечивается согласованное решение следующих важных задач для повышения качества обслуживания потоков пользователей: распределение поступающих потоков между отдельными очередями маршрутизатора (Congestion Management); выделение пропускной способности (ПС) интерфейса для каждой из очередей (Resource Allocation); превентивное ограничение интенсивности поступающих на интерфейс потоков пакетов (Congestion Avoidance).

Пусть в рамках предлагаемой модели на обслуживание сетевого узла поступает M потоков со следующими характеристиками: a_i – интенсивность i-го потока, pr_i – приоритет пакетов i-го потока ($i=\overline{1,M}$). Отличительной особенностью модели является возможность превентивного ограничения интенсивности потоков, поступающих на интерфейс маршрутизатора. Тогда в предлагаемую модель вводится множество управляющих переменных первого типа α_i, ($i=\overline{1,M}$), каждая из которых характеризует долю i-го потока, получившего отказ в обслуживании на интерфейсе маршрутизатора при реализации функций Congestion Avoidance. По своему физическому смыслу переменные α_i численно определяют вероятность отбрасывания пакетов i-го потока на рассматриваемом интерфейсе маршрутизатора.

Пакеты, поступившие на обслуживание, должны распределяться между N очередями в ходе решения задач Congestion Management путем расчета множества переменных второго типа $x_{i,j}$ ($i=\overline{1,M}$, $j=\overline{1,N}$), каждая из которых характеризует долю i-го потока, направленного на обслуживание в j-ю очередь. Для решения задач класса Resource Allocation в рамках предлагаемой модели необходимо обеспечить расчет множества переменных третьего типа – b_j, каждая из которых определяет величину пропускной способности интерфейса, выделенную для обслуживания j-й ($j=\overline{1,N}$) очереди. Пусть b – пропускная способность канала связи. Далее искомые переменные всех трех типов удобно представить в виде соответствующих управляющих векторов $\vec{x}$, $\vec{\alpha}$, $\vec{b}$ с координатами $x_{i,j}$, α_i и b_j соответственно.

Для обеспечения приблизительно равного качества обслуживания пакетов одного и того же потока каждый их пакетов целесообразно обрабатывать в рамках одной из очередей. Таким образом, переменная $x_{i,j}$ является булевой, т.е.

$$x_{i,j} \in \{0,1\}. \quad (1)$$

Дифференциация качества обслуживания обеспечивается за счет того, что потоки с разными приоритетами (требованиями к качеству обслуживания) обрабатываются в различных очередях. Согласно физическому смыслу переменных α_i и b_j на них накладываются следующие ограничения:

$$0 \le \alpha_i \le 1, (i = \overline{1, M}), \tag{2}$$

$$\sum_{j=1}^{R} b_j \le b, \quad 0 \le b_j, (j = \overline{1, N}). \tag{3}$$

Взаимосвязь между управляющими переменными первого и второго типа, развивая подход, предложенный в работах [3-5], можно отразить в рамках следующих условий сохранения потока на интерфейсе маршрутизатора:

$$\sum_{j=1}^{N} x_{ij} + \alpha_i = 1, (i = \overline{1, M}). \tag{4}$$

Согласно условию (4) пакеты i-го потока могут быть либо направлены на обслуживание одной из очередей интерфейса, либо отброшены. С целью обеспечения управляемости процессом предотвращения перегрузки важно удовлетворить условие:

$$\sum_{i=1}^{M} a_i x_{i,j} < b_j, (j = \overline{1, N}), \tag{5}$$

выполнение которого гарантирует, что суммарная интенсивность потоков, направленных на обслуживание в j-ю очередь, не превысит пропускную способность интерфейса, выделенную для данной очереди. Условия (5) отражают функциональную взаимосвязь между переменными второго и третьего типа.

Для предотвращения перегрузки очереди по ее длине (в пакетах) условия (1)-(5) могут также быть дополнены нелинейными ограничениями:

$$\overline{n}_j < n_j^{\max}, \tag{6}$$

где $n_j^{\max}$ – максимальный размер j-й очереди; $\overline{n}_j$ – средняя длина j-й очереди, которая в зависимости от характеристик, формирующих данную очередь потоков, поддерживаемой дисциплины обслуживания пакетов, может быть рассчитана с использованием выражений, описанных в [3].

Расчет управляющих переменных целесообразно осуществить в ходе решения оптимизационной задачи, связанной с минимизацией как использования пропускной способности интерфейса, так и возможных отказов в обслуживании, вызванных превентивным ограничением интенсивности потоков

$$\min_{x,b,\alpha} F,$$

$$F = \vec{x}^t H_x \vec{x} + \vec{\alpha}^t H_\alpha \vec{\alpha} + \vec{b}^t H_b \vec{b}, \tag{7}$$

где $(\cdot)^t$ – операция транспонирования, H_x – диагональная матрица с координатами $h_{i,j}^x$; H_α – диагональная матрица с координатами h_i^α; H_b – диагональная матрица с координатами h_j^b; $h_{i,j}^x$ – условная стоимость (метрика) обслуживания i-го потока j-й очередью; h_i^α – условная стоимость отбрасывания пакетов i-го потока; h_j^b – условная стоимость выделения пропускной способности интерфейса для j-й очереди. Метрики $h_{i,j}^x$, h_i^α и h_j^b должны прямо пропорционально зависеть от приоритета пакетов обслуживаемых потоков pr_i, $(i = \overline{1, M})$.

Расчетные решения, полученные в ходе использования модели (1)-(7), должны обеспечивать адаптивный характер ограничения интенсивности потока при перегрузке

интерфейса. Кроме необходимости учета приоритета пакетов обслуживаемых потоков в ходе решения важно обеспечить превентивный характер отказов в обслуживании по аналогии с функционалом механизма RED/WRED. Это сопряжено с обоснованием параметров самой модели (1)-(7), что, прежде всего, касается выбора численных значений и соотношения весовых коэффициентов $h_{i,j}^{x}$, h_i^{α} и h_j^{b} в целевой функции (7), отвечающих за величины удельной стоимости при согласованном решении задач Congestion Management, Congestion Avoidance и Active Queue Management.

Исследование предложенной модели основывалось на результатах аналитического моделирования, в ходе которого минимизация функции (7) с учётом ограничений (1)-(6) производилась с использованием пакета Optimization Toolbox среды Matlab 7. Особенности решения задач по активному управлению очередями продемонстрированы на численном примере. Пусть на вход маршрутизатора поступал трафик, состоящий из пяти потоков. Интенсивность первого потока изменялась от 1 до 500 1/с ($a_1 = 1 \div 500$ 1/с), тогда как интенсивность остальных потоков оставалась постоянной ($a_2 = 160$ 1/с, $a_3 = 235$ 1/с, $a_4 = 200$ 1/с, $a_5 = 98$ 1/с). Пропускная способность канала связи составляла 1200 1/с. Обслуживание потоков организовывалось с использованием трёх очередей.

Результаты исследования показали, что в случае, если $h_{i,j}^{x} << h_i^{\alpha}$, т.е. соотношение $h = h_{i,j}^{x} / h_i^{\alpha}$ составляло $1:600$ и выше, ограничение интенсивности потока наблюдалось лишь в условиях перегрузки, когда интенсивность поступающего на интерфейс трафика превосходит пропускную способность канала связи, что аналогично поведению механизма Tail Drop. В случае, когда условная стоимость за отбрасывание пакетов меньше, чем метрика распределения пакетов между очередями ($h_i^{\alpha} < h_{i,j}^{x}$), пакеты отбрасывались даже в случае наличия на интерфейсе достаточного объема свободных ресурсов по пропускной способности. Вероятность отбрасывания пакетов i-го потока численно оценивалась через параметр α_i.

Изменением соотношения весовых коэффициентов можно регулировать степень превентивности при отбрасывании пакетов в зависимости от загруженности интерфейса: в области низких нагрузок на интерфейс (при интенсивности потока 1÷150 1/с) отбрасывание пакетов нецелесообразно в ввиду наличия достаточного объема пропускной способности, весовые коэффициенты должны выбираться из соотношения $h_{ij}^{x} / h_i^{\alpha} = 1:200$ и выше; в областях средних (151÷300 1/с) и высоких нагрузок (301÷500 1/с) можно организовать ограничение интенсивности потоков пакетов по аналогии с механизмом WRED, когда вероятность отбрасывания зависит от приоритета пакета.

Например, для потоков низкого приоритета, весовые коэффициенты стоит выбирать в пределах $h_{ij}^{x} / h_i^{\alpha} \approx 1:200 \div 1:400$, для потоков с более высоким приоритетом стоит выбирать весовые коэффициенты в пределах $h_{i,j}^{x} / h_i^{\alpha} \approx 1:400 \div 1:600$. Важно отметить, что для данного примера при соотношении $h_{i,j}^{x} / h_i^{\alpha} \approx 1:550$ вероятность отбрасывания пакетов будет соответствовать результатам работы механизма RED с параметрами, установленными «по умолчанию», т.е. для знаменателя граничной вероятности, равного десяти. Согласно полученным результатам в табл. 1 представлены рекомендованные значения для соотношения весовых коэффициентов h для потоков пакетов с различными IP-приоритетами (pr_i, $i = \overline{1,M}$).

Таблица 1. Соотношения весовых коэффициентов для потоков различного приоритета

IP-приоритет	0	1	2	3	4	5	6	7
Рекомендуемое отношение весовых коэффициентов, $h = h_{i,j}^{x} / h_{i}^{\alpha}$	1:200	1:250	1:300	1:400	1:450	1:500	1:550	1:600

Литература:

1. Вегенша Ш. Качество обслуживания в сетях IP: пер. с англ. – М.: Издательский дом «Вильямс», 2003, 386 с.

2. Tsai T.-Y., Chung Y.-L., Tsai Z. Introduction to Packet Scheduling Algorithms for Communication Networks // Communications and Networking, Jun Peng, 2010, 434 p.

3. Лемешко А.В., Симоненко А.В., Ватти Махмуд. Потоковая модель управления очередями с динамическим распределением пропускной способности исходящего канала связи // Наукові записки УНДІЗ, 2008, №3(5), с. 34-39.

4. Али С. Али, Симоненко А.В. Потоковая модель динамической балансировки очередей в MPLS–сети с поддержкой Traffic Engineering Queues [Электронный ресурс] // Проблеми телекомунікацій, 2010, № 1 (1), с. 59-67. Режим доступа: http://pt.journal.kh.ua/2010/1/1/101_ali_balancing.pdf.

5. Семеняка М.В., Симоненко А.В., Али С. Али. Разработка и исследование метода динамической балансировки очередей на маршрутизаторах мультисервисной телекоммуникационной сети [Электронный ресурс] // Проблеми телекомунікацій, 2012, № 3 (8), с. 64-78. Режим доступа: http://pt.journal.kh.ua/2012/3/1/123_semenyaka_balancing.pdf.

Киндиа Самаке, С.Д. Ерохин

РАЗВИТИЕ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ МАЛИ

Московский Технический Университет Связи и Информатики, г. Москва, Россия

Ключевые слова: информационные и коммуникационные технологии, сетевая готовность, телефонная связь, Интернет, инфокоммуникационная отрасль, информационная политика.

Одной из наиболее актуальных тенденций в развитии современных информационных и коммуникационных технологий выступает рост численности пользователей Интернет-сервисов и объема Интернет-трафика. Развитие связанной с Интернетом инфраструктуры становится важнейшей составляющей конкурентоспособности государств на мировом рынке, где появляются все новые формы онлайн-торговли, цифровых технологий логистики и управления персоналом. Глобальные тренды оказывают влияние на развитие разных стран и континентов, при этом состояние ИКТ в каждом конкретном случае зависит от многих факторов – от геополитического положения и уровня социально-экономического развития до местной историко-культурной специфики. Целью настоящей работы выступает выявление особенностей развития информационных и коммуникационных технологий в республике Мали.

Kindia Samake, S.D. Erokhin

INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE REPUBLIC OF MALI

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: information and communication technology, networked readiness, telephone communications, Internet, infocommunication industry, information policy.

One of the most current trends in the development of modern information and communication technology (ICT) supports the growth of the number of users of Internet services and the volume of Internet traffic. The development of Internet-related infrastructure is becoming an essential component of the competitiveness in the global market, where there are new forms of online trading, digital logistics and personnel management. Global trends influence the development of different countries and continents, with the state of ICT in each case depends on many factors - the geopolitical situation and the level of socio-economic development to the local historical and cultural specificity. The aim of this work serves to determine the characteristics of information and communication technologies in the Republic of Mali.

Одной из наиболее актуальных тенденций в развитии современных информационных и коммуникационных технологий выступает рост численности пользователей Интернет-сервисов и объема Интернет-трафика. Информация в современном мире – самый востребованный товар, стратегический ресурс и новый источник власти. Развитие связанной с Интернетом инфраструктуры становится важнейшей составляющей конкурентоспособности государств на мировом рынке, где появляются все новые формы онлайн-торговли, цифровых технологий логистики и управления персоналом [1, 2]. Глобальные тренды оказывают влияние на развитие разных стран и континентов, при этом состояние ИКТ в каждом конкретном случае зависит от многих факторов – от геополитического положения и уровня социально-экономического развития до местной историко-культурной специфики. Целью настоящей работы выступает выявление особенностей развития информационных и коммуникационных технологий в республике Мали.

Для просвещенной части общества современных стран Африки, в том числе, республики Мали, характерно понимание принципиальной важности развития информационных и коммуникационных технологий. Прогресс в этой сфере воспринимается как залог решения ключевой задачи по повышению уровня технико-технологического, научного и социально-экономического отставания [1] от развитых стран как в мировом масштабе (здесь ориентиром выступают США и Западная Европа), так и в пределах африканского континента (лидирующие позиции занимает ЮАР). С учетом исторической специфики развития африканских государств вполне объяснимо, что основные надежды в сфере распространения новых технологий возлагаются на меры государственной поддержки. В республике Мали отмечается общая закономерность, связанная с географией распространения Интернет-сервисов и технологий: первым этапом их освоения становится внедрение в деятельность официальных органов власти, затем постепенно начинается распространение в крупных городах, еще более медленными темпами Интернет проникает в сельскую местность.

Мали находится на начальном этапе развития ИКТ, многое еще предстоит сделать, однако важно отметить значительный потенциал роста этого рынка. В настоящее время можно выделить ряд ключевых игроков в инфокоммуникационной отрасли:

- Государственный орган по регулированию телекоммуникаций/ИКТ и почтовой связи (AMRTP) [3]
- Агентство по информационным и коммуникационным технологиям (AGETIC) [4]
- Оператор сотовой связи MALITEL
- Оператор сотовой связи ORANGE MALI

Наиболее влиятельным игроком в сфере продвижения новых информационных и коммуникационных технологий выступает государство в лице AMRTP.Этот орган отвечает за реализацию государственной информационной политики по следующим основным направлениям [3]:

- продвижение национальных интересов в области телекоммуникаций/ИКТ и почтовой связи
- обеспечение принципов честной конкуренции, т.е. равноправного статуса операторов связи и иных игроков телекоммуникационной отрасли и почтовой связи в их взаимодействии с органами государственной власти
- содействие продвижению и распространению новых технологий в Мали
- нормативное обеспечение деятельности министерства, ответственного за развитие телекоммуникаций /ИКТ и почтовой связи, в том числе, по вопросам, связанным с защитой прав потребителей соответствующих услуг

– обеспечение соблюдения экологических и санитарных норм в работе компаний в сфере телекоммуникаций/ИКТ
– обеспечение соблюдения действующего законодательства в сфере телекоммуникаций/ИКТ, в том числе, путем контроля и надзора за деятельностью основных игроков отрасли.

Агентство по информационным и коммуникационным технологиям в Мали было создано законодательным актом №05-002 10 января 2005 года. Сфера его компетенции довольно широка: в число возложенных на агентство функций входит проектирование, развитие и обслуживание национальной инфраструктуры в области информационных и коммуникационных технологий, а также разработка и реализация национальной стратегии по развитию ИКТ [4].

Одним из важных решений агентства, способствующим развитию Интернет-пространства Мали, стало открытие для общего пользования доменной зоны .ML. Большая часть доменов при этом предоставляется пользователям бесплатно и без дополнительных ограничений, что предусмотрено специальным законодательным актом [4,5]. Эта мера для стран Африки уникальна, она направлена на популяризацию Интернета в Мали и продвижение социально востребованных онлайн-сервисов. Реализацией и раскруткой проекта занималась компания Freedom Registry, которая уже имела подобный опыт с доменом .tk. В конечном итоге, большая степень информатизации общества за счет расширения доступа населения к передовым технологиям будет способствовать улучшению не только качества жизни местных жителей, но и имиджа Мали, прежде всего, в рамках африканского континента.

Рынок услуг сотовой связи в Мали пока не слишком развит, но весьма перспективен. Ключевыми направлениями развития можно назвать расширение широкополосного доступа в Интернет, повышение безопасности телекоммуникационного трафика, развитие национальной и международной спутниковой связи.

Основными операторами мобильной связи являются Malitel (www.malitel.com.ml) и Orange Mali, объединяющий в сеть по оптоволоконному кабелю Мали, Марокко и, в перспективе, Мавританию и Буркина-Фасо (www.orangemali.com). Обе компании создавались при участии государства и работают по системе prepaid, причем в силу высокой стоимости разговоров исключительной популярностью пользуются специальные программы sms-сообщений. Стоит отметить высокую популярность сотовой связи: уровень распространения мобильных телефонов значительно вырос за последние годы, чтонаглядно подтверждает статистика (см.ниже). Высокий уровень приема сигнала обеспечивается во всех городах и населенных пунктах страны, таких, как Бамако, Сикасо, Каес, Мопти, Сегу, Ниоро, Маркала, Кутиала, Кати, Колокани, Гао, Томбукту, Кидаль и многих других.

Таблица 1.Статистика подключения к мобильной связи (на 100 человек) [6].

Страна	2009	2010	2011	2012	2013
МАЛИ	33	53	75	98	129

Для формирования более целостной картины развития информационных и коммуникационных технологий в Мали стоит учесть и такой показатель, как Индекс сетевой готовности (Networked Readiness Index). Этот индекс используется в качестве средства анализа для построения сравнительных рейтингов, отражающих уровень развития информационного общества в различных странах.

Индекс измеряет уровень развития ИКТ по 53 параметрам, объединенным в три основные группы:

– Наличие условий для развития ИКТ - общее состояние деловой и нормативно-правовой среды с точки зрения ИКТ, наличие здоровой конкуренции, инновационного потенциала, необходимой инфраструктуры, возможности финансирования новых проектов, регуляторные аспекты и так далее.
– Готовность граждан, деловых кругов и государственных органов к использованию ИКТ - государственная позиция относительно развития информационных технологий, государственные затраты на развитие сферы, доступность информационных технологий для бизнеса, уровень проникновения и доступность сети Интернет, стоимость мобильной связи и так далее.

– Уровень использования ИКТ в общественном, коммерческом и государственном секторах - количество персональных компьютеров, интернет-пользователей, абонентов мобильной связи, наличие действующих интернет-ресурсов государственных организаций, а также общее производство и потребление информационных технологий в стране.

Согласно статистике[8], индекс сетевой готовности Республики Мали составил 3.00 в 2014 году, страна занимала 127-ое место в международном рейтинге. Стране предстоит пройти еще долгий путь по развитию современных технологий.

В заключение рассмотрим такой важный параметр, как развитие Интернета. Первый интернет-провайдер появился в Мали в 1994 г. (Malinet), в дальнейшем его развитие шло усилиями Национальной телекоммуникационной компании, однако ареал доступности онлайн-сервисов был весьма ограниченным. Ситуация изменилась в 2006 г., когда на рынок вышла компания Orange Mali: доступ в Интернет стал проще и дешевле. Сейчас Интернет в стране доступен через обычные модемы dial-up, через GPRS, ADSL, 3G и 3G+. Тем не менее, использование широкополосного интернета пока крайне ограничено: в основном, оно сосредоточено в крупных городах. Это связано не только с несовершенством технических возможностей, но и с недостаточной осведомленностью граждан, нехваткой доступной и понятной информации о новых возможностях, связанных с использованием «всемирной паутины».

Эту картину наглядно иллюстрирует Индекс развития Интернета (разработан World Wide Web Foundation в 2012 году под руководством Тимоти Бернерса-Ли). В рамках составления индекса проводится оценка уровня и интенсивности использования Интернета в стране, включая уровень развития и качества коммуникационной инфраструктуры, а также институциональной инфраструктуры и инструментов регулирования. Также оценивается уровень гражданских свобод, включая права на получение информации, высказывание мнений, безопасность и конфиденциальность в Интернете. Проводится также оценка уровня использования гражданами и доступность контента с акцентом на том, насколько различные группы заинтересованных граждан могут получить доступ к информации в национальном сегменте Интернета через доступные платформы и каналы на языке, который они используют. Наконец, принимаются во внимание социальные, экономические и политические показатели развития государства в контексте влияния на них Интернета.

Согласно данным Индекса, рейтинг развития Интернета в Мали выглядит следующим образом [9]

Таблица 2. The Web Index 2013

Страна	Рейтинг	Индекс	Проникновение	Качество контента	Свобода и открытость	Права и возможности
Мали	79	7.7	10.1	4.7	34.9	0.0

По итогам исследования можно сделать следующие выводы. К особенностям развития информационных и коммуникационных технологий в республике Мали относятся характерное для стран Африки позднее распространение современных технологий, низкая конкурентность рынка ИКТ (небольшое число компаний, преобладание игроков с государственным участием), ограниченность использования Интернет-сервисов населением. Основным пользователем Интернета в Мали остается государство, при этом информация, размещаемая на сайтах официальных властных структур, носит справочно-описательный характер. Перспективы развития информационных и коммуникационных технологий в Мали связаны с расширением рынка связи и цифровых услуг, повышением его конкурентоспособности, а также распространением современного образования и формированием целевой аудитории с качественно иными потребностями в информационном обеспечении и социальных услугах.

Литература:

1. African Education Knowledge Warehouse. SchoolNet Africa. http://www.schoolnetafrica.org

2. К. А. Панцерев / Страны тропической Африки в глобальном обществе знаний: возможность прорыва // Вестник Волгогр. гос. уни-та. Сер. 4, Ист. 2011. №2 (20).

3. Государственный орган по регулированию электронной и почтовой связи (AMRTP) http://www.amrtp-mali.org/

4. Agetic Mali http://www.agetic.gouv.ml/
5. Бесплатная доменная регистрация в зоне .ml http://www.dot.ml/en/faq.html
6. ICT Data and Statistics (IDS) http://www.itu.int/ITU-D/ict/statistics/explorer/index.html
7. The Global Information Technology Report 2014. http://gtmarket.ru/ratings/telephony-development/info
8. The Global Information Technology Report 2014. http://gtmarket.ru/ratings/networked-readiness-index/networked-readiness-index-info
9. The Global Information Technology Report 2014. http://gtmarket.ru/news/2013/11/25/6418

Т.Е. Сечко, М.И. Дмитриев,
А.А. Лысак, Н.В. Руденко, А.Г. Сукиязов

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ НА ОСНОВЕ РАЗРЫВА КОМПЬЮТЕРНОГО ЦИКЛА

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: профессиональные компетенции, компьютерные технологии, метод разрыва компьютерного цикла, формирование компетенций.

Предложено применение метода разрыва компьютерного цикла для формирования профессиональных компетенций студентов. Суть метода заключается в том, что места разрывов компьютерного цикла обусловлены теми компетенциями, которые должны формироваться в ходе занятия. Разработанная методика позволяет гармонично сочетать формирование у студентов всех требуемых компетенций и может быть использована как при очном, так и при дистанционном обучении, поскольку позволяет достаточно легко создавать блоки заданий для системы дистанционного обучения, а также выполнять контроль качества формирования требуемых компетенций с помощью тестов.

T.E. Sechko, M.I. Dmitriev,
A.A. Lysak, N.V. Rudenko, A.G. Sukiyazov

FORMATION OF COMPETENCES ON THE BASIS OF THE GAP COMPUTER CYCLE

Don State Technical University, Rostov-on-Don, Russia

Keywords: professional competences, computer technologies, method of a rupture of a computer cycle, formation of competences.

Application of a method of a rupture of a computer cycle for formation of professional competences of students is offered. The essence of a method is that places of ruptures of a computer cycle are caused by those competences which have to be formed during occupation. The developed technique allows to combine harmoniously formation at students of all demanded competences and can be used both at internal, and at distance learning as allows to create rather easily blocks of tasks for system of distance learning, and also to carry out quality control of formation of the demanded competences by means of tests.

Постановка задачи. В настоящее время современные информационные технологии становятся инструментом, качество владения которым определяет профессионализм и конкурентоспособность специалиста, в том числе бакалавров по направлению подготовки 210400 Радиотехника. Успешное решение задачи подготовки современных специалистов возможно на основе новых информационно-педагогических технологий и методов образования. Федеральный государственный образовательный стандарт высшего профессионального образования по указанному направлению подготовки требует формирования у выпускников множества

компетенций при проведении различных видов занятий, в том числе, способность выполнять математическое моделирование объектов и процессов по типовым методикам с использованием стандартных пакетов прикладных программ (профессиональная компетенция (ПК)-19) [1].

Информационная среда обучения (ИСО) (компьютер и программное обеспечение) превращается в универсальный инструмент и является активным помощником при обеспечении учебного процесса. Однако этот инструмента требует особого подхода к его использованию для того, чтобы выпускник не получил однобокого образования, а приобрел все требуемые компетенции. В настоящее время еще нет теории, которая бы определила, в каком количестве и когда целесообразно использовать компьютерные технологии, а когда этого делать не следует.

Разработке рекомендаций по использования ИСО для формирования необходимых компетенций на практических видах занятий посвящена настоящая статья.

Материалы исследования. ИСО рассматривается как интеллектуальный инструмент, обладающий огромными возможностями и универсальностью. При этом объект исследования находится вне компьютера: это или небольшая реальная лабораторная установка, на которой проводятся измерения, или скомпонованная заранее преподавателем таблица данных, которые надо обработать и сделать соответствующие выводы в соответствии с заданием.

Универсальность и мощь компьютерных технологий позволяет автоматизировать практически любой процесс. Однако для реализации обучающих функций при планировании занятия описанный выше компьютерный цикл должен быть в определенных местах сознательно разорван, а соединяющим звеном должен стать обучаемый. В этом состоит предлагаемый метод построения занятия с использованием компьютерных технологий [2, с.38; 3, с.213], который в дальнейшем будем называть методом разрыва компьютерного цикла (РКЦ).

Рисунок 1. Иллюстрация метода разрыва компьютерного цикла

Суть метода заключается в том, что места разрывов компьютерного цикла обусловлены теми компетенциями, которые должны формироваться в ходе занятия. Это поясняется рисунком 1.

Так разрывы цикла на участках 1 и 2 соответствуют формированию следующих компетенций [1]:

- готовности организовать метрологическое обеспечение производства (ПК-16);
- способности реализовать программы экспериментальных исследований, включая выбор технических средств и обработку результатов (ПК-20).

При этом учащийся должен сам произвести отсчет значения измеряемой физической величины и ввести ее в компьютер с помощью клавиатуры. Обучающим моментом данного разрыва цикла является получение навыков работы с измерительной техникой, клавиатурой и осмысление численного значения данных.

Разрывы цикла на участке 3 соответствуют формированию способности владеть основными приёмами обработки и представления экспериментальных данных (ПК-5) [1].

Этот разрыв цикла соответствует необходимости самому студенту построить график функциональной зависимости между величинами, которые выдает компьютер в виде таблицы. На

этом этапе компьютер освобождает от большого числа нудных и однообразных вычислений. В результате осуществляется обучение построению графиков и знакомству с достоинствами графического представления информации.

Разрывы цикла на участке 4 соответствуют формированию готовности участвовать в составлении аналитических обзоров и научно-технических отчетов по результатам выполненной работы (ПК-21) [1]. При этом требуется сформулировать выводы по полученным результатам, также ручное составление отчета по лабораторной работе.

Разрыв цикла на участке 5 соответствует формированию способности владеть правилами и методами монтажа, настройки и регулировки узлов радиотехнических устройств и систем (ПК-28) [1]. При этом студенты на основе анализа выводов, составляют научный прогноза поведения объекта в новых условиях и экспериментально проверяют прогноз с помощью имеющихся в компьютере программных средств (творческие задания).

На практических и лабораторных занятиях ИСО позволяет помочь обучаемому понять реальную ситуацию и свести её к одной из основных моделей путем допустимого абстрагирования. После этого производится математическое описание логически обоснованной упрощенной модели реального процесса и расчет искомой величины. Затем наступает этап анализа полученных результатов, на котором компьютер обеспечивает значительное увеличение производительности труда, фактически сводящееся к возрастанию интенсивности учебного процесса. Именно в такой ситуации применение компьютера не столько как средства накопления, хранения и передачи информации, сколько как инструмента для развития ассоциативного научного мышления позволяет достичь наиболее высоких результатов.

Например, очень полезен анализ поведения выбранной модели в различных практически важных случаях, которые учащиеся могут варьировать сами, меняя значения параметров модели. При этом физический смысл параметров осознается гораздо глубже и легче запоминается.

Целесообразность использования метода РКЦ при проведении лабораторных работ определяется тем, что в современных условиях обучаемые потеряли понимание значащего числа и не знают до какого разряда следует округлить измеряемую величину, тем более, что измерительные приборы и калькуляторы выдают более 7 разрядов. Поэтому, весьма эффективным оказался РКЦ на 4 участке (рисунок 1), когда обработка результатов эксперимента осуществляется с помощью компьютера с очень высокой точностью, а обучаемые должны сами определить значимые разряды, округлить полученные результаты и соответствующим образом рассчитать доверительный интервал.

Все это может быть сделано с помощью компьютера, но преподаватель сознательно включает в процесс человека, который при этом обучается. Опыт работы авторов показывает, что очень неплохих результатов при использовании метода РКЦ в лабораторном практикуме можно достичь с помощью электронных таблиц *EXCEL*, входящих в *Microsoft Office*. Есть примеры использования *EXCEL* в инженерных расчетах и некоторых приложениях элементарной физики. Однако имеются очень хорошие простые математические программы, написанные профессионально и доступные в Интернете. Это оказывается удобным при реализации элементов дистанционного обучения.

Предложенные рекомендации могут быть обобщены в виде методики формирования компетенций на основе разрыва компьютерного цикла. Эта методика содержит следующую последовательность действий [3, с. 217].

1. Формулирование темы, цели и задач исследования. Уяснение компетенций, которые необходимо формировать на занятии (в соответствии с Основной образовательной программой по направлению подготовки и Рабочей программой дисциплины).
2. Выбор программного обеспечения для выполнения исследования, обработки и графического представления результатов. Формирование компьютерного цикла.
3. Определение мест разрыва компьютерного цикла в соответствии с требуемыми компетенциями. Уточнение исходных данных и средств формирования компетенций на каждом этапе работы.
4. Разработка критериев оценки работы студентов по приобретению знаний и навыков в рамках требуемых компетенций. Формализация контроля полученных знаний и навыков в форме итогового теста, содержащего вопросы требуемых компетенций.
5. Составление плана проведения занятия с примерным распределением времени и разработка методических рекомендаций для преподавателя и студентов.

6. Отладка занятия на практике и уточнение методических рекомендаций и расчета времени.

Рассмотрим пример разработанного на кафедре «Радиоэлектроника» лабораторного занятия по исследованию колебательного контура. Задание имеет следующий вид. Для каждого варианта, с помощью программы *MathCad* строится график затухающих колебаний напряжения на конденсаторе в колебательном контуре. Значения параметров колебательного контура – индивидуальны. Этот график распечатывается на бумаге и представляется как запись реального эксперимента (игровая ситуация). Задание во всех вариантах одно и то же: при заданных значениях емкости и индуктивности контура, а также цены делений по осям графика определить:

- добротность колебательного контура,
- найти величину активного сопротивления контура,
- по графику затухающих колебаний построить резонансную кривую;
- на основании исследований представить подробный отчет.

Ход выполнения задания состоит в следующем:

С помощью линейки производят обмер графика и находят время и амплитуду каждого максимума напряжения на конденсаторе. Данные заносят в таблицу. Далее в соответствии с приведенными в методичке формулами производят расчет искомых величин и рассчитываются данные для построения резонансной кривой, которая строится также с использованием компьютерных средств.

Выводы:

1. Разработанная методика позволяет гармонично сочетать формирование у студентов всех требуемых компетенций.
2. Компьютерные технологии используются как вспомогательный инструмент, расширяющий возможности исследования и облегчающий рутинные операции.
3. Предложенная методика может быть использована как при очном, так и при дистанционном обучении, поскольку позволяет достаточно легко создавать блоки заданий для системы дистанционного обучения, а также выполнять контроль качества формирования требуемых компетенций с помощью тестов.

Литература:

1. Учебно-методическое объединение по образованию в области радиотехники, электроники, биомедицинской техники и автоматизации. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 210400 Радиотехника. [Электронный ресурс]. URL:http://umo.eltech.ru/assets/files/fgos-vpo/210400-radiotehnika/bakalavry/vgos-vpo.pdf. (Дата обращения 04.03. 2015 г.)

2. Сукиязов А.Г., Крамаров С.О. Принципы использования активных компьютерных технологий для предметного обучения // Дистанционное и виртуальное обучение. 2003. № 6. С. 38-39

3. Сукиязов А.Г., Руденко Н.В. Методики формирования компетенций на основе разрыва компьютерного цикла. Современные проблемы многоуровневого образования. Международный научно-методический симпозиум – Ростов н/Д: ДГТУ, 2014. С. 213-218

В.Н. Смоляков, Е.В. Крамар

МОДЕРНИЗАЦИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НОВОШАХТИНСКОГО ПОЧТАМТА УФПС РОСТОВСКОЙ ОБЛАСТИ - ФИЛИАЛА ФГУП «ПОЧТА РОССИИ»

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: локальная вычислительная сеть, беспроводной доступ, персональ-ный компьютер, система связи и передачи данных, сетевая архитектура и топология ЛВС, программное обеспечение ЛВС, отделение почтовой связи.

Рассматриваются вопросы модернизации ЛВС Новошахтинского почтамта УФПС Ростовской области - филиала ФГУП «Почта России». Успешная работа любой организации в значительной степени определяется тем, насколько быстро и безотказно функционирует ее корпоративная сеть. Особенно важно грамотное принятие решений о развитии сети при расширении масштабов деятельности предприятия. Модернизация ЛВС обеспечит существенное повышение уровня автоматизации работы почтамта, позволит повысить точность и оперативность работы с документацией и клиентами, автоматизировать формирование различных отчетных документов, что значительно уменьшит временные и материальные затраты при реализации всех основных функций почтамта..

V.N. Smolaykov, E.V. Kramar

MODERNIZE LOCAL NETWORK NOVOSHAHTINSK GPO AFPS ROSTOV REGION - FSUE «RUSSIAN POST»

Moscow State Technical University, North Caucasian Branch, Rostov-on-Don, Russia

Keywords: local area network, wireless, personal computer, data communications, network architecture and topology LAN software LAN, post office.

The problems of modernization LAN Novoshakhtinsk post office AFPS Rostov region - a branch of "Russian Post". The successful operation of any organization-tion is largely determined by how quickly and smoothly function nates its corporate network. It is particularly important competent decisions about the development of the network in scaling up the business. Modernization of LAN will provide a significant increase in the level of automation of the post office, will improve the accuracy and efficiency of work with documentation and customers to automate the formation of different accounting documents, which will greatly reduce the time and, therefore, material costs and the implementation of all the main functions of the post office.

Сегодня Почта России включает в себя 86 филиалов, около 42000 объектов почтовой связи, оказывающих услуги почтовой связи на всей территории Российской Федерации, включая все города и сельские населенные пункты и является одним из самых больших трудовых коллективов – около 380000 сотрудников. Ежегодно почтовые работники России принимают, обрабатывают и доставляют более 1,5 млрд. писем, 48 млн. посылок и 113 млн. ед. денежных переводов. Всего Почта предлагает своим клиентам свыше 80 почтовых, финансовых, инфокоммуникационных и прочих услуг.

Решение всех вышеперечисленных задач невозможно без использования современных информационных технологий, персональных компьютеров (ПК) и вычислительных сетей. ПК уже давно стал неотъемлемой частью жизни людей. Он помогает решать множество вопросов. Образовательные программы, медицинское обслуживание, промышленные процессы, почтовая связь – везде применяются ПК.

Под ЛВС понимают совместное подключение нескольких отдельных ПК - рабочих станций (РС) - к единому каналу передачи данных. Благодаря вычислительным сетям, мы получили возможность одновременного использования программ и баз данных (БД) несколькими пользователями одновременно.

Сегодня существует большое количество способов объединения ПК в ЛВС. Разного размера проводные и беспроводные ЛВС сотнями появляются каждый день. При этом если большие корпоративные сети требуют соответствующих знаний и уровня подготовки для их создания, то небольшие офисные и тем более домашние сети могут создавать простые пользователи.

В настоящем проекте рассматриваются вопросы модернизации ЛВС Новошахтинского почтамта УФПС Ростовской области - филиала ФГУП «Почта России».

Успешная работа любой организации в значительной степени определяется тем, насколько быстро и безотказно функционирует ее корпоративная сеть. Особенно важно грамотное принятие решений о развитии сети при расширении масштабов деятельности предприятия. Модернизация ЛВС обеспечит существенное повышение уровня автоматизации работы почтамта, позволит повысить точность и оперативность работы с документацией и клиентами, автоматизировать формирование различных отчетных документов, что значительно уменьшит временные, а, следовательно, и материальные затраты при реализации всех основных функций почтамта. Для достижения поставленных целей и задач необходимо выполнить следующие этапы работы:

- ознакомление с деятельностью организации, с организационно-штатной и управленческой структурой почтамта;
- изучение базовых технологий построения ЛВС и выбор основных компонентов ЛВС (ее топологии, кабельной системы связи, управляющего сервера);
- рассмотрение программных и технических характеристик предприятия;
- проектирование схемы прокладки кабеля и монтаж сетевого оборудования;
- отладка и тестирование ЛВС и планирование ее информационной без-опасности;
- расчет экономического эффекта от модернизации ЛВС.

После модернизации ЛВС существенно ускорится получение необходимой информации в сети Интернет, более эффективная работа электронной почты позволит ускорить производственный процесс, и, следовательно, увеличить обороты предприятия за счет роста объемов продаж услуг, предоставляемым Новошахтинским почтамтом, как частным клиентам, так и юридическим лицам.

Немаловажным является решение проблемы повышения надежности и эффективности доступа к корпоративной информации, хранящейся на сервере БД, а также защиты этой информации от несанкционированного доступа (НСД).

Экономическая эффективность предложенных в проекте решений обуславливается сокращением трудозатрат по ведению бухгалтерского учета, поиску информации, сокращением времени приема, передачи и обработки различной служебной информации, а также снижением цены и времени обслуживания клиентов за счет использования современных сетевых информационных технологий.

Помимо экономии времени улучшение показателей качества работы связано со своевременным получением информации, хранящейся в БД, повышением контроля правильности ввода информации, использования более информативных и наглядных документов, сокращение рутинных вычислений при получении выходных.

Из всего выше перечисленного можно сделать вывод об актуальности, целесообразности, и необходимости разработки проекта модернизации ЛВС Новошахтинского почтамта.

В ходе обследования Новошахтинского почтамта изучена организационная структура предприятия, произведен анализ целей, документооборот информационной системы, изучена функциональная модель предприятия, технические и программные средства, функционирующие в нем.

Анализ проблемных ситуаций выявил, что основной наиболее важной проблемой предприятия является необходимость снижения трудозатрат сотрудников при выполнении своего функционала. Выявленная проблемная ситуация затрудняет эффективную работу предприятия. Для устранения данной проблемной ситуации необходимо провести модернизацию ЛВС почтамта путем увеличения числа РС до 57 ПК. Кроме того требуется обеспечить 25%-ый запас для подключения новых ПК в будущем простым подключением ПК к ЛВС в заранее созданных 15-ти местах подключения. Это позволит при необходимости без труда довести количество РС до 72-х. Все это приведет к существенному росту эффективности функционирования Новошахтинского почтамта.

Сформированы основные критерии и требования для реализации проекта модернизации Новошахтинского почтамта.

Проведен подробный анализ технологии построения и функционирования ЛВС. Выполнен обзор среды передачи данных в ЛВС и сетевого оборудования. Рассмотрены структура и особенности протокола TCP и сетевого программного обеспечения.

На основании проведенного анализа принято решение при модернизации ЛВС Новошахтинского почтамта сохранить существующую топологию – «иерархическую звезду», витую пару в качестве среды передачи и ОС Windows 7 в качестве основной ОС ЛВС почтамта.

Для подключения новых РС целесообразно использовать беспроводной доступ к ПК ЛВС.

При модернизации предполагается внести существенные изменения в активное оборудование ЛВС.

В состав ЛВС вводится еще один сервер, который будет использоваться как сервер базы данных ЛВС, а имеющийся в данный момент сетевой сервер в дальнейшем будет использоваться как файл-сервер.

Структура ЛВС с двумя серверами позволит существенно повысить надежность сети и оперативность обмена информацией и доступа к БД. В качестве сервера выбираем модель Fujitsu (VFY:T1003SC070IN) PRIMERGY TX100S3p Xeon E3-1220v2 3.10 GHz/8 MB, 2x4GB DDR3-1600, 2xHD SATA 6G 1 TB, DVD-RW - как наиболее оптимальный по соотношению «цена – качество» и полностью удовлетворяющую потребностям ЛВС в области хранения и обмена данными с учетом перспективы развития ЛВС.

Вместо прежних концентраторов, уже не обеспечивающих требуемую скорость обмена данными (с учетом перспективы развития ЛВС), в состав ЛВС вводятся четыре switch-коммутатора D-link DGS-1024D.

Коммутатор D-Link Gigabit Ethernet DGS-1024D обладает неблокирующей архитектурой, что позволяет осуществлять фильтрацию и продвижение пакетов на скорости подключения, обеспечивая максимальную пропускную способность. Таблица MAC-адресов размером 8000 адресов обеспечивает хорошую масштабируемость даже для крупных сетей. Гигабитный коммутатор DGS-1024D поддерживает автоматическую установку plug and play. При этом никаких дополнительных настроек не требуется. Все порты поддерживают автоматическое определение полярности MDI/MDIX. Это исключает необходимость использования кроссированных кабелей или выделенных портов uplink. Кроме того, коммутатор поддерживает автоматическое определение скорости (10, 100 или 1000 Мбит/с) на каждом порту, выбирая максимально возможную в данном случае скорость и обеспечивая оптимальную производительность.

В результате анализа рынка стационарных ПК, которые предполагается использовать для расширения ЛВС Новошахтинского почтамта при модернизации, выбор был остановлен на моноблоке. Основными преимуществами этого класса современных ПК являются их компактность, минимальное количество кабелей (достаточно кабеля питания и сетевого кабеля, а при беспроводном доступе - только кабеля питания) и достаточно высокая мобильность (легко перенести ПК на другой стол и даже в другую комнату, организовав доступ к ЛВС по WiFi). Проанализировав российский рынок моноблоков и взяв за основу критерий оптимального соотношения «цена – качество», выбираем моноблок Acer Aspire ZS600 (размер экрана 23 дюйма, разрешение экрана 1920x1080, экран сенсорный, установлена ОС Windows 8, линейка процессора Intel Core i3, частота процессора - 3300 Мгц , количество ядер процессора – 2, размер жесткого диска - 1000 Гб, размер оперативной памяти - 4096 Мб, размер памяти видеокарты - 2048 Мб, тип графического процессора nVidia GeForce GT 640M, тип оптического привода DVD-RW, кардридер, Wi-Fi, Bluetooth, Web-камера, аудиосистема, микрофон.

Рассмотрено технико-экономическое обоснование эффективности решений проекта. В ходе экономического анализа данной разработки были вычислены полные затраты на создание локальной вычислительной сети – они составляют 590393 руб. Эти затраты окупаются за срок 0,953 года или 11,44 месяцев. Внутренняя норма доходности составит 49,17 %. Разработка сохранит эффективность не менее пяти лет. За пять лет эксплуатации она принесет чистый дисконтированный доход в размере 976753 руб. Расчеты показывают, что разработка является выгодной.

Литература:

1. Акропов П.Ц. Компьютерные сети. Принципы, технологии, протоколы. 2009. - 332с.

2. Блэк Ю. «Сети ЭВМ: протоколы, стандарты, интерфейсы». М.: Мир, 2010 г. – 358 с.
3. Боккер П. Цифровая сеть с интеграцией служб. Понятия, методы, системы: Пер. с нем. М.: Радио и связь, 2010. – 212 с.
4. Булгак В.Б., Варакин Л.Е., Ивашкевич Ю.К., Москвитин В.Д., Осипов В.Г. Концепция развития связи Российской Федерации. М.: Радио и связь, 2010. - 310 с.

Ю.В. Соболев

АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЁННЫХ ЦЕНТРОВ ОБСЛУЖИВАНИЯ ВЫЗОВОВ

Поволжский Государственный Университет Телекоммуникаций и Информатики (ПГУТИ), г. Самара

Ключевые слова: распределенные центры обслуживания вызовов, автоматическое распределение вызовов, весовые коэффициенты, операторы, заявки, Байесовская модель.

Проведен анализ алгоритмов функционирования распределенных центров обслуживания вызовов. Для анализа работы распределенных схем применима Байесовская модель обработки нечисловой, неточной и неполной информации о состоянии объекта. Данная модель позволяет определить вероятность некоторого события на основе данных о других событиях (в данном случае, насколько полная будет информация о состоянии ресурсов другого центра).

U.V. Sobolev

ALGORITHMS OPERATING THE DISTRIBUTED CALL CENTERS

Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara

Keywords: distributed call centers, automatic call distribution, weights, operators, application, Bayesian model.

The analysis of the algorithms of distributed call centers. For performance analysis of distributed schemes apply Bayesian model for non-numeric processing, inaccurate and incomplete information about the state of the object. This model allows to determine the probability of some event based on other events (in this case, how complete is the information about the state of other resources centre).

Под распределённым центром обслуживания вызовов (РЦОВ) понимается совокупность территориально разнесенных и информационно связанных между собой региональных ЦОВ, предоставляющих услуги клиентам с помощью операторов или автоматически и использующих единые правила обработки и маршрутизации вызовов [1].

Принципиальным отличием распределённого ЦОВ от централизованного является возможность обеспечения более высокого качества обслуживания вызовов и более экономичного использования ресурсов за счет перемаршрутизации вызовов в другой центр при отсутствии свободных ресурсов в данном центре [2].

Распределённые центры могут иметь различную структуру. При использовании иерархической структуры в сети имеется один центральный ЦОВ, в котором хранится база данных о состоянии всех ЦОВ сети. Информация из этой базы данных используется всеми центрами для осуществления оптимальной маршрутизации вызова в сети. В полностью распределенной структуре все ЦОВ функционально равнозначны и обмениваются информацией непосредственно друг с другом [2, 3].

В настоящее время имеющиеся теоретические исследования посвящены в основном централизованным ЦОВ. В моделях распределенных ЦОВ должны быть учтены особенности используемых алгоритмов маршрутизации вызовов к другому центру сети.

При рассмотрении алгоритмов маршрутизации вызовов в распределённом ЦОВ можно выделить три основных варианта использования информации о состоянии ресурсов других центров [1]:

- наличие полной информации (например, состояние очереди ожидающих вызовов, занятость операторов, наличие свободного оператора с требуемым уровнем знаний и др.), что позволяет обеспечить наивысшее качество обслуживания вызова;
- полное отсутствие какой-либо информации, при этом вызов направляется случайным образом в один из центров;
- наличие частичной информации, причём полнота информации может описываться некоторым случайным законом.

Последний вариант в наибольшей степени соответствует практическим ситуациям и интересен с точки зрения теоретических исследований.

Для уменьшения времени нахождения вызова в очереди к операторам распределенного ЦОВ могут применяться различные комбинированные схемы обслуживания. Например, схема, которая позволяет виртуально выстраивать вызовы в очередь в два и более ЦОВ. Понятие «виртуально» означает, что фактически резервируется свободная соединительная линия к тем ЦОВ, у которых предполагаемое пороговое значение нахождения вызова в очереди минимальное (или, возможно, ее нет). При каждом поступлении вызова оценивается время его ожидания в очереди. Если ожидается обслуживание в заданных временных рамках, например, 20 секунд, тогда вызов ждёт ответа оператора в этом ЦОВ. Если же ожидаемая задержка выше этого порогового значения, тогда происходит передача вызова в другой ЦОВ, имеющий наименьшую прогнозируемую задержку [4].

Именно комбинированные схемы способны обеспечить наибольшую производительность и качество работы распределенных ЦОВ. Однако в этом случае необходимо использовать более сложные модели теории массового обслуживания, учитывающие нестационарность и неточность представления параметров модели.

Для анализа работы подобных схем применима Байесовская модель обработки нечисловой, неточной и неполной информации о состоянии объекта. Данная модель позволяет определить вероятность некоторого события на основе данных о других событиях (в нашем случае, насколько полная будет информация о состоянии ресурсов другого центра). Это решение описывается формулой полной вероятности [2, 4]:

$$P\left(p(B);w\right)=\sum_{i=1}^{m} w_i\, p\left(B/A_i\right), \qquad (1)$$

где $p(B/A_i)$ - вероятность события «B» при условии, что произошло альтернативное событие $A_i:\left(A_i\cap A_j=0, i\neq j, A_1\cup\ldots\cup A_m=\Omega\right)$.

w_i - весовой коэффициент, который характеризует вероятность и частоту появления данного события;

Ω - пространство всех возможных событий A;

m – число возможных событий A_i;

$p(B)$ – вероятность события «B».

В нашем случае событие «B» – направление вызова в другой (какой-то конкретный) ЦОВ.

События «A_i» - то множество постоянно меняющихся событий, которые описывают состояние i-го ЦОВ в данный момент времени.

Основной проблемой является нахождение весовых коэффициентов $w_1\ldots w_n$, каждый из которых, есть – часть информации о состоянии распределённых ЦОВ, необходимой для маршрутизации вызовов.

Так называемые «весовые коэффициенты» $w_1\ldots w_n$ формируются и хранятся в конкретных блоках ACD (автоматическое распределение вызовов), а именно:

- в блоке RIS (Router of Internal Signaling), где формируется и кодируется, а также подготавливается информация о текущем состоянии операторов для возможной передачи в другие ЦОВ сети;

– в блоке DB (Database Server), где находится информация обо всех операторах данного ЦОВ, а также их состояние в режиме реального времени.

Необходимо, чтобы в процессе обслуживания вызовов распределёнными ЦОВ, ACD различных ЦОВ обменивались между собой информацией для случая возможной маршрутизации вызовов.

Возможные варианты сбора информации, описываемой весовыми коэффициентами $w_1 \ldots w_n$ [5]:

1. При наличии центрального ЦОВ. В центральный ЦОВ поступает информация необходимая для маршрутизации вызовов, которая собирается путём периодического опроса ACD ЦОВ, входящих в сеть. При поступлении вызова в любой из ЦОВ входящий в сеть, одновременно из центрального ЦОВ поступает информация необходимая для возможной маршрутизации вызова в другие ЦОВ.
   Этот метод обеспечивает наиболее корректную (с наименьшими затратами ресурса сети) работоспособность распределённого ЦОВ, за счёт существования алгоритма по сбору информации со всех ЦОВ сети.
2. Отсутствует центральный ЦОВ. Текущая информация о состоянии операторов хранится непосредственно в ACD каждого из ЦОВ. При поступлении вызова в один из ЦОВ, одновременно с ним с каждого из ЦОВ входящих в сеть поступает информация необходимая для возможной маршрутизации.

Этот метод отличается от предыдущего тем, что в этом варианте ёще не рассмотрены следующие моменты:

1. В каком порядке ACD ЦОВ будут передавать информацию в запрашиваемый ЦОВ.
2. Как будет осуществляться анализ поступающей информации.
3. Сколько времени потребуется для принятия единственно верного оптимального решения.

Таким образом, для реализации эффективной работы центров необходимо своевременно получать максимальную информацию о загрузке.

Литература:

1. Росляков, А.В. Анализ гомогенной модели распределенного центра обслуживания вызовов как единой команды / А.В. Росляков, Е.В. Глушак // T-Comm. Телекоммуникации и транспорт. - 2013. - №7. – С. 102 – 105.

2. Глушак, Е.В. Анализ гомогенной модели распределенного центра обслуживания вызовов / Е.В. Глушак, А.В. Росляков // Инфокоммуникационные технологии. – 2013. – Т.12, №3. – С. 23 – 26.

3. Глушак, Е.В. Оценка эффективности применения алгоритма интеллектуального управления входящими вызовами при различных вариантах информированности о состоянии центров обслуживания вызовов / Е.В. Глушак // Инфокоммуникационные технологии. – 2014. – Т.12, №2. – С. 25 – 31.

4. Глушак, Е.В. Экспериментальное исследование модели РЦОВ на основе имитационного моделирования / Е.В. Глушак, А.В. Росляков // T-Comm. Телекоммуникации и транспорт. - 2014. - №11. – С. 42 – 46.

5. Глушак, Е.В. Исследование рефлексивной модели функционирования распределенных центров обслуживания вызовов / Е.В. Глушак // Труды Международной молодежной научно-практической конференции СКФ МТУСИ «ИНФОКОМ-2013», Ростов-на-Дону, 2013. – С. 381 – 384.

В.А. Кочетков, И.В. Солдатиков, А.Е. Черкасов

АНАЛИЗ ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЕЙ КОНВЕРГИРОВАННЫХ СИСТЕМ MIMO-UWB

Академия Федеральной службы охраны, г. Орел, Россия

Ключевые слова: сверхширокополосная беспроводная связь, антенные системы со многими входами и выходами, высокоскоростная передача данных, многоэлементные антенны, подавление помех, среда с многолучевым распространением.

Представлены результаты качественного анализа потенциальных возможностей систем *UWB* и *MIMO* при решении задач расширения частотного диапазона, повышения скорости передачи данных, подавления помех, обеспечения ЭМС РЭС и возможные направления упрощения технологической реализации приемопередатчиков систем сверхширокополосной беспроводной связи.

V.A. Kochetkov, I.V. Soldatikov, A.E. Cherkasov

THE ANALYSIS OF MIMO-UWB CONVERGED SYSTEMS POTENTIALITY

Academy of Federal Guard Service of Russian Federation, Orel, Russia

Keywords: wideband wireless communication, antenna systems with many entries and outputs, high-speed data communication, multiple-unit antenna, interference rejection, ambience with multiracing spreading.

The presented results of the qualitative analysis of the potential possibilities of the UWB and MIMO systems when soloing problems of the expansion of the frequency range, multiple antenna balancings, provision EMS RES and possible directions of the simplification to technological realization transmitting –receiving systems of wideband wireless communication enhancing the speed of date transmission.

За последние 10–15 лет интерес к системам сверхширокополосной связи – системам *UWB* (*ultra wideband*) как за рубежом, так и в нашей стране значительно вырос, о чем свидетельствует постоянно увеличивающийся поток публикаций и изданий [1-5]. Это одно из динамичных направлений развития беспроводных телекоммуникационных технологий. Изначально, родившись из радиолокации, направление сверхширокополосной связи как технологии беспроводного доступа нашло отражение сегодня в ряде международных стандартов, поддержано многими производителями и промышленными альянсами телекоммуникационного радиооборудования, такими как *Intel* и *Motorolla* [3].

На развитие систем сверхширокополосной связи значительное влияние оказали отечественные ученые и специалисты – Л.Ю. Астанин, Ю.Б. Кобзарев, А.Ф. Кардо-Сысоев, В.В. Мелешко, Н.В. Зернов и ряд других. Пионерские работы по *UWB* системам с кодовым разделением каналов были проведены в СССР в восьмидесятых годах в Горьковском политехническом институте [4, С.16]. Затем была взята пауза в теоретических исследованиях анализа возможностей и построения систем *UWB* вплоть до середины 2000-х годов, когда существующие системы широкополосного беспроводного доступа – *Wi-Fi* и *WiMax*, прежде всего, столкнулись с трудностями по передаче и предоставлению высокоскоростных мультисервисных контентов своим абонентам.

За рубежом, причем как на западе (США, Германия), так и на востоке (Япония, Китай, Корея) теоретические и экспериментальные работы в области сверхширокополосных систем связи не только не прекращались, но и активизировались. В западных странах уже с начала 90-х годов было введено понятие "сверхширокополосная система", которое после неоднократных корректировок в 2000-х годах составило основу международных стандартов семейства 802.15.

К достоинствам систем *UWB* исследователи относят высокую помехозащищенность, адаптивность к сложной помеховой обстановке, низкий, шумоподобный уровень сигнала,

рациональное использование частотного ресурса, сложность перехвата и постановки различного вида преднамеренных помех, обеспечение передачи данных в условиях многолучевости, сравнительно простую техническую реализацию компонентов системы – приемопередающих устройств, антенн, источников питания. В UWB системах для связи используется самый широкий из распространённых сегодня технологий беспроводной связи диапазон частот – от 3 до 10,6 ГГц [5, С.1279] (диапазон, выделенный в США; в России этот диапазон ограничен полосой частот 4,95 – 8 ГГц [2, С.52]).

Широкая полоса частот позволяет системам *UWB* достигать больших значений скорости передачи данных – до 480 Мбит/с, но на очень малых расстояниях – до 3 м. На расстоянии до 10 м технология позволяет достичь скорости передачи около 110 Мбит/с. Количественные значения скорости передачи и расстояния, на которые передаются сверхширокополосные сигналы, определяют сущность основной проблемы технологии *UWB*: пропускная способность резко падает с увеличением расстояния – гораздо быстрее, чем у стандарта беспроводных сетей 802.11a/b/g, обеспечивающих до 54 Мбит/с на дистанции до 100 м. Это связано с тем, что дисперсия излучения электромагнитной волны в радиоканале приводит к значительным искажениям фронта широкополосного сигнала по сравнению с узкополосными радиосигналами. С увеличением расстояния искажение накапливается и приводит к тому, что сигнал на входе приемного устройства уже имеет форму, сильно отличающуюся от той, что была сформирована передающим трактом. В системах *UWB* приемопередающая антенна, как правило, в отличие от узкополосных систем беспроводной связи, не сохраняет свои характеристики неизменными в диапазоне частот шириной в несколько гигагерц. Для оценки качественных характеристик антенных систем *UWB* используют передаточную функцию. Однако, точное представление передаточной функции для передающей и приемной антенны сверхширокополосной системы в аналитическом виде представляет трудную задачу из-за сложных частотно-зависимых свойств антенн.

Одним из возможных инструментов, способных изменить ситуацию в решении проблемы с малыми расстояниями передачи в системах сверхширокополосной связи, являются системы *MIMO* (*Multiple Input Multiple Output*), реализующие следующие подходы улучшения системных показателей беспроводных технологий: пространственное мультиплексирование, пространственное разнесение, формирование диаграммы направленности (ДН) специальной формы. Системы *UWB* можно классифицировать по видам используемой модуляции [4, С. 271-272]:

- импульсное радио с коррекцией во временной области;
- передача сигналов на одной несущей с коррекцией в частотной области;
- передача на нескольких несущих с использованием соответствующего кодирования (*OFDM*).

Реализация тех или иных подходов улучшения системных показателей технологий беспроводного доступа, позволяет говорить об общности задач, решаемых системами *MIMO* и *UWB*. Конвергенция технологий *MIMO* и *UWB*, подразумевает использование различных комбинаций перечисленных подходов, например, формирование диаграммы направленности специальной формы с передачей сигналов методом импульсного радио или объединение функций сверхширокополосной системы с несколькими несущими и пространственное мультиплексирование.

Качественный анализ потенциальных (теоретических) возможностей конвергированных технологий *MIMO-UWB*, показывает, что увеличение зоны покрытия системы сверхширокополосной связи возможно за счет использования антенных решеток (АР) с многоэлементными антеннами. Многоэлементные АР при каждом удвоении числа излучающих элементов решетки обеспечивают усиление, примерно, равное 3 дБ [6, С. 59], что является основным фактором увеличения области покрытия. Если же многоэлементные антенные системы *MIMO-UWB* разнести пространственно, то получаемый выигрыш увеличится, что приведет к еще большей области покрытия. При этом необходимо учитывать ряд сложностей, как теоретического, так и технологического (конструктивного) характера:

- выигрыш от пространственного разнесения уменьшается с ростом полосы пропускания радиотехнической системы;
- количественное значение дополнительного усиления от пространственного разнесения предстоит определять на практике с учетом характеристик антенн;

– применение многоэлементных АР для формирования ДН специальной формы потребует соблюдения жестких норм на значения ЭИИМ, установленных регулирующими и контролирующими органами (*FCC* в США, ГКРЧ – в нашей стране).

Формирование диаграммы направленности с учетом пространственного разнесения, кроме увеличения зоны покрытия, может существенно снизить уровни помех за счет компенсации амплитудно-фазовых распределений мешающих сигналов, в том числе созданных преднамеренно, которые попадают с разных направлений на антенную решетку приемника. В системе *UWB* без технологий *MIMO* такая компенсация должна выполняться на весь рабочий частотный диапазон, что определяет необходимость в каждой ветви многоэлементной антенны фильтра с одинаковыми задержками времени или управляемых фазовращателей. Совокупность фильтров и фазовращателей может быть технологически выполнена на аналоговой элементной базе, так как цифровое формирование ДН на сегодняшний день затруднительно из-за высоких частот дискретизации, составляющих гигагерцы [7, С.13]. Последнее обстоятельство безусловно будет играть против высокой технологичности, малых массогабаритных показателей и веса устройств сверхширокополосных систем. Здесь также необходимы дальнейшие исследования для более глубокого понимания рассматриваемых явлений и разработки достоверных положений, пригодных для практики.

Другим аспектом анализа совместного использования технологий *UWB* и *MIMO*, является оценка увеличения скорости передачи такой беспроводной системы связи за счет роста числа передающих и приемных антенн. Для модели замираний Накагами в каналах *UWB* [8, С.661-662] пропускная способность канала *MIMO-UWB* системы должна возрастать по линейному закону. Аналогия узкополосных и широкополосных каналов *MIMO*- систем с релеевскими замираниями обусловила большой исследовательский интерес в области систем связи *MIMO* в тех случаях, когда важно обеспечить эффективное использование спектра частот [4, С.273], технология *MIMO* становится применимой и для сверхширокополосных каналов.

Технологические аспекты анализа касаются вопросов реализуемости систем UWB с учетом особенностей частотного диапазона 3-10 ГГц. На современном этапе развития элементной базы и технологических возможностей промышленности серьезной задачей является разработка миниатюрных антенн, усилителей и фильтров для работы в СВЧ диапазонах, которые должны обеспечивать требуемое усиление и малую потребляемую мощность. В схемах, реализующих методы *OFDM* (*Orthogonal frequency-division multiplexing* – мультиплексирование с ортогональным частотным разделением каналов), с несколькими несущими требуется больше аппаратных средств, реализующих методы цифровой обработки сигналов, так как расширение рабочего диапазона частот происходит за счет использования нескольких поднесущих. В таком случае системы *MIMO-UWB* могут стать альтернативой, с технологической точки зрения, системам сверхширокополосной связи с одной антенной. Качественный анализ процедур аппаратной реализации обработки сигналов в *MIMO-UWB* системах, показывает, что при использовании N поднесущих и двух передающих и приемных антенн необходимо выполнить два БПФ на $N/2$ точек, тогда как в системе *SISO* (*Single Input Single Output*) необходимо произвести одно БПФ, но для N точек.

Таким образом, в отличие от узкополосных систем беспроводного доступа (*Wi-Fi, WiMax*), в которых технология *MIMO* применяется, как правило, для эффективного использования спектра, в системах сверхширокополосной связи применение этой технологии может привести к более простой реализации технических устройств систем *UWB* и как минимум к не удорожанию серийно выпускаемых компонентов и подсистем, входящих в их состав.

На современном этапе развития технологий сверхширокополосной связи, основные трудности разработки таких систем могут быть преодолены путем проведения качественной и всесторонней количественной оценки применимости традиционных методов, использующих многоэлементные антенные системы наряду с методами пространственного мультиплексирования и моделированием пространственных каналов передачи радиосигналов.

Итак, проведенный анализ потенциальных возможностей объединения технологий *MIMO* и *UWB*, свидетельствует о линейной зависимости пропускной способности канала сверхширокополосной системы от количества приемопередающих антенн и числа излучателей многоэлементных антенных систем. Возможно увеличение зон покрытия системами сверхширокополосной связи за счет пространственного разнесения, реализуемого на основе

технологий *MIMO*. Формирование диаграмм направленности специальной формы в системах сверхширокополосной связи для подавления помех не приведет к технологическому усложнению процессов производства подсистем и компонентов *UWB* и их удорожанию.

Литература:

1. Урядников Ю.Ф., Аджемов С.С. Сверхширокополосная связь. Теория и применение. – М.: СОЛОН-Пресс, 2005.
2. Соколова М.В. Сверхширокополосная беспроводная связь: история и перспективы развития // T-Comm – Телекоммуникации и Транспорт, 2008, № 2, с. 50-53.
3. Лурье С. Сверхширокополосная связь UWB: что это такое и для чего это нужно? Связь с периферийными модулями – с проводами и без // http://www.ixbt.com/comm/uwb-tech.shtml.
4. Арслан Х., Чен Чж. Н., Бенедетто М. Сверхширокополосная беспроводная связь. – М.: Техносфера, 2012.
5. Дмитриев А.С., Ефремова Е.В., Клецов А.В. и др. Сверхширокополосная беспроводная связь и сенсорные сети // Радиотехника и электроника, 2008, том 53, № 10, с. 1278-1289.
6. Хансен Р.С. Фазированные антенные решетки. Пер. с англ. Под ред. А.И. Синани. Второе изд. – М.: Техносфера, 2012.
7. Ганзий Д.Д., Трошин Г.И. Элементная база и узлы адаптивных антенных устройств. – М.: Новые технологии, 2011.
8. Прокис Дж. Цифровая связь. Пер с англ. / Под ред. Д.Д. Кловского. – М.: Радио и связь, 2000.

И.А. Сосновский, А.А. Манин, В.Е. Герасименко

АВТОМАТИЗИРОВАННЫЙ РАСЧЕТ ПАРАМЕТРОВ ТРАФИКА СЕТИ ETHERNET С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПРОДУКТА MICROSOFT EXCEL

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: Сеть Ethernet, сеть компании, расчёт трафика, автоматизация расчёта, программное обеспечение, Microsoft Excel.

В статье рассматривается возможность применения среды Microsoft Excel для решения задач автоматизированного расчёта параметров сети Ethernet. Показана возможность применения методики приближённого расчета трафика в ветвях сети. Продемонстрирован один из возможных вариантов построения сети и его графическое представление. Отмечены особенности реализации методик в рассматриваемой среде и возможности математического аппарата. Показанная возможность автоматизации расчёта трафика в ветвях сети, позволит значительно сократить время оценки влияния изменения нагрузки в существующей сети.

I.A. Sosnovsky, A.A. Manin, V.E. Gerasimenko

AUTOMATED CALCULATION OF TRAFFIC PARAMETERS ETHERNET NETWORK USING SOFTWARE MICROSOFT EXCEL

North-Caucasian branch of the Moscow technical university of communications and informatics, Rostov-on-Don, Russia

Keywords: Network Ethernet, network companies, the calculation of traffic, the automation of calculation software, Microsoft Excel.

The article discusses the possibility of using Microsoft Excel environment to meet the challenges of the automated calculation of the parameters of the Ethernet. The possibility of using methods of

approximate calculation of traffic in the branches of the network. Demonstrated one possible construction of a network and its graphical representation. The features of the implementation techniques in the medium and possibilities of the mathematical apparatus. Shown the ability to automate the calculation of traffic in the branches of the network, will greatly reduce the time assessments of the load on the existing network.

В современном мире все большую роль играют инфокоммуникации. Уже невозможно представить предприятие, корпорацию или компанию, не имеющую в своём составе локальной вычислительной сети, с возможностью выхода в глобальную сеть Internet. Эти сети могут выполнять различные функции, а значит, включают в себя оборудование широкого спектра (ПК, IP-телефоны, видеокамеры, специальные терминалы).

К настоящему времени разработано множество методик по расчету параметров сети. Они реализуются в существующем программном обеспечении, которое реализуется как коммерческий продукт. Стоимость такого продукта велика, а применяется он не ежедневно.

Необходимость применения таких продуктов связана с тем, что структура сети не статична. Она периодически подвергается изменению для решения новых задач или более эффективного решения текущих. Например, потребность реализовать в компании дополнительные меры по контролю за территорией объекта приводит к необходимости подключения к сети камер наблюдения, при работе которых появляется весьма не малая дополнительная нагрузка на сеть.

Это приводит к необходимости очередного расчёта сети с изменёнными исходными данными. А при рассмотрении различных вариантов подключения оборудования к сети задача становится чрезмерно трудозатратной.

В свою очередь это приводит к необходимости создания инструментария для расчетов параметров сети, а также выбора коммутационного оборудования, способного выполнять возложенные на него задачи.

Отличным решением задачи проектирования и расчета параметров сети является продукт Microsoft Excel, входящий в пакет офисных программ. Его использование целесообразно, так как данное программное обеспечение установлено почти на всех рабочих компьютерах и не требует специальных навыков и умений. Интерфейс позволяет в наглядной форме в виде графиков, таблиц, диаграмм представлять необходимую информацию по потокам в ветвях, нагрузке, а также тяготение в сети. Для непосредственного расчёта в программе имеются множество стандартных расчётных функций.

С помощью данного инструмента можно проектировать сеть любой сложности, с учетом изменения состава оборудования и изменения параметров трафика. Методика расчета реализована в методическом описании «Расчет локальной вычислительной сети Ethernet» [1,2]. На рисунке 1 представлен фрагмент реализации локальной вычислительной сети предприятия, выполненный с помощью программы Microsoft Excel.

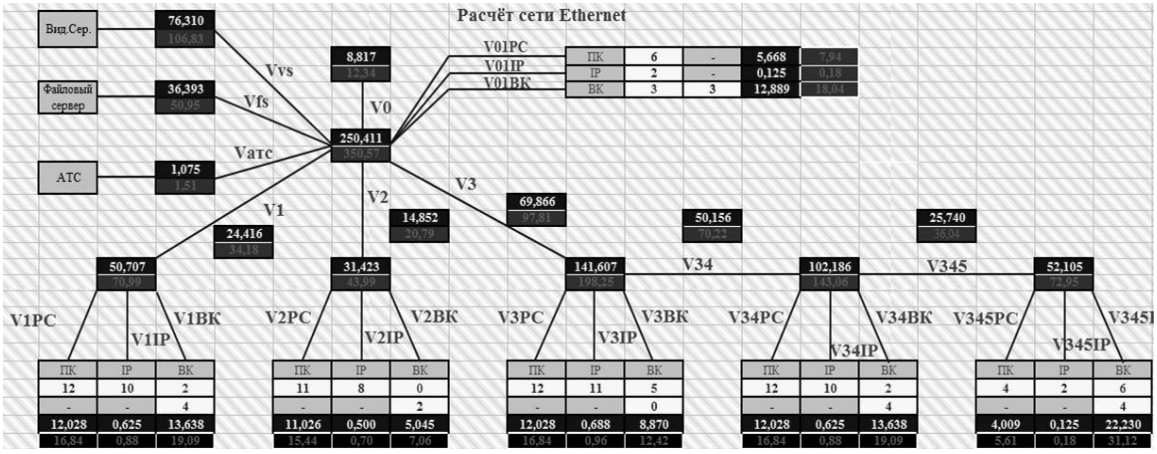


Рисунок 1. Фрагмент, представляющий структурную схему сети

На предприятии имеются 5 основных отделов, снабженных ПК, IP-телефонами, а также видеокамерами. Каждое из оконечных устройств генерирует разный тип трафика. Количество оборудования прописано в полях таблицы, отмеченных светлым фоном. Таблицы стоит

располагать возле коммутаторов. Кроме этого, в схеме имеются автоматическая телефонная станция (АТС), файловый сервер и видеосервер. На предприятии установлены видеокамеры наружного и внутреннего наблюдения, что вносит различия в величину трафика самих камер, так как размер и частота смены кадров наружной видеокамеры обычно должна быть выше, чем у внутренней. Это диктуется решаемыми задачами. Также примем во внимание, что вне отделов будет располагаться определенное количество ПК и IP-телефонов.

В расчётах величина трафика с камер рассчитывается с учётом кодека, используемого камерой, размера кадра, глубины цвета и количества кадров, предаваемых в секунду. Трафик, исходящий от ПК, может носить различный характер: как «волновой», при передаче данных, так и потоковый, при передаче аудио и видео. Телефонный поток будем считать одинаковым и примем 64 кбит/с.

В данной методике рассчитывается как фактический трафик (представлен на синем фоне), так и трафик с учетом запаса на развитие сети (на черном фоне).

Как было сказано раньше, благодаря большим функциональным возможностям Microsoft Excel, был реализован более глубокий анализ сети по средствам регулирования интенсивности нагрузки в прямом и обратном направлениях (так, к примеру, при общении ПК-сервер величина информационного потока обычно выше в направлении сервер-ПК, нежели наоборот). Введен коэффициент пульсации трафика, чтобы максимально приблизить характер трафика к реальному, объединен трафик группы компьютеров, видеокамер и IP-телефонов с возможностью ручной конфигурации интенсивности нагрузки. На рисунке 2, на светлом фоне, представлена величина трафика с возможностью ручной корректировки, кбит/с.

34	**ПК-Int**	**0,05**	36	Кбит	40	% отправляется в телефонную сеть общего пользования
35	**Int-ПК**	**0,17**	122,4	Кбит		
36	**Кп**	**90**				
37	**Пк-Серв**	**0,15**	60	Кбит		
38	**Серв-ПК**	**1,5**	600	Кбит		
39	**Кп**	**50**				
40	**ПКгр-ПКгр**	**0,4**	160	Кбит		
41	**Кп**	**50**				
42	**ПКобщ-ПКобщ**	**0,12**	48	Кбит		
43	**Кп**	**50**				
44	**Внут**	**1816,5**	1816,5	Кбит		
45	**Видеокам внеш.**	**2583**	2583	Кбит		
46	**IP-тел.**	**64**	64	Кбит		

Рисунок 2. Фрагмент с окном ввода исходных

Весь информационный поток, проходящий непосредственно по ветвям, а также по сумме ветвей, можно представить в виде таблиц, которые наиболее информативно проиллюстрируют необходимую пользователю информацию. Фрагмент такой таблицы представлен на рисунке 3.

	V345PC	V345IP	V345BK	V345	V34PC	V34IP	V34BK	V34	V3PC	V3IP	V3BK	V3	V2PC	V2IP	V2BK	V2
ПК-Int	432	-	-	432	1296	-	-	1296	1296	-	-	1296	1188	-	-	1188
Int-ПК	489,6	-	-	489,6	1468,8	-	-	1468,8	1468,8	-	-	1468,8	1346,4	-	-	1346,4
Пк-Серв	240	-	-	240	720	-	-	720	720	-	-	720	660	-	-	660
Серв-ПК	2400	-	-	2400	7200	-	-	7200	7200	-	-	7200	6600	-	-	6600
ПКгр-ПКгр	640	-	-	-	1920	-	-	-	1920	-	-	-	1760	-	-	-
ПКобщ-ПКобщ	192	-	-	192	576	-	-	576	576	-	-	576	528	-	-	528
Видеокам внут	-	-	15498	15498	-	-	3633	3633	-	-	9082,5	9082,5	-	-	0	0
Внеш.	-	-	7266	7266	-	-	10332	10332	-	-	0	0	-	-	5166	5166
IP-тел.	-	128	-	128	-	640	-	640	-	704	-	704	-	512	-	512
Траф. в ветви	4393,6	128	22764	26645,6	13180,8	640	13965	52511,4	13180,8	704	9082,5	73558,7	12082,4	512	5166	16000,4
Скорость в ветви	4,291	0,125	22,230	26,021	12,872	0,625	13,638	51,281	12,872	0,688	8,870	71,835	11,799	0,500	5,045	15,625

Рисунок 3. Фрагмент таблицы информационных потоков в ветвях сети

Возможности использования данной среды ограничены лишь поставленной задачей. На примере реализованной методики видно, насколько информативно и практично может быть представлено оборудование, таблицы и необходимые численные значения. Также при внедрении нового оборудования не требуется переделывать или изменять всю схему сети, достаточно лишь изменить численные значения количества оборудования, а при необходимости добавить новые математические формулы, позволяющие объективно охарактеризовать величины информационного потока, специфичного для данного устройства.

Литература:
1. Нерсесянц А. А. Методическое пособие: Расчёт сети Ethernet. СКФ МТУСИ. - Ростов н/ Д, 2009. - 12с.
2. Манин А.А., Сосновский И.А., Герасименко В.Е. Автоматизированный расчет сети Ethernet. Инфоком-2014, труды Северо-Кавказск. филиала Московск. технич. ун-та связи и информатики, 22-25 апр./ СКФ МТУСИ. - Ростов н/ Д, 2014. С. 191-193.

И.А. Сосновский, А.А. Манин, В.Е. Герасименко

ИНТЕРАКТИВНАЯ СРЕДА ДЛЯ ИЗУЧЕНИЯ ПРОЦЕССОВ КОММУТАЦИИ В СЕТЯХ ETHERNET

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: Сеть Ethernet, коммутатор, коммутатор, программное обеспечение, моделирование.

В статье описано одни из возможных решений повышения эффективности подготовки специалистов в области связи. Повышение ожидается за счёт создания и применения программного обеспечение для моделирования логических процессов, происходящих при коммутации. Рассмотрено создание информационно логической модели коммутатора, которая позволяет показать внутренние процессы, происходящие в коммутаторе при решении задачи коммутации. Приведены вопросы, и последовательность их отработки, которые будут доступны при использовании программы. Определён общий вид форм и их информационное наполнение.

I.A. Sosnovsky, A.A. Manin, V.E. Gerasimenko

INTERACTIVE ENVIRONMENT FOR STUDYING THE PROCESS OF SWITCHING ETHERNET NETWORKS

North-Caucasian branch of the Moscow technical university of communications and informatics, Rostov-on-Don, Russia

Keywords: Network Ethernet, switch, switch, software modeling.

This article describes some of the possible solutions to improve the effectiveness of training in the field of communications. Rise is expected due to the creation and application software to simulate the logical processes occurring during switching. Consider creating awareness logical model of the switch, which allows you to show the internal processes occurring in the switch in solving the problem of switching. Are the questions, and the sequence of their mining, which will be available when using the program. Defined forms and the general form of their content.

В настоящее время существует большое количество разнообразного программного обеспечения (ПО) для выполнения расчётов по сетевым проектам, моделированию сетей. Однако ощущается нехватка программного продукта, направленного на пояснение механизмов и логики работы коммутационного оборудования. Данное ПО в процессе подготовки позволило бы значительно повысить эффективность изучения материала.

В работах [1,2] уже описывалось создание такого продукта. Его непосредственное применение на практике позволило получить устойчивые знания обучаемых при контроле знаний по данной теме.

Одним из непростых моментов для понимания и логического восприятия являются процессы, происходящие в коммутаторах Ethernet при решении задачи перенаправления информационных потоков в сети (коммутации). Однако от их понимания существенно зависит дальнейшее восприятие многих особенностей и нюансов работы сети.

Данная особенность требует разработки такого программного обеспечения, которое позволило бы наглядно показать процессы, протекающие в коммутаторе во все возможные моменты его работы, от ожидания кадра с информацией на входном порту до отправления его в адрес следующего сетевого узла.

Разрабатываемое ПО будет аналогичным по структуре программе, рассматриваемой в [1,2], и даст возможность реализовывать следующие функции:

- тестирование обучаемого и автоматическая оценка результатов;
- создание схемы сети, установленной заданием;
- определение необходимой информации для подключенных устройств;
- обучение коммутатора (заполнение таблиц коммутации);
- моделирование передачи информации между узлами сети;
- настройка виртуальных локальных сетей VLAN;
- моделирование работы сети с настроенными VLAN;
- проверка правильности выполняемых заданий;
- информационная поддержка проводимой работы;
- формирование отчёта о работе.

Тестирование будет организовано в стандартном виде с возможностью изменения критериев оценки, так как в различных дисциплинах данное тестирование будет иметь различную степень важности.

На рабочей панели будут установлены три соединённых между собой коммутатора. Подключение различных устройств будет производиться пользователем из выпадающего списка. Общий вид панели представлен на рисунке 1.

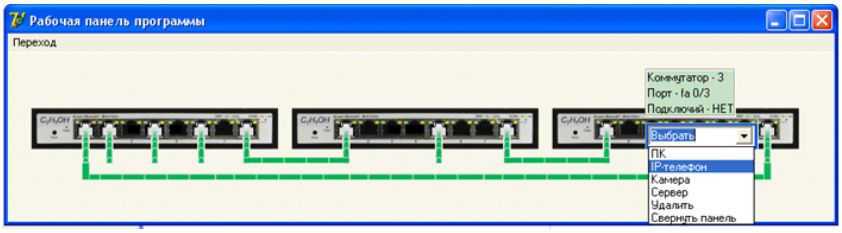


Рисунок 1. Общий вид рабочей панели программы

Состояние портов будет подсвечиваться при наведении на них указателем графического манипулятора.

Определение необходимой информации для подключённых устройств включает выбор для устройства MAC адреса. На этом же поле расположен конструктор для отправки информации в адрес других устройств. В нём определяются количество полей, их длина и содержание.

Текущее состояние коммутатора определяется содержанием записей в таблице коммутации. В программе для каждого коммутатора предусматривается возможность вызова формы с таблицей коммутации. Общий вид этой таблицы представлен на рисунке 2.

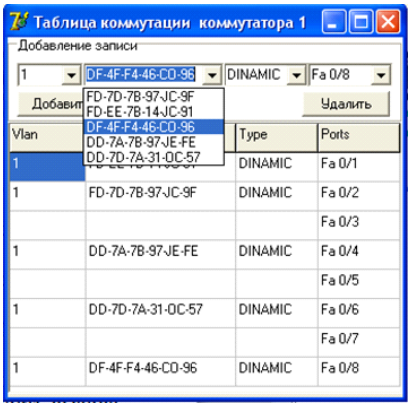


Рисунок 2. Общий вид таблицы коммутации

На форме существует поле добавления записи. В этом поле необходимо выбрать из выпадающих списков требуемые записи. При нажатии на кнопку «Добавить» запись будет введена в таблицу коммутации.

Моделирование передачи информации будет начинаться с формы устройства. На нём будут формироваться структура и содержание кадра Ethernet. Для этого обучаемый должен будет выбрать количество полей и их длину, а также произвести заполнение указанных полей.

После того, как кадр будет сформирован, нажимается кнопка «Отправить» и кадр отправляется на вход соответствующего порта коммутатора. Для избежания ошибок при заполнении полей кадра используется поля с автозаполнением поля из выпадающего списка. Общий вид формы представлен на рисунке 3.

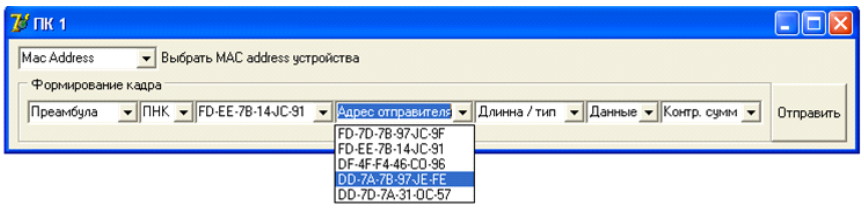


Рисунок 3. Форма сетевого устройства

При правильном заполнении появится таблица коммутации коммутатора и форма с моделью внутренней работы коммутатора. Данная форма приведена на рисунке 4.

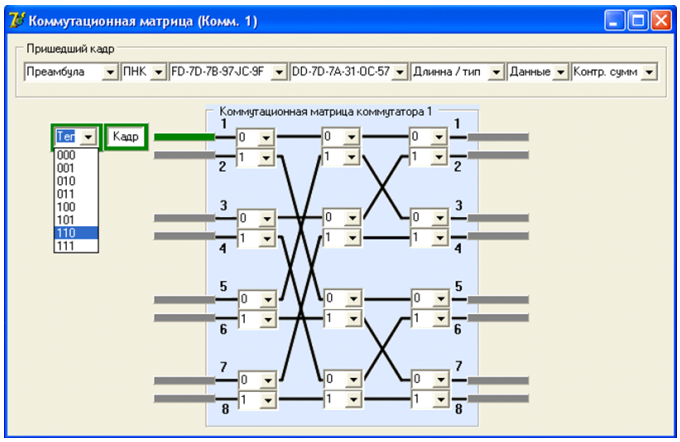


Рисунок 4. Форма с представлением коммутационной матрицы

На данной форме обучаемый производит поэтапное продвижение кадра от входного порта в направлении выходного. После того как кадр попадает на выходной порт, выводится либо коммутационная матрица следующего коммутатора, либо оконечное сетевое устройство.

Аналогичным образом программное обеспечение позволит осуществлять моделирование передачи кадров с учётом настроенных виртуальных сетей VLAN.

Все действия обучаемого будут отслеживаться и оцениваться модулем автоматической оценки.

Информационное сопровождение и вид представляемых графических материалов будет приближен к рекомендованному учебному материалу [3]. Это позволит улучшить восприятие тонкостей работы коммутатора.

С точки зрения автономности программный продукт будет способен работать без использования дополнительного программного обеспечения, однако для сохранения результатов требуется формирование отчёта. Данный отчёт будет представляться в среде Microsoft Excel и содержать информацию о выполненном тестовом занятии (количество правильных и неправильных ответов, оценка), выполненных заданиях и ошибках, допущенных при их выполнении.

Разрабатываемое программное обеспечение будет функционировать под управлением операционных систем Windows версий XP, 7, 8.

Литература:
1. Сосновский И. А., (75) Васильченко И.О. (25). Специальное программное обеспечение для изучения вопросов коммутации виртуальных каналов. Инфоком-2012: труды Северо-Кавказск. филиала Московск. технич. ун-та связи и информатики, 20-21 апр. / СКФ МТУСИ. – Ростов н/ Д, 2012. С. 146-149.
2. Сосновский И.А. (70), Болдырихин Н.В. (15), Венжега В.В. (15). Интерактивная среда изучения и моделирования процессов маршрутизации в IP-сетях. Инфоком-2013: труды Северо-Кавказск. филиала Московск. технич. ун-та связи и информатики, 22-25 апр./ СКФ МТУСИ. – Ростов н/ Д, 2013. С.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 3-е изд. – СПб.: Питер, 2009. – 958 с.

А.П. Пшеничников, М.С. Степанов

МОДЕЛИРОВАНИЕ ПРОЦЕССА ОБСЛУЖИВАНИЯ ВЫЗОВОВ В СОВРЕМЕННЫХ КОНТАКТ-ЦЕНТРАХ

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: контакт-центр, повторные вызовы, IVR, операторы, консультанты

Отмечены основные особенности построения контакт-центров указаны области их использования. Введены основные структурные элементы контакт-центра (IVR, ACD, операторы, консультанты) и рассмотрено их взаимодействие друг с другом. Построена обобщенная математическая модель контакт-центра, учитывающая основные особенности современных справочно-информационных служб. Приведена структурная схема обобщенной математической модели, включающая три основные стадии обслуживания заявки, подробно описаны ее компоненты. Сформулированы выводы и указано направление дальнейших исследований.

A.P. Pshenichnkov, M.S. Stepanov

THE MODELLING OF CALS SERVICING IN MODERN CONTACT-CENTERS

Moscow Technical University of Communication and Informatics

Keywords: contact-centers, repeated calls, contact-centers, mathematical models, IVR

Main features of contact-center design are mentioned, Basic structural elements of contact-center (IVR, ACD, operators, consultants) are described. Mathematical model of contact-center that include all the main features is obtained. Structural scheme of model is designed, all its components are described. Conclusions are made, direction for next researches is provided.

1.Введение.

В последние года индустрия контакт-центров развивается быстрыми темпами. Интерес к этой области телекоммуникаций не случаен и объясняется возможностями, которые предоставляют контакт-центры для повышения эффективности ведения бизнеса компаний, работающих в сфере торговли, транспорта, связи, банковского дела, обучения и безопасности. Контакт-центр предоставляет собой физическое (а в последнее время чаще виртуальное) место, где большое количество вызовов, поступающих от абонентов посредством телефонной связи, а также по сети Интернет, обрабатывается в целях предоставления клиенту затребованной информации. Ресурс, используемый в контакт-центре для обработки поступающих заявок, состоит из линий доступа, устройств интерактивного речевого ответа (IVR), операторов и консультантов. На практике каждая из перечисленных компонент ресурса ограничена, поэтому оценка необходимой по нагрузке величины ресурса и взаимосвязи ее отдельных составляющих является важной и актуальной задачей, решение которой необходимо для организации эффективной работы

контакт-центра. Для решения сформулированной задачи используется математическая модель. Прежде чем перейти к ее построению, перечислим основные составляющие функциональной модели контакт-центра.

К ним, прежде всего, относится система интерактивного речевого ответа IVR (Interactive Voice Response) позволяющая абонентам получать справочную информацию посредством ввода данных в режиме тонального набора. Обычно является первой стадией обработки клиентских заявок и применяется практически во всех контакт-центрах. Процент запросов, полностью обсуживаемых в IVR, зависит от сферы деятельности компании, но, согласно статистике, в среднем составляет 60-70% от общего числа поступивших вызовов. [1]. Далее заявка обрабатывается системой ACD (Automatical Call Distribution), в случае, если обслуживания на IVR оказалось недостаточно. Заявка ставится в очередь, и в процессе ожидания клиент может прослушать, например, различную справочную или рекламную информацию. Фактически ACD осуществляет маршрутизацию вызовов в различные операторские группы. Информация, на основе которой выполняется маршрутизация, собирается в процессе обработки вызова на IVR. Операторы выполняют обработку входящих и осуществляют вторую стадию обслуживания поступающих заявок. В некоторых случаях общей информации, предоставляемой операторами, может быть недостаточно. В таком случае вызов маршрутизируется в одну из групп консультантов для получения специализированной информации. Это третья стадия обслуживания. Стоит отметить, что заработная плата операторов и консультантов является основной статьей расходов для компаний, имеющих свой контакт-центр [1].

2. Описание модели.

В [2-3] построена математическая модель контакт-центра, учитывающая наличие системы интерактивного речевого ответа IVR и разделения операторов по квалификации. В модели присутствуют три введенные выше стадии обслуживания вызова в контакт-центре. Структурная схема модели показана на рис.1.

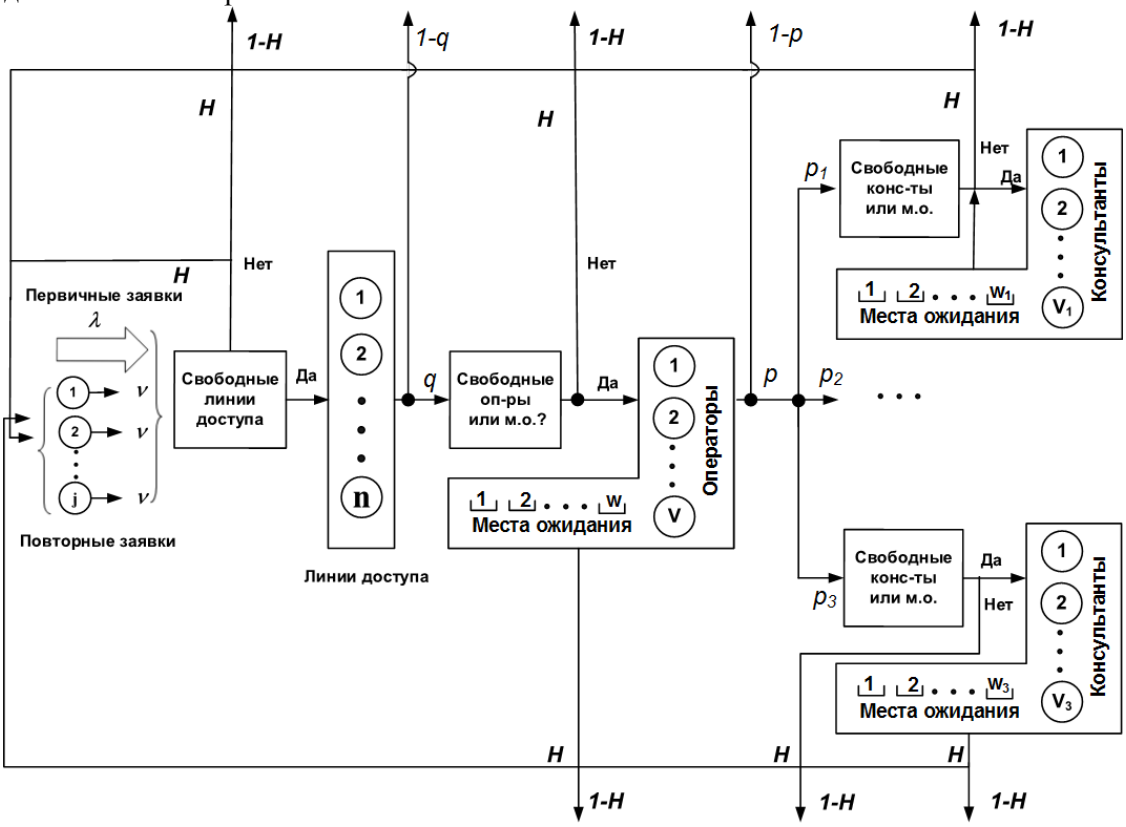


Рисунок 1. Структурная схема обобщенной математической модели современного контакт-центра.

Рассмотрим ее компоненты более детально. Пусть n - максимально возможное число вызовов, которые одновременно могут обслуживаться в IVR, v - число операторов, а через v_k -

число консультантов в k-ой группе, $k=1,2,...,m.$ Будем считать, что поток первичных запросов на обслуживание от пользователей услуг контакт-центра подчиняется закону Пуассона с интенсивностью λ. Кроме того в системе присутствует потоки повторных запросов, образованные в результате отсутствия свободных мест в IVR, операторов или консультантов, а также после неудачного завершения времени ожидания начала обслуживания. Предположим, что длительность обслуживания вызова системой IVR имеет экспоненциальное распределение с параметром α_1, оператором - экспоненциальное распределение с параметром α_2, k-ой группой консультантов - экспоненциальное распределение с параметром β_k. Обозначим через q и p вероятности того, что что после обслуживания на IVR клиенту потребуется помощь соответственно оператора и консультанта. Количество групп консультантов в системе обозначим через m. Вероятность выбора k-ой группы примем за p_k, где $k=1,2,...,m.$ В случае получения отказа в обслуживании, клиент независимо от различаемой в модели причины отказа в обслуживании с вероятностью H предпринимает повторную попытку дозвониться, которая обслуживается по тем же, правилам, что и первичная а с дополнительной вероятностью $1-H$ клиент покидает систему необслуженным

В модели учитывается возможность постановки вызова на ожидание, в случае, если в момент его поступления отсутствуют свободные операторы и консультанты. Примем за L число мест ожидания освобождения одного из v занятых операторов, а за L_k - число мест ожидания освобождения одного из v_k занятых консультантов, $k=1,2,...,m.$ Время ожидания оператора ограничено случайной величиной, имеющей экспоненциальное распределение с параметром σ, у консультанта - σ_k, где $k=1,2,...,m.$

Заключение.

Приведена структурная схема математической модели современной справочно-информационной службы, учитывающая основные особенности и этапы обслуживания клиентских запросов. В [3] для построенной модели приведен алгоритм оценки основных показателей качества обслуживания поступающих заявок, основанный на решении системы уравнений равновесия. В дальнейшем предполагается использование модели для разработки методик оценки различных характеристик работы контакт-центров.

Литература:

1. Shrinivasan R., Talim J., Wang J. Perfomance analysis of a call center with interactive voice response units / Sociedad de Estadistica e Investigacion Operativa Top (2004) Vol. 12, No. 1, pp. 91-110

2. Пшеничников А.П., Степанов М.С. Обобщенная модель call-центра /T-comm. Телекоммуникации и транспорт. 2011. №7. С.125-129

3. Степанов С.Н., Степанов М.С. Построение и анализ обобщенной модели контакт-центра /АиТ. 2014. №11. С.55-69.

А.Б. Суворов, *Т.В. Суворова, **Е.А. Усошина

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ВИБРОДИАГНОСТИКИ ДЛЯ ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК ПРОХОДЯЩЕГО ЖЕЛЕЗНОДОРОЖНОГО СОСТАВА

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия
*Ростовский государственный университет путей сообщения, г. Ростов-на-Дону, Россия
**ООО "Датум Групп", г. Ростов-на-Дону, Россия

Ключевые слова: вибродагностика, параметры проходящего подвижного состава, спектральный анализ, вейвлет-анализ.

Описываются современные информационные технологии решения одной из задач вибродиагностики: определение характеристик проходящего подвижного состава: момент времени прохождения контрольной точки железнодорожного пути, номер пути, тип локомотива, тип вагонов; скорость подвижного состава; количество вагонов. При этом используется спектральный анализ и непрерывное вейвлет преобразование.

A.B. Suvorov, *T.V. Suvorova, **E.A. Usoshina

DEFINITION MOVING TRAIN VIBRATING CHARACTERISTICS BY INFORMATICS TECHNOLOGY

North -Caucasian Branch of the Moscow technical university of communication and informatics
Rostov-on-Don, Russia
*Rostov State Transport University, Rostov-on-Don, Russia
**OOO "Datum Grupp", Rostov-on-Don, Russia

Key words: vibration diagnostics, parameters of moving train, the spectral analysis, the wavelet analysis.

The way of the decision of one of problems of vibration diagnostics is described: definition of integrated parameters of moving train: the moment of time of passage of a control point of a railway way, number of a way, type of the locomotive, type of cars; speed of a train; quantity of cars. Thus the spectral analysis and continuous wavelet transformation is used.

Одним из экспериментальных методов исследования и неразрушающего контроля технических объектов различного назначения является вибрационная диагностика. Основные ее методы стали применяться более полувека назад, когда впервые появилась техника анализа вибрации. Практическая реализация этих методов ограничивалась низкой эффективностью аналоговых измерительных систем и резко ограниченными возможностями обработки данных эксперимента. Переход на цифровые измерительные системы с использованием компьютерных технологий регистрации измерений и обработки данных сделало доступным сложные виды анализа сигналов не только учёным, но и инженерам-эксплуатационникам. Современный инструмент вибродиагностики – это компьютеризированный виброизмерительный комплекс с специализированным программным обеспечением для регистрации и обработки данных, состав которого определяется решаемой задачей.

Диагностика машин и оборудования с использованием вибрационных методов широко распространена в машиностроении, судостроении, дефектоскопии, чего нельзя сказать о вибродиагностике протяжённых объектов, например, жд магистралей. Проблема мониторинга и диагностики современных жд магистралей является крайне сложной и требует развития, как теоретических методов, так и натурных экспериментальных исследований. Данная задача является многоплановой, требующей для своего эффективного решения использование достижений нескольких научных направлений, решения целого класса модельных задач теории упругости, вычислительной математики, математического моделирования вибрационных процессов, инженерной сейсмологии. Создание экспериментальных средств и методов, позволяющих в реальных условиях изучать напряженно-деформированное состояние системы "верхнее строение пути – земляное полотно" и прилегающего грунта при динамических воздействиях, диагностика и изучение признаков, характеризующих работоспособное состояние верхнего строения пути, зарождение и развитие дефектов, предшествующих нарушению работоспособности является актуальной задачей.

Решение задачи вибродиагностики базируется на сочетании расчетных методов решения модельных задач и экспериментальных методов исследования динамических откликов сложных технических систем [1, 3]. Такими системами являются: верхнее строение железнодорожного пути, подстилающий грунтовой массив, движущиеся нагрузки, придорожные искусственные сооружения, жд переезды и переходы. К оборудованию вибродиагностики сложных технических систем предъявляются самые жесткие требования. Здесь требуется виброизмерительный

комплекс, позволяющий проводить измерения в полосе частот от 0,1 до 500 Гц, имеющий чувствительность не менее 200 мВ*m^{-1} *$сек^2$ и динамический диапазон входных сигналов порядка 90дб. В качестве датчиков в большинстве случаев используются пьезоакселерометры. Это обосновывается наличием в вибродиагностике в качестве обязательного компонента локализации дефекта – силового воздействия (удар, вибрация, природные и техногенные волны), которое линейно связано с измерением ускорения возбуждаемого волнового поля. В таких датчиках электрический заряд на выходе преобразователя пропорционален действующему силовому полю, а основными потребительскими характеристиками являются рабочий диапазон частот, коэффициент преобразования, динамический диапазон входных сигналов. Аппаратно-программное обеспечение вычислительной системы должно обеспечивать расширенные возможности анализа полученных данных – амплитудный, спектральный, корелляционный, статистический, вейвлет-анализ. Особое внимание уделяется вопросам, линейности преобразования волнового поля силового воздействия в точке замера в цифровой сигнал, сохраняемый на жёстком диске ПК. Замеры производят в конструктивно значимых точках сложных технических систем, при этом в качестве диагностической информации, как правило, используются следующие параметры:

- частоты собственных форм колебаний объекта и его структурных компонентов;
- характерные значения амплитудно-временных характеристик откликов на разные виды динамических воздействий;
- характерные значения спектров относительных амплитуд и спектров мощности откликов;
- характерные значения автокорреляционных характеристик откликов;
- передаточные функции;
- изменение динамического коэффициента.

Одной из задач практического использования вибродиагностики является определение характеристик проходящего подвижного состава. Метод решения этой задачи защищен патентом авторов [2]. Под характеристиками проходящего подвижного состава понимаются: моменты времени начала и конца прохождения фиксированной контрольной точки жд пути подвижным составом, путь прохождения подвижного состава, тип подвижного состава (товарный, пассажирский, дрезинатяговый, моторвагонный), тип локомотива, тип вагонов; скорость подвижного состава, количество вагонов.

При движении жд состава в верхнем строении железнодорожного пути возникает поле механических перемещений исследуемой многослойной системы. Динамические усилия, вызываемые прохождением каждой колёсной тележкой подвижного состава, через элементы рельсошпальной решетки передаются балластной призме и распространяются в ее теле в виде перемещений, образующих волновое поле. Основные характеристики распространения волновых полей в гомогенных грунтах практически совпадает с законами распространения колебаний в упругих, вязкоупругих, гетерогенных средах. При этом каждая шпала железнодорожного пути передаёт основанию периодические колебания, закон изменения которых соответствует временному закону приложения нагрузки. Как показывает аналитико-численный анализ модельной задачи [2], возбуждаемые волновые поля несут в себе информацию с одной стороны о характеристиках проходящего подвижного состава, а с другой о характеристиках балластной призмы и подстилающей грунтовой среды.

Теоретические результаты подтверждаются натурными экспериментами. В ближней зоне – зоне балластной призмы наиболее полно проявляются сигналы отклика, характеризующие параметры проходящего подвижного состава. На рисунке 1. представлена амплитудно-временная характеристика отклика вертикальной составляющей виброускорений волнового поля при проходе контрольной точки пассажирским поездом.

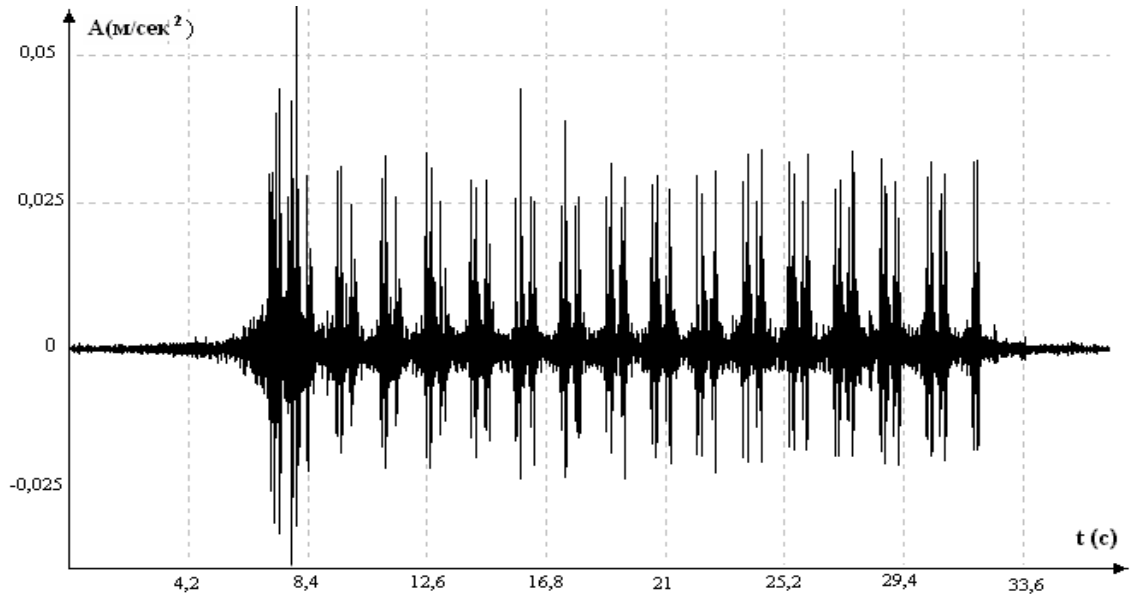


Рисунок 1. Амплитудно-временная характеристика отклика вертикальной составляющей виброускорений при проходе пассажирского поезда

Пьезоакселерометры, используемые в качестве датчиков волновых полей, устанавливаются на поверхности тела балластной призмы посредством специальных конструкций – антенных устройств – см. рисунок 2. Именно антенными устройствами, назначение которых состоит в амплитудно-частотном согласовании конструкции датчика с телом балластной призмы, обеспечивается корректность преобразования физических изменений во времени волнового поля в точке замера в цифровой сигнал. Определение способа установки антенных устройств и оптимального положения относительно рельса пути производилось с учётом следующих факторов. С одной стороны, балласт является низкочастотным фильтром и уменьшение высокочастотных составляющих в спектре сигнала ухудшает точность расчёта временных соотношений анализируемого сигнала, а с другой стороны, в непосредственной близости от рельса возможны нелинейные процессы, искажающие полезные сигналы.

Таким образом, подбор оптимального расстояния установки антенного устройства от ближайшего рельса производится на основе эксперимента и зависит от чувствительности пьезоакселерометров и конструкции антенного устройства.

Рисунок 2. Компьютеризированный виброизмерительный комплекс.

Запуск программы регистрации и расчёта временных соотношений может осуществляться автоматически при приближении подвижного состава, с учётом временной синхронизации всех процессов. Результаты обработки в виде интегральных параметров подвижного состава передаются в режиме реального времени в автоматизированную систему диспетчерского центра и сохраняются в базе данных проходящих составов данную точку пути. Предлагаемый для достижения технический результат: получение временных соотношений и спектров силовых

воздействий, определяющих интегральные параметры проходящего по железнодорожному пути подвижного состава, реализуется в несколько этапов.

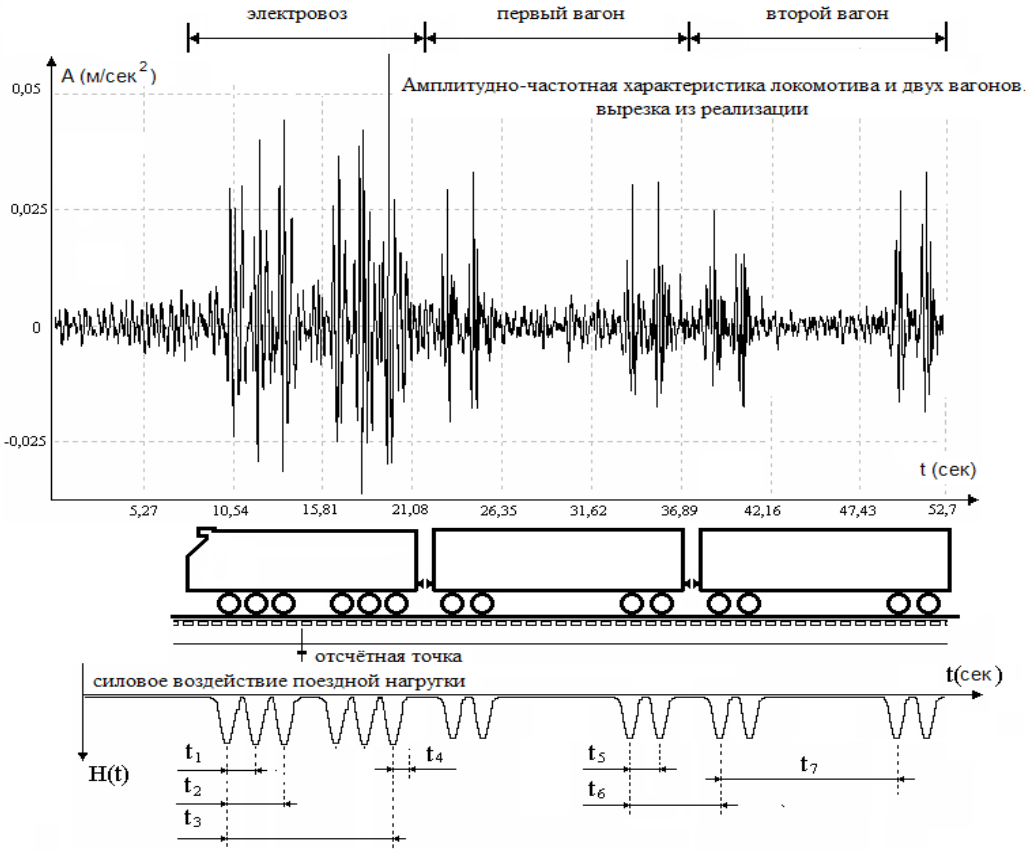


Рисунок 3. Принцип формирования временных отрезков между осями колёсных пар локомотивных и вагонных тележек.

Первый этап обработки амплитудно-временных характеристик, полученных временных реализаций прохода подвижного состава контрольной точки, заключается в формировании заданной последовательности значений временных отрезков, которые с высокой точностью определяют соотношения расстояний между осями колёсных пар локомотивных и вагонных тележек. Принцип формирования временных отрезков между осями колёсных пар локомотивных и вагонных тележек представлен на рисунке 3.

Второй этап обработки заключается в последовательном сравнении в заданном порядке полученных значений межосевых расстояний с межосевыми расстояниями, заложенными в базу данных вычислительной системы, которые соответствуют определённым типам вагонов и локомотивов. Очевидно, что предварительно необходимо сформировать базу данных типов вагонов и локомотивов по межосевым расстояниям колёсных тележек. Результатом сравнения является идентификация конкретного типа локомотива и конкретного типа каждого вагона подвижного состава. Заданная последовательность значений полученных временных отрезков, а также заданный порядок сравнения полученных межосевых расстояний определяются программным алгоритмом обработки. Для улучшения точности определения значений временных отрезков и соответственно точности идентификации каждой единицы подвижного состава, антенные устройства располагаются с обеих сторон по траверзу жд пути, а на каждом устанавливаются пьезоакселерометры в трёх взаимно-ортогональных плоскостях (см. рисунок 2) с последующим усреднением данных.

Значительное расширение возможностей по идентификации каждой единицы подвижного состава обеспечивается за счёт обработки нормализованных частотных спектров каждой конкретной единицы проходящего подвижного состава и последующего сравнения по заданному алгоритму с базой данных нормализованных частотных спектров этих же единиц. При этом дополнительно обеспечивается возможность автоматической идентификации конкретных номеров вагонов и локомотива, а также оценка загрузки каждого вагона. Таким образом, на основе

предложенного авторами метода возможно создание единой дорожной автоматической системы контроля железнодорожным движением.

Существенное расширение возможностей вибродиагностики обеспечивается за счёт обработки и последующего анализа экспериментальных данных с помощью вейвлет-преобразований. Как известно [4], коэффциенты непрерывного вейвлет-преобразования от временного ряда *s(t)* определяются формулой:

$$C_{a,b} = \int_R s(t)\psi\left(\frac{t-b}{a}\right)dt \qquad (1)$$

Здесь параметр *b* определяет время вырезки, параметр *a* является аналогом обратной величины частоты колебаний. $\psi(t)$ - вейвлет. Вейвлет-спектрограмма представляет собой зависимость коэффициентов формулы (1) от времени.

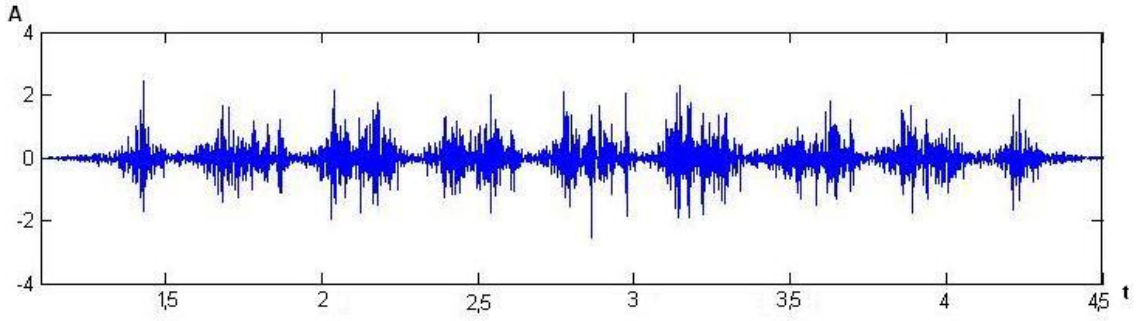


Рисунок 4. АВХ вертикальной составляющей виброускорений при проходе электропоезда

На рисунке 4 приведена амплитудно-временная характеристика виброускорений, зарегистрированных при натурном эксперименте на расстояния 6 м от пути прохождения электропоезда из 8 вагонов. На рисунке 5 показана соответствующая вейвлет-спектрограмма, полученная с помощью вейвлет-функции Симлета 4-го порядка системы Matlab. Вейвлеты Симлета относятся к классу ортогональных, имеют компактный носитель и почти симметричную форму. С их помощью построено непрерывное вейвлет-преобразование. На горизонтальной оси спектрограммы номера отсчетных значений приведены к реальному времени, на вертикальной оси отложены масштабы *a* , обратно пропорциональные частоте колебаний.

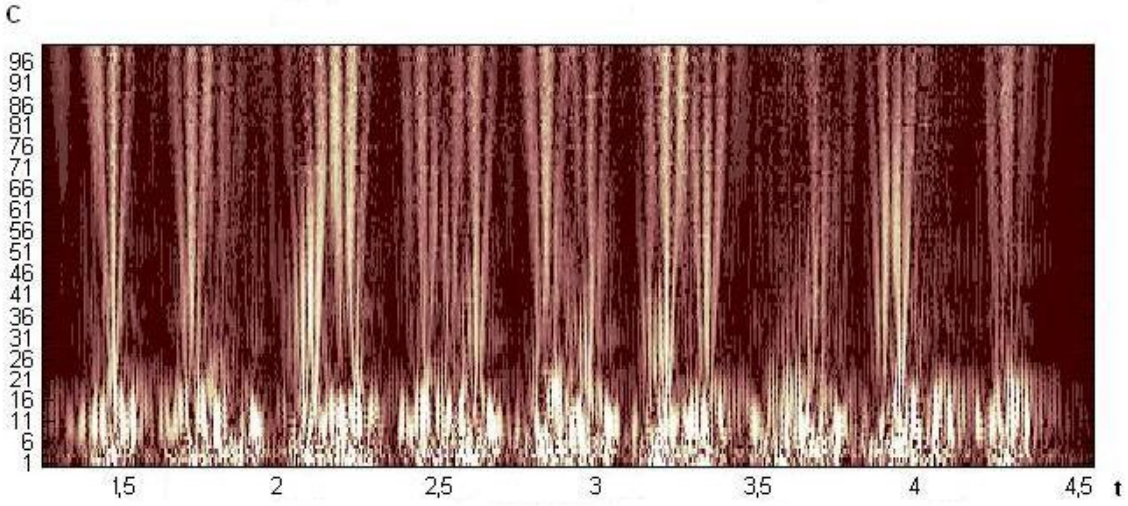


Рисунок 5. Вейвлет- спектрограммы данных натурного эксперимента.

Светлые участки спектрограммы соответствуют максимумам перемещений. Картина спектрограммы с увеличением масштаба выглядит более стабильной, ясно прослеживаются максимумы, соответствующие проходу колесных тележек. В нижней части спектра видна весьма сложная структура высокочастотных шумов. На основании математической модели и вейвлет-

преобразования можно выделять сигнал, соответствующий по частоте изучаемому процессу и реконструировать его с помощью обратного вейвлет-преобразования.

В отличие от классического спектрального анализа, применение вейвлет-преобразования позволяет получить спектрограмму динамического процесса и проанализировать эволюцию всех составляющих колебания частот во времени. Это особенно важно для поиска и регистрации нестационарных неэргодических кратковременных сигналов, связанных, например, с повышенным износом одной из колесных тележек. Также именно с помощью вейвлетов возможно разделение сигналов, амплитуды которых отличаются на порядки, что обусловлено высокой разрешающей способностью вейвлет-преобразования. С помощью вейвлет-преобразования хорошо локализуются нестационарные составляющие сигналов как по частоте, так и по времени, а также эволюция определенных гармонических составляющих во времени.

На основе описанных методов возможно проведение экспресс диагностики сверхнормативного износа ходовой части проходящего подвижного состава, создание единой автоматической системы контроля железнодорожным движением в стране. Методы вибродиагностики могут быть также применены при прогнозировании деформируемости верхнего строения пути, для контроля качества работы рельсошпальной решётки и земляного полотна, качества уплотнения грунтовых насыпей; эффективности укрепляющих конструкций насыпей, загрязнённости балласта.

Литература:

1. Колесников, В.И., Суворова, Т.В. Моделирование динамического поведения системы «верхнее строение железнодорожного пути – слоистая грунтовая среда» / В. И. Колесников, Т. В. Суворова.-М. : ВИНИТИ РАН, 2003. - 232 с.

2. Суворов А.Б., Суворова Т.В. и др. Способ контроля интегральных параметров проходящего по железнодорожному пути подвижного состава Патент на изобретение РФ № 2380260, зарег. в Гос. Реестре РФ 27.01.2010.

3. Суворов А.Б., Суворова Т.В.,Сумбатян М.А.,Усошина Е.А. О распространении ударных волн в пористоупругой слоистой среде. сб.тр. междунар. науч.-практ. конф. Механика ударно-волновых процессов в технологических система / ДГТУ.– Ростов н/Д, 2012 71-76с

4. Добеши И., Десять лекций по вейвлетам. − М. :РХД, 2001.

И.В. Щербань, *С.А. Судаков, *Д.А. Знаменский

КАНАЛ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ ОТВЕТНЫХ РЕАКЦИЙ МОЗГА ИСПЫТУЕМОГО НА ТРАНСКРАНИАЛЬНУЮ МАГНИТНУЮ СТИМУЛЯЦИЮ

Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия
*Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: транскраниальная магнитная стимуляция, измерение электроэнцефалограммы, наводимые помехи.

При формировании магнитных импульсов транскраниальной магнитной стимуляции в измерительных цепях наводятся импульсы ЭДС самоиндукции, амплитуда которых на порядок превышает максимальную амплитуду информационных сигналов электроэнцефалограммы (ЭЭГ). Предлагается способ решения проблемы измерения ЭЭГ человека в ходе транскраниальной магнитной стимуляции.

I.V. Shcherban, *S.A. Sudakov, *D.A. Znamensky

THE DATA TRANSMISSION CHANEL FOR THE MEASUREMENT SYSTEM OF A TRANSCRANIAL MAGNETIC STIMULATION BRAIN'S RESPONSE

The North Caucasian Branch of the Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia
*Southern Federal University, Rostov-on-Don, Russia

Key words: transcranial magnetic stimulation, the electroencephalogram measurements, magnetically induced voltages.

Under individual transcranial magnetic stimulation (TMS) pulses there are magnetically induced voltages in measuring circuits. The amplitude of the magnetically induced voltages approximately on a order greater, than the maximum amplitude of the information signals of electroencephalogram (EEG). The problem of the measurements of the individual EEG during TMS has been considered.

В настоящее время в НИИ "Нейрокибернетики" Южного федерального университета проводятся исследования вопросов организации нейронных систем, ответственных за билатеральное тактильное восприятие и кодирование пространственных параметров тактильных стимулов. Исследования на крысах проводятся в условиях острого опыта, когда животное обездвижено и переведено на искусственное дыхание. Так как проведение острого опыта на человеке является невозможным, то используется транскраниальная магнитная стимуляция (ТМС), позволяющая неинвазивно стимулировать кору головного мозга при помощи коротких магнитных импульсов.

ТМС требует наличия ряда специализированных аппаратных и программных средств. В данном конкретном случае аппаратный комплекс содержит магнитный стимулятор Нейро-МС [1], цифровой многоканальный усилитель BrainAmp DC [2] и ЭВМ (фотография 1). На голове испытуемого закрепляются электроды для снятия текущей электроэнцефалограммы (ЭЭГ). Структурная схема комплекса показана на рисунке 2.

Рисунок 1. Аппаратный комплекс для исследования вопросов билатерального тактильного восприятия человека

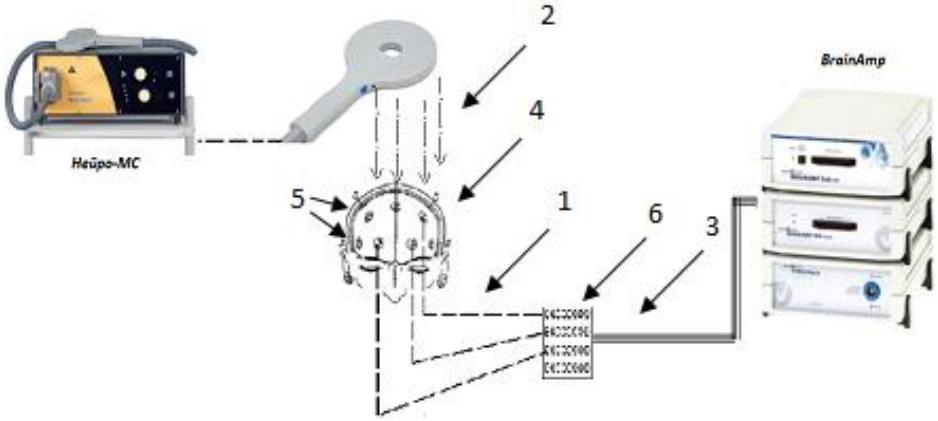


Рисунок 2. Структурная схема аппаратного комплекса

На рисунке 2 обозначено: 1 – электрические измерительные цепи, 2 – условные линии магнитной индукции ТМС, 3 – шина цифровых данных, 4 – голова испытуемого, 5 – электроды для снятия ЭЭГ, 6 – интерфейс цифрового усилителя.

Вследствие естественного замыкания измерительных цепей на участках коры головного мозга измерительные цепи 1 (рисунок 2), фактически, представляют собой замкнутые электрические контуры. Соответственно, при формировании магнитных импульсов ТМС в измерительных цепях наводятся импульсы ЭДС самоиндукции. Из практики известно [3], что амплитуда наводимых импульсов напряжения в измерительных цепях значительная и, практически, на порядок превышает максимальную амплитуду информационных сигналов ЭЭГ. В результате происходят кратковременные потери данных измерений ЭЭГ.

В подобных экспериментах основным параметром является время восстановления работоспособности схемы после действия магнитного стимулирующего импульса. В комплексах, предназначенных для регистрации относительно поздних ответов стимулируемых долей головного мозга, время восстановления входных каскадов усилителей может составлять от 200 мс до 2 с. При исследовании же возбудимости и взаимосвязей нейронных сетей мозга это время, вследствие необходимости регистрации самых ранних ответных реакций мозга, не должно превышать всего 1-2 мс. Поэтому наиболее актуальной проблемой использования вышеописанного аппаратного комплекса на сегодняшний день является проблема борьбы с наводками в информационных цепях, обусловленными магнитными импульсами ТМС.

Традиционное решение названной проблемы реализовано на основе разрыва за счет каскадов высокоскоростных реле информационных цепей ЭЭГ 1 (рисунок 2) и, таким образом, разрыва электрических контуров [3]. Цепи замыкаются после окончания действия магнитного импульса. Подобное решение имеет все тот же недостаток, связанный с потерей измерительной информации, так как измерительные каналы, фактически, оказываются отключенными в течение примерно около 1с. Например, при частоте обработки сигналов 5 КГц порядка 5000 измерений в каждом канале оказываются потерянными.

Предлагается использовать единый оптический канал передачи данных от электродов 5 к интерфейсу цифрового усилителя 6 вместо электрических цепей 2 (рисунок 2). При этом измерения ЭЭГ оцифровываются и преобразуются в групповой оптический сигнал в микроконтроллере и электронно-оптическом преобразователе, размещенных в магнитно-экранированном корпусе на голове испытуемого. Оптический групповой сигнал в инфракрасном диапазоне подается на оптико-электронный преобразователь на входе интерфейса усилителя по атмосферному каналу или по оптоволокну с соответствующим окном прозрачности.

Разработана подобная экспериментальная система передачи данных. Отличительной ее особенностью является использование простых, имеющихся в свободной продаже неспециализированных оптоэлектронных преобразователей, работающих в инфракрасном диапазоне с длиной волны 930 нм. Для схемотехнической реализации используются аппаратные средства National Instruments (NI). Программное обеспечение канала передачи, соответственно, выполнено средствами LabVIEW. Интеграция с аппаратурой NI упростила задачу синтеза

функциональных блоков шифрации-дешифрации, модуляции, приема и передачи данных, а также аппаратную совместимость схем реализованного оптического канала.

Разработанная система передачи данных достаточно проста с точки зрения ее приборной реализации, построена на основе современной цифровой электронной базы и позволяет решить проблему наводок в информационных цепях, обусловленных магнитными импульсами ТМС.

Литература:

1. Магнитный стимулятор для диагностического и лечебного воздействия на моторные зоны коры головного мозга Нейро-МС (http://www.neurosoft.ru/rus/product/neuro-ms)

2. Rugged portable amplifier for multiple applications (http://www.brainproducts.com/productdetails.php?id=1)

3. J. Virtanen, J. Ruohonen, R. Näätänen, R. J. Ilmoniemi Instrumentation for the measurement of electric brain responses to transcranial magnetic stimulation // Med. Biol. Eng. Comput., 1999, №37, p.p. 322-236.

А.А. Сулейманов

КАЧЕСТВО ПОТОКОВОГО ВИДЕО В ОБЛАЧНЫХ УСЛУГАХ ТИПА DAAS

Московский Технический Университет Связи и Информатики, г. Москва, Россия

Ключевые слова: Облачные услуги, потоковое видео, качество сервиса (QoS), воспринимаемое качество (QoE).

Описана проблема обеспечения качества потокового видео, просматриваемого пользователями облачных услуга типа DaaS (Desktop as a Service).Указаны требования и спецификации такого сервиса.

A.A. Suleymanov

QUALITY OF STREAMING VIDEO IN CLOUD SERVICES SUCH AS DAAS

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: Cloud services, streaming video, Quality of Service (QoS), Quality of Experience (QoE).

The problem of ensuring the quality of streaming video for users of cloud services such as DaaS (Desktop as a Service) is described. The requirements and specifications of the service are specified.

На сегодняшний день облачные услуги получают активное развитие, набирая популярность не только у рядовых пользователей, но и в бизнес-сегменте, социальной сфере, в учреждениях и на предприятиях. Конкурентными преимуществами таких услуг являются масштабируемость, экономичность, гибкость в развертывании, круглосуточный доступ без привязки к рабочему месту, доступ к мультимедиа контенту и др. К способам доставки последнего относится, в частности, потоковое видео.

Говоря об услуге типа DaaS (Desktop as a Service, рабочий стол как услуга) следует отметить, что такая услуга изначально позиционируется для применения в качестве стандартного рабочего места офисного сотрудника, специфика работы которого предполагает использование веб-браузера, офисного приложения, файлового менеджера. Эти приложения при работе в режиме терминальной сессии клиент – сервер не потребляют много ресурсов сети и не требуют больших мощностей серверов в облаке и на пользовательских устройствах. Такая схема применения услуг DaaS является рекомендованной и проверенной.

Однако, существуют примеры на практике, когда пользователями DaaS становятся и другие категории сотрудников какого-либо учреждения. Это могут быть аналитики, журналисты,

тестировщики приложений, архитекторы и др. Их работа может быть сопряжена с более широким спектром приложений (AutoCAD, Autodesk, Solidworks, Enovia и др.) и, в частности, с запуском видео. Кроме того, многим современным корпоративным работником необходимо просматривать новостные видео по продуктам, обучающие видео, участвовать в видео-конференциях с использованием веб-камеры и т.п.

Согласно прогнозу, приведенному в [1], рост трафика потокового видео в промежутке между 2015 и 2017 годами может составить до 15 Петабайт в месяц. Безусловно, просмотр видео из сети запускают не только пользователи из дома, но и корпоративные клиенты, рабочие места которых могут быть организованы по архитектуре DaaS.

В этой связи становится актуальным сформулировать определенные рекомендации, относящиеся к поставщикам облачных услуг и администраторам, организующим локальную сеть и пользовательское оборудование (тонкие клиенты, смартфоны, планшеты и т.п.)

В Рекомендации Y. 3503 МСЭ-Т [2] приведены требования к облачной платформе и клиентским устройствам. В контексте обсуждаемого вопроса следует выделить следующие четыре:

1. Поддержка (платформой) аппаратного графического ускорения.
2. Рендеринг на стороне сервера.
3. Поддержка стандартных видеокодеков.
4. Поддержка прогрессивного кодирования.

Поясним каждое в отдельности. Под поддержкой аппаратного графического ускорения понимается наличие на материнской плате сервера физической видеокарты. При ее наличии становится возможным использования таких технологий, как Microsoft RemoteFX или Citrix HDX, обеспечивающих передачу видео от графического процессора к пользовательскому терминалу поверх протоколов виртуализации (Microsoft RDP, Citrix ICA и др.). Возможные варианты реализации лежат за пределами обсуждения, однако в свете рассматриваемого вопроса представляется важным сформулировать требование, которое заключается в наличии поддержки программного клиента MS Remote FX и Citrix HDX в прошивке клиентского устройства.

Рендеринг на стороне сервера означает, что удаленный сервер должен полностью сформировать ту картинку, которую видит пользователь на своем мониторе. Суть в следующем: услуга DaaS построена таким образом, что на сервере организуется виртуальная машина (индивидуально для каждого пользователя или одна для группы) и во время работы в режиме терминальной сессии пользователь, подключаясь к ней, пройдя аутентификацию, видит свой рабочий стол с ярлыками, окнами и прочим. С точки зрения облачной платформы и канала связи упрощенно это выглядит как последовательность кодированных картинок, ежесекундно передаваемых от сервера к клиенту. Требование состоит в том, чтобы такие картинки были полностью сформированы на серверной стороне, а значит, экономится ресурс процессора терминального устройства, тем самым защищая само устройство от «зависаний» и т.д., что напрямую влияет на воспринимаемое качество (QoE, Quality of Experience).

Поддержка стандартных видео кодеков подразумевает аппаратную либо программную поддержку распространенных кодеков, например H.264, H.265 и др. Не вдаваясь в подробности, можно отметить, что подавляющее большинство устройств на том или ином уровне имеют необходимые кодеки.

Поддержка прогрессивного кодирования означает применение специализированных алгоритмов, позволяющих последовательно в несколько этапов кодировать на стороне сервера и декодировать на стороне клиента поток изображений. Это необходимо для поддержания приемлемого качества в случаях, когда на сети возникает «бутылочное горлышко» – сужение полосы пропускания на каком-либо из устройств в цепочке следования трафика.

Практика показывает, что в большинстве клиентских устройств, которые можно подключить в качестве терминального оборудования по схеме DaaS, за обработку видео отвечает процессор устройства (CPU). Одним из вариантов реализации может быть детектирование интерфейсом видео потока и перенаправление его на второе ядро, выделенное специально под обработку видео. Таким образом, разгружается основное ядро, которое берет на себя все остальные функции. Другим вариантом может быть наличие на клиентском устройстве отдельного графического процессора, полностью отвечающего за обработку видео потока. Но этот вариант более дорогой.

Резюмируя, следует отметить, что проигрывание потокового видео в архитектуре DaaS является возможным с технической точки зрения, хотя и не является рекомендованным производителями «облачного» (серверного) программного обеспечения сценарием использования таких услуг. Тем не менее, практика показывает, что у ряда категорий пользователей имеется потребность в видео. Для обеспечения приемлемого качества следует учитывать рекомендации, перечисленные выше. Однако данная тема мало исследована, в частности, открытыми остаются следующие вопросы: модернизация существующих или разработка новых кодеков, формирующих картинки, которые передаются от сервера к клиенту, с целью добиться такого соотношения полосы пропускания и качества изображения, которое бы позволило, меньше занимая ресурс сети, соблюсти приемлемое качество услуги; анализ факторов, влияющих на общее время клиент-серверного взаимодействия, для нахождения путей его сокращения, что важно для решения задачи предоставления приемлемого качества на этапах проектирования и эксплуатации сети.

Литература:

1. Berger T. Video in Enterprise Environments (VDI and more) [Electronic resource] // Citrix Systems Inc. [Official website]. The Citrix blog. 2015. URL: http://blogs.citrix.com/2014/04/14/video-in-enterprise-environments-vdi-and-more (дата обращения: 14.02.2015)

2. ITU-T Y.3503 (05/14) Cloud computing framework and high-level requirements.

В.Л. Стерин, А.С. Еременко, Тарики Надия

ДИНАМИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ОВЕРЛЕЙНОЙ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

Харьковский национальный университет радиоэлектроники

Ключевые слова: модель, очередь, маршрутизатор, перегрузка, поток, пакеты.

Предложена динамическая модель синтеза оверлейных виртуальных частных сетей. Использование модели позволяет обеспечить эффективное управление ресурсами сети провайдера при создании оверлейных виртуальных частных сетей за счет более полного учета динамики процессов информационного обмена, протекающих в ней. Предложенные решения адаптированы как под модель изолированного канала (pipe-модель), так и под распределенную модель (hose-модель), которые поддерживаются в решениях, основанных на MPLS-технологии.

V.L. Sterin, O.S. Yeremenko, Tariki Nadia

DYNAMIC MODEL OF OVERLAY VIRTUAL PRIVATE NETWORK SYNTHESIS

Kharkiv National University of Radio Electronics

Keywords: model, queue, router, overload, flow, packets.

The dynamic model of overlay virtual private networks synthesis proposed. Using the model allows efficient provider`s network resource management when creating overlay virtual private networks due to better reflection of the information interchange process dynamics within it. The proposed solutions are adapted as a model of an isolated channel (pipe-model) and a distributed model (hose-model) that are supported in the solutions based on the MPLS.

Эффективное обеспечение высокой (заданной) производительности создаваемых виртуальных частных сетей (VPN) может быть реализовано лишь на основе оптимизации во времени процесса управления (перераспределения) топологическим, канальным и буферным ресурсом сети сервис-провайдера (Р-сети) в интересах множества создаваемых на ее основе виртуальных частных сетей. К сожалению, ввиду непроработанности этих задач производительность VPN-сетей всегда оставляет желать лучшего, особенно в условиях высокой

динамики числа и характеристик клиентских потоков и связанных с ними требований к качеству обслуживания (QoS). Ввиду того, что современные телекоммуникационные сети (ТКС) по определению мультисервисные, при синтезе VPN-сетей необходимо предусмотреть комбинированную реализацию моделей изолированного канала и hose-модели [1]. Учитывая высокую динамику состояния IP/MPLS-сетей, на базе которых, как правило, и создаются VPN, математические модели, описывающие процессы создания и управления ресурсами виртуальных частных сетей, должны относиться к классу динамических [2]. Поэтому предложенные в работах [3, 4] математические модели, представленные разностными уравнениями состояния, будут в настоящей статье адаптированы под новые цели исследования, предметную область и терминологию.

Пусть структура сети провайдера описывается с помощью графа $G=(R,L)$, где $R=\{R_i, i=\overline{1,m}\}$ – множество маршрутизаторов сети провайдера, $L=\{L_{i,j}, i,j=\overline{1,m}, i\neq j\}$ – множество трактов передачи между маршрутизаторами той же Р-сети.

Тогда мощность множества $|R|=m$ определяет общее число маршрутизаторов в Р-сети, а $|L|=n$ – число трактов передачи в ней же. Все множество маршрутизаторов (устройств) сети провайдера в соответствии с принципами построения сети VPN-сетей можно разбить на два подмножества: $R^{pe}=\{R_i^{pe}, i=\overline{1,m_{pe}}\}$ – подмножество приграничных устройств (маршрутизаторов) сети сервис-провайдера (PE); $R^{p}=\{R_j^{p}, j=\overline{1,m_{p}}\}$ – подмножество устройств (маршрутизаторов) сети сервис-провайдера (P). Каждой дуге $L_{i,j}\in L$ графа, моделирующей соответствующий тракт передачи в Р-сети, ставится в соответствие ее пропускная способность $c_{i,j}^{P}$.

Пусть общее число создаваемых VPN-сетей равно m_c, это же число определяет количество типов клиентских С-сетей, функционирующих в интересах одной и той же компании (предприятия). Тогда все множество поступающих в сеть провайдера потоков F можно декомпозицировать на подмножества $\{F_g, g=\overline{1,m_c}\}$, где F_g – множество потоков, циркулирующих в g-й VPN. Каждому потоку из множества F_g сопоставляется ряд параметров: R_s^{pe} – s-й PE-маршрутизатор, на который поступает поток пакетов в Р-сеть; R_d^{pe} – d-й PE-маршрутизатор, через который поток пакетов убывает из Р-сети; $r^{(l,g)}$ – интенсивность l-го потока, циркулирующего в g-й VPN.

В случае моделирования процесса синтеза оверлейных VPN, основанных на туннелировании трафика, модель дополняется следующими обозначениями: $c_{i,j}^{(l,g)}(k)$ – пропускная способность (ПС) тракта передачи, который представлен дугой $L_{i,j}\in L$, выделенная для l-го туннеля (l-го для потока) g-й VPN на k-м временном интервале (*бит/с*); $u_{i,j}^{(l,g)}(k)$ – доля пропускной способности $c_{i,j}^{P}$ тракта передачи, представленного дугой $L_{i,j}\in L$, которая берется со знаком плюс, если выделяется для наращивания ПС $c_{i,j}^{(l,g)}(k)$ g-й VPN, или со знаком минус при ее перераспределении в интересах других туннелей и (или) виртуальных частных сетей на k-м временном интервале.

Тогда система уравнений, описывающих динамику состояния (топологии и изменения пропускных способностей трактов передачи) создаваемых оверлейных VPN-сетей при распределении ресурсов сети сервис-провайдера, принимает форму:

$$c_{i,j}^{(l,g)}(k+1) = c_{i,j}^{(l,g)}(k) + u_{i,j}^{(l,g)}(k) c_{i,j}^{P} \quad (1)$$

На переменные состояния и управления, исходя из их физического смысла, накладываются следующие условия-ограничения:

$$0 \le c_{i,j}^{(l,g)}(k), \quad (g = \overline{1, m_c}), \quad (2)$$

$$\sum_{g=1}^{m_c} \sum_{l} c_{i,j}^{(l,g)}(k) \le c_{i,j}^{P}, \quad (3)$$

$$-1 \le u_{i,j}^{(l,g)}(k) \le 1. \quad (4)$$

При этом пропускная способность тракта передачи $L_{i,j} \in L$, выделенная для соответствующего канала $L_{i,j}^{VPN_g}$ g-й оверлейной VPN на k-м временном интервале (*бит/с*), может быть рассчитана следующим образом:

$$c_{i,j}^{g}(k) = \sum_{l} c_{i,j}^{(l,g)}(k). \quad (5)$$

Дополнительной управляющей переменной, вводимой для решения задач маршрутизации в рамках VPN-сетей, служит величина $x_{i,j}^{(l,g)}$, которая характеризует долю l-го потока, протекающего в канале $L_{i,j}^{VPN_g}$ g-й VPN. В соответствии с физикой решаемой задачи на переменные $x_{i,j}^{(l,g)}$ накладываются следующие ограничения

$$x_{i,j}^{(l,g)} \in \{0,1\}, \quad (6)$$

что соответствует реализации оверлейной VPN на основе туннелирования, т.к. между каждой парой PE-маршрутизаторов будет для l-го потока рассчитан один путь (туннель).

Условия сохранения потока на PE и P-маршрутизаторах имеют вид

$$\sum_{j:(i,j)} x_{i,j}^{(l,g)}(k) = 1; \quad (7)$$

$$\sum_{j:(i,j)} x_{i,j}^{(l,g)}(k) - \sum_{j:(j,i)} x_{j,i}^{(l,g)}(k)\left(1 - p_{j,i}^{(l,g)}(k)\right) = 0; \quad (8)$$

$$\sum_{j:(i,j)} x_{j,i}^{(l,g)}(k)\left(1 - p_{j,i}^{(l,g)}(k)\right) = \varepsilon^{(l,g)}(k), \quad (9)$$

где $p_{i,j}^{(l,g)}$ – вероятность потерь пакетов l-го потока на j-м интерфейсе i-го P-маршрутизатора g-й VPN по причине перегрузки очереди; $\varepsilon^{(l,g)}$ – доля интенсивности l-го потока пакетов, обслуженного g-й VPN.

Условия (7) должны быть справедливы для приграничного PE-маршрутизатора, к которому через CE-маршрутизатор подключена C-сеть отправитель пакетов, условия (8) – для всех транзитных P-маршрутизаторов, а условия (9) – для приграничного PE-маршрутизатора, к которому через CE-маршрутизатор подключена C-сеть получатель пакетов. Для примера, в случае моделирования процесса обслуживания пакета системой массового обслуживания $M/M/1/N$, вероятность потерь пакетов на интерфейсе маршрутизатора (для удобства индексы опущены) может быть рассчитана как

$$p = \frac{(1-\rho)(\rho)^N}{1-(\rho)^{N+1}}, \quad (10)$$

где ρ – коэффициент загруженности канала; $N = \Theta_{буф} + 1$ – максимальное число пакетов, которое может находиться на интерфейсе, включая буфер ($\Theta_{буф}$) и сам канал.

В ходе расчета маршрутных переменных $x_{i,j}^{(l,g)}$ необходимо, чтобы для l-го потока вероятность потерь пакетов была не больше допустимой ($p_{\text{доп}}^{(l,g)}$), что в рамках выражений (7)-(9) может быть сформулировано как

$$1 - \varepsilon^{(l,g)} \le p_{\text{доп}}^{(l,g)}. \quad (11)$$

Численные значения допустимой вероятности потерь пакетов для того или иного типа потока, для примера, указаны в рекомендации ITU-T Y.1541. Для каждой конкретной поддерживаемой услуги эти значений могут несколько отличаться.

При реализации распределенной модели обеспечения качества обслуживания в MPLS/VPN-сетях сумма всех интенсивностей $r^{(l,g)}$ потоков, исходящих от одного PE-маршрутизатора не должна превышать установленное значение согласованной входной скорости ICR. А сумма всех произведений $r^{(l,g)}\varepsilon^{(l,g)}$ для потоков, которые поступают на данный PE-маршрутизатор, не должна превышать значения согласованной выходной скорости ECR.

Для предотвращения перегрузки каналов создаваемых виртуальных сетей клиентскими потоками необходимо обеспечить выполнение условий:

$$\sum_{l} r^{(l,g)} x_{i,j}^{(l,g)}(k) \le c_{i,j}^{g}(k), \ (g = \overline{1, m_c}). \quad (12)$$

Для предотвращения перегрузки каждого конкретного туннеля в рамках создаваемых оверлейных VPN маршрутизируемыми по ним клиентскими потоками необходимо обеспечить выполнение условий:

$$r^{(l,g)} x_{i,j}^{(l,g)} \le c_{i,j}^{(l,g)}(k), \ (g = \overline{1, m_c}). \quad (13)$$

Подобное решение адекватно подходит под реализацию модели изолированного канала (pipe-модели) при построении MPLS/VPN-сети, где параметр $r^{(l,g)}$ определяет уровень гарантированного качества обслуживания по пропускной способности такого канала (туннеля). В технологии MPLS подобные туннели представляют собой пути коммутации по меткам с гарантированной пропускной способностью (guaranteed bandwidth LSP).

В качестве критерия оптимальности решений по созданию оверлейной VPN может служить минимум следующего функционала

$$J = \sum_{k=1}^{K^{VPN}} \left[\sum_{g=1}^{m_c} \sum_{l} \sum_{L_{i,j} \in L} f_{i,j}^{(l,g)}(k) x_{i,j}^{(l,g)}(k) + \sum_{g=1}^{m_c} \sum_{l} \sum_{L_{i,j} \in L} v_{i,j}^{(l,g)}(k) c_{i,j}^{(l,g)}(k) + \right.$$
$$\left. + \sum_{g=1}^{m_c} \sum_{l} \sum_{L_{i,j} \in L} \gamma_{i,j}^{(l,g)}(k) u_{i,j}^{(l,g)}(k) \right], \quad (14)$$

в котором $f_{i,j}^{(l,g)}(k)$ – маршрутная метрика канала, представленного дугой $L_{i,j}^{VPN_g}$, для l-го потока на k-м временном интервале; $v_{i,j}^{(l,g)}(k)$ – относительная стоимость использования единицы пропускной способности канала, представленного дугой $L_{i,j}^{VPN_g}$, в интересах l-го туннеля на k-м временном интервале; $\gamma_{i,j}^{(l,g)}(k)$ – условная стоимость процесса перераспределения пропускной способности трактов передачи сети сервис-провайдера между туннелями создаваемых оверлейных VPN-сетей на k-м временном интервале.

Использование критерия (14) позволяет минимизировать условные суммарные затраты на синтез оверлейных VPN-сетей (второе и третье слагаемое), представленных в виде туннелей, и на

их функционирование с точки зрения маршрутизации по ним клиентских потоков (первое слагаемое). Управление созданием оверлейных VPN-сетей организуется на некотором упреждающем временном интервале – интервале прогнозирования, что позволяет более гибко перераспределять ресурсы сети сервис-провайдера между VPN-туннелями одной или различных виртуальных частных сетей.

Литература:

1. Олвейн В. Структура и реализация современной технологии MPLS: Пер. с англ. – М.: Издательский дом «Вильямс», 2004, 480 с.
2. Поповский В.В., Лемешко А.В., Евсеева О.Ю Математические модели телекоммуникационных систем. Часть 1. Математические модели функциональных свойств телекоммуникационных систем [Электронный ресурс] // Проблеми телекомунікацій, 2011, № 2 (4), с. 3-14. Режим доступа: http://pt.journal.kh.ua/2011/2/ 1/112_popovsky_functional.pdf.
3. Лемешко А.В., Стерин В.Л. Динамическая модель структурно-функционального синтеза транспортной ТКС [Электронный ресурс] // Проблеми телекомунікацій, 2011, № 3 (5), с. 8-17. Режим доступа: http://pt.journal.kh.ua/2011/3/1/113_lemeshko _synthesis.pdf.
4. Лемешко А.В., Стерин В.Л. Оптимизация структурного и функционального синтеза транспортной телекоммуникационной сети // Системи обробки інформації, 2012, Вип. 9 (107), с. 186-190.

В.Ю. Титов, Е.М. Хорольский

МАТРИЧНОЕ ПРЕДСТАВЛЕНИЕ ЭНЕРГЕТИЧЕСКИХ ПАРАМЕТРОВ ПЕРЕДАЮЩИХ МОДУЛЬНЫХ АНТЕННЫХ РЕШЕТОК

Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г.Ростов-на-Дону, Россия

Ключевые слова: передающая модульная антенная решетка, коэффициент усиления, коэффициент направленного действия, матрица сопротивлений, матрица рассеяния, вертикальный вибратор.

В статье рассмотрен один из вариантов определения основных энергетических параметров передающих модульных антенных решеток. Представлен порядок нахождения выражений для определения коэффициента усиления и коэффициента направленного действия передающих модульных антенных решеток, в основе которого лежит матричное описание эквивалентного многополюсника системы. Приведен результат расчета коэффициента усиления 4-элементной передающей модульной антенной решетки, состоящей из вертикальных вибраторов на экране с несимметричным возбуждением их генераторами, включенными в зазоры между основаниями вибраторов и экранов.

V.Yu. Titov, E.M. Horolsky

MATRIX REPRESENTATION OF THE PARAMETERS ARE PASSED MODULAR POWER ANTENNA ARRAYS

The Federal government institution scientific and production association special equipment and telecoms of the Ministry of the Internal Affairs of the Russian Federation,
Rostov-on-Don, Russia

Keywords: transmitting a modular array, gain antenna, coefficient of directional antennas, resistance matrix, scattering matrix, vertical vibrator.

The article deals with one of the options to define the basic parameters of the transmitting power of modular antenna arrays. Presents the order of finding expressions for determining the gain and the

directivity of the transmission modular antenna arrays, which is based on the equivalent multipole matrix description of the system. The results of calculation of the gain 4-cell transmission modular antenna array consisting of vertical vibrators on the screen with an asymmetric excitation of generators included in the gaps between the bases of the vibrators and screens.

Моделирование передающих модульных антенных решеток (ПМАР) с заданными параметрами усложнено необходимостью учета главного обстоятельства – взаимное влияние излучателей. Оценке процессов, происходящих при таком влиянии, посвящено большое количество научных исследований, основным направлением которых являлось оперирование весовыми коэффициентами [1, С.19; 2, С.252]. Однако, как показывает практика, такое представление ПМАР является не всегда удобным, особенно если система имеет неэквидистантное расположение излучателей.

Одним из вариантов упрощения учета взаимного влияния излучателей ПМАР, может быть представление системы в виде эквивалентного многополюсника [2, С.255]. В таком случае соотношения между токами и напряжениями на физических входах ПМАР, обозначаемых в дальнейшем с индексом α, определяются матрицей сопротивлений Z. При этом энергетические параметры ПМАР можно выразить матрицей рассеяния $S = \begin{bmatrix} S_{\alpha\alpha} & S_{\alpha\beta} \\ S_{\beta\alpha} & S_{\beta\beta} \end{bmatrix}$, включающей комплексные векторные характеристики направленности по входам системы из пространства (с индексом β) [3, С.115].

Известно, что основными энергетическими параметрами антенн, в том числе и ПМАР, являются коэффициент усиления (КУ) G и коэффициент направленного действия (КНД) D. КУ представляет собой отношение вектора Пойтинга в дальней зоне к вектору Пойтинга от идеальной изотропной антенны при одинаковых мощностях на входах антенн [3, С.121]:

$$G = \frac{\left|\vec{\varepsilon}\right|^2 4\pi r^2}{P_{подводимая}}. \qquad (1)$$

Для расчета угловой зависимости интенсивности излучения $\vec{\varepsilon}(\theta,\phi)$ целесообразно использовать выражение [2, С.260]:

$$\vec{\varepsilon}(\theta,\phi) = \frac{\vec{E}_n}{\sqrt{Z_B}} = \vec{i}_n \sqrt{\frac{g_n r_{nn}}{4\pi}} \frac{e^{-jkr}}{r} \vec{F}_n^0(\theta,\phi), \qquad (2)$$

где $\vec{E}_n$ – электрическое поле изолированного излучателя с нормированным на волновое сопротивление Z_B током

$$\vec{i}_n = \vec{I}_n \sqrt{Z_B}, \qquad (3)$$

коэффициентом усиления g_n, нормированным сопротивлением r_{nn} и векторной характеристикой направленности $\vec{F}_n^0(\theta,\phi)$ в сферической системе координат (r,θ,ϕ), начало которой совмещено с центром системы.

С учетом представления мощности [2, С.267]

$$P = \left(\vec{J}^*, \overline{\overline{R}}\vec{J}\right), \qquad (4)$$

излучаемой током с плотностью $\vec{j}$, выражение (1) будет иметь вид

$$G(\theta,\phi) = \frac{4\pi \left\langle i^* \vec{f}^*(\theta,\phi)\right\rangle \left\langle \vec{f}(\theta,\phi) i\right\rangle}{\left\langle i^* r i\right\rangle}. \qquad (5)$$

В этом выражении $i\rangle$ – вектор нормированных токов в произвольно выбранных взаимовлияющих элементах системы с соответствующими ненормированными характеристиками направленности в общей системе координат $\vec{f}(\theta,\phi)$.

При подстановке в (5) вектора [2, С.269]

$$\langle i_э = \langle a_\alpha (E_\alpha - S_{\alpha\alpha}), \tag{6}$$

выражение для КУ в терминах падающих волн мощности и матрицы рассеяния, которое учитывает рассогласование системы с генераторами, будет иметь вид:

$$G(\theta,\phi) = \frac{4\pi \left\langle a_\alpha^* (E_\alpha - S_{\alpha\alpha}) + \vec{f}^*(\theta,\phi) \right\rangle \left\langle \vec{f}(\theta,\phi)(E_\alpha - S_{\alpha\alpha}) a_\alpha \right\rangle}{\left\langle a_\alpha^* a_\alpha \right\rangle}. \tag{7}$$

Разность единичной матрицы E_α и блока $S_{\alpha\alpha}$ определяется через блок $S_{\beta\alpha}$ матрицы рассеяния и матрицу преобразующих токов:

$$S_{\beta\alpha} = [i_0]^{-1}(E_\alpha - S_{\alpha\alpha}). \tag{8}$$

С учетом ненормированной характеристики направленности

$$\vec{f}(\theta,\phi) = \sqrt{\frac{g_n r_{nn}}{4\pi}} \vec{F}_n^0(\theta,\phi), \tag{9}$$

при единичном векторе возбуждения системы, а так же матрицы преобразующих токов [4, С.171]

$$[i_0] = O diag\left(1/\sqrt{\rho}\right)_N U, \tag{10}$$

где, O – набор собственных векторов матричного аналога добротности излучающей системы, U – произвольная унитарная матрица спектрального разложения, матрицы нормированных активных сопротивлений [5]

$$r = O diag \rho_N O', \tag{11}$$

выражение (7) можно представить в виде функционала:

$$G(\theta,\phi) = S_{\beta\alpha}^+ \overline{\overline{g}}(\theta,\phi) S_{\beta\alpha}. \tag{12}$$

В (12) матричный КУ элементов системы $\overline{\overline{g}}(\theta,\phi)$, представляющий собой тензор второго ранга (диадик) можно определить по формуле:

$$\overline{\overline{g}}(\theta,\phi) = \overline{\overline{g}}_\theta(\theta,\phi) + \overline{\overline{g}}_\phi(\theta,\phi). \tag{13}$$

Аналогично известному соотношению КУ с КНД и коэффициентом полезного действия η [2, С.272]

$$G = D\eta, \tag{14}$$

находится матричный КНД при единичном векторе возбуждения:

$$D(\theta,\phi) = \frac{S_{\beta\alpha}^+ \overline{\overline{g}}(\theta,\phi) S_{\beta\alpha}}{S_{\beta\alpha}^+ S_{\beta\alpha}}. \tag{15}$$

Необходимо отметить, что при синтезе и оптимизации ПМАР целесообразно использовать среднее значение КУ $\overline{G}$ по всем углам заданного сектора телесных углов Ω:

$$\overline{G} = \frac{1}{\Omega_0} \iint_{\Omega_0} G_{\max}(\Omega') d\Omega' \tag{16}$$

и средний КУ $\overline{G}_f$ на частоте f по частотной области Δf

$$\overline{G}_f = \frac{1}{\Delta f}\int_{\Delta f} G(f)\,df \quad . \tag{17}$$

Результат расчета по рассмотренному выше порядку определения энергетических параметров ПМАР в виде картографической проекции представлен на Рисунке 1. Полученный график описывает КУ 4-элементной ПМАР, состоящей из вертикальных вибраторов на экране (см. Рисунок 2) с несимметричным возбуждением их генераторами, включенными в δ-образные зазоры между основаниями вибраторов и экранов. При этом использовалась фазировка напряжений, соответствующая максимуму излучения в направлении θ_0=30°, φ_0=30°.

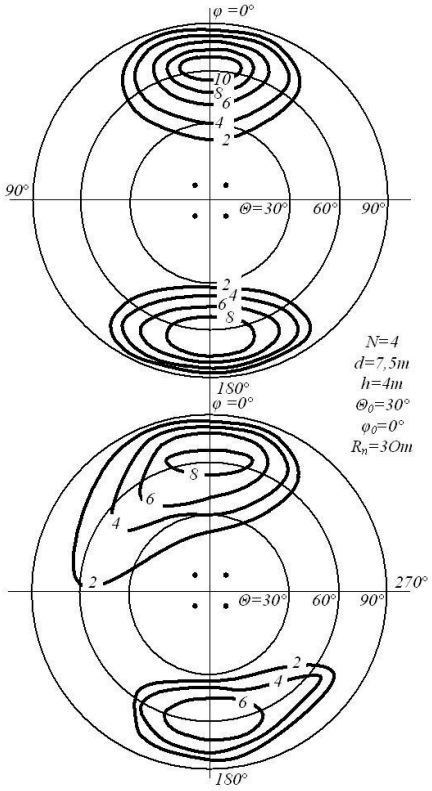


Рисунок 1. КУ 4-элементной ПМАР в равновеликой картографической проекции

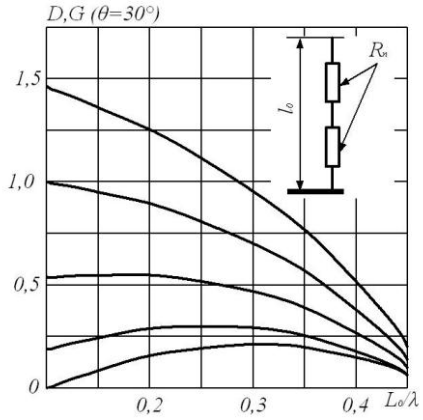


Рисунок 2. КНД и КУ вибратора

Литература:

1. Ksienski A. Equivalence between continuous and discrete radiation arrays Canad Journ Phys, 1961, February, v. 39, p. 335.Фитенко Н.Г. Анализ и синтез модульных антенн. ВАС, 1990, с. 6-90.

2. Сазонов Д.М. Антенны и устройства СВЧ. – М.: Высшая школа. 1988, с. 252-278.

3. Сазонов Д.М. Основы матричной теории антенных решеток // Сборник научно-методических статей по прикладной электродинамике. – М.: Высшая школа, 1983, вып.6, с. 111-162.

4. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления.– М.: Наука, 1984, с.170-202.

Ш.Т. Тошматов

УСИЛИТЕЛЬ МОЩНОСТИНА ИНЖЕКЦИОННО-ВОЛЬТАИЧЕСКИХ ТРАНЗИСТОРАХ СО СТАБИЛИЗАЦИЕЙ ТОКОВ ПОКОЯ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан.

Ключевые слова: усилители мощности с заданным током покоя, усилитель мощности на инжекционно-вольтаических транзисторах, Многокаскадные гомо и гетеросоставные транзисторы по схеме Дарлингтона и Шиклаи, методы стабилизации выходных каскадов радиотехнических устройств.

Предлагается схема усилителя мощности с током покоя, не нуждающимся ни в первичной настройке, ни в последующем контроле. Данный усилитель устойчив к изменениям температуры, напряжения источников питания и разбросу параметров транзисторов.АЧХ и ФЧХ предложенного усилителя мощности на инжекционно-вольтаических транзисторах до частот 350 кГц АЧХ и ФЧХ практически линейны.Ток покоя практически не изменяется при изменениях напряжения питания от 2 В до 60 В и температуры от 200 К до 400 К.Изменение THD при изменении входного напряжения от 3 В до 16 В составляет от 0,009% до 0,0055% соответственно.

Sh.T. Toshmatov

POWER AMPLIFIER WITH INJECTION-VOLTAIC TRANSISTOR WITH QUIESCENT CURRENT STABILIZATION

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: power amplifiers with a predetermined quiescent current, power amplifier on injection-voltaic transistors, Multistage homo and geterocomposite Darlington and Shiklai transistors, methods of stabilization of output stages radio devices.

The scheme of the power amplifier with no need of initial or subsequent adjustments of quiescent current, resistant to temperature variations, supply voltage variations and the scatter of parameters of transistors.Frequency and phase responsesof the proposedpower amplifieroninjectionvoltaic transistors up to frequenciesof 350kHzpractically linear.Quiescent current practically does not change with changes of the supply voltage from 2 V to 60 V and a temperature from 200 K to 400 K.Variation of THDwhen the inputvoltage changes from 3V to 16 Vis from0.009% to 0.0055%, respectively.

Усилители мощности на симметричной паре комплементарных транзисторов, выполняется по двухтактной схеме [1, С.198].

Характеристики транзисторов нелинейные, поэтому реальные усилители работают в режиме усиления АВ или А в зависимости от величины напряжения смещения.Недостаток таких усилителей – невозможность стабилизации тока покоя. Величина тока покоя транзисторов определяет коэффициент нелинейных искажений усилителя, потребляемую мощность и его надежность.С возрастанием температуры окружающей среды и транзисторов ток покоя может увеличиваться, что приводит к их тепловому пробою. [2, С.232-254].

Недостатком существующих усилителей мощности является то, что в процессе изготовления необходимо подбирать транзисторы с близкими параметрами и то, что они нуждается в дополнительной настройке. При этом необходимо устанавливать начальное значение тока покоя оконечного каскада. С учетом того что входная вольтамперная характеристика транзистора имеет экспоненциальный характер, требуемая точность задания величины напряжения смещения может составлять до десятых долей милливольта.Неточность в установке значений напряжений смещения приводит к разбалансу плеч усилителя и протеканию значительного тока покоя через транзисторы и нагрузку. Недостатком также является и экспоненциальная зависимость величины тока покоя от температуры транзистора.

При неизменном напряжении смещения база-эмиттер коллекторный ток транзистора возрастает на 8 % на каждый градус увеличения температуры, что может привести к тепловому пробою транзистора.

Задачей работы является создание усилителя мощности с заданным током покоя, без дополнительной настройки и без контроля тока покоя, устойчивым к изменениям температуры, изменению напряжения источников питания и разбросу параметров транзисторов.

Предложенный усилитель мощности (Рисунок.1.) состоит из биполярных транзисторов 1,2, каждый из которых выполнен из трех составных инжекционно-вольтаических транзисторов 15,17,19, построенных по схеме «общий коллектор - общий коллектор - общий коллектор» и аналогичных транзисторов 14,16,18, построенных по схеме «общий эмиттер - общий коллектор - общий коллектор», соответственно. Коллекторы транзисторов 20,21,22,23,24,25 представляют собой общий коллектор, эмиттеры транзисторов 26,27,28,29,30,31 представляют собой общий эмиттер, базы транзисторов 32 и 20, 33 и 21, 34 и 22, 35 и 23, 36 и 24, 37 и 25 представляют собой общую базу составных инжекционно-вольтаических транзисторов 14,15,16,17,18,19 соответственно.

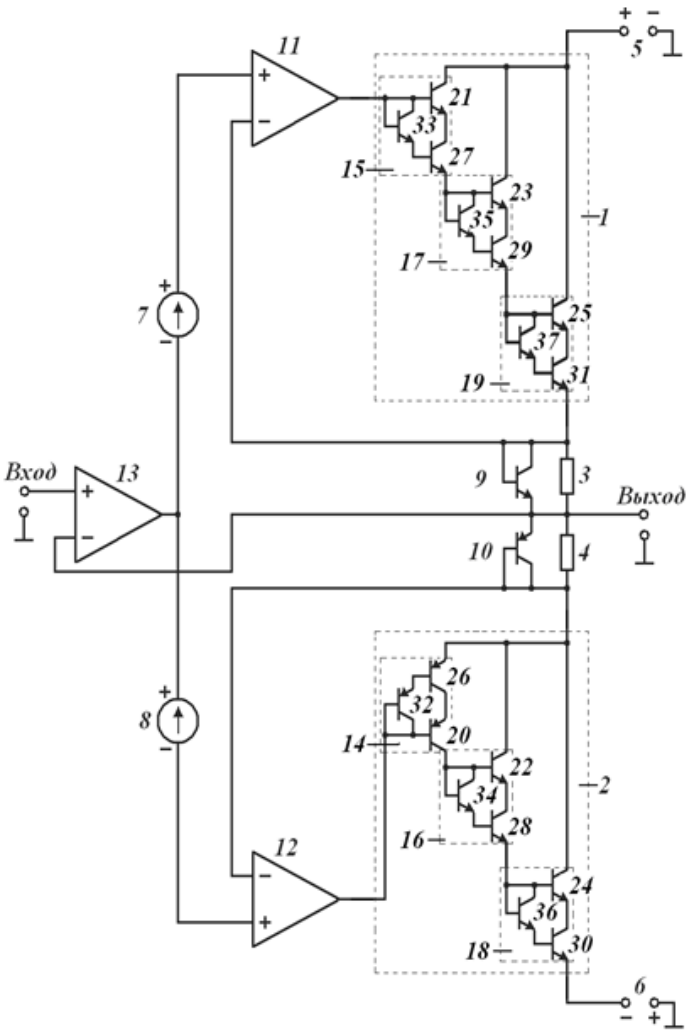


Рисунок.1. Схема усилителя мощности на составных инжекционно-вольтаических транзисторах.

Для улучшения стабильности тока покоя в усилителе мощности используются составные инжекционно-вольтаические транзисторы 14-19 (Рисунок.1.).Усилитель мощности на биполярных транзисторах работает следующим образом.Биполярные транзисторы 1,2 включены по схеме с общим коллектором. Величина тока покоя в каждом плече усилителя мощности определяется отношением напряжений смещения к величине эмиттерного сопротивления.

При отсутствии входного сигнала величина токов покоя в каждом плече усилителя мощности автоматически регулируется операционными усилителями 11 и 12, охваченными отрицательной обратной связью. Падение напряжения на эмиттерных резисторах 3,4 сравнивается с напряжениями соответствующих источников смещения 7,8.Результат сравнения напряжений

усиливается операционными усилителями 11,12 и в противофазе подается на базы соответствующих биполярных транзисторов 1,2 и таким образом восстанавливаются прежние значения токов покоя.

Токи покоя плеч усилителя мощности могут отличаться от требуемых значений за счет разброса параметров биполярных транзисторов 1,2, эмиттерных сопротивлений 3,4 и источников смещения 7,8. В этом случае напряжение на выходе усилителя мощности отличается от нуля и через нагрузку (на схеме не показана) будет протекать ток. Операционный усилитель 13 предназначен для установления баланса нуля выходного напряжения усилителя мощности и охвачен отрицательной обратной связью.

При подаче входного сигнала напряжение на выходе усилителя мощности повторяется.

В усилителе мощности используются источники питания 5,6 напряжением ±30 В и источники смещения 7,8 напряжением ±0,5 В, эмиттерные резисторы 3,4 значением 5 Ом. Усилитель мощности создан для двух стандартных значений сопротивления нагрузки R_H.Выходная мощность усилителя составляла 30 Вт при R_H=8 Ом и 60 Вт при R_H=4 Ом. Токпокоя$I_П$=100 мА.

Усилитель мощности на биполярных транзисторах реализован для случая, когда количество составных инжекционно-вольтаических транзисторов равнялось шести.

Биполярные транзисторы в одном плече усилителя мощности образованы соединением трех составных инжекционно-вольтаических транзисторов, каждый из которых состоит из дискретных транзисторов n-p-n типа КТ503Е–15, КТ815Г–17 и КТ819Г–19. В другом плече усилителя мощности биполярные транзисторы образованы соединением трех составных инжекционно-вольтаических транзисторов, каждый из которых состоит из дискретных транзисторов типа n-p-n КТ819Т–14, КТ815Г–16 и типа p-n-p КТ502Е–18. Таким образом, в каждом плече усилителя мощности содержится 9 соединенных биполярных транзисторов (21,27,33,23,29,35,25,31,37 и 20,26,32,22,28,34,24,30,36).

Для улучшения надежности усилителя мощности биполярные транзисторы 20-25, входящие в состав инжекционно-вольтаических транзисторов 14-19, коллекторы которых выполняют роль общего коллектора, располагают на отдельных теплоотводах.

В общем случае количество составных инжекционно-вольтаических транзисторов может составлять 2N, где N – количество составных инжекционно-вольтаических транзисторов в плече усилителя мощности.

В качестве биполярных транзисторов могут быть использованы комплементарные составные биполярные транзисторы, включенные по схеме «общий коллектор - общий коллектор - общий коллектор» в обоих плечах усилителя мощности.

Входное и выходное напряжения совпадают по амплитуде и фазе.

Изменение THD при изменении входного напряжения от 3 В до 16 В составляет от 0,009% до 0,0055% соответственно.

Ток покоя практически не изменяется при изменениях напряжения питания от 2 В до 60 В и температуры от 200 К до 400 К.

Описанный вариант усилителя мощности позволяют стабилизировать его ток покоя. Приэтомдвухтактныйусилительмощностиработаетврежиме АВ. Когда оба плеча двухтактной схемы совместно участвуют в формировании тока нагрузки, то при этом одновременно ток в одном плече усилителя мощности увеличивается, а в другом уменьшается, или наоборот. Для такого усилителя мощности отсутствует область переходных искажений. И это усилитель мощности с малыми искажениями способен устойчиво работать и в режиме А.

Усилитель мощности может использоваться в качестве оконечного каскада усилителей звука, в качестве вторичных источников электропитания, в медицинской технике и так далее.

Литература:

1. П. Шкритек. Справочное руководство по звуковой схемотехнике. - М.: Мир, 1991., с. 198

2. Douglas Self. Audio power amplifier design. Sixth edition. New York and London. 2013 ., p.232-354

А.Н. Фадеев

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ В OMNET++

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: *OMNeT++*, протоколы маршрутизации

В статье описаны, способы реализации наиболее популярных протоколов маршрутизации (*AODV, DYMO, DSR*) в библиотеке *INET* для среды имитационного моделирования *OMNeT++* и показано, что разработанные программные модули легко расширяемые, следовательно, они могут быть использованы для моделирования разрабатываемых протоколов маршрутизации беспроводных самоорганизующихся сетей в будущем.

A.N. Fadeev

IMPLEMENTATION OF MOBILE AD-HOC ROUTING PROTOCOLS IN OMNET++

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: *OMNeT++*, routing protocols

This paper describes how some of ad hoc routing protocols (DYMO, DSR, AODV) have been implemented for the INET library of OMNeT++. The developed modules have been programmed so they can be easily extensible to include future routing MANET protocols..

Моделирование – это основное средство для изучения и анализа коммуникационных протоколов, особенно в случае с беспроводными самоорганизующимися сетями. Потребность в имитационном моделировании в данном направлении исследований вызвана сложностью и дороговизной построения подобной сети, включающей в себя огромное количество узлов и разнообразные сценарии использования. Тестовые стенды беспроводных самоорганизующихся сетей разработанные для экспериментальных оценок содержат недостаточное количество узлов, порядка нескольких десятков. Также, учитывая большое число и сложность факторов влияющих на работу беспроводных сетей (распространение сигнала в среде, подвижность узлов, взаимодействие протоколов и пр.) описание данного типа сетей посредством аналитической модели без большого числа упрощений сложная задача.

В настоящее время существует большое число сред имитационного моделирования. Наиболее популярные из них применяемые для моделирования сетей связи: *Network Simulator-2* или *NS-2 [1]*, затем *OPNET[2]* и *OMNeT++[3]*. Наибольшее распространение среди исследователей беспроводных самоорганизующихся сетей получила среда моделирования *OMNeT++*. *О*сновные плюсы среды моделирования *OMNeT++:*

1. Это среда моделирования с открытым исходным кодом, таким образом исследователь может создать новые библиотеки или адаптировать существующие в соответствии с используемыми технологиями и сценарием применения.
2. Она предоставляет простой и дружественный интерфейс для программирования, упрощающий разработку нового кода.
3. В ней используется модульная структура, упрощающая реализацию новых протоколов связи. Таким образом, добавление нового протокола не требуют полного знания о том, каким образом работают остальные части кода. Более того, различные сетевые уровни и протоколы взаимодействуют посредством сообщений, таким образом программисту необходимо быть знакомым только с форматом этих сообщений.
4. Код *OMNeT++* высокоэффективен, что приводит к значительному уменьшению времени моделирования в сравнении с другими средами моделирования [кто сказал?] (в частности, *NS-2*).
5. Сообщество *OMNeT++* получило широкое распространено в глобальной сети интернет.

В настоящее время библиотеки для *OMNeT++* включают в себя реализацию стека протоколов *UDP/TCP/IP* наряду с различными реализациями интерфейсов физического и канального уровня, включая *IEEE802.11*, которые применяются для анализа и оценки беспроводных самоорганизующихся сетей. Следовательно, *OMNeT++* удобное средство для исследований беспроводных самоорганизующихся сетей. Более того, распределенная природа беспроводных самоорганизующихся сетей ограничивает применение классических протоколов маршрутизации, таких как *OSPF*. Таким образом, за последние десять лет, появилось большое число специфичных протоколов маршрутизации беспроводных самоорганизующихся сетей. Некоторые из них были включены в состав основных библиотек для *OMNeT++*. Рассмотрим наиболее популярные из них: *AODV(Ad hoc On Demand Distance Vector [4]), DYMO (Dynamic MANET On-demand Routing Protocol* [6]*), DSR (Dynamic Source Routing* [5]*).*

В процессе разработки протоколов маршрутизации в беспроводных самоорганизующихся сетях в *OMNeT++,* в большей степени были адаптированы существующие общедоступные версии протоколов, используемые для других сред моделирования, а не программирование протоколов маршрутизации с нуля на основе документов *IETF RFC.* Таким образом, был использован готовый, уже проверенный код, что значительно сократило время разработки. В дополнении, адаптация уже разработанного программного обеспечения позволила произвести более тщательное сравнение результатов моделирования с исследованиями, проведенными в других средах.

Существует несколько доступных реализаций протоколов маршрутизации беспроводных самоорганизующихся сетей. Тем не менее, наилучшими кандидатами для миграции на *OMNeT++* были выбраны те, что разработаны для работы с ядром линукс. Эти реализации часто используются в малых и энергоэффективных портативных устройствах под управлением линукс-подобной операционной системы. Выбор любой из этих реализаций в среде моделирования *OMNeT++* позволит сопоставить результаты моделирования с результатами работы реальных сетей. Таким образом, за основу для моделирования беспроводных самоорганизующихся сетей в среде *OMNeT++* были использованы одни из наиболее популярных и используемых реализаций протоколов *AODV* и *DSR* разработанных в Университете Уппсалы [7]. Аналогично для протокола *DYMO* была использована реализация протокола, разработанная в университете Мурции[7]. Это версия была получена от реализации *AODV-UU* разработанной в университете Уппсалы, что облегчило её адаптацию после того внедрения протоколов *AODV* и *DSR* в этой среде моделирования.

Для описания протоколов маршрутизации беспроводных самоорганизующихся сетей в *OMNeT++* используется модуль (Рисунок 1) *manetRouting* который в свою очередь включает модуль управления *Manet Manager.* Этот модуль кроме реагирования на события маршрутизации, также управляет таблицами *IP* маршрутизации. К примеру, при старте моделирования *Manet Manager* удаляет все записи из таблицы маршрутизации, поэтому сетевой уровень передает сгенерированные пакеты этому новому модулю, который начинает процесс поиска пути до узла назначения пакета. Процесс поиска осуществляется модулем в котором реализован алгоритм маршрутизации беспроводной самоорганизующейся сети. Соответствующие реализации протоколов маршрутизации выполнены в виде 3 подмодулей в модуле *Manet Manager*. После того, как маршрут был найден, *Manet Manager* обновляет таблицу маршрутизации соответствующим образом. В момент, когда сетевой уровень не находит адекватного маршрута для пришедшего пакета, начинается процесс поиска маршурта. Так как протоколы маршрутизации реализованы в различных модулях, то используется только инициированный модуль протокола маршрутизации. Это оптимизирует использование ресурсов средой моделирования, так как не используемые модули не занимают место в памяти.

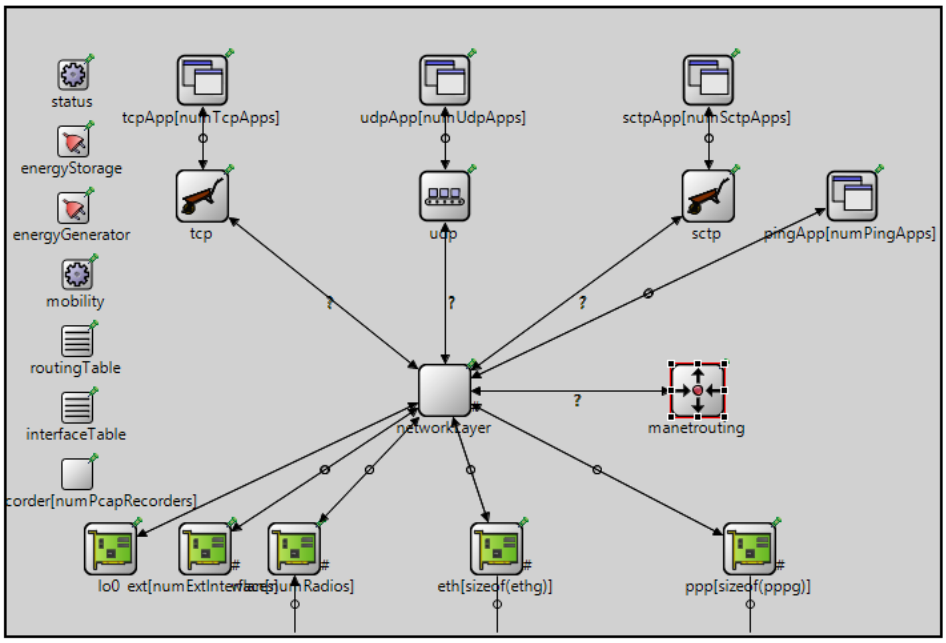


Рисунок 1. Модель узла сети с модулем *ManetRouting*

Базовым сообытием в *OMNeT++* является сообщение, первый шаг для разработки новых модулей - определение и настройка форматов сообщений протоколов, которые будут использоваться. Реализация сообщений основана на структурах языка C "*struct*", где каждое поле сообщения определено элементом, который является частью конструкции "*struct*" доступной в коде. Эти поля определены как публичные атрибуты классов *C++* которые описывают сообщения. Реализация пакетов посредством конструкций C (вместо использования проприетарного формата сообщений *OMNeT++*) позволила уменьшить изменения в адаптированном коде оригинального протокола маршрутизация и увеличило совместимость кода с другими средами моделирования, такими как *ns2*.

Таблица 1.

Протокол	Родительский класс	Предоставляет	Тип сообщений
AODV	*cPacket*	*TLV(Time Length Values) Fields*	*RREQ, RREP, RRER, HELLO*
DYMO	*cPacket*	*TLV Fields*	*RE, UERR, RRER, HELLO*
DSR	*IPDatagram*	*Header DSR*	*RREQ, RREP, RRER, Source Forwarding*

Все применяемые сообщения (Таблица 1) определены сходными способами и содержат специальное поле, позволяющее передавать информацию в бинарном векторе. Это поле создано для передачи специфических данных используемых в протоколах маршрутизации беспроводных самоорганизующихся сетей. Оператор копирования используется для распространения этой информации как пакетов (и сообщений OMNeT++) распространяющихся по сети

В случае с *AODV* и *DYMO*, когда сетевой уровень получает пакет он ищет путь в соответствующей таблице маршрутизации которая содержится в модуле *routingTable* (Рисунок 1). Если нет подходящего маршрута в таблице, пакет пересылается в модуль *manetRouting*. В этот момент модуль маршрутизации откладывает пакет в буфер и начинает процесс поиска пути, с целью найти существующий путь до назначения. После того как путь найден, таблица маршрутизации обновляется и пакет передается на сетевой уровень, так как может быть передан к следующему узлу. С другой стороны, так как *DSR* схема маршрутизации от источника она

предлагает альтернативную маршрутизацию для сетевого уровня, так весь список адресов узлов через которые должен пройти пакет чтобы достичь назначения содержится в заголовке. Т.е. модуль *DSR* не изменяет таблицу маршрутизации. Более того все возможные пути от источника хранятся в специальной отдельной структуре. Таким образом сетевой уровень не принимает участие в маршрутизации пакетов, а эта операция полностью поддерживается модулем *DSR*.

Беспроводная и совместная природа беспроводных самоорганизующихся сетей также требуют модификации механизма поиска в таблицах маршрутизации. В обычных *IP* сетях этот поиск основан на префиксе *IP* адреса. С другой стороны в случае с маршрутизацией в беспроводных самоорганизующихся сетях, адрес пришедшего пакета должен полностью совпадать с одной из записей в таблице маршрутизации. В классической схеме маршрутизации стоит задача определения исходящего интерфейса через который будет передан принятый пакет. Но в беспроводных самоорганизующихся сетях узел обладает одним интерфейсом (например 802.11) и маршрутизация заключается в разрешение адреса соседнего узла, которому должен быть передан принятый пакет. Как только этот адрес будет найден в таблице маршрутизации, соответствующий MAC адрес будет определен посредством протокола *ARP* или ему подобных.

Результаты моделирования в среде OMNeT++ должны быть сравнимы с результатами, полученными в реальных беспроводных самоорганизующихся сетях, так как реализация этих протоколов получены путем адаптации кода написанного для других сред моделирования. Описанные в этой работе описаны адаптации различных протоколов маршрутизации беспроводных самоорганизующихся сетей планируется сравнить с реализациями протоколов в других средах имитационного моделирования. А именно рассмотреть протоколы *AODV*, *DSR* и *DYMO,* которые наиболее распространены в работах посвященных беспроводным самоорганизующимся сетям.

Литература:

1. Network Simulator 2, http://www.isi.edu/nsnam/ns/

2. Opnet, http://www.opnet.com

3. OMNeT++, http://www.omnetpp.org

4. Perkins, C., Royer, E. and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, RCF-3561, IETF, 2003.

5. D. Johnson, Y. Hu, D. Maltz “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, RCF-4728, IETF, 2007.

6. I. D. Chakeres and C. E. Perkins "Dynamic MANET On demand Routing Protocol". IETF Internet Draft, draft-ietfmanet-dymo-10.txt, July 2007 (Work in Progress).

7. Implementation of AODV and DSR routing protocols University of Uppsala (Sweden), available at: http://www.it.uu.se/research/group/coregroup/software

Э.Л. Портнов, Т.Д. Фатхулин

ТЕХНОЛОГИИ УВЕЛИЧЕНИЯ СКОРОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В СОВРЕМЕННЫХ DWDM СИСТЕМАХ СВЯЗИ

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: когерентные системы, емкость формата, суперканал, скорость передачи, формат модуляции.

Целью данной статьи является анализ разрабатываемых технологий, направленных на достижение максимальных скоростей передачи информации в современных DWDM системах. Рассмотрены два варианта технического решения проблемы. Наиболее эффективным представляется вариант DWDM системы, предполагающей разработку и производство оборудования с возможностью перестройки лазера с шагом сетки частот 33ГГц, использования C и L диапазонов, применения формата модуляции DP-QPSK, обеспечивающего необходимую

спектральную эффективность. Предлагается метод управления каналами при использовании DWDM систем. В заключении сделаны выводы.

E.L. Portnov, T.D. Fatkhulin

TECHNOLOGIES INCREASING DATA TRANSMITTION RATE IN MODERN DWDM COMMUNICATION SYSTEMS

The Moscow Technical University of Communication and Informatics, Moscow, Russia

Keywords: coherent systems, format capacity, super-channel, data rate, modulation format.

The purpose of this article is to analyze emerging technologies to achieve maximum data transmission rate in modern DWDM systems. Two variants of the technical solution to the problem are considered. The most effective option seems to be DWDM systems, involving the development and production of equipment with the possibility of tuning the laser frequency grid of 33GHz, use C and L bands, the use of modulation format DP-QRSK providing the necessary spectral efficiency. A method of channel management using DWDM systems is worked out. Finally, the conclusion is made.

Целью современных систем передачи информации является достижение максимально возможных скоростей передачи с применением наиболее эффективного оборудования. Современные транспондеры с канальной скоростью 100Гбит/с обеспечивают скорость передачи до 8,8 Тбит/с, используя С-диапазон и сетку частот с шагом 50 ГГц. Применяя C+L диапазон с такой же сеткой частот, возможно добиться увеличения скорости до 18 Тбит/с. Уменьшив сетку частот до 33 ГГц, возможно получить DWDM систему, обеспечивающую скорость передачи информации 25 Тбит/с.

Технически это можно реализовать, используя 250 каналов. Канальная скорость в каждом из них составляет 100 Гбит/с с применением формата модуляции DP-QPSK. С целью повышения эффективности управления системой используются суперканалы со скоростью передачи 1 Тбит/с в каждом [3, С.24].

Существуют два способа технической реализации систем с емкостью 25 Тбит/с, различающихся используемым шагом между каналами. Первый вариант основан на стандартной сетке частот 50 ГГц с гибридными EDFA усилителями в полосе C и L+UL. При этом необходимо применение рамановских усилителей с полной шириной спектра усиления около 100 нм. При таком решении, хотя и используются пассивные компоненты, выпускаемые промышленностью, активные передатчики и приемники, работающие в L диапазоне отсутствуют. Нет и усилителей с полосой усиления около 100 нм.

При осуществлении второго варианта необходимо применение усилителей с полосой усиления около 70 нм, использование сетки частот с шагом 33 ГГц и EDFA или гибридных усилителей, работающих в диапазонах C и L. Несмотря на то, что усилители с такой полосой усиления не производятся современной промышленностью, их разработка и создание значительно проще в сравнении с первым вариантом. При этом необходимо отметить, что требуется разработка активных и пассивных компонентов, работающих с нестандартной сеткой частот в 33 ГГц. В перспективе для технического решения проблемы предпочтение отдается второму варианту. В предлагаемых оптических модулях предлагается создание задающих, а также опорных лазеров, которые могут перестраивать длину волны излучения в диапазонах C и L с шагом перестройки 33 ГГц. Полоса усиления оптических усилителей, составляющая 70нм, может быть достигнута путем использования двухканальных усилителей с полосовым мультиплексором и демультиплексором. Структурная схема реализуемой системы представлена на Рисунке 1.

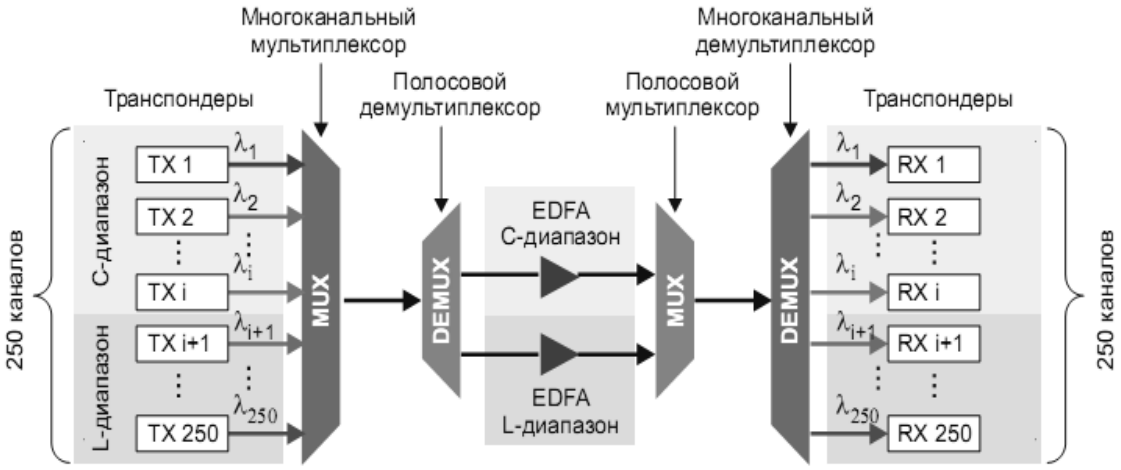


Рисунок 1.Структурная схема реализуемой системы связи: TX i - передающие части транспондеров, RX i – принимающие части транспондеров

С целью минимизации помех в соседних каналах из-за применения сверхплотного мультиплексирования наиболее оптимальным является формирование спектра сигналов, близкий к прямоугольному [3, С.26]. Технологически это становится возможным при применении жесткой оптической фильтрации с прямоугольным спектром пропускания, а также электронного метода управления спектром сигнала. При фильтрации неравномерность спектров центральной части можно скомпенсировать, применяя фильтры, согласованные с сигналом. В таких фильтрах происходит увеличение потерь в центральной части полосы пропускания, а по краям полосы пропускания потери минимальные.

Как было отмечено выше, количество передаваемых каналов составляет 250. Для оптимизации управления сетью следует применять суперканалы, содержащие некоторое количество несущих, называемых поднесущими. Суперканалы, проходящие по системе передачи, будут управляться как единое целое при помощи оптических маршрутизаторов и коммутаторов. При этом, так как скорости передачи будут терабитными, станет возможной поддержка стандарта Terabit Ethernet.

Благодаря возрастанию скорости передачи в одном канале использованию новых рабочих диапазонов возможно повышение емкости современных систем передач. Так как существуют физические ограничения на скорость передачи символов в пределах 50 Гбод, то возникают трудности при переходе на скорость передачи в одном канале 100 Гбит/с, что может быть решено применением многоуровневых форматов модуляции. В настоящее время использование когерентных систем позволяет применять многоуровневые форматы модуляции, что дает существенное возрастание скорости передачи информации, определяемое емкостью формата. Система связи, построенная при использовании формата DP-QPSK, способна иметь спектральную эффективность свыше 3бит/с/Гц при применении сетки частот с шагом в 33 ГГц. Это позволит иметь суммарную скорость 25 Тбит/с при работе в диапазоне от 1540 нм до 1610 нм [4, С.851]. Стоит отметить, что применение многоуровневых nQAM модуляций позволит достичь канальных скоростей передачи от 200 Гбит/с до 400 Гбит/с (Рисунок 2). Однако, при увеличении количества символов пространство между ними быстро уменьшается, что приводит к увеличению чувствительности к шумам и требуемому оптическому отношению сигнал-шум [1,2].

Gbps	# Pol.	Gbaud	Grid (GHz)	Bits/Symbol	Modulation	OSNR (dB) min.
112	2	28	50	2	DP-QPSK	12.6
224	2	28	50	4	DP-16QAM	17.4
448	2	112	200	2	DP-QPSK	18.6
448	2	56	100	4	DP-16QAM	22.4
448	2	42	75	6	DP-64QAM	26.6
448	2	28	50	8	DP-256QAM	31.9

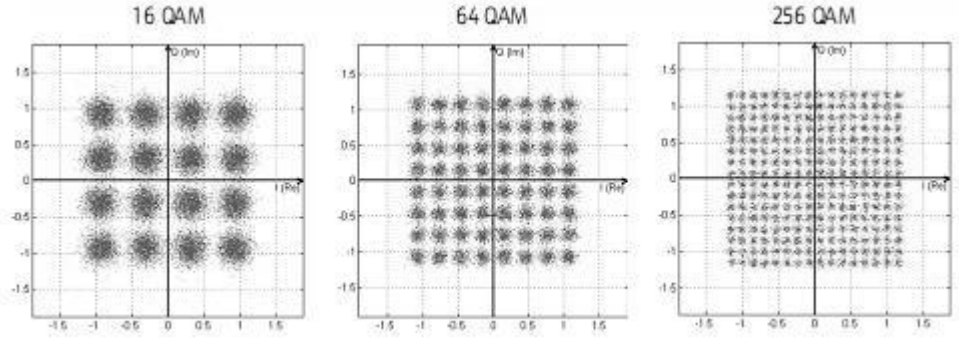


Рисунок 2. Сигнальные созвездия, используемые фирмой FUJITSU:
Gbps-Гбит/с; #Pol.-количество поляризаций; Gbaud-Гбод; Grid (GHz)–сетка частот (ГГц); Bits/Symbol- Бит/символ; Modulation- модуляция; OSNR-ООСШ (оптическое отношение сигнал-шум)

Таким образом, можно сделать следующие выводы: предлагаемая техническая реализация обеспечивается использованием формата модуляции DP-QPSK, что позволит получить спектральную эффективность около 3 бит/с/Гц; это в свою очередь обусловит возможность применения 250 каналов со скоростью 100 Гбит/с в одном канале в C+L диапазоне около 70нм; для решения проблемы с управлением каналами предлагается их объединение в суперканалы. Все это позволит построить высокоэффективную систему передачи информации с суммарной скоростью 25Тбит/с.

Литература:

1. Гордиенко В.Н., Крухмалев В.В., Моченов А.Д., Шарафутдинов Р.М. Оптические телекоммуникационные системы. – М.: Горячая линия – Телеком, 2011 – 370 с.

2. Портнов Э.Л. Оптические кабели связи, их монтаж и измерение. Учебное пособие для вузов. – М: Горячая линия-Телеком, 2012. – 448 с: ил.

3.Трещиков В.Н. Разработка DWDM-системы емкостью 25 Тбит/с.// Фотон-экспресс, 2013, № 2 (106), С.24–28.

4. Winzer P. J. Energy-efficient optical transport capacity scaling through spatial multiplexing. // Photon. Technol. Lett., 2011, v. 23, pp. 851–853.

В.В. Федотов. *Б.П. Борисов

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ АППАРАТУРЫ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ

Ростовский филиал ОАО «Ростелеком», г. Ростов-на-Дону
* Северо-Кавказский филиал Московский Технический Университет связи и информатизации г. Ростов-на-Дону, Россия

Ключевые слова: Нейрокомпьютеры, технологии, системы, маршрутизация, эволюция, сети, алгоритмы, каналы, кодирование.

Детальный анализ зарубежных разработок нейрокомпьютеров позволил выделить основные, перспективные направления современного развития нейрокомпьютерных технологий: нейропакеты, нейросетевые экспертные системы, СУБД с включением нейросетевых алгоритмов, обработка изображений, управление динамическими системами и обработка сигналов, маршрутизация, управление финансовой деятельностью, оптические нейрокомпьютеры, виртуальная реальность.

V.V. Fedotov, *B.P. Borisov

MODEL OF FUNCTIONING COMMUNICATIONS EQUIPMENT USING NEURAL NETWORK ALGORITHMS

Rostov branch of OAO "Rostelecom", Rostov-na-Donu
* North Caucasian branch of the Moscow Technical University of Communications and Informatization of Rostov-on-Don, Russia

Keywords: neurocomputers, technologies, systems, routing, evolution, network, algorithms, channels, encoding.

Detailed analysis of foreign elaborations of neurocomputers made it possible to find main, perspective directions of modern development of neurocomputer technologies: neuropackets, neuronetwork expert systems, database management system using neuronetwork algorithms, images processing, dynamic systems management, signal processing, routing, financial management, optical neurocomputers, virtual reality.

Мировые тенденции конца 90-х годов в области телекоммуникаций характеризуются широким внедрением новых технологий, позволяющих не только существенно расширять перечень предоставляемых услуг, но повысить их качество. Вместе с тем, сети электросвязи становятся все более компьютеризированными. Указанные факторы, определяющие эволюцию сетей электросвязи, в первую очередь обусловлены влиянием заказчиков или конечных пользователей сети и определяют необходимость управления процессами эксплуатации сетей электросвязи в рыночных условиях. Развитие техники автоматической коммутации, взаимное проникновение вычислительной техники в технику связи и техники связи в вычислительную технику привели к разработке высокоорганизованных динамических систем управления сетями связи, потоками информации и процессами обслуживания заявок абонентов на передачу информации. Такие динамические системы управления обеспечивают устранение или ослабление влияния возникающих неисправностей отдельных элементов сети и изменения во времени потоков информации между абонентами и узлами сети на качество обслуживания заявок абонентов и качество передачи информации. Например, система управления, обнаружив ухудшение качественных характеристик тех или иных каналов, перестраивает порядок выбора каналов так, что эти каналы будут заниматься в последнюю очередь. Аналогично может быть построена динамическая система управления, позволяющая уменьшить либо вероятность потерь вызовов, либо время задержки установления соединения, т.е. время нахождения информации (например, данных) в сети за счет выбора оптимального пути ее передачи в условиях, создавшихся в этот момент времени на сети.

Последний по времени всплеск интереса к сетям коммутации каналов имел место в 90-е гг. в связи с появлением существенных технологических изменений в системах управления телефонными сетями, что привело к появлению серии работ по методам динамической маршрутизации в телефонных сетях. Однако основное внимание в этот период уделялось не столько получению новых теоретических результатов, относящихся к вопросам моделирования таких сетей и процессов управления в них; сколько применению уже имеющихся методов с учетом появившихся новых возможностей по организации управления.

Исходными данными для модели являются: информация о структуре вторичной телефонной сети и входном трафике; организация маршрутизации в сети; критерий оптимизации функционирования сети; наличие ограничений на гарантированные минимальные уровни обслуживания.

Область применения искусственных нейронных сетей постоянно расширяется. В телекоммуникационных системах они находят применение при решении следующих важных задач [3]: управление коммутацией, адаптивная маршрутизация, управление трафиком, оптимальное распределение загрузки каналов сети. Кроме того, перспективным является использование нейросетевых алгоритмов в задачах кодирования и декодирования информации.

Сеть управления, в данном случае, должна отвечать таким требованиям как малая инерционность, умение самостоятельно решать поставленные перед ней задачи, иметь большую память (для сетей с большим количеством узлов).

Для решения задачи управления был выбран аппарат нейронных сетей. Нейронные сети – мощный аппарат для имитации процессов и явлений, который предоставляет возможность воспроизводить достаточно сложные зависимости. Нейронные сети позволяют находить решения для задач с высокой размерностью. Другая особенность нейронных сетей – возможность обучения такой сети.

Адаптивная маршрутизация является одной из важнейших задач для телекоммуникационных сетей различного назначения. Эти задачи, связанные с выбором маршрута, планированием работы маршрутизаторов относятся к классу комбинаторно-оптимизационных задач, не имеющих простых аналитических решений. Кроме того, вычислительные затраты экспоненциально возрастают при увеличении количества узлов в сети. В то же время для решения таких задач можно использовать модели построения на основе нейронной сети Хопфилда, впервые примененные для решения задачи коммивояжера. Большинство последующих работ в этой области, так или иначе базируются на использовании таких моделей.

Искусственная нейронная сеть состоит из простейших элементов сети – искусственных нейронов. Модель искусственного нейрона: векторный или скалярный входной сигнал умножается на векторный или скалярный весовой коэффициент, результирующий взвешенный вход является аргументом функции активации нейрона (единичная, логистическая).

Задачей разработчика системы управления маршрутизацией является: выбор сети с определенной технологией, определение набора параметров, которые необходимы для управления, подбор структуры нейронной сети. После определения количества слоев сети и число нейронов в каждом из них, назначается значение весов и смещений, которые минимизируют ошибку решения. Это достигается с помощью процедур обучения. Процесс обучения – процесс подгонки параметров той модели процесса или явления, которая реализуется нейронной сетью. Алгоритмы обучения нейронных сетей аналогичны алгоритмам поиска глобального экстремума функций многих переменных. Алгоритм обучения должен обеспечивать универсальность модели управления маршрутизацией.

Алгоритм управления потоками на одном узле состоит в следующем. В течение некоторого времени гипотетический прибор собирает информацию о состоянии сети. На вход нейронной сети, с одним слоем и числом нейронов N поступает некоторая информация, в соответствии с которой, сеть находит образ на выходе и устанавливается в состояние равновесия. От анализатора сети поступает информация в закодированном виде: число узлов в сети, число каналов, объединяющих эти узлы, узел назначения, количество возможных маршрутов до узла назначения. На выходе такой сети должен образоваться маршрут в зависимости от всех этих факторов.

Применительно к классической задаче коммивояжера, задача формулируется следующим образом [1]: в нейронной сети из $N = n^2$ нейронов из *n!/2n* маршрутов выбрать один с наименьшей длиной. Причем состояние каждого нейрона описывается двумя индексами.

Для решения данной задачи составляется функция вычислительной энергии для нейронной сети, предназначенной для решения задачи коммивояжера. Пусть состояние с наименьшей энергией соответствует самому короткому маршруту. В общем виде такая функция для рассматриваемой нейронной сети может иметь следующий вид [4]:

$$E = -\frac{1}{2}\sum_i \sum_j w_{ij} Y_i Y_j - \sum_j I_j Y_j - \sum_j T_j Y_j \quad , \qquad (1)$$

где E - искусственная энергия сети, w_{ij} - вес от входа нейрона i к входу нейрона j, Y_j - выход нейрона j, I_j – внешний вход нейрона j, T_j – порог нейрона j.

Изменение энергии, вызванное изменением состояния j – нейрона, можно вычислить следующим образом:

$$\delta E = \left(\sum \left(w_{ij} Y_i \right) + I_j - T_j \right) \delta Y_j , \quad (2)$$

где δY_j - изменение выхода j-го нейрона.

Развитие системы – нахождение из множества состояний такое, в котором энергия достигнет минимального значения.

Однако для рассматриваемой системы функция энергии должна удовлетворять следующим требованиям [2]. Во-первых, она должна поддерживать устойчивые состояния. Во-вторых, из всех возможных решений функция энергии должна поддерживать те, которые соответствуют коротким маршрутам. Этим требованиям удовлетворяет функция энергии вида (при этом, Y_i =0,1):

$$E = \frac{A}{2} \sum_x \sum_i \sum_{j \neq 1} Y_{xi} Y_{xj} + \frac{B}{2} \sum_i \sum_x \sum_{k \neq 1} Y_{xi} Y_{ki} + \frac{C}{2} \left(\sum_x \sum_i Y_{xi} - n \right)^2 + \frac{D}{2} \sum_x \sum_{k \neq x} \sum_i d_{xk} Y_{xi} \left(Y_{kj+1} + Y_{kj-1} \right) . \quad (3)$$

Первые три члена выражения (3) поддерживает первое требование, четвертый член – второе; A, B, C, D – положительные множители. Первый член равен нулю, если посещается город только один раз, второй член равен нулю, если в каждый момент посещается только один город. Третий член равен нулю, если посещаются все города. Таким образом, при правильно решенной задаче коммивояжера, без учета четвертого члена, функция энергии имеет минимумы во всех состояниях, соответствующих посещению всех городов, причем в каждый момент посещается только один город и каждый город посещается один раз. Все другие состояния имеют более высокую энергию. Короткие маршруты поддерживает четвертый член. В нем индексы i, беруться по $mod\ n$, для того, чтобы показать, что i –й город соседствует в маршруте с (n-1) –м и первым. Т.е. $Y_{k,n+j} = Y_{kj}$. Четвертый член численно равен длине маршрута.

Раскрывая скобки в (3) и приравнивая коэффициенты при квадратичных и линейных членах в полученном выражении и общей формуле:

$$x(k+1)=f(x(k),u(k)), \quad (4)$$

где $u(k)$–вектор входных сигналов, $x(k+1)$- вектор выходных сигналов, k=0,1,.. -дискретное время.

Определяем матрицу связей и внешние взаимодействия:

$$w_{xi,ki} = -A\delta_{xk}(1-\delta_{ij}) - B\delta_{\square\square}(1-\delta_{xk}) - C - Dd_{xk}(\delta_{j,i+1}+\delta_{j,i-1}), \quad (5)$$

где, δ_{ij} =1, если $i=j$, в противном случае δ_{ij} =0. Кроме того, каждый нейрон имеет смешанный вес $I_{xi}=Cn$.

Первый член в (5) задает связи нейронов в каждой строке, второй – внутри каждого столбца, третий и четвертый глобальные связи. И в (3) и в (5) три первых члена отвечают за общие ограничения для любой задачи коммивояжера и приводят нейронную сеть в устойчивое состояние. Четвертый член управляет тем, какое из $\frac{n!}{2n}$ возможных различных финальных состояний соответствует самому короткому маршруту.

Рассмотрим другую постановку задачи [4]. Выбор маршрутов, максимизирующих степень узла в сети, предоставляет возможность планирования работы сети таким образом, чтобы время выполнения работы в сети было бы минимальным. Степень узла определяется как сумма всех потоков, поступающих в узел и исходящих от узла. Критерий качества работы, который выбирается для задач маршрутизации, должен отражать цели, связанные с соответствующей задачей, составления плана работы линий связи.

Пусть задана сеть, состоящая из нескольких узлов и линий связи, соединяющих эти узлы. Считаем, что трафик в такой сети примерно одинаковый. Однако при приближении к ЧНН (час наибольшей нагрузки) нагрузка на узлы извне лавинообразно возрастает, а внутри сети имеются маршруты, по которым может быть распределен приходящий трафик. Требуется выбрать маршрут между парой источник – приемник с таким расчетом, чтобы минимизировать критерий качества работы.

Показатель качества работы должен согласовываться со структурой нейронной сети Хопфилда. Итак, по аналогии с вышерассмотренной моделью, показатель, называемый “энергией перегрузки” задается формулой:

$$E_b = \frac{1}{2}\sum_{i=1}^{N_{SD}}\sum_{k=1,k\neq i}^{N_{SD}}\sum_{j=1}^{N_p(i)}\sum_{k=1}^{N_p(k)}\left|P_{ij}\cap P_{kl}\right|V_{ij}V_{kl}, \quad (6)$$

где P_{ij} – j-ый маршрут между i-ой парой источник – приемник,

$\left|P_{ij}\cap P_{kl}\right|$ - число узлов, которые совместно используют маршруты P_{ij} и P_{kl},

$Np(i)$ – V_{ij}= { 1, если выбирается P_{ij}; 0, если не выбирается P_{ij}

число вариантов маршрутов, определенных между i –ой парой источник – приемник.

Нейронная сеть эволюционирует от некоторого начального состояния до состояния равновесия функции энергии Ляпунова, которая составляется по аналогии с (1):

$$E_{total} = -\frac{1}{2}\sum_{i=1}^{N_{SD}}\sum_{k=1}^{N_{SD}}\sum_{j=1}^{N_p(l)}\sum_{i=1}^{N_p(l)}T_{ij,kl}V_{ij}V_{kl} - \sum_{i=1}^{N_{SD}}\sum_{j=1}^{N_p(l)}V_{ij}I_{ij}, \quad (7)$$

где $T_{ij,kl}$ –вес соединения между нейронами ij и kl, I_{ij} –ток смещения, прикладываемый к нейрону.

Задача имеет целый ряд ограничений, которыми можно пренебречь, если ввести ограничения на целевую функцию. Учитывая эти обстоятельства можно сказать, что конечное состояние зависит от начального состояния.

Литература:

1. Комашинский В.И., Смирнов Д.А. Нейронные сети и их применение в системах управления и связи. - М.: Горячая линия – Телеком,2002.

2. Уоссерман Ф. Нейрокомпьютерная техника: Теория и практика.- М.: Мир,1990.

3. Галушкин А.И. Нейрокомпьютеры в разработке военной техники США – Зарубежная радиоэлектроника, 1995. №6 стр. 4-21.

4. Комашинский В.И., Смирнов Д.А. Внедрение в нейро-информационные технологии. – СПб.: Тема,1999.

***В.В. Федотов, Б.П. Борисов**

МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ И ИНФОРМАЦИОННОЙ ИНТЕГРАЦИИ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ

*Ростовский филиал ОАО «Ростелеком»
Северо-Кавказский филиал Московский Технический Университет связи и информатизации г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии в области обеспечения реализации процессов жизненного цикла.

Одним из направлений повышения эффективности отраслевого и промышленного секторов экономики является применение современных информационных технологий для обеспечения процессов, протекающих в ходе всего жизненного цикла продукции и ее компонентов.

***V.V. Fedotov, B.P. Borisov**

PREDICTIVE SUPPORT AND INFORMATION MANAGEMENT INTEGRATION OF PRODUCTION PROCESSES

*Rostov branch of JSC "Rostelecom"
North Caucasian branch of the Moscow Technical University of Communications and Informatization of Rostov-on-Don, Russia

Keywords: information technology in the field of implementation of life cycle processes. One of the ways of increasing the efficiency of the industry and the industrial sector is the use of modern information technology to ensure the processes that occur during the life cycle of the product and its components.

Современные условия характеризуются все более жесткой конкуренцией на международном рынке, повышением сложности и наукоемкости продукции, что ставит перед промышленниками и предпринимателями страны новые проблемы. К их числу относятся:

- критичность времени, требующегося для создания изделия и организации его продажи;
- снижение всех видов затрат, связанных с созданием и сопровождением изделия;
- повышение качества процессов проектирования и производства;
- обеспечение гибкого и надежного эксплуатационного обслуживания.

Действенным средством решения этих проблем в последнее десятилетие выступают новые информационные CALS-технологии сквозной поддержки сложной наукоемкой продукции на всех этапах ее жизненного цикла (ЖЦ) от маркетинга до утилизации. Базирующиеся на стандартизованном едином электронном представлении данных и коллективном доступе к ним, эти технологии позволяют существенно упростить выполнение этапов ЖЦ продукта и повысить производительность труда, согласно западному опыту, примерно на 30%, автоматически обеспечить заданное качество продукции.

Жизненный цикл (ЖЦ) продукта, как его определяет стандарт ISO 9004-1, - это совокупность процессов, выполняемых от момента выявления потребностей общества в определенной продукции до удовлетворения этих потребностей и утилизации продукта.

Все многообразие этих процессов можно представить в виде прямых и обратных связей поставщика с субпоставщиком и потребителем.

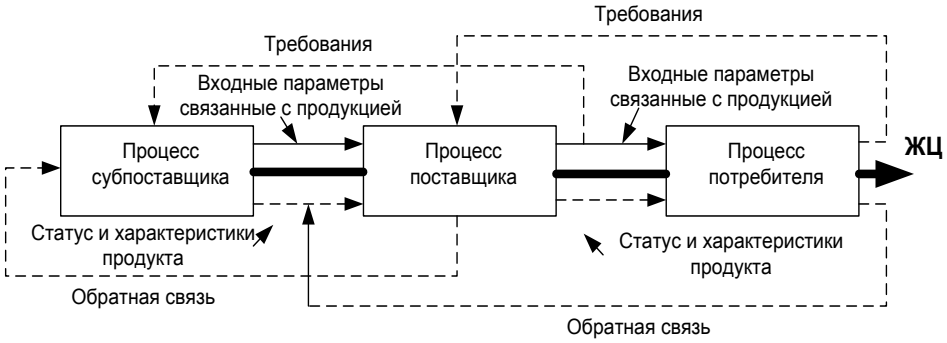


Рисунок 1. Жизненный цикл продукта.

В общем случае ЖЦ необходимо рассматривать как совокупность ЖЦ конечного продукта и ЖЦ входящих в него компонентов, результатов деятельности субпоставщиков. С этой точки зрения ЖЦ представляет собой древовидную структуру, состоящую из следующих компонентов:

- Маркетинг и изучение рынка;
- Проектирование и разработка продукции;
- Планирование и разработка процессов;
- Закупки;

- Производство;
- Упаковка и хранение;
- Реализация;
- Установка и ввод в эксплуатацию;
- Техническая помощь и обслуживание;
- Эксплуатация или потребление;
- Утилизация.

Информационное взаимодействие субъектов, участвующих в поддержке ЖЦ, должно осуществляться в едином информационном пространстве. В основе концепции единого информационного пространства лежит использование открытых архитектур, международных стандартов и апробированных коммерческих продуктов обмена данными.Стандартизации подлежат форматы представления данных, методы доступа к данным и их корректной интерпретации.

Информационная интеграция базируется на применении следующих интегрированных моделей:

- продукта;
- ЖЦ продукта и выполняемых в его ходе бизнес-процессов;
- производственной и эксплуатационной среды.

Интегрированная модель продукта обеспечивает обмен конструкторскими данными между проектировщиком и производителем, является источником информации для расчета потребности в материалах и создания электронных справочников по эксплуатации продукта и т. д.

Моделирование жизненного цикла продукта и выполняемых бизнес-процессов. Первый шаг к повышению эффективности организационной структуры, поддерживающей одну или несколько стадий ЖЦ продукта, - моделирование и анализ ее функционирования.

Цель бизнес-анализа - выявить существующее взаимодействие между составными частями и оценить его рациональность и эффективность. Для этого с использованием CALS- технологий разрабатываются функциональные модели, содержащие детальное описание выполняемых процессов в их взаимосвязи. Формат описания регламентирован стандартами IDEF/0 и ISO 10303 AP208. Полученная функциональная модель не только является детальным описанием выполняемых процессов, но также позволяет решать целый ряд задач, связанных с оптимизацией, оценкой и распределения затрат, оценкой функциональной производительности, загрузки и сбалансированности составных частей, т. е. вопросов анализа и реинжиниринга бизнес-процессов (Business Process Reengineering, BPR).

Решение проблемы заключается в переводе эксплуатационной документации на изделие, поставляемой потребителю, в электронный вид. При этом, комплект электронной эксплуатационной документации следует рассматривать как составную часть единой интегрированной информационной модели изделия.

Концепция MRPII.

Эта система планирования должна чётко отвечать на вопрос: "Что конкретно нужно в тот или иной момент времени в будущем?". Для этого она должна планировать потребности в материале, производственные мощности, финансовые потоки, складские помещения и т.д., принимая во внимание текущий план производства продукции (или услуг - здесь и далее) на предприятии. Такая система называется системой планирования ресурсов предприятия, или MRPII-системой (Manufacturing Resource Planning System.

Схематический план работы MRPII-системы можно отобразить следующей диаграммой:

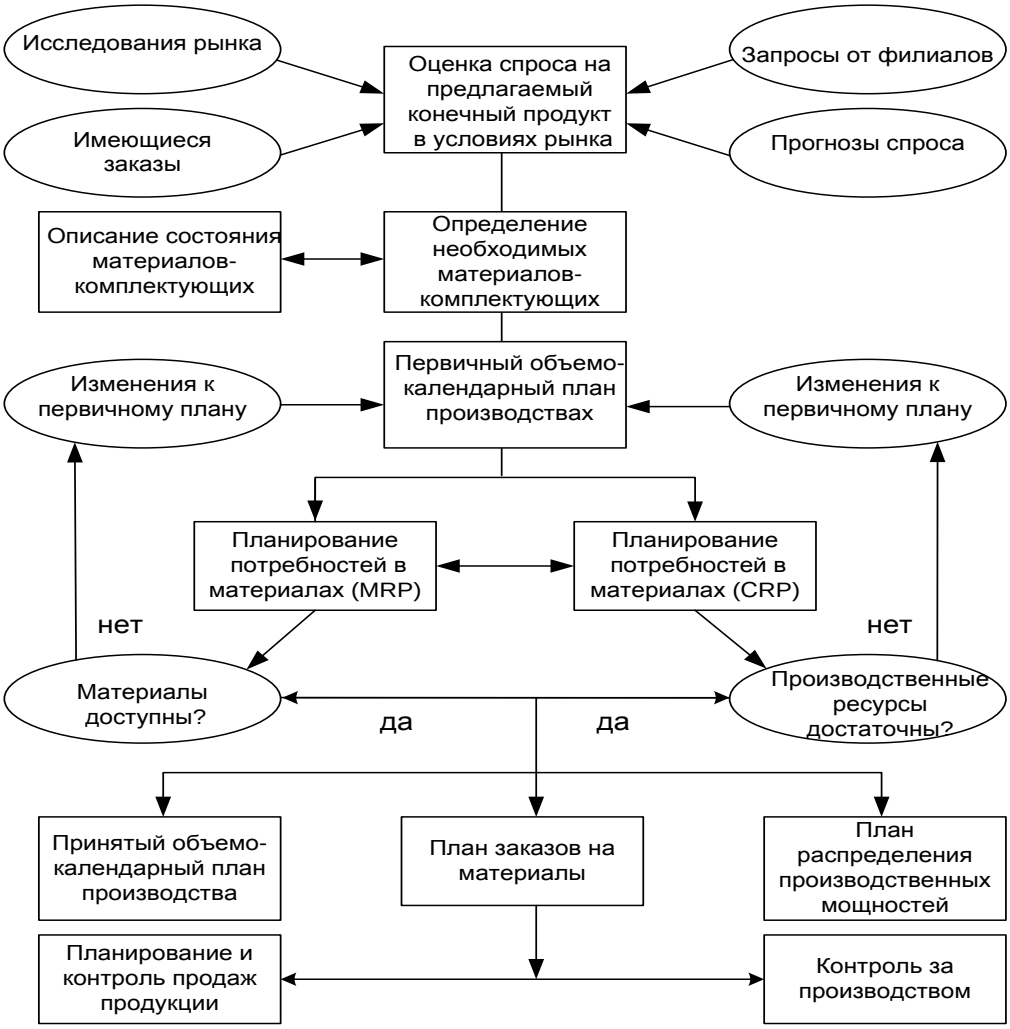


Рисунок 2. Схематический план работы MRPII-системы**.**

Система MRPII состоит из следующих модулей:

- Модуль планирования развития бизнеса;
- Модуль планирования продаж;
- Модуль планирования производства;
- Модуль планирования потребности в материалах;
- Модуль планирования производственных мощностей;
- Модуль обратной связи.

Логика работы MRPII системы достаточно проста. Рассмотрим её на конкретном примере. Первым этапом является составления плана деятельности предприятия. Для этого, сначала определим производственную программу (Master Production Schedule-MPS) в виде следующего выражения: "Будем производить 5 цифровых АТС типа Si-2000 ёмкостью 265 номеров в месяц". Далее, при определении плана деятельности, принимаем во внимание следующие факторы:

1. Текущий инвентарный запас изделий на складе;
2. Определение необходимого количества поддерживаемого инвентарного запаса на складе в тот или иной момент времени в течение всего периода планирования;
3. Прогнозы продаж продукции на планируемый период.

Полный бизнес-план на производственном предприятии, разумеется, включает в себя затраты на новые разработки и развитие, а также ряд других затрат, напрямую не связанных с производством и продажами, но нам для начала достаточно рассмотреть его облегченный вариант. С точки зрения MRPII-системы, план деятельности и бизнес-план не являются независимыми, и, каждый раз, при обновлении плана деятельности, вносятся изменения и в бизнес-план. На основании главной программы производства ("Что собираемся производить?"),

MRPII-система составляет инвентарный список (Bill of materials file) материалов- комплектующих ("Что для этого нужно?") и, сравнивая его с инвентарными запасами имеющимися в наличие (на складе или в позициях активных заказов - "Что имеем в данный момент?"), определяет потребность в материалах ("Что должны приобрести?").

Модуль планирования потребностей в материалах (**MRP - Materials Requirements Planning**) исторически является тем самым зерном, из которого выросла концепция MRPII (Manufacturing Resources Planning, Римская цифра "II" появилась на конце ввиду аналогичности аббревиатур с MRP). Цель этого модуля - так спланировать поставку всех комплектующих, чтобы исключить простои производства и минимизировать запасы на складе.

Входными элементами MRP-модуля являются:

Описание состояния материалов (Inventory Status File)

Этот элемент является основным входным элементом MRP-модуля. В нем должна быть отражена максимально полная информация о всех типах сырья и материалах- комплектующих, необходимых для производства конечного продукта. В этом элементе должен быть указан статус каждого материала, определяющий, имеется ли он на руках, а складе, в текущих заказах или его заказ только планируется, а также описания, его запасов, расположения, цены, возможных задержек поставок, реквизитов поставщиков. Информация по всем вышеперечисленным позициям должна быть заложена отдельно по каждому материалу, участвующему в производственном процессе.

Программа производства (Master Production Schedule)

Этот элемент представляет собой оптимизированный график распределения времени для производства необходимой партии готовой продукции за планируемый период или диапазон периодов.

Перечень составляющих конечного продукта (Bills of Material File)

Этот элемент представляет собой список материалов и их количество, требуемое для производства конечного продукта. Таким образом, каждый конечный продукт имеет свой перечень составляющих.

Результатами работы MRP-модуля являются следующие основные элементы:

План Заказов (Planned Order Schedule)

Этот элемент определяет, какое количество каждого материала должно быть заказано в каждый рассматриваемый период времени в течение срока планирования. План заказов является руководством для дальнейшей работы с поставщиками и, в частности, определяет производственную программу для внутреннего производства комплектующих, при наличии такового.

Изменения к плану заказов (Changes in planned orders)

Этот элемент несёт в себе модификации к ранее спланированным заказам. Некоторые заказы могут быть отменены, изменены или задержаны, а также перенесены на другой период.

Планирование потребностей в производственных мощностях (CRP-Capacity Requirements Planning)

Для того чтобы производственная программа была осуществима, необходимо, чтобы имеющиеся в наличие производственные мощности смогли обработать то количество сырья и материалов-комплектующих, которое предписывает составленный MRP модулем план заказов, и изготовить из них готовые изделия. Собственно MRP-план является основным входным элементом модуля планирования потребностей в производственных мощностях (CRP-модуля). Другим немаловажным входным элементом является технологическая схема обработки/сборки конечного готового изделия (routing plan).

Таким образом, предвидя возможные проблемы заранее, и создавая руководству предприятия условия для предварительного их анализа, MRPII-система является надежным средством прогнозирования и оценки последствий внесения тех или иных изменений в производственный цикл.

Эти методологии и принципы не являются универсальными и определяются исходя из постановки конкретной задачи, применительно к конкретному коммерческому предприятию.

Благодаря всем вышеперечисленным методам и процедурам интеграции и управления процессами производства в современной рыночной среде предприятие сможет:

1. Расширить области деятельности предприятий (рынки сбыта) за счет кооперации с другими предприятиями, обеспечиваемой стандартизацией представления информации на разных стадиях и этапах жизненного цикла. Благодаря современным телекоммуникациям, уже не принципиально географическое положение и государственная принадлежность партнеров. Новые возможности информационного взаимодействия позволяют строить кооперацию в форме виртуальных предприятий, действующих в течение ЖЦ продукта. Становится возможной кооперация не только на уровне готовых компонентов, но и на уровне отдельных этапов и задач: в процессах проектирования, производства и эксплуатации.
2. Повысить эффективность бизнес-процессов, выполняемых в течение ЖЦ продукта; за счет информационной интеграции и сокращения затрат на бумажный документооборот, повторного ввода и обработки информации обеспечить преемственность результатов работы в комплексных проектах и возможность изменения состава участников без потери уже достигнутых результатов.
3. Повысить "прозрачность" и управляемость бизнес-процессов путем их реинжиниринга, на основе интегрированных моделей ЖЦ и выполняемых бизнес-процессов, сократить затраты в бизнес-процессах за счет лучшей сбалансированности звеньев.
4. Повысить привлекательность и конкурентоспособность изделий, спроектированных и произведенных в интегрированной среде с использование современных компьютерных технологий и имеющих средства информационной поддержки на этапе эксплуатации.
5. Обеспечить заданное качество продукции в интегрированной системе поддержки ЖЦ путем электронного документирования всех процессов и процедур.

Литература:

1. Шалумов А.С., Никишкин С.И., Носков В.Н. Введение в CALS-технологии: Учебное пособие. Ковров: КГТА, 2002. - 137 с.

Мартин Дж. Планирование развития автоматизированных систем. – М.: Финансы и статистика, 1984. – 196с.

2. Хаббард Дж. Автоматизированное проектирование баз данных. – М.: Мир, 1984. – 294с.

3. Е.Судов. Информационная поддержка жизненного цикла продукта.//PC Week/RE № (169)45 от 17.11.1998

4. К.Де Роза Планирование ресурсов, синхронизированное с покупателем (CSRP). http://www.socap.ru

5. Питер Пин-Шен-Чен. Модель "Сущность-Связь" - шаг к единому представлению данных. //СУБД №3/1995

6. Орел А. А., Ромакина О.М. Учебное пособие по дисциплине Информационные системы для специальностей ПИЭ и ПИЮ Саратов 2001

А.В. Хабибулин, А.Ю. Орлова

СРАВНЕНИЕ ПЛАТФОРМ РАЗРАБОТКИ И ВНЕДРЕНИЯ КОРПОРАТИВНЫХ ПОРТАЛОВ

Северо-Кавказский Федеральный Университет, г. Ставрополь, Россия

Ключевые слова: повышение эффективности, производительность, взаимодействие, автоматизация, управление, документооборот.

Описана проблема выбора платформы разработки и внедрения корпоративных порталов между Microsoft Sharepoint Server 2010 и 1С-Битрикс: Корпоративный портал. Описаны возможности этих платформ и их функционал. Рассчитана примерная стоимость их покупки для

крупных и средних компаний и малых компаний. После проведенного анализа предпочтение отдано платформе Microsoft Sharepoint Server, поскольку она обладает большими возможностями.

A.V. Habibulin, A.Yu. Orlova

COMPARISON OF THE DEVELOPMENT PLATFORM AND IMPLEMENTATION OF CORPORATE PORTALS

North-Caucasus Federal University, Stavropol, Russia

Keywords: efficiency, productivity, collaboration, automation, control, workflow.

Described the problem of choosing the platform of development and implementation of enterprise portals between Microsoft Sharepoint Server 2010 and 1C-Bitrix Intranet Portal. Describes the features of these platforms and their functionality. Estimate the cost of their purchases for large and medium-sized companies and small companies. After analysis, preference is given to the platform Microsoft Sharepoint Server, because it possesses the big possibilities.

На сегодняшний день рынок корпоративных порталов один из самых быстрорастущих. Понятие корпоративный портал претерпело значительные изменения, как в России, так и во всем мире. Теперь это не только среда, объединяющая классические инструменты, такие как совместная работа с документами, календари, задачи, но и новые - блоги, социальная сеть, интерактивные коммуникации. Главным направлением сейчас является повышение эффективности работы компании за счет создания удобной среды работы для сотрудников и раскрытие потенциала людей.

Все больше компаний в своей деятельности начинают использовать корпоративные порталы, стараясь получить конкурентное преимущество и развить свой бизнес. Для таких компаний становится актуальным вопрос о выборе платформы для разработки и внедрения корпоративного портала. На российском рынке представлено большое количество программных продуктов позволяющих создать собственный корпоративный портал, но формально выбор становится между «1С-Битрикс: Корпоративный портал» и Microsoft Sharepoint Server. Сравнение этих решений и будет темой данной статьи.

При выборе конкретной программной платформы необходимо учесть целый ряд факторов таких как: размер компании, количество сотрудников, структура филиалов, установленное в компании ПО, стандарты существующей ИС, цена, сроки внедрения.

Microsoft Sharepoint Server давно представлена на российском рынке и пользуется большой популярностью среди многих компаний. MS SharePointServer предоставляет собой систему управления корпоративным контентом и совместной работы, используемую в качестве корпоративного портала. MS Sharepoint Server содержит множество расширений и интегрированных систем и позволяющих выполнять такие важные задачи, как управление содержимым и бизнес-процессами, совместного использования информации и ее поиск. SharePoint Server - внутренняя корпоративная система, которая объединяет данные в единый информационный банк, позволяет организовать документооборот компании и работу с корпоративной информацией.

Перечислим основные возможности SharePoint Server [1]:

- система документооборота, работа с документами – коллективная и индивидуальная;
- контроль версий документов;
- хранилище документов;
- поиск документов;
- высокая степень интеграции с Microsoft Outlook, Office;
- опросы и форумы;
- календари событий;
- оповещения;
- списки задач.

Компания, создавшая портал на основе SharePoint получает:

- систему документооборота;

- повышение эффективности работы за счет сотрудничества в режиме реального времени;
- повышение эффективности процессов;
- платформу для последующего развития организации.

1С-Битрикс: Корпоративный портал – самостоятельный программный продукт, выпущенный в 2008 году. 1С-Битрикс: Корпоративный портал построеный на платформе BitrixFramework, на которой также разработан другой популярный продукт компании «1С-Битрикс: Управление сайтом».

Поставка продукта осуществляется в 4 редакциях, различающихся по функционалу. Также, существует сервис «Битрикс24», позволяющий использовать корпоративный портал в режиме SaaS (Software as a Service).

1С-Битрикс: Корпоративный портал предоставляет потребителю следующие возможности [2]:

- корпоративные коммуникации: внутренние – корпоративный мессенджер, видеозвонки; внешние – архивирование e-mail, допуск сторонних пользователей в ограниченную зону с возможностями коммуникаций;
- коллективная работа основанная на задачах и поручениях, совместная работа с документами на портале с помощью MS Office или OpenOffice;
- взаимодействие с партнерами, клиентами, поставщиками;
- поиск по порталу и рабочим группам;
- библиотека общих документов и файлов;
- календари, график отсутствий сотрудников;
- автоматизация бизнес-процессов компании через портал;
- визуальный редактор для проектирования собственных бизнес-процессов, поддерживающий функции drag&drop.

Широкие возможности для доработки портала под собственные задачи компании.

Обе платформы имеют схожий функционал, поэтому решающим фактором при выборе конкретного решения, особенно для средних и малых компаний будет цена. Сравним стоимости лицензий программных продуктов.

Microsoft Sharepoint Server. Подборка оптимального состава лицензий для функционирования корпоративного портала на Sharepoint – сложная задача, верно выполнить которую, даже по мнению Microsoft может только опытный специалист. Поставка Microsoft Sharepoint Server 2010 сопряжена с приобретением следующих лицензий:

- серверная лицензия Microsoft Sharepoint Server 2010 295 029 руб.;
- клиентские лицензии на пользователя и устройства, работающие с сервером 1 755 руб.;
- лицензия на ОС Windows Server 2008 Standart 43 437 руб.;
- лицензия на СУБД SQL Server Standard Edition 429 462 руб.

Лицензирования «1С-Битрикс: Корпоративный портал» намного проще. Поставка продукта осуществляется в двух редакциях: «Корпоративный портал» – 199 500 руб. и «Холдинг» - 499 500 руб.

Лицензия приобретается на одну инсталляцию, вне зависимости от количества серверов. Редакции различаются функциональными возможностями, которые доступны пользователям портала. В большинстве случаев рекомендуется редакция «Бизнес-процессы», обладающая полным набором функциональных возможностей, за исключением многодепартаментности и некоторых специфичных модулей, необходимых для крупных компаний, либо для решений специальных задач. Редакция «Холдинг» предназначена для крупных и территориально распределенных компаний, также позволяет реализовать многофилиальную портальную структуру.

Серверные лицензии не накладывают каких-либо ограничений на возможность доступа к порталу для пользователей из Интернета, следовательно, не возникает дополнительных расходов для организации удаленной работы извне офиса.

Стоимость дополнительного пользователя составляет 1400 рублей и не зависит от редакции. Кроме того в стоимость редакции продукта уже входят 25 пользовательских лицензий.

Также существует лицензия на неограниченное количество пользователей стоимостью 599 000 руб. Эта лицензия выгодна компаниям с количеством пользователей портала более 400 человек

Итого стоимость на компанию в 100 сотрудников, использующую MS SharePoint Server составляет 1 508 028 рублей, для «1С-Битрикс: Корпоративный портал» 304 500 рублей. Для компаний в 500 сотрудников 3 118 029 и 864 500 рублей соответственно.

Исходя из стоимости программных продуктов Microsoft Sharepoint Server будут использовать крупные компании с собственным ИТ отделом, которые уже наслышаны о Sharepoint Server и могут себе позволить многомесячное внедрение. Для предприятий малого и среднего бизнеса, которые часто не располагают собственным ИТ отделом главным критерием будет цена и поэтому выбор будет сделан в пользу «1С-Битрикс: Корпоративный портал».

Литература:

1. Ноэл М., Спенс К. - Microsoft SharePoint. Полное руководство - Пер. с англ. — М.: ООО !И.Д. Вильямс!, 2011.

2. Басыров Р. И. 1С-Битрикс: Корпоративный портал. Повышение эффективности компании 2-е изд. — СПб.: Питер, 2012. — 416 с.: ил.

М.З. Халбаева

УЧЕТ КЛИМАТИЧЕСКИХ ОСОБЕННОСТЕЙ ПРИ ПРОЕКТИРОВАНИИ ОТКРЫТЫХ ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ В АНДИЖАНСКОМ РЕГИОНЕ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: атмосферные оптические системы передачи, достоинства и недостатки технологии, интегральная функция распределения, метеорологическая дальность видимости, километрическое затухание.

По метеорологическим данным, полученным с метеостанций аэропорта г. Андижан, составлена статистика по минимальной дальности видимости. На основании этих данных вычислена интегральные функции распределения минимальной дальности видимости и километрического затухания, необходимая для операторов связи, при учете климатических особенностей данного географического района, при проектировании открытых оптических систем передачи.

M.Z. Halbaeva

CONSIDERATION OF CLIMATIC FEATURES IN DESIGNING OF OPEN OPTICAL TRANSMISSION SYSTEMS IN ANDIZHAN REGION

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Key words: atmospheric optical transmission systems, advantages and disadvantages of the technology, cumulative distribution function, meteorological range of visibility, kilometric attenuation.

According to the meteorological data received from the meteorological station of Andizhan airport, the statistics on meteorological range of visibility has been developed. On the basis of this data the cumulative distribution function of the minimal range of visibility (CDF-MRV), as well as the cumulative distribution function of kilometric attenuation (CDF-KA) are calculated, which are necessary for telecommunication operators for consideration of climatic features of this geographical region in designing of open optical transmission systems.

Организация и развертывание широкополосных сетей, а также поиск альтернативных путей для решения проблем «последней мили» на сегодняшний день является актуальной задачей для многих операторов связи. В качестве решения вышеизложенных проблем, некоторые

операторы выбирают открытые оптические системы связи (ООСП), которые являются следующим поколением беспроводной связи и представляют собой альтернативу проводной, оптоволоконной и радиосвязи [1-2]. Самым весомым преимуществом является использование нелицензируемого диапазона частот, что делает его одним из менее затратных методов организации связи типа «точка-точка».

Достоинствами ООСП являются [2]:

- сверхширокая полоса частот (обуславливает возможность передачи больших объемов информации на большой скорости);
- малая угловая расходимость луча (позволяет не только концентрировать энергию в строго определенном направлении, но и обеспечивает скрытность и высокую помехоустойчивость передаваемых сообщений);
- полное отсутствие боковых лепестков;
- имеют малые габариты приемо-передающих устройств, при сохранности большого коэффициента усиления антенн;
- низкая удельная стоимость бита передаваемой информации;
- совместимость с другими устройствами передачи цифровой информации;
- возможность быстрого и дешевого построения широкополосной сети в условиях города, по сравнению с прокладкой оптического кабеля;
- простота наращивания сети и изменение ее структуры;
- возможность теоретически достичь скорости 160 Гбит/с за счет отсутствия дисперсионных свойств среды;
- отсутствие необходимости получения лицензии радиочастотного органа на использование этого диапазона.

ООСП также имеют ряд недостатков, главным из них является подверженность влиянию атмосферных явлений. К этим явлениям относятся атмосферное затухание и рассеяние ИК – излучения, турбулентность, которая приводит к возникновению таких последствий как:

- изменение траектории луча (флуктуация углов прихода);
- расширение (размытие) луча (приводит к изменению пространственной плотности мощности на входе приемника);
- поляризационные флуктуации;
- сцинтилляция луча (приводит к маломасштабным интерференционным явлениям в пределах поперечного сечения луча);
- дрожание изображения (вызывает движение точки фокуса в плоскости изображения);
- ухудшение пространственной когерентности (нарушение фазовой когерентности в сечении фазового фронта лазерного пучка).

Выше описанные атмосферные воздействия на сигнал в канале ООСП, можно оценивать по интегральной функции распределения метеорологической дальности видимости (ИФР – МДВ), которую получают по метеоданным аэропортов каждого географического региона [3-4]. В соответствии с этим, были получены и обработаны эмпирические статистические данные по ИФР-МДВ с аэропорта в Андижанском регионе, которые приведены в табл.1.

Таблица 1. ИФР – МДВ г. Андижан

S (км)/ F(Sm)		**10**	**7**	**4,1**	**3,5**	**3**	**2,2**	**1,5**	**1,3**	**1,1**	**0,7**	**0,45**
Месяцы	**I**	1.00	0.95	0.86	0.76	0.69	0.56	0.43	0.31	0.31	0.22	0.12
	II	1.00	0.90	0.64	0.49	0.40	0.27	0.17	0.06	0.06	0.02	-
	III	1.00	0.72	0.24	0.13	0.09	0.06	-	-	-	-	-
	IV	1.00	0.36	0.04	0.01	0.01	-	-	-	-	-	-
	V	1.00	0.06	-	-	-	-	-	-	-	-	-
	VI	1.00	0.03	-	-	-	-	-	-	-	-	-
	VII	1.00	0.06	0.01	0.01	0.01	-	-	-	-	-	-
	VII	1.00	0.05	-	-	-	-	-	-	-	-	-
	IX	1.00	0.37	0.02	-	-	-	-	-	-	-	-
	X	1.00	0.49	0.11	0.04	0.04	0.02	-	-	-	-	-
	XI	1.00	0.60	0.15	0.09	0.09	0.05	0.01	-	-	-	-
	XII	1.00	0.8	0.47	0.33	0.30	0.25	0.16	-	0.14	0.11	0.09
Среднегодовая		1.00	0.44	0.21	0.15	0.13	0.10	0.06	0.04	0.04	0.03	0.02

На основе этих данных по метеорологической дальности видимости вычисляется интегральная функция распределения километрического затухания (ИФР – КЗ) по формуле [2,4].

$$\beta(S,\lambda) = \frac{C}{S_{МДВ}}\left[\frac{\lambda|мкм|}{0,55}\right]^{-q(S_{МДВ})}, \qquad \left[\frac{дБ}{км}\right] \tag{1}$$

здесь, С = 13 дБ;

$q(S_{МДВ})$ – показатель степени, является функцией $S_{МДВ}$.

В работах [3-5], приводились результаты исследований зависимости $q = f(S_{МДВ})$. Однако применение (2), дает возможность более точно описать эту зависимость:

$$q = \begin{cases} 1,6 & \text{при } S_{МДВ} > 50 \text{ км}, \\ 1,3 & \text{при } S_{МДВ} = 6 \div 50 \text{ км}, \\ 0,16*S_{МДВ}+0,34 & \text{при } 1\text{км} < S_{МДВ} \leq 6 \text{ км} \\ S_{МДВ} - 0,5 & \text{при } 0,5\text{км} < S_{МДВ} \leq 1\text{км} \\ 0 & \text{при } S_{МДВ} < 0,5 \text{ км} \end{cases} \tag{2}$$

Использование формулы (1) и зависимости (2), позволяет рассчитать километрическое затухание для длин волн, на которых работают современные оптические передатчики. Как правило, для уменьшения затухания в атмосфере, длины волн должны находиться в «окнах прозрачности». Подобные расчеты приведены в [2,4,5], также представлены в табл.2.

Таблица 2.

$S_{МДВ}$	**10**	**7**	**4,1**	**3,5**	**3**	**2,2**	**1,5**	**1,3**	**1,1**	**0,7**	**0,45**
$q(S_{МДВ})$	1,3	1,3	0,996	0,9	0,82	0,692	0,58	0,548	0,516	0,2	0
F[β(λ ср.год)]	1	0,105	0,0808	0,029	0,03	0,023	0,018	0,009	0,01	0,01	0,0025
F[β(λ лет. мес)]	1	0,027	0,02	0,003	0,003	0,003	0,003	0	0	0	0
F[β(λ зим. мес)]	1	0,217	0,18	0,077	0,087	0,07	0,053	0,033	0,03	0,02	0,01
$\beta(\lambda_{0,55})$	1,3	1,85	3,25	3,71	4,33	5,90	8,66	10	11,81	18,57	28,88
$\beta(\lambda_{0,78})$	0,82	1,17	2,29	2,71	3,25	4,64	7,07	8,25	9,86	17,31	28,88
$\beta(\lambda_{0,83})$	0,76	1,08	2,15	2,56	3,09	4,44	6,82	7,98	9,55	17,10	28,88
$\beta(\lambda_{0,85})$	0,73	1,05	2,10	2,51	3,03	4,37	6,73	7,87	9,44	17,02	28,88
$\beta(\lambda_{0,91})$	0,67	0,96	1,92	2,36	2,86	4,17	6,47	7,58	9,11	16,79	28,88
$\beta(\lambda_{0,98})$	0,61	0,87	1,82	2,20	2,69	3,96	6,19	7,28	8,77	16,54	28,88
$\beta(\lambda_{1,06})$	0,55	0,79	1,69	2,05	2,53	3,75	5,92	6,98	8,42	16,28	28,88
$\beta(\lambda_{1,55})$	0,33	0,48	1,15	1,46	1,85	2,88	4,75	5,66	6,92	15,09	28,88

Отличительные особенности волн оптического диапазона, по сравнению с волнами радиодиапазона, открывают огромные возможности для передачи больших объемов информации, соответственно при достижении высокой концентрации излучаемой энергии. Эти выше перечисленные особенности вызывают повышенный интерес к использованию этого диапазона для телекоммуникационных нужд.

Литература:

1. Telecom Regulatory Authority of India. FSO in next generation wireless networks. Technology Digest, Issue 8, February 2012.

2. Ибраимов Р.Р., Халбаева М.З. Интегральная функция распределения километрического затухания атмосферного канала связи в Самаркандском регионе. Вестник Алматинского университета энергетики и связи. №2 (25) 2014.

3. Павлов Н.М. Атмосферные оптические линии передачи и перспективы их внедрения в местных сетях доступа России. LIGHTWAVE Russian Edition № 3-2007.

4. Ибраимов Р.Р., Насыров Т.А., Статическая оценка состояния атмосферного канала открытых оптических систем передачи // Вестник Алматинского университета энергетики и связи, №3-22, 2013.

5. Ибраимов Р.Р., Насыров Т.А., Статистическая оценка метеорологической дальности видимости для Самаркандского региона // МТК «Актуальные проблемы развития инфокоммуникаций и информационного общества». 26-27.06.2012, Ташкент.

Е.М. Хорольский, В.Ю. Титов

МОДЕЛИРОВАНИЕ ФУНКЦИОНИРОВАНИЯ РАДИОЭЛЕКТРОННОГО СРЕДСТВА С ПРИМЕНЕНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА И ЧИСЛЕННОГО МЕТОДА ЭЛЕКТРОДИНАМИКИ

Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия

Ключевые слова: электромагнитное поле, система связи, радиоэлектронное средство, точечный излучатель.

В статье рассмотрен один из способов моделирования электромагнитного поля при функционировании радиоэлектронного средства, а также решение задачи рационального размещения радиоэлектронного средства и способ расчета напряженности электромагнитного поля с учетом моделирования взаимного влияния электромагнитных полей при их функционировании, поиск наилучшего варианта размещения. При использовании данного подхода задача моделирования сводится к оптимизационной задаче определения параметров точечного излучателя.

E.M. Horolsky, V.Yu. Titov

SIMULATION OF THE ELECTRONIC MEANS USING GENETIC ALGORITM AND NUMERICAL METHODS OF ELECTRODYNAMICS

The Federal government institution scientific and production association special equipment and telecoms of the Ministry of the Internal Affairs of the Russian Federation,
Rostov-on-Don, Russia

Keywords: electromagnetic field, the communication system, radio-electronic means, point radiator.

The article describes one way of modeling the electromagnetic field in the operation of electronic money, as well as solution to the problem of rational allocation of radio-electronic means and method of calculation of the electromagnetic field simulation based on the mutual influence of electromagnetic fields in their functioning, finding the best options for placement. Using this approach, the task of simulation optimization problem is reduced to determining the parameters of a point source.

В настоящее время эффективность управления в значительной степени определяется процессом обмена информации, т. е. состоянием системы связи. При организации связи неизбежно возникает вопрос по размещению радиоэлектронных средств (РЭС) смонтированных на транспортной базе или на стационарных объектах связи. При этом необходимо учитывать требования руководящих документов по защите государственной тайны, эргономики рабочих мест, а также учитывать действующие в настоящее время санитарные нормы и правила.

Для расчета напряженности электромагнитного поля (ЭМП) при функционировании РЭС, наиболее подходящими являются математические методы. Математическая модель описывает реальный процесс с некоторой степенью приближения к действительности, охватывая только некоторые его свойства. Для разработки математической модели функционирующего РЭС,

необходимо выбрать наиболее подходящий из совокупности существующих методов решения электродинамических задач. Метод должен быть адаптирован для решения задач расчета напряженности ЭМП в ближней зоне излучения. Он должен иметь возможность расчета величины напряженности ЭМП при сложной геометрии граничных условий и различных материальных параметров среды без ущерба для точности, устойчивости и сходимости. При введении вышеперечисленных требований для решения поставленной задачи целесообразно использовать численный метод [2, С.17], например, метод конечных разностей во временной области [4], моделируя функционирование РЭС точечным излучателем, размещенном в ограниченный металлическими стенками объем, имитирующем корпус РЭС (рис. 1).

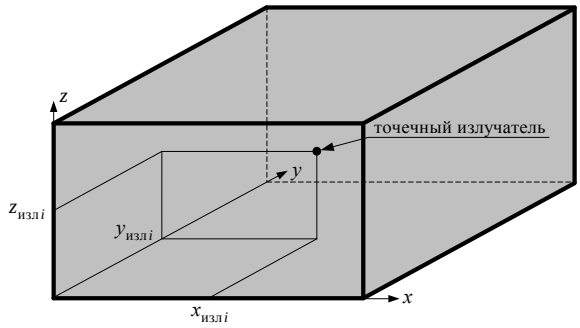


Рисунок 1. Модель радиоэлектронного средства

Параметры точечного излучателя (амплитудно-частотная характеристика и координаты размещения) должны обеспечить заданный уровень напряженности ЭМП на определенном расстоянии от корпуса РЭС.

Действующие в настоящее время руководящие документы [1, С.51] регламентируют максимальный уровень напряженности ЭМП при функционировании РЭС, в зависимости от их предназначения (рис. 2).

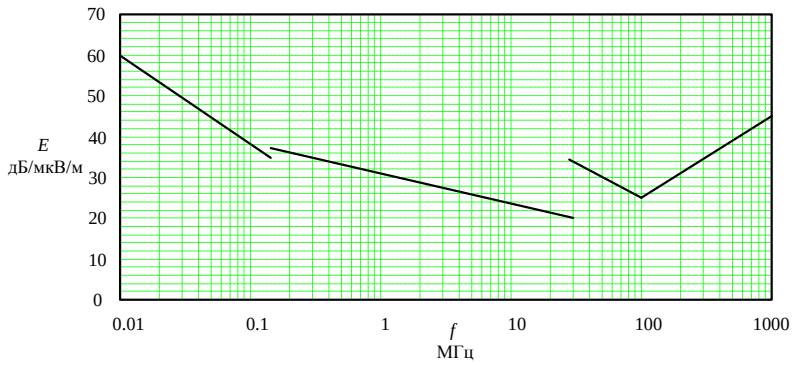


Рисунок 2. Нормы напряженности поля радиопомех при функционировании радиоэлектронных средств.

Квазипиковые значения напряженности поля радиопомех на расстоянии 1 метр от РЭС определяются по следующим формулам:

$$E = 60 - 20,4 \lg \frac{f}{0,01}$$ – в полосе частот (0,009–0,15) МГц, (1)

$$E = 37 - 7,39 \lg \frac{f}{0,15}$$ – в полосе частот (0,15–30) МГц, (2)

$$E = 36 - 21 \lg \frac{f}{30}$$ – в полосе частот (30–100) МГц, (3)

$$E = 25 + 20\lg\frac{f}{100}$$ – в полосе частот (100–1000) МГц, (4)

где f – частота, МГц.

Следовательно, необходимо для каждой частоты излучения найти такие параметры точечного излучателя, чтобы уровень напряженности ЭМП на определенном расстоянии от корпуса РЭС соответствовал требованиям руководящих документов:

$$\left.\Phi\left(x_{\text{изл}\,j}, y_{\text{изл}\,j}, z_{\text{изл}\,j}, A_{\text{изл}\,\text{j}}\right)\right|_{f=\text{const}} \to \Phi_{\text{треб}}$$

$$\Phi_{треб} \Leftrightarrow E(f_i) = E_{треб}(f_i) \pm \Delta E \quad , \quad (5)$$

где $\Phi, \Phi_{треб}$ – искомая функция и функция цели соответственно, $\left(x_{\text{изл}}, y_{\text{изл}}, z_{\text{изл}}, A_{\text{изл}}\right)$ – координаты и амплитуда точечного излучателя, f – частота излучения, E – напряженность ЭМП на расстоянии 1 метр от РЭС, ΔE – погрешность, вводимая исследователем.

Необходимо отметить, что решение задачи (5) сводится к нахождению комбинации параметров точечного излучателя с применением методов оптимизации. Одним из вариантов такого решения может быть использование генетических алгоритмов, предназначенных для поиска глобального экстремума многопараметрической функции.

Основная суть этого подхода заключается в формировании зависящей от некоторого числа параметров функции, глобальный максимум (или минимум).

Основоположником современной теории генетических алгоритмов считается Холланд (J. Holland), чья работа «Adaptation in Natural and Artificial Systems» (1975), стала классикой в этой области. В ней Холланд впервые ввел термин «генетический алгоритм», который в настоящее время называют классическим (или каноническим). Последователи Холланда Кеннет Де Йонг (Kenneth De Jong) и Дэвид Голдберг (David E. Goldberg) внесли огромный вклад в развитие ГА. На книгу Голдберга «Genetic algorithms in search optimization and machine learning» (1989), ссылаются авторы практически каждой работы по этой теме [2].

Пусть некоторая функция по заданному набору численных параметров возвращает некоторое значение (многопараметрическая функция). Далее создается множество строк, каждая из которых кодирует вектор чисел (длина вектора равна количеству параметров функции). Те строки, для которых это значение достаточно велико (в случае поиска глобального максимума функции), считаются более «приспособленными», чем те, для которых это значение достаточно мало. Применяя «механизм эволюции» к сформированным строкам, последующие строки (строки нового «поколения») будут соответствовать все большими значениями функции.

Для применения генетического алгоритма необходимо закодировать каждый параметр строкой бит. Длина строки зависит от степени дискретизации пространства (размера пространственной ячейки применяемого численного метода решения электродинамической задачи) и требуемой точности вычисления напряженности ЭМП. Следовательно, параметр может принимать только дискретные значения в некотором заданном диапазоне. Используя для описания каждого параметра 8 бит, ошибка дискретизации не превысит 1 % а длинна строки составит 32 символа (Табл. 1), что, с учетом возможностей современных программно-аппаратных средств, вполне приемлемо.

Таблица 1. Представление параметров кодом

Строка бит	00101101	01001001	10011010	01010001
Представляемый параметр	$x_{\text{изл}\,j}$	$y_{\text{изл}\,j}$	$z_{\text{изл}\,j}$	$A_{\text{изл}\,j}$

При поиске оптимальных параметров точечного излучателя необходимо проводить расчет напряженности ЭМП для всех исходных вариантов и каждого вновь формируемого и сравнивать результаты с требуемыми значениями. Структурная схема алгоритма поиска параметров точечного излучателя представлена на рисунке 3. На первом этапе производится ввод начальных значений параметров точечного излучателя, допустимых погрешностей и пр., после чего эти

параметры кодируются строкой бит (блок 1, 3). Далее производится расчет напряженности ЭМП методом конечных разностей во временной области (блок 6). Если значение напряженности ЭМП на определенной частоте удовлетворяет введенным требованиям (блок 8), то вариант (популяция) сохраняется в таблице результатов (блок 10) и осуществляется переход к следующей частоте (блок 5). В обратном случае формируется новая популяция (блоки 7, 4, 2,3) и весь цикл расчета повторяется заново.

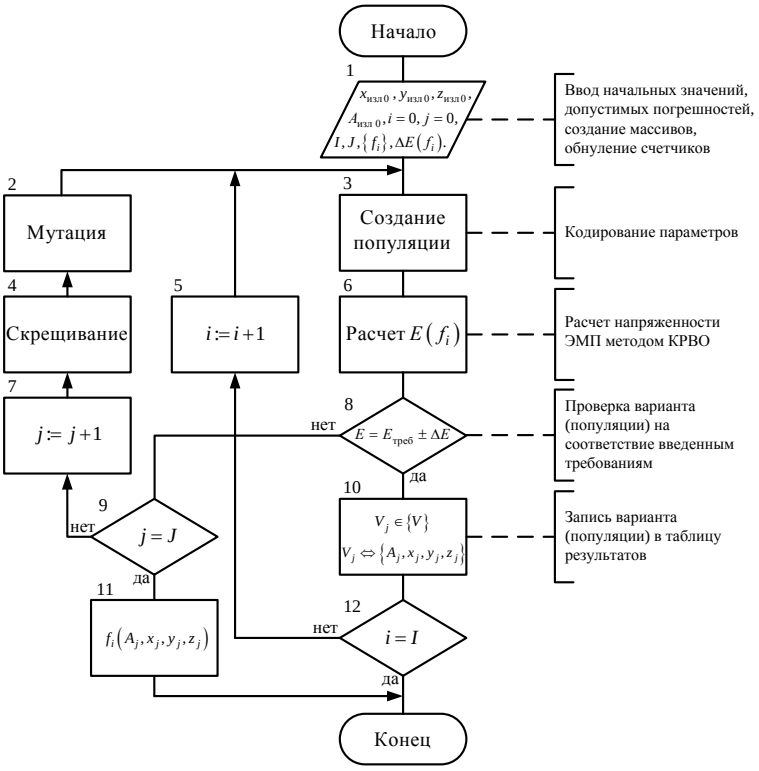


Рисунок 3. Структурная схема алгоритма поиска параметров точечного излучателя.

После нахождения наилучшего варианта решения моделирование функционирования РЭС заканчивается и результат сохраняется в виде таблицы (Табл. 2).

Таблица 2. Представление результатов моделирования

Параметр / Частота	$x_{изл\,j}$	$y_{изл\,j}$	$z_{изл\,j}$	$A_{изл\,j}$
f_1	x_1	y_1	z_1	A_1
f_2	x_2	y_2	z_2	A_2
...	...	...	...	...
f_n	x_n	y_n	z_n	A_n

Литература:

1. Зарубин В.С. и др. Приближенные методы математической физики М.: Издательство МГТУ им. Н.Э. Баумана, 2001.

2. Яминов Б.С. Генетические алгоритмы. // Материалы с сайта http://rain.ifmo.ru.

3. ГОСТ 30429-96. Радиопомехи индустриальные от оборудования и аппаратуры, устанавливаемых совместно со служебными и радиоприемными устройствами. – М. 1996.

4. Taflove A. Computational Electromagnetics: The Finite-Difference Time-Domain Method, Artech Hose Publishers, 1995.

Д.А. Чудин, К.Л. Костюченко

3D-ПЕЧАТЬ: ТЕХНОЛОГИЧЕСКИЕ ВОЗМОЖНОСТИ И ПРАВОВЫЕ ПРОБЛЕМЫ

Уральский юридический институт МВД России, г. Екатеринбург, Россия

Ключевые слова: 3D-печать, 3D-принтер, технологии, угрозы безопасности.

В статье дана общая характеристика 3D-технологиям, 3D-печати, 3D-принтерам, сферам их применения; рассмотрены технические, экономические, правовые, организационные и иные аспекты 3D-печати; показаны выявляющиеся новые угрозы реализации 3D-технологий – криминальные, террористические, экстремистские и др. Показаны примеры распечатки пластиковых деталей и сборки из них стреляющих образцов оружия. Сформулированы предложения по решению проблем, возникающих с развитием 3D-печати – в правовом, организационном, информационном и морально-воспитательном аспектах.

D.A. Chudin, K.L. Kostyuchenko

3D PRINTING: TECHNOLOGICAL CAPABILITIES AND LAW PROBLEMS

Ural Law Institute of the Ministry of the Interior Affairs of the Russian Federation, Ekaterinburg, Russia

Keywords: 3D printing, 3D printer, technology, security threats.

The article presents an overview of the 3D technology, 3D printing, 3D printers, areas of their application; consider technical, economic, law, organizational and other aspects of 3D printing; it is shown emerging new threats to the implementation of 3D-technology – criminal, terrorist, extremist and other. Shows examples of print plastic parts and assemblies of them firing of weapons. Proposals for solving problems arising with the development of 3D-printing – in the legal, organizational, informational, moral and educational aspects.

Технологии 3D-печати развиваются высокими темпами. Еще какой-то десяток лет назад с техникой объемной печати проводились лишь первые эксперименты. Несколько позже появились профессиональные системы 3D-печати. При помощи них можно было получать небольшие по размерам пластиковые объекты (но несоизмеримо дорогие), используемые в основном как макеты или прототипы.

Сегодня 3D-принтеры работают с металлами, пластмассами, керамикой, биоматериалами и множеством различных их сочетаний, производя достаточно большие объекты (размером до нескольких метров), характеризующимися уникальными свойствами и высоким качеством поверхностей. Наиболее распространенными областями применения 3D-принтеров являются [3, С. 60-63]: архитектура (изготавливаются макеты зданий, микрорайонов или городов с дорогами, деревьями и др. элементами инфраструктуры); строительство (есть первые примеры «распечатанных» готовых стен домов и целых зданий, полученных при помощи специальных систем, а в планах – создание жилых модулей на Луне методом распечатки из имеющегося там грунта); машиностроение и дизайн **(**3D-принтеры используют для создания концепт-моделей и прототипов и будущих изделий или их отдельных деталей); медицина (новая технология облегчает изготовление протезов, ортопедических изделий, а также создает муляжи и макеты органов пациента для подготовки врачей к операциям); образование (3D-принтеры позволяют разрабатывать самые разнообразные наглядные пособия хорошего качества для школьников и студентов); легкая и текстильная промышленность (создается бытовая техника, одежда и обувь по индивидуальным характеристикам); ювелирное дело (производство моделей, по которым в дальнейшем выполняется отливка готовых изделий); пищевая сфера (уже сегодня «печатают» кондитерские изделия самых сложных форм и вкусов); оборонная промышленность (есть сведения, что некоторые детали для ядерных боеголовок печатаются на 3D-принтерах); военная топография (карты любой точки земного шара, например, в Центрах геопространственной информации военных округов Российской армии); правоохранительная сфера (оперативная

распечатка макетов зданий и местности при тактическом планировании); театр, кино, хобби (изготовление различных предметов, декораций, муляжей редких музейных экспонатов, мелкосерийное производство, штучные и коллекционные изделия) и др. Уже ясно, что 3D-принтеры, как и их предшественники – 2D-принтеры – достаточно скоро они будут достаточно дешевы и станут привычными бытовыми устройствами, как и лазерные и струйные принтеры [2, С. 60].

3D-печать открывает перед человечеством новые горизонты. Вместе с тем возникают и определенные проблемы. Развитие технологии 3D-печати может привести к закрытию промышленных предприятий (люди распечатают в домашних условиях любую понравившуюся вещь). Сокращение промышленного производства, в свою очередь, приведет к повышению уровня безработицы, тогда экономика может оказаться в кризисе.

Уже есть факты изменения логистики промышленности. Одна из крупнейших почтово-транспортных компаний открывает сеть мастерских с 3D-принтерами. Это решение будет экономически выгодней, т.к. исключит пересылку по миру широкого ассортимента высокотехнологичных товаров (простые из-за низкой себестоимости будут штамповаться массово) [1, С. 73]. Трансформируется и мировая производственная инфраструктура. Фактор дешевой рабочей силы уже не будет решающим, что, следовательно, также отразится на социально-экономической сфере. Например, Индонезия очень рассчитывает на развитие своей экономики через активизацию такой области «3D-промышленности», как производство на дому. Остро встанет проблема с соблюдением авторских прав, так как новая технология дает возможность напечатать любую понравившиеся вещь, не соблюдая при этом никаких интеллектуальных прав и не выплачивая никакой финансовой компенсации его автору.

3D-печать может составлять серьезную угрозу общественной безопасности, потому что с помощью новой технологии можно довольно просто создать (распечатать) стреляющее огнестрельное пластиковое оружие. В скором времени, при наличии 3D-принтера любой человек в будущем сможет наладить производство оружия у себя дома. А это оружие (и даже точные копии) наиболее вероятно будет использовано в криминальных, террористических, экстремистских целях.

Американский оружейный мастер Хэйв Блу (Have Blue) стал первым в мире, кто собрал огнестрельное оружие, ствольная коробка которого напечатана на 3D-принтере. Естественно, ствол, боёк и другие механизмы невозможно сделать из пластика, так что в этом пистолете используются оригинальные металлические детали от винтовки M16.

Еще один американец – студент Коди Уилсон (Cody Wilson), успешно протестировал первый в мире пистолет «The Liberator», распечатанный на 3D-принтере. При этом его затраты на материалы составили всего $25, а печать длилась не более суток. С сайта, где он выложил чертежи, их тут же скачали более 100 тысяч раз. Появилась ситуация когда любой пользователь без каких-либо специальных знаний в области проектирования и разработки оружия может распечатать все детали и собрать полностью работоспособную модель пистолета.

Последователи только увеличивали опасность: подбирали материалы и режимы изготовления для увеличения прочности ствола (для производства нескольких десятков выстрелов), распечатывали винтовку, создавали пластиковые пули со свинцовой дробью внутри, научились создавать металлические образцы оружия, приближая по характеристикам распечатки к боевому оружию

Журналисты пошли дальше. В Израиле они провели эксперимент, дважды проникнув в здание парламента с распечатанным на 3D-принтере пистолетом сквозь охрану и рамки металлодетекторов. После того как они побывали на совещании, где присутствовал премьер-министр, оружие было испытано в тире стрельбой боевыми патронами. Журналисты Daily Mail смогли проехать на поезде Eurostar из Лондона в Париж с распечатанным пистолетом «The Liberator». Следовательно, явно проявляется тот факт, что распечатка неотслеживаемого правоохранительными органами оружия может быть проведена скрытно (в домашних или подобных условиях) с высоким качеством, с постоянно повышающейся точностью и мощностью выстрела. Легкость же одновременного получения чертежей стреляющих устройств (и других опасных приборов и механизмов) в разных географических точках с последующим созданием большого количества копий становится острой криминальной и террористической угрозой, превращающуюся в угрозу национальной безопасности.

С помощью 3D-принтера можно создать и огнемет. Дизайнер Иван Оуэн решил подготовиться, как говорится «на всякий случай», и с помощью 3D-принтера самостоятельно

собрал надежное оружие для отталкивания зомби – Flamethrower. Используя листовой вентилятор на батарейках, пропановую горелку и 3D-печатные детали, создано оружие, которое работает на основе кукурузного крахмала, который вспыхивает при контакте с пропаном. Пока огнемет против зомби еще воспринимается как курьез, но при определенной доработке может стать грозным и опасным оружием.

Таким образом, можно заключить, что преимущества 3D-технологий оборачиваются рядом самых различных проблем (см. табл. 1).

Таблица 1. Технологические прорывы 3D-печати и возникающие проблемы

Результаты развития 3D-технологий («позитив»)	Возникающие проблемы («негатив»)
Широкие возможности технологии	Бесконтрольная распечатка оружия (криминал, терроризм, экстремизм)
Печать в требуемом месте (дома, в экспедиции, в авто и т.п.)	Изготовление изделия (запрещенного) может быть проведено скрытно
Получение изделия с требуемыми характеристиками	Адаптация под конкретного нарушителя, маскировка
Легкость получения чертежей, одновременная печать множества копий	Внезапность появления большого количества изделий (запрещенных)
Доступные (простые) материалы, дешевизна производства	Массовость производства (например, несколько одноразовых стреляющих устройств = одному пистолету)
Точность и качество	Эстетическая привлекательность оружия для потребителя – потенциального нарушителя (преступника)
Оперативное изготовление изделия	Сложность обнаружения и контроля
Простота получения чертежей и последующей распечатки	Нарушение авторских прав
Повышение гибкости производства, снижение себестоимости производства	Изменение инфраструктуры производства, снижение числа рабочих мест

Число «потребительских» домашних 3D-принтеров в домах россиян уже перешагнуло порог в 10 тыс. Растет и число проблем, которые нужно решать. Какие-то – уже сейчас, какие-то – в ближайшем будущем. Вот основные из них.

1. Скрытная бесконтрольная распечатка оружия в больших количествах.

Наиболее значимая проблема. Оружие (пистолет, ружье и т.п.) может быть изготовлено при помощи 3D-принтера в домашних (или подобных) условиях. Тайно созданное, оно может быть использовано в криминальных, террористических, экстремистских целях. Возможно, придется внести в некоторые нормативные правовые акты корректировки, связанные с уточнением формулировок деталей оружия. Прежде всего, в Федеральный закон «Об оружии», (по аналогии с добавлением оружия, произведенного с помощью 3D-принтера, в перечни огнестрельного оружия некоторых штатов США). Пресечение данного правонарушения – бесконтрольной распечатки оружия – ляжет на плечи правоохранительных органов и спецслужб государства. Основной путь решения – методы оперативно-розыскной деятельности. Теоретически возможен и административно-правовой путь – поставить под контроль органами внутренних дел приобретение и эксплуатацию 3D-принтеров. Подобный пример уже был – в начале 90-х годов XX века лицензионно-разрешительная система МВД России регистрировала цветные принтеры с целью пресечения попыток фальшивомонетничества. Однако должный эффект контроля достигнут не был из-за стремительного роста количества и разнообразия принтеров.

2. Быстрое распространение чертежей для распечатки оружия в телекоммуникационных системах.

Проблема выявления таких случаев – сфера деятельности правоохранительных органов, а также некоторых гражданских ведомств, например, Роскомнадзора.

3. Привлекательность 3D-печати как простого метода получения точных копий оружия и других опасных устройств.

Решение (профилактика) состоит в целенаправленной морально-воспитательной работе со стороны СМИ и информировании потенциального нарушителя об уголовно-правовой ответственности.

4. Нарушение авторских прав при распечатке на 3D-принтере.

При использовании технологии 3D-печати, вероятно, будет самой популярной проблемой. В различных ситуациях может наступить гражданско-правовая, административная и уголовная ответственность. Чертежи для 3D-печати – это интеллектуальная собственность. Гражданско-правовая ответственность наступает в случае предъявления требований от обладателей исключительных имущественных авторских прав. Правообладатель вправе сам выбрать, какое требование, из предоставленных законом, предъявить к нарушителю авторских прав. Из-за специфики технологии 3D-печати возможно также потребуются корректировки гражданско-правового законодательства.

5. Изменение производственной инфраструктуры и логистики, снижение числа рабочих мест.

Экономическую часть названной проблемы решит рынок. А социальную часть, связанную с возможным высвобождением работников (безработица, миграции, снижение доходов населения и т.п.), может и должно взять на себя государство с его правовыми и налоговыми рычагами. Учитывая длительный характер принятия нормативных правовых актов, эта работа должна начинаться уже сейчас.

Таким образом, можно сделать вывод, что 3D-принтеры, как и любые новинки в технико-технологической сфере (роботы, радиоуправляемые модели, беспилотные летательные аппараты) являют собой определенные прорывы. Однако они также несут и серьезные угрозы безопасности. Поэтому уже в самое ближайшее время государству с его правоохранительными органами, необходимо создавать организационно-правовые и программно-технические средства нейтрализации указанных угроз.

Литература:

1. Даер Э. Авто из принтера / Э. Даер. // Популярная механика. – № 12 – 2014. – С. 72-74.

2. Динаев А. Немного о 3D-печати / А. Динаев. // Мир ПК. – № 10 – 2014. – С. 44-46.

3. Канесс Э. Доступная 3D-печать для науки, образования и устойчивого образования / Э. Канесс, К. Фонд, М. Зеннаро. – М., 2013. – 194 с.

Б.Р. Шаакбарова, Ф. Шарипходжаева

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ КАК ПРОГРЕССИВНОЕ НАПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ташкентский государственный педагогический университет,
г. Ташкент, Республика Узбекистан

Ключевые слова: информационные технологии, информационная интеллектуальная система, экспертная система, классы экспертных систем.

В данная статья посвящена прогрессивному направлению информационных технологий − интеллектуальным системам. В статье анализированы функции и признаки информационных интеллектуальных систем, классифицированы их виды.

B.R. Shaakbarova, F. Sharipxodjayeva

INTELLIGENT SYSTEMS AS A PROGRESSIVE DIRECTION OF INFORMATION TECHNOLOGY

Tashkent state pedagogical university, Tashkent city, The Republic of Uzbekistan

Keywords: information technologies, intelligent information system, expert system, classes of expert systems.

In this article dedicated to the progressive direction of information technology - intelligent systems. In the article the functions and characteristics of intelligent information systems are analyzed, their types are classified .

В настоящее время в Узбекистане информатизация как технико-технологическая база становления информационного общества выступает национальным стратегическим ресурсом, определяющим не только общий уровень социального и культурного развития государства, но и его место в глобальном процессе мирового развития.

Информационная интеллектуальная система является одним из прогрессивних направлением информационных технологий. Системы искусственного интеллекта развиваются в направлении понимания процессов человеческого познания.

Интеллектуальная информационная система (ИИС) - компьютеризированная система сбора, хранения, обработки, представления информации, работа которой основывается на имитации (воспроизведении) интеллектуальных возможностей человека. ИИС есть та информационная система, которая для выполнения своих функций работы с информацией использует методы и алгоритмы искусственного интеллекта. Интеллектуальная ИС решает задачи работы с информацией в реальных сложных условиях «как человек». После анализа этого предложения, уточнения понятия «реальные, сложные условия», анализа поведения и возможностей человека в этих условиях мы вполне логично приходим к понимаю того, какими свойствами должна обладать ИИС.

Любая информационная система (ИС) выполняет следующие функции: 1) воспринимает вводимые пользователем информационные запросы и необходимые исходные данные, 2) обрабатывает введенные и хранимые в системе данные в соответствии с известным алгоритмом и формирует требуемую выходную информацию.

С точки зрения реализации перечисленных функций ИС можно рассматривать как фабрику, производящую информацию, в которой заказом является информационный запрос, сырьем - исходные данные, продуктом - требуемая информация, а инструментом (оборудованием) - знание, с помощью которого данные преобразуются в информацию. Если в ходе эксплуатации ИС выяснится потребность в модификации одного из двух компонентов программы, то возникнет необходимость ее переписывания. Это объясняется тем, что полным знанием проблемной области обладает только разработчик ИС, а программа служит “недумающим исполнителем” знания разработчика. Этот недостаток устраняются в интеллектуальных информационных системах .

Интеллектуальная информационная система (ИИС) - это ИС, которая основана на концепции использования базы знаний для генерации алгоритмов решения задач различных классов в зависимости от конкретных информационных потребностей пользователей.

Для интеллектуальных информационных систем, ориентированных на генерацию алгоритмов решения задач, характерны следующие признаки:

- развитые коммуникативные способности;
- умение решать сложные плохо формализуемые задачи;
- способность к самообучению.

Коммуникативные способности ИИС характеризуют способ взаимодействия (интерфейса) конечного пользователя с системой.

Сложные плохо формализуемые задачи - это задачи, которые требуют построения оригинального алгоритма решения в зависимости от конкретной ситуации, для которой могут быть характерны неопределенность и динамичность исходных данных и знаний.

Условно каждому из признаков интеллектуальности соответствует свой класс ИИС:

- Системы с интеллектуальным интерфейсом;

- Экспертные системы;
- Самообучающиеся системы.

Экспертная система (ЭС) - это ИИС, предназначенная для решения слабоформализуемых задач на основе накапливаемого в базе знаний опыта работы экспертов в проблемной области

Экспертная система является инструментом, усиливающим интеллектуальные способности эксперта, и может выполнять следующие роли:

- консультанта для неопытных или непрофессиональных пользователей;
- ассистента в связи с необходимостью анализа экспертом различных вариантов принятия решений;
- партнера эксперта по вопросам, относящимся к источникам знаний из смежных областей деятельности.

Исторически, ЭС были первыми системами искусственного интеллекта, которые привлекли внимание потребителей.

Классы экспертных систем. По степени сложности решаемых задач экспертные системы можно классифицировать следующим образом:

- По способу формирования решения экспертные системы разделяются на два класса: аналитические и синтетические. Аналитические системы предполагают выбор решений из множества известных альтернатив, а синтетические системы - генерацию неизвестных решений. Аналитическая экспертная система - это ЭС, осуществляющая оценку вариантов решений (проверку гипотез). Синтетическая экспертная система - это ЭС, осуществляющая генерацию вариантов решений (формирование гипотез).
- По способу учета временного признака экспертные системы могут быть статическими или динамическими. Статические системы решают задачи при неизменяемых в процессе решения данных и знаниях, инамические системы допускают такие изменения.

Статическая экспертная система - это ЭС, решающая задачи в условиях, не изменяющихся во времени исходных данных и знаний.

Динамическая экспертная система - это ЭС, решающая задачи в условиях изменяющихся во времени исходных данных и знаний.

Система с интеллектуальным интерфейсом - это ИИС, предназначенная для поиска неявной информации в базе данных или тексте для произвольных запросов, составляемых, как правило, на ограниченном естественном языке. Самообучающаяся система - это ИИС, которая на основе примеров реальной практики автоматически формирует единицы знаний.

П.С. Шевчук, *Д.В. Попандопуло, **И.Д. Попандопуло

АЛГОРИТМ АВТОМАТИЗАЦИИ ОГРАНИЧЕНИЯ ДОСТУПА К ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИЯ НА ОСНОВЕ ПРИНЦИПА УПРАВЛЕНИЯ ДОСТУПОМ ФАЙЛОВЫХ СИСТЕМ В ОПЕРАЦИОННЫХ СИСТЕМАХ UNIX

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия
*Ростовский юридический институт Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия
**Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г Новочеркасск, Россия

Ключевые слова: оперативно-розыскная информация, ресурс, автоматизация ограничения доступа, файловые системы, доступ к файлам.

Описан один из вариантов решения задачи по автоматизации ограничения доступа к информации, возникающей в процессе оперативно-розыскной деятельности, основанном на существующем методе разграничения правд доступа в Unix-подобных операционных.

P.S. Shevchuk, *D.V. Popandopulo, ** I.D. Popandopulo

THE ALGORITHM AUTOMATION RESTRICT ACCESS TO INVESTIGATIVE INFORMATION (BASED ON THE PRINCIPLE OF FILE ACCESS PERMISSION UNIX OPERATING SYSTEMS)

North-Caucasus branch of the Moscow technical university of communications and informatics, Rostov-on-Don, Russia
*Rostov law Institute of the Ministry of internal Affairs Russian Federation, Rostov-on-don, Russia
**South-Russian state Polytechnic University (NPI) name M. I. Platov, Novocherkassk, Russia

Keywords: operational-investigative information, resource, automation restrict access, file system access to files.

Describes one solution to the problems of automation of restricting access to information arising in consequence of the operational-search activity. The construction algorithm is based on the existing method of distinguishing truths Unix-like operating, with joint use of data encryption.

В современном мире вопросы автоматизации ограничения доступа к информации, возникающей в ходе оперативно-розыскной деятельности (ОРД) МВД России, включая составляющую государственную тайну, требуют соответствующего совершенствования. В настоящее время в качестве носителей информации, как правило, используются цифровые носители информации значительного объема, такие как USB-накопитель, карта памяти и другие. Основой безопасности информации, хранящейся на цифровых носителях, является метод ее технического шифрования либо организационно-физическое ограничение доступа к внешнему носителю, предотвращающие утечку. Второй метод в органах внутренних дел реализуется за счёт правил пользования цифровой техникой либо физического и технического ограничения доступа к носителю. Сегодня в используемых оперативными подразделениями средствах программно-технической защиты информации не нашли широкого применения совместное шифрование данных и автоматическое определение уровня доступа к оперативно-розыскной информации (ОРИ), исключающие возможность использования внешнего носителя в сторонних ЭВМ, неаттестованных на соответствие требованиям по технической защите информации.

Для реализации автоматического ограничения доступа к ОРИ и снятия ограничения необходимо сформировать алгоритм действий. Различают два основных подхода к определению прав доступа.

1. Избирательный доступ - для каждого объекта информатизации владелец файла определяет допустимые операции с ним. Между пользователями и группами пользователей в системах с избирательным доступом нет жестких иерархических взаимоотношений, то есть взаимоотношений, которые определены по умолчанию и которые нельзя изменить. Исключение делается только для администратора, по умолчанию наделяемого всеми правами.
2. Мандатный доступ (от mandatory – обязательный, принудительный) - подход к определению прав доступа, при котором система наделяет пользователя определенными правами по отношению к каждому разделяемому ресурсу (в простейшем случае - файлу) в зависимости от того, к какой группе пользователь отнесен. От имени системы выступает администратор, а владельцы объектов лишены возможности управлять доступом к ним по своему усмотрению. Все группы пользователей в такой системе образуют строгую иерархию, причем каждая группа пользуется всеми правами группы более низкого уровня иерархии, к которым добавляются права данного уровня. Членам какой-либо группы не разрешается предоставлять свои права членам групп более низких уровней иерархии.

Второй способ является наиболее подходящим для создания правил автоматического ограничения доступа при работе с ОРИ, электронными документами, содержащими государственную или служебную тайну.

Рассмотрим схему взаимодействия в операционных системах. Пользователи являются субъектами доступа, идентифицируемыми по имени и паролю, а разделяемые ресурсы -

объектами. Для каждого типа объектов существует набор операций, которые с ними можно выполнять. Например, для файлов и папок есть следующие атрибуты для работы с документами[5]:

1. Право на чтение (просмотр) информации. В случае ОРИ данный пункт аналогичен наличию определенной степени допуска к информации ограниченного доступа.
2. Право на исполнение файлов. Применительно к ОРИ рассматривается доступ к информации, то есть непосредственному ознакомлению и использованию. При этом лица, имеющие допуск, не всегда могут иметь доступ.
3. Право на запись (изменение) информации. В случае с ОРИ данный пункт можно рассматривать, как право на ограничение доступа, а также снятие ограничений с ОРИ. Также сюда можно внести права на непосредственно изменение данных.
4. Права изменения атрибутов, которыми обычно обладает операционная система, администратор и в некоторых случаях владелец документа. Если рассматривать применение данного права к ОРИ, то группы лиц, имеющие доступ к секретной информации различного уровня, определяются нормативными правовыми актами, но в случае внесения поправок в них администратор системы вправе изменить атрибуты доступа.

Перейдём к непосредственному описанию алгоритма, представленного на рис.1:

1. Определить отношения, связывающие тип ОРИ, лиц, имеющих к ней доступ, а так же лиц, имеющих право на ограничение доступа и снятие ограничений доступа к ОРИ. В том числе:
   - определить категории допуска к работе документам;
   - привязать лиц, имеющие доступ к цифровым носителям информации, к категориям допуска;
   - определить существующие типы ОРИ и связать их с категориями допуска;
   - определить параметры доступа для отдельных лиц, имеющих категорию допуска (различные группы лиц при нахождении в одной категории допуска, могут либо не могут иметь возможность получения доступа к информации в связи с её привязанностью к специализации).

Реализация алгоритма для разделения прав доступа должна основываться на определении того, что обладателем информации, появившейся в процессе ОРД, являются органы государственной власти, уполномоченные ФЗ «Об ОРД» [1] на осуществление такой деятельности, их оперативные подразделения и сотрудники. Для разделения пользователей на группы можно использовать средства авторизации и аутентификации в операционных системах.

2. Определить, к какому типу принадлежит ОРИ и закрепить за документом степень ограничения доступа: а) открытая информация; б) конфиденциальная либо служебная информация; в) информация, составляющая государственную тайну.

Для автоматизации определения типа ОРИ следует использовать программно-реализованный контекстный анализ (tip(fileinfo)). В качестве определения ключевых значений поиска и анализа необходимо применять положения нормативных правовых актов [1 - ст. 12; 2 - ст. 2, 5 и др.]. Так же следует учитывать, какие сведения представляют собой конфиденциальную (служебную) ОРИ [3]. Изменять тип ОРИ в критериях аналитической программы могут только уполномоченные должностные лица.

3. Обеспечить ограничение доступа в соответствии с построенными выше отношениями и определенным типом ОРИ (setaccess(n)). Для этого необходимо:
   - реализация программного ограничения доступа по типу ОРИ (isPerm(user, access)).
   - реализация шифрования и дешифрования файлов, содержащих ОРИ, с целью ограничения доступа к информации на ЭВМ, неаттестованных на соответствие требованиям по технической защите информации. При дешифровании должна сохраняться возможность использования стандартных текстовых и визуальных редакторов операционных систем. Упрощая подход к защите данных на конкретных используемых в подразделении ЭВМ, возможно, применить программную модификацию метаданных файлов (fileinfo), автоматическое присвоение пароля документам;

– реализация программной надстройки над файловой системой, способной определять параметры ограничения доступа к файлу (getacces(fileinfo)).

Первый шаг алгоритма является предварительным и реализуется в виде таблиц соответствия, используемых в дальнейшем для установки критериев ограничения доступа и допуска. Второй и третий шаг алгоритма, реализован в виде обработчика событий, который ожидает событие «e» от системы в случае, если пользователь производит операции с файлом.

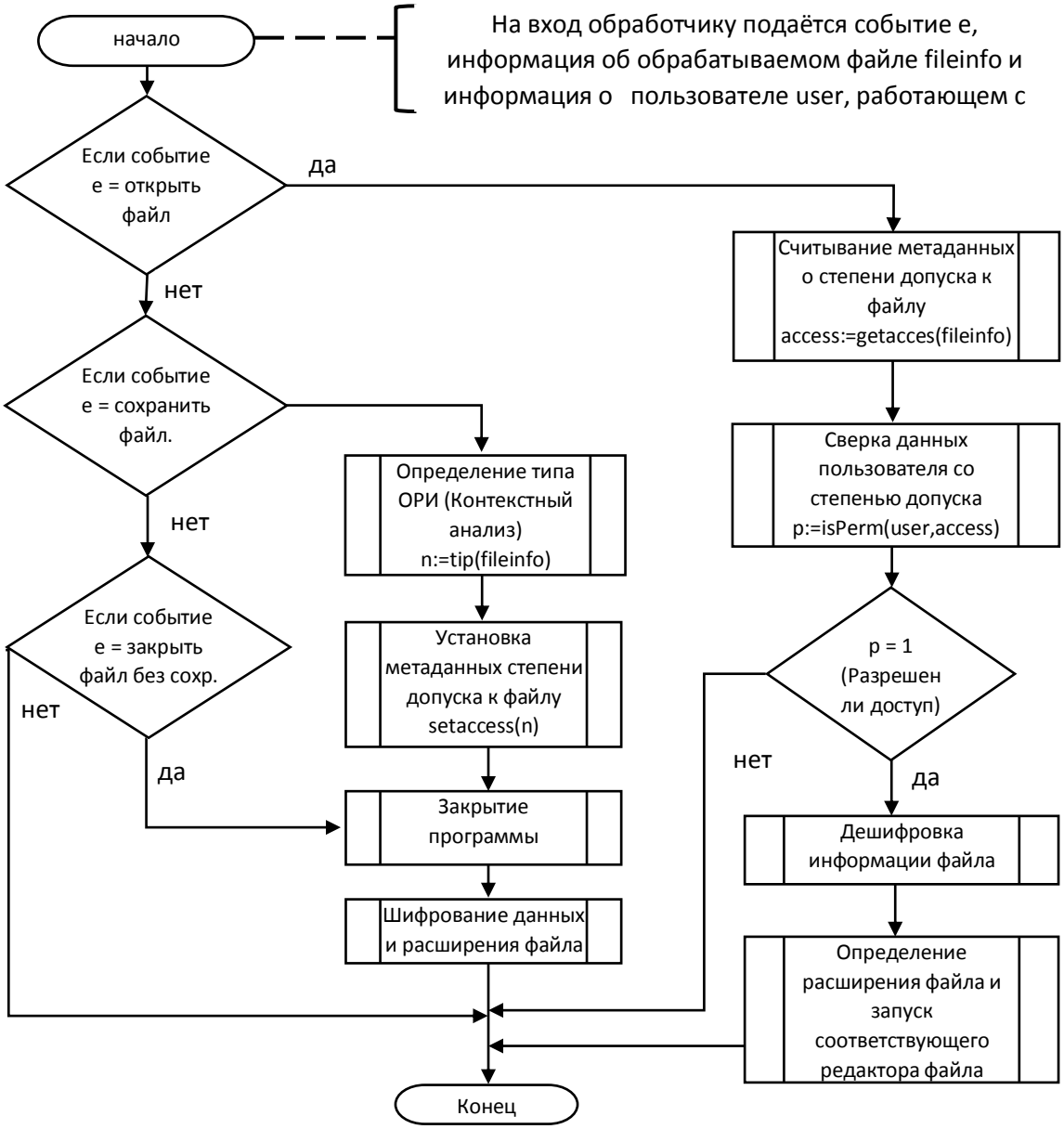


Рисунок 1. Алгоритм автоматизации ограничения доступа к оперативно-розыскной информации

По аналогии с файловыми системами современных операционных систем права на доступ к ОРИ разделяются на:

1. Права отдельного пользователя (лица).
2. Права для определённой группы лиц (категории допуска либо доступа).
3. Права для всех лиц вне зависимости от уровня и категории.

Так, в случае открытой информации матрица доступа к документам в файловой системе большинства операционных Unix-подобных систем будет представлена в виде 3-х десятичных цифр от 0 до 7, например, для открытой информации – атрибут «764». Расшифровка значений следующая:

1. Первая «7» – отдельные лица имеющие права на доступ, а также ограничение доступа к информации и снятие ограничения (такие как руководитель органа, осуществляющего ОРД).
2. Вторая «6» означают, что группы лиц с определенным уровнем допуска имеют доступ для чтения и использования данной информации до ограничения доступа к ней.
3. Последняя «4» означает, что даже лица, не имеющие никакого уровня допуска, могут получить доступ к ней.

В случае, если по решению руководителя органа или по критерию необходимо ограничить доступ к документу, система на основе программной реализации должна среагировать и автоматически изменить права доступа, например, на атрибут «732», что будет означать запрет доступа, если пользователь не принадлежит к группе с необходимой степенью допуска, соответствующей степени секретности документа. При этом, если вместо 3 будет стоять 2, то означает, что только лица, имеющие право доступа к информации, могут использовать её. Снятие ограничений происходит в обратном порядке.

Таким образом, работа данного алгоритма во многом будет зависеть от конкретной программной реализации контекстного анализа. Основной критерий качества анализа – быстрота и точность определения типа ОРИ. Представленный алгоритм является не только решением вопросов, связанных с автоматическим разделением доступа при работе с конфиденциальной информацией, но и реализацией автоматического ограничения доступа к информации, не соответствующей уровню допуска или доступа лиц, даже в случае, если они изначально являются владельцами электронного документа, содержащего ОРИ.

Литература:

1. Федеральный закон РФ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Российская газета. 1995. № 160.

2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220 – 8235.

3. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127.

4. Таненбаум. Э. Современные операционные системы [Текст]. СПб.: Питер, 2010. – 314-316 с.

5. Гвидо Сочер. Файлы - управление доступом: [Электронный ресурс] // LinuxFocus. 1999. URL: http://www.linuxfocus.org/Russian/January1999/article77.html. (Дата обращения: 05.02.2015).

Д.Н. Шубин

АНАЛИТИЧЕСКИЙ ОБЗОР АНСАМБЛЕЙ ДВОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СИСТЕМ РАДИОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Московский Технический Университет Связи и Информатики, г. Москва, Россия

Ключевые слова: псевдослучайная последовательность, двоичная последовательность, моделирование систем передачи информации.

В статье приведен обзор псевдослучайных последовательностей максимальной длины, последовательностей множества Голда, последовательностей большого и малого множества Касами, последовательностей Гордона-Миллза-Уэлча. Рассмотрены их авто- и взаимно-корреляционные свойства, размер ансамбля и сложность генерации.

D.N. Shubin

ANALYTICAL REVIEW OF THE ENSEMBLES OF BINARY PSEUDO-RANDOM SEQUENCES FOR SPECIAL PURPOSES RADIO COMMUNICATION SYSTEMS

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords. Pseudorandom sequences, binary sequences, modeling of communication systems.

The article gives an overview of pseudorandom sequences of maximum length, Gold sequences, small and big set of Kasami sequences, Gordon-Mills-Welch sequences. Consider their auto- and cross correlation properties.

Для систем радиосвязи специального назначения одним из главных требований является обеспечение сложности расшифровки структуры передаваемых радиограмм. Сложность расшифровки радиограммы зависит, в частности от сложности и объема используемого ансамбля сигнально-кодовых конструкций (СКК). При использовании СКК на основе фазоманипулированных сигналов сложность расшифровки радиограммы напрямую зависит от свойств используемого семейства псевдослучайных последовательностей (ПСП). В качестве основных свойств ПСП можно выделить возможную длину ПСП, размер ансамбля ПСП, сложность формирования ПСП, а также сложность её «расшифровки», виды авто- и взаимно-корреляционных функций ПСП. Существует большое число видов всевозможных псевдослучайных последовательностей. В этой статье мы коснемся основных видов ПСП, рассмотрим их свойства и корреляционные функции.

Наиболее распространенной ПСП, а также основой для формирования некоторых других видов ПСП является последовательность максимальной длины или М-последовательность. Её основные свойства выражаются в почти идеальной автокорреляционной функции, сбалансированности количества «0» и «1» на длине ПСП, простоте формирования. Эта ПСП формируется с помощью регистра сдвига с линейными обратными связями (РСЛОС). Этот способ формирования не требует больших вычислительных ресурсов как при аппаратной генерации, так и при программной генерации ПСП в том числе и большой длины. РСЛОС состоит из ячеек памяти и отводов от них образующих обратную связь. Характер отводов от ячеек задается формирующим полиномом. Для получения последовательности максимальной длины формирующий полином степени n должен быть примитивным (то есть являться делителем полинома $x^m + 1$ только при $m = 2^n - 1$, и не быть делителем при $m < 2^n - 1$). Длина М-последовательности формируемой таким РСЛОС будет равна $2^n - 1$, где n – разрядность регистра сдвига (степень формирующего полинома). Размер ансамбля М-последовательности заданной длины определяется количеством неприводимых полиномов заданной степени. При больших значениях степени n число примитивных полиномов весьма велико [1]. В частности для М-последовательности длины 1023 всего имеется 60 неприводимых полиномов. Ненормированная периодическая АКФ любой М-последовательности имеет постоянный уровень боковых лепестков, равный -1 независимо от длины последовательности. Максимальный выброс корреляционной функции равен длине ПСП. На рисунке 1 показана ПАКФ М-последовательности длины 63. Взаимно-корреляционная функция М-последовательностей может иметь достаточно большие выбросы достигающие трети от размера длины последовательности [2]. На рисунке 2 изображена взаимно корреляционная функция двух М-последовательностей длины 63.

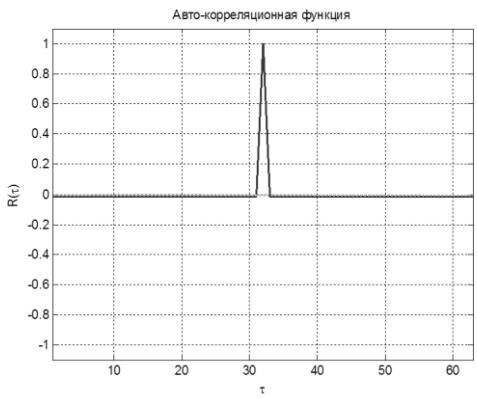


Рисунок 2.

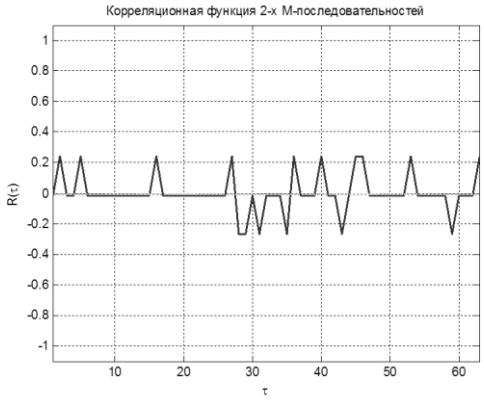


Рисунок 3.

В множестве М-последовательностей существуют такие ПСП которые имеют взаимно-корреляционные свойства лучшие чем у других ПСП множества. Такие последовательности называются предпочтительными парами. Боковые выбросы взаимно-корреляционной функции таких предпочтительных пар М-последовательностей принимают значения $-1, -1-2^{\left[\frac{n}{2}+1\right]}, -1+2^{\left[\frac{n}{2}+1\right]}$, где $[x]-$ целая часть x. Пары полиномов порождающих эти последовательности также называются предпочтительными [3, С.120]. Число таких предпочтительных пар М-последовательностей крайне невелико.

Кроме неудовлетворительных свойств взаимно корреляционной функции, для М-последовательности характерны такие недостатки как небольшой размер ансамбля и простота формирования, которая приводит к слабой защищенности ПСП от «вскрытия». Достаточно прочитать *2n* (где n – разрядность регистра) символов ПСП для восстановления отводов обратной связи РСЛОС и последующему получению М-последовательности полной длины [4].

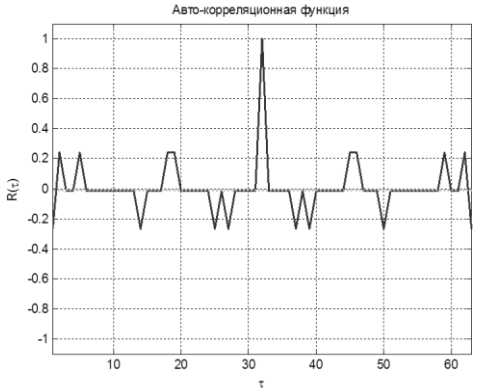


Рисунок 4.

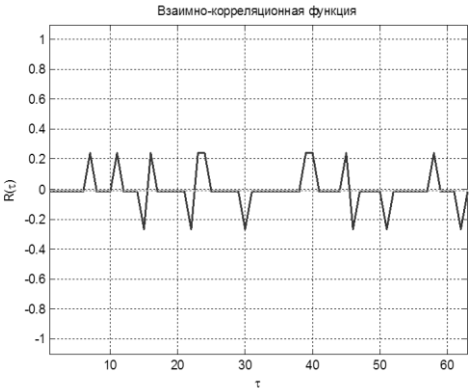


Рисунок 5.

Последовательности Голда характеризуются большим размером ансамбля и однородными и ограниченными значениями взаимно-корреляционной функции. Любая последовательность Голда образуется сложением по модулю 2 двух М-последовательностей, которые образуют предпочтительную пару. В множестве Голда всего 2^n+1 последовательностей включая две исходные М-последовательности. Например для последовательностей длины 1023 существуют 1025 последовательностей Голда. Множества последовательностей Голда имеют трехуровневые корреляционные функции принимающие значения: $\left\{-1, -2^{\frac{n+1}{2}}-1,\ 2^{\frac{n+1}{2}}-1\right\}$ для нечетных n, и $\left\{-1, -2^{\frac{n}{2}+1}-1,\ 2^{\frac{n}{2}+1}-1\right\}$ для четных n [1]. На рисунке 3 изображена авто-корреляционная функция последовательности Голда длины 63, на рисунке 4 изображена взаимно-корреляционная функция последовательностей Голда длины 63.

Большое множество последовательностей Касами включает в себя также и малое множество Касами. Они отличаются размером ансамбля и значениями боковых пиков корреляционных функций. Последовательности в этих множествах имеют длину $2^n - 1$.

Кодовые последовательности малого множества Касами формируются с помощью сложения по модулю 2 исходной М-последовательности и всех возможных сдвигов последовательности полученной из исходной путем децимации с коэффициентом $2^{\frac{n}{2}} + 1$.

Количество последовательностей малого множества Касами равно $2^{\frac{n}{2}}$, что приводит к наличию 32 последовательностей длины 1023. Боковые выбросы ПАКФ и максимальные значения ПВКФ последовательностей Касами малого множества относятся к классу трехуровневых и принимают значения $\left\{-1, -2^{\frac{n}{2}} - 1,\ 2^{\frac{n}{2}} - 1\right\}$ [1]. На рисунке 5 изображена авто-корреляционная функция последовательности малого множества Касами длины 63, на рисунке 6 изображена взаимно-корреляционная функция последовательностей малого множества Касами длины 63.

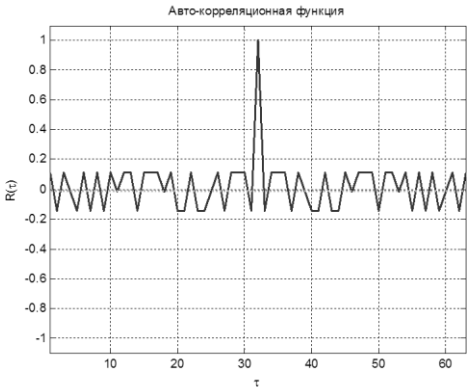


Рисунок 6.

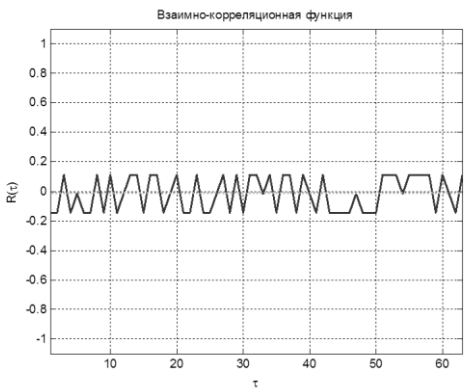


Рисунок 7.

Большая система последовательностей Касами образуется при сложении по модулю 2 исходной М-последовательности и всех возможных сдвигов 2-ух последовательностей полученных путем децимации исходной последовательности с коэффициентами $-2^{\frac{n}{2}} - 1$ и $2^{\frac{n}{2}+1} + 1$ соответственно. Объем ансамбля последовательностей большого множества Касами при n mod 4 = 2 равен $2^{\frac{n}{2}}(2^n + 1)$, а при n mod 4 = 0 равен $1 + 2^{\frac{n}{2}}(1 + \frac{1}{3}(2^n - 1))$. Для последовательностей длины 1023 в большом множестве Касами существует 32800 последовательностей. Боковые выбросы ПАКФ и максимальные значения ПВКФ последовательностей Касами большого множества являются пятиуровневыми и могут принимать значения $\left\{-1, \left(-2^{\frac{n}{2}} - 1\right), \left(2^{\frac{n}{2}+1} - 1\right), \left(2^{\frac{n}{2}} - 1\right), \left(-2^{\frac{n}{2}+1} - 1\right)\right\}$ [2]. На рисунке 7 изображена авто-корреляционная функция последовательности большого множества Касами длины 63, на рисунке 8 изображена взаимно-корреляционная функция последовательностей большого множества Касами длины 63.

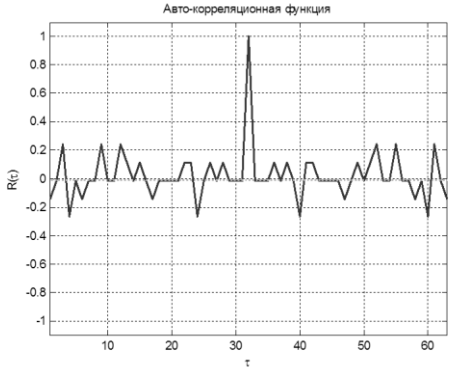


Рисунок 8.

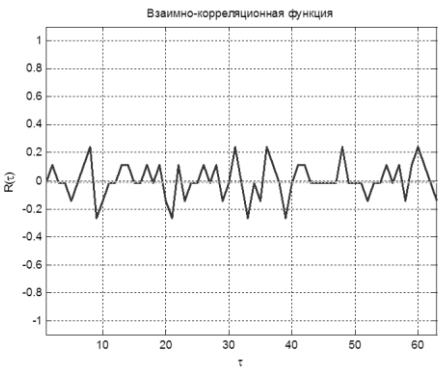


Рисунок 9.

Последовательности Гордона-Миллза-Уэлча (ГМВ) формируются из исходной М-последовательности и существуют для степеней формирующего полинома являющегося составным число в котором один из множителей больше или равен 3. Длина ГМВ-последовательности также равна $2^n - 1$.

Способ формирования ГМВ-последовательностей основан на замене в исходной М-последовательности характеристической М-последовательности и всех её сдвигов на другую такой же длины [6]. Количество ГМВ-последовательностей равно количеству формирующих «длинных» М-последовательностей умноженному на количество «коротких» характеристических М-последовательностей минус 1. При длине 1023 можно сформировать 300 ГМВ-последовательностей. Авто-корреляционная функция ГМВ последовательностей является такой же, как у М-последовательностей.

Максимальные выбросы взаимно-корреляционных функций возможных комбинаций пар последовательностей ГМВ не превышают уровня максимальных выбросов взаимно-корреляционных функций М-последовательностей [5]. На рисунке 9 изображена авто-корреляционная функция ГМВ-последовательности длины 63, на рисунке 10 изображена взаимно-корреляционная функция ГМВ-последовательностей длины 63.

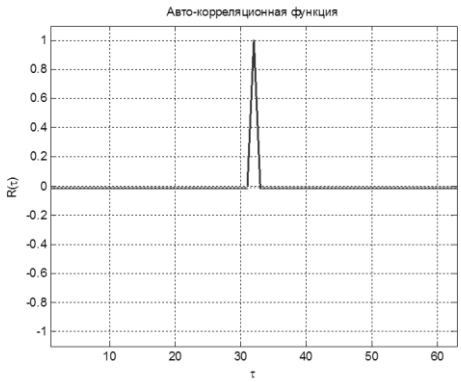


Рисунок 10.

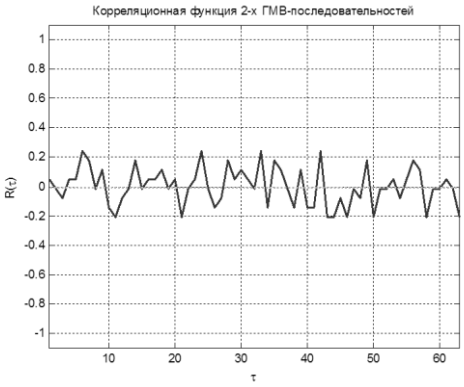


Рисунок 11.

Выводы. Взаимно-корреляционная функция М-последовательностей может иметь достаточно большие выбросы достигающие 30-60% от размера длины последовательности, можно выбрать предпочтительные пары М-последовательностей с ограниченными и определенными выбросами ВКФ, но число таких последовательностей будет мало. Последовательности множества Голда имеют определенные и ограниченные выбросы ВКФ, имеют большой объем ансамбля и достаточную простоту генерации. Последовательности Касами большого множества имеют максимальный объем ансамбля из всех рассмотренных нами ПСП и удовлетворительные значения выбросов корреляционных функций. Вышеперечисленные семейства ПСП имеют линейный алгоритм генерации, а значит обладают слабой стойкостью к их расшифровке. ГМВ-последовательности имеют свойства корреляционных функций похожие на свойства М-последовательностей, но алгоритм формирования ГМВ-последовательностей имеет нелинейный принцип, а значит он более устойчивый к декодированию структуры ПСП что позволяет применять их в системах радиосвязи специального назначения.

Литература:

1. Прокис Джон. Цифровая связь. Пер с англ. / Под ред. Д.Д. Кловского – М.: Радио и связь, 2000. – 800с.

2. Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. Заказная статья. ТИИЭР. 1980.

3. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985, 384с.

4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. — М.: Мир, 1986. — 576с.

5. Бессарабова А.А. М-последовательности: пособие для тех, кто о них кое-что знает, но хочет знать больше. – Воронеж. 2010г. – 223с.

6. Стародубцев В.Г. Алгоритм формирования последовательностей Гордона-Миллза-Велча. Приборостроение Т.55 №7 2012г.

О.Г. Щербань, Я.В. Молчанова

РЕШЕНИЕ ЗАДАЧИ ИДЕНТИФИКАЦИИ НЕСТАЦИОНАРНЫХ ПАРАМЕТРОВ ДИНАМИЧЕСКОЙ МОДЕЛИ

Южный федеральный университет, г.Ростов-на-Дону, Россия

Ключевые слова: идентификация динамической модели, теория чувствительности, нестационарные параметры.

Рассмотренный подход позволяет осуществлять оптимальную по квадратичному критерию идентификацию детерминированной и известной с точностью до вектора нестационарных параметров динамической модели. Решение получено на основе использования идеи обратной задачи теории чувствительности.

O.G. Shcherban, J.V. Molchanova

THE DYNAMIC MODEL IDENTIFICATION PROBLEM'S SOLUTION ON THE SINGLE PRECISE OBSERVATION OF ITS STATE

Southern Federal University, Rostov-on-Don, Russia

Key words: the dynamic model identification, the sensitivity theory, single precise observation.

An approach, having been considered, allows a quadratic criterion optimal identification of a deterministic (non-stochastic) and known for a non-stationary vector-parameter dynamic model. The identification procedure has been synthesized on the basic of the reserve problem idea of the sensitivity theory.

Известные методы решения задач идентификации базируются на упрощающем допущении о постоянстве вектора неизвестных идентифицируемых параметров модели p ($\dot{p} = 0$) [1-3], которое не позволяет учесть возможные низкочастотные флуктуации этих параметров и, соответственно, может существенно снизить потенциальную точность оценивания. Поэтому проблема решения задачи идентификации нестационарных параметров динамической модели

$$\frac{dx}{dt} = f\left(x,t;\, p(t)\right), \tag{1}$$

по зашумленным измерениям

$$z = x\left(t, p(t)\right) + \xi_t, \tag{2}$$

где x – вектор состояния; f – известная нелинейная вектор-функция; $p(t)$ – вектор-функция искомых нестационарных параметров $\left(x \in R^n, p \in R^m,\ \dot{p} \neq 0,\ n > m,\ t \in [t_0, t_k]\right)$; $z(t)$ – модель информационных сигналов наблюдателя ($z \in R^q$); ξ_t - белый гауссовский шум с нулевым средним и матрицей интенсивностей $D_\xi(t)\delta(t-\tau)$,

до сих пор является актуальной.

Как видно из постановочной части, предполагается случай непосредственного наблюдения вектора состояния модели x [1], что значительно упрощает ее решение. Оптимальная оценка вектора p определяется при этом из условия минимума квадратичного функционала [1-4]

$$J(p) = \int_{t_0}^{t_k} \left(z^{\text{и}} - x(t,p)\right)^{\text{т}} D_\xi^{-1} \left(z^{\text{и}} - x(t,p)\right) dt, \tag{3}$$

где $z^{и}(t)$ – вектор реальных измерений.

При решении задачи целесообразным является использование априорных данных p_i^* $\left(p_i^* = \text{const}\right)$ об идентифицируемых компонентах p_i, которые обычно доступны из результатов предыдущих калибровок, технических характеристик модели и т.п. Тогда

$$p_i(t) = p_i^* + \Delta p_i(t),$$

где $\Delta p_i(t)$ – искомые флуктуации параметров, отклонения реальных значений идентифицируемых коэффициентов от их априорных значений. (В частном случае можно принять $p_i^* = 0$). При этом физически обоснованным является предположение о малости отклонений $\Delta p_i(t)$. В то же время, подобное допущение позволяет представить зависимость вектора состояния x от вектора идентифицируемых параметров p как

$$x(t, p(t)) \approx x(t, p^* + \Delta p(t)),$$

и, следуя работам [1,3], построим аппроксимацию

$$x(t, p^* + \Delta p) = x^*(t, p^*) + M_x(t)\Delta p,$$

где $M_x(t)$ – матрица чувствительности, являющаяся решением матричного дифференциального уравнения

$$\frac{dM_x}{dt} = \frac{\partial \hat{f}(x^*, t; p^*)}{dx^*} M_x(t) + \frac{\partial \hat{f}(x^*, t; p^*)}{\partial p} \quad \text{при} \quad p = p^*; \; M_x(t_0) = 0,$$

а $x^*(t,p^*)$ – вектор состояния, определяемый путем интегрирования модели (1) при априорно известных значениях p_i^* :

$$\frac{dx^*}{dt} = \hat{f}(x^*, t; p^*), \quad x^*(t_0) = x_0.$$

Функционал (3) при этом имеет вид:

$$J(p) = \int_{t_0}^{t_k} \left(\Delta x\left(z^{и}, x^*, t; p^*\right) - M_x(t)\Delta p\right)^{т} D_\xi^{-1} \left(\Delta x\left(z^{и}, x^*, t; p^*\right) - M_x(t)\Delta p\right) dt,$$

где $\Delta x\left(z^{и}, x^*, t; p^*\right) = z^{и} - x^*(t, p^*)$,

из условия наличия экстремума которого получаем искомое алгебраическое уравнение $\Psi_1 \Delta p = \Psi_2$,

где матрица Грама Ψ_1 и вектор Ψ_2 определяются как

$$\Psi_1 = \int_{t_0}^{t_k} M_x^{т} D_\xi^{-1} M_x \, dt; \qquad \Psi_2 = \int_{t_0}^{t_k} M_x^{т} D_\xi^{-1} \Delta x \, dt,$$

а неравенство $\det \Psi_1 \neq 0$ является условием идентифицируемости. При выполнении этого условия естественным образом определяется искомый вектор флуктуаций $\Delta p(t)$ как

$$\Delta p = \Psi_1^{-1} \Psi_2.$$

Ограничением рассмотренного подхода является предположение о малости отклонений $\Delta p_i(t)$ идентифицируемых параметров.

Литература:

1. Справочник по теории автоматического управления / Под ред. А.Красовского. - М.: Наука, 1987. - 712с.

2. Степанов О.А. Применение нелинейной фильтрации в задачах обработки навигационной информации. - СПб: ГНЦРФ - ЦНИИ "Электроприбор", 1998. - 370с.

3. Розенвассер Е.Н., Юсупов Р.М. Чувствительность систем управления. М: Наука, 1981.

А.В. Балобанов, Р.С. Селимов

ОБЗОР МЕТОДОВ ФОРМИРОВАНИЯ ТЕЛЕВИЗИОННОГО СИГНАЛА В СИСТЕМЕ DVB-T2

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: сигнал, телевидение, обработка, модуляция, кодирование.

Рассмотрена проблема формирования телевизионного сигнала в системе DVB-T2: применение предварительной обработки сигнала, его кодирования и передачи.

A.V. Balobanov, R.S. Selimov

REVIEW OF METHODS OF FORMING OF TELEVISION SIGNAL IN DVB-T2 SYSTEM

Moscow technical university of communications and informatics

Keywords: signal, television, processing, modulation, coding

This review descrides the problem of forming of television signal in DVB-T2 system, signal pre-processing, signal coding and broadcasting.

Изначально система DVB-T предназначалась для передачи транспортного потока MPEG-TS, но в DVB-T2 представлена возможность передачи любых иных транспортных потоков, для этого введена предварительная обработка входного транспортного потока. Входной поток заключается в канал физического уровня PLP (Physical Layer Pipe), каждый из потоков может иметь один из следующих форматов [1]:

- транспортный поток (Transport Stream, TS)
- обобщённый инкапсулированный поток (Generic Encapsulated Stream, GSE)
- обобщенный непрерывный поток (Generic Continuous Stream, GCS)
- обобщённый поток с фиксированной длиной пакета (Generic Fixed-Length Packetized Stream, GFPS), эта форма сохраняется для совместимости с DVB-S2, но предполагается, что вместо неё будет использоваться GSE.

Далее из входных потоков собираются потоковые кадры (Baseband frame, BBFRAME, BB-кадры). Входной интерфейс содержит три подсистемы: синхронизатор входных потоков, обнаружитель нулевых пакетов и циклический избыточный кодер CRC-8 (полином $x^8 + x^7 + x^6 + x^4 + x^2 + 1$). Далее получившийся поток разделяется на поля данных и к началу каждого приставляется BB-заголовок (Baseband Header, BBHEADER).

Затем следует адаптация потока, состоящая из двух действий (для режима «A»):

- наполнение (создание одинаковой длины потоковых кадров, возможно использование для сигнализации о типе потока)
- скремблирование (для уравнивания энергии по длине кадра).

Схема модуля входной обработки для режима "A" (один канал PLP) приведена на рисунке 1.

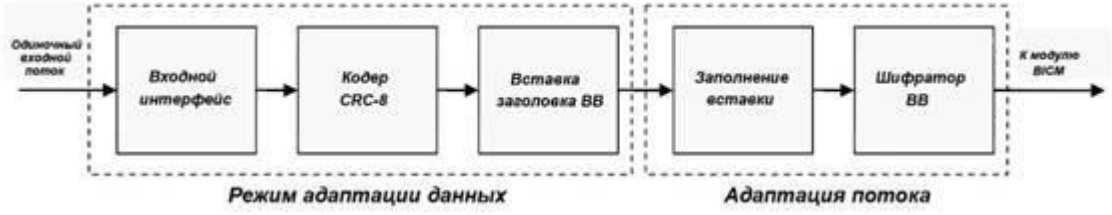


Рисунок 1. Схема модуля входной обработки для режима "A" (один канал PLP)

На выходе получаются BB-кадры одинаковой длины и строения, готовые к последующей обработке.

Кодирование и модуляция с битовым перемежением (Bit-interleaved coding and modulation, BICM).

BB-кадр проходит через блок прямой коррекции ошибок (Forward Error Correction, FEC), где наполняется избыточными битами путём внешнего БЧХ кодирования и внутреннего LDPC кодирования (формат кадра до перемежения показан на рисунке 2), после чего следует битовое перемежение.

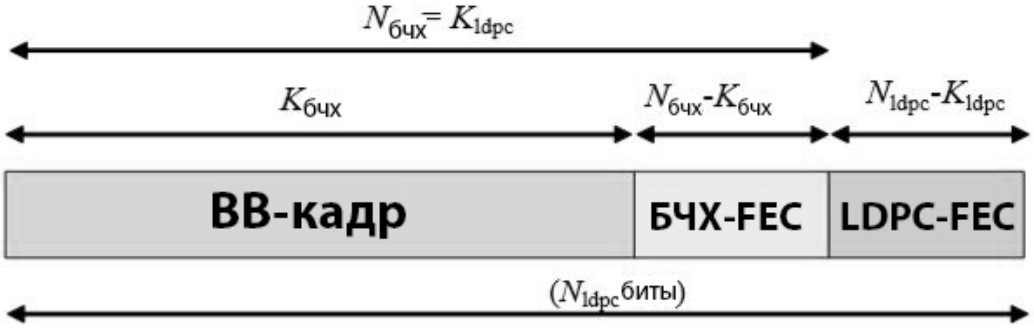


Рисунок 2. Формат кадра до перемежения

Полная длина нормального FEC-кадра с наложенным помехозащитным кодированием 64800 бит, короткого FEC-кадра – 16200 бит. Длины блоков после кодирования (для нормального FEC-кадра) приведены в таблице 1.

Таблица 1. Длины блоков после кодирования (для нормального FEC-кадра)

LDPC код	Не кодированный блок	Блок, кодированный БЧХ кодом	Блок, кодированный LDPC кодом
1/2	32208	32400	64800
3/5	38688	38880	64800
2/3	43040	43200	64800
3/4	48408	48600	64800
4/5	51648	51840	64800
5/6	53840	54000	64800

Код БЧХ способен исправить 10 ошибок для случаев 2/3 и 5/6 (добавляется 160 проверочных бит БЧХ кода) и 12 ошибок для остальных случаев (добавляется 192 проверочных бита).

Полином БЧХ имеет 16 степень для нормального FEC-кадра и 14 степень для короткого FEC-кадра.

Далее FEC-кадр попадает на перемежитель, где из кадра, содержащего 64800 бит, строятся столбцы:

16КАМ – 8 столбцов по 8100 бит

64КАМ – 12 столбцов по 5400 бит

256КАМ – 16 столбцов по 4050 бит

Каждый следующий столбец считывается с определенного элемента, порядковый номер которого задан стандартом, таблица приведена ниже:

Таблица 2. Параметр считывания столбцов

Модуляция	количество столбцов	кол-во бит	Порядковый номер первого считываемого бита в столбце															
			Столб. 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16-QAM	8	64 800	0	0	2	4	4	5	7	7	-	-	-	-	-	-	-	-
		16 200	0	0	0	1	7	20	20	21	-	-	-	-	-	-	-	-
64-QAM	12	64 800	0	0	2	2	3	4	4	5	5	7	8	9	-	-	-	-
		16 200	0	0	0	2	2	2	3	3	3	6	7	7	-	-	-	-
256-QAM	16	64 800	0	2	2	2	2	3	7	15	16	20	22	22	27	27	28	32
	8	16 200	0	0	0	1	7	20	20	21	-	-	-	-	-	-	-	-

Далее поток бит из перемежителя поступает на демультиплексор бит по ячейкам кодовых слов, где разделяется на подпотоки: QPSK делится на 2 подпотока, 16-QAM – на 8, 64-QAM – на 12, 256-QAM – на 16 (короткий – на 8).

Демультиплексированные потоки попадают на модулятор, в котором используются следующие методы модуляции: QPSK, 16-QAM, 64-QAM, 256-QAM, также, возможно использование BPSK для сигнализации.

Применено Греевское кодирование, в котором соседние элементы сигнального созвездия отличаются только в одном бите. В DVB-T2 используется так же вращение сигнального созвездия. Пример поворота сигнального созвездия для 16-QAM приведен на рисунке 3. Поворот сигнального созвездия дает выигрыш в отношении сигнал/шум до 5 дБ. Углы поворота созвездия приведены в таблице 3.

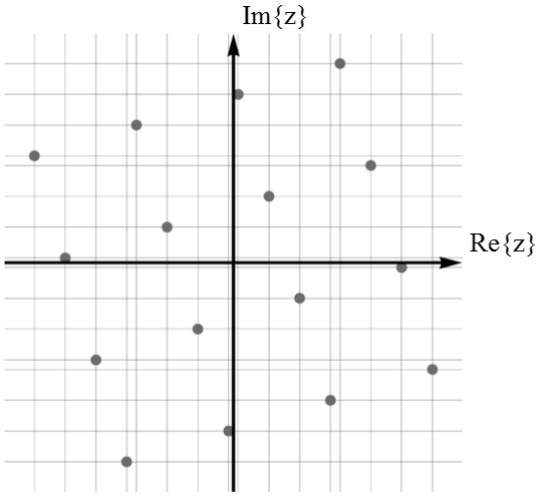


Рисунок 3. Сигнальное созвездие 16-QAM

Таблица 3. Углы поворота сигнального созвездия

Модуляция	QPSK	16-QAM	64-QAM	256-QAM
Угол (градусы)	29.0	16.8	8.6	Arctg(1/16)

Суть поворота сигнального созвездия заключается в том, что проекции точек созвездия на синфазную и квадратурную оси не совпадают и, имея одну из координат, можно вычислить другую.

Наряду с поворотом сигнального созвездия имеется возможность борьбы с пик–фактором путем введения резервных пилот-тонов. С их помощью, там где это необходимо, появляется возможность изменения формы передаваемого сигнала путем перераспределения задействованных в формировании символа активных поднесущих. Режим введения резервных пилот-тонов, так же как и вращения сигнального созвездия не является обязательным при вещании.

В стандарте также описано псевдослучайное перемежение ячеек FEC-кадра, которое позволяет избежать коррелированных ошибок, но не менее важным является временное перемежение: FEC-блоки из перемежителя ячеек группируются в кадры перемежения, каждый кадр перемежения содержит динамически изменяемое число FEC-блоков (не более 1023). Возможно три варианта размещения блоков перемежения:

- каждый TI-блок (блок перемежения, Time Interleaving) помещается в кадр перемежения, который в свою очередь помещается в T2-кадр (T2-frame);
- каждый TI-блок помещается в кадр перемежения, который занимает два или более T2-кадра;
- несколько TI-блоков помещаются в один кадр перемежения, который занимает один T2-кадр.

Одной из важнейших особенностей, отличающих систему DVB-T2 от предыдущего поколения - DVB-T является увеличение числа поднесущих, добавлены режимы 1К, 4К, 16К, 32К. Наибольший интерес представляет режим 32К (27841 поднесущих), ведь при увеличении числа

поднесущих - можно увеличивать длительность передающихся символов, что позволяет сокращать длину защитных интервалов. Так, для сравнения, в DVB-T максимальная длина суперкадра в режиме 8К - 0.896мс, а в DVB-T2, в режиме 32К - 3.584мс. Введен расширенный режим, для 8К, 16К, 32К поднесущих. Расширенный режим используется в случаях, когда нет строгих требований по совместимости со станциями в соседнем канале, добавляют дополнительные несущие по краям спектра так, что они находятся внутри маски, но спад спектра более крутой. Такое расширение спектра на 1-2% для канала 8 МГц (7,77 МГц вместо 7,61 МГц) позволяет увеличить эффективность его использования. На рисунке 4 показана детализация теоретического спектра DVB-T2 для длительного защитного интервала 1/8 (для 8 МГц каналов).

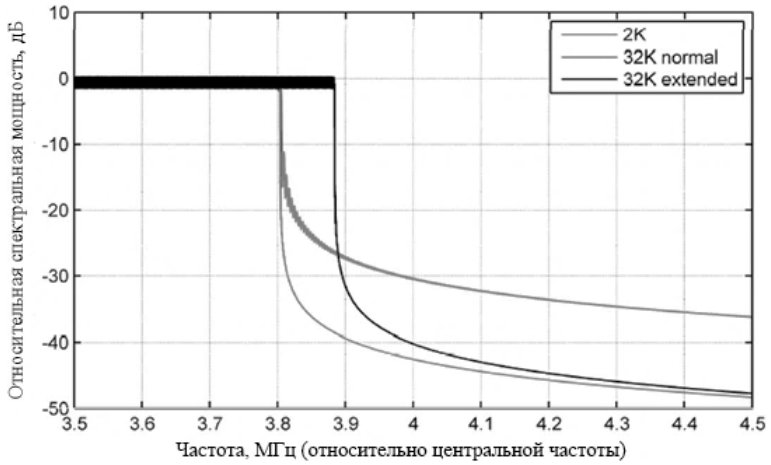


Рисунок 4. Детализация теоретического спектра DVB-T2 для длительности защитного интервала 1/8 (для 8 МГц каналов)

Выводы:

1. Стандарт DVB-T2 предлагает новые методы канального кодирования, обеспечивающие лучшую помехоустойчивость, в сравнении с предыдущей версией стандарта, в многолучевых каналах, характерных для городской застройки.

2. Используются также различные варианты распределения пилот-сигналов, позволяющие оптимизировать их количество, с учетом условий приема сигнала передачи.

3. Расширение вариантов числа поднесущих обеспечивает свободу выбора и организацию, например, передачи в условиях подвижного приема, с учетом скорости относительного смещения. С другой стороны в условиях стационарного приема увеличение числа поднесущих позволяет снизить относительную протяженность защитного интервала.

4. В части борьбы с пик-фактором используются 2 новые методики - расширение активного созвездия и резервирование пилот-тона, позволяющие снизить пик-фактор без увеличения ошибок и внеполосного излучения.

5. Добавлен режим передачи с расширенными несущими, позволяющий в стандартной полосе 8 МГц передавать большее количество данных (примерно на 2%), при этом не выходя за границы разрешённой спектральной маски.

Литература:

1. ETSI EN 302 755 V1.4.1 02.2015. Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)

2. Серов А. DVB-T2 - цифровое телевидение второго поколения. Научно-технический журнал. Июль 2009.

Г.С. Хасоян, В.В. Кормильченко, Н.О. Светличная

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В СОВРЕМЕННОМ МИРЕ

Северо-Кавказский филиал Московского технического университета связи
и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: Облако, Облачные технологии, облачные вычисления, облачные хранилища, виртуальная инфраструктура, провайдер, веб-сервис,

В данной статье рассматривается значимость использования технологии облачных вычислений, её вклад в развитие телекоммуникационной отрасли, а так-же её влияние на успешное ведение бизнеса. В статье описывается сама технология, включая её преимущества, проблемы и тенденции к развитию.

G.S. Hasoyan, V.V. Kormilchenko, N.O. Svetlichnaya

CLOUD TECHNOLOGY IN THE MODERN WORLD

North-Caucasus branch of the Moscow technical university of communication and informatics,
Rostov-on-Don, Russia

Keywords: cloud technologies, cloud computing, cloud storage, virtual infrastructure provider, web service, business, information security.

The paper considers importance of using cloud computing technologies, as a contribution in the telecommunications industry development, and an important factor for the successful business operation. The paper describes the technology including its advantages, problems, and future trends.

В последние годы в IT-сообществе широко распространилось мнение о том, что современные cloud-технологии способны существенно сократить расходы, и сегодня многие компании все чаще переносят свои корпоративные системы и бизнес-приложения в облако.

Облачные вычисления (cloud computing) — информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему набору конфигурируемых вычислительных ресурсов (сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам - как вместе, так и по отдельности). Они могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру.

История и ключевые факторы ключевые облачных вычислений. Впервые идея того, что мы сегодня называем облачными вычислениями была озвучена J.C.R. Licklider, в 1970 году. В эти годы он был ответственным за создание ARPANET (Advanced Research Projects Agency Network). Его идея заключалась в том, что каждый человек на земле будет подключен к сети, из которой он будет получать не только данные на и программы. Другой ученый John McCarthy высказал идею о том, что вычислительные мощности будут предоставляться пользователям как услуга (сервис). На этом развитие облачных технологий было приостановлено до 90-х годов, после чего ее развитию поспособствовал ряд факторов:

1. Расширение пропускной способности Интернета, в 90-е годы не позволило получить значительного скачка в развитии в облачной технологии, так как практически ни одна компания не технологии того времени не были готовы к этому. Однако сам факт ускорения Интернета дал толчок скорейшему развитию облачных вычислений.
2. Одним из наиболее значимых событий в данной области было появление Salesforce.com в 1999 году. Данная компания стала первой компанией предоставившей доступ к своему приложению через сайт, по сути данная компания стала первой компанией предоставившей свое программное обеспечение по принципу – программное обеспечение как сервис (SaaS).
3. Следующим шагом стала разработка облачного веб-сервиса компанией Amazon в 2002 году. Данный сервис позволял хранить, информацию и производить вычисления.

4. В 2006, Amazon запустила сервис под названием Elastic Compute cloud (EC2), как веб-сервис который позволял его пользователям запускать свои собственные приложения. Сервисы Amazon EC2 и Amazon S3 стали первыми доступными сервисами облачных вычислений.
5. Другая веха в развитие облачных вычислений произошла после создания компанией Google, платформы Google Apps для веб-приложений в бизнес секторе.
6. Значительную роль в развитии облачных технологий сыграли технологии виртуализации, в частности программное обеспечение позволяющее создавать виртуальную инфраструктуру.
7. Развитие аппаратного обеспечения способствовало не столько быстрому росту облачных технологий, сколько доступности данной технологии для малого бизнеса и индивидуальных лиц.

Что касается технического прогресса, то значительную роль в этом сыграло создание многоядерных процессоров и увеличения емкости накопителей информации.

Использование облачных технологий в России.

Российский бизнес относится к «облакам» гораздо осторожнее, чем западный. Провайдеры говорят, что подавляющее число вопросов к провайдеру, SLA и прочим документам связано с вопросами информационной безопасности. Если отечественный клиент задумался об использовании внешних облачных сервисов, то почти наверняка он пристально изучил законодательные требования к сохранности персональных данных , технологические возможности по обеспечению информационной безопасности и непрерывности сервисов. И способен проконтролировать любого провайдера.

На Западе «облакам» доверяют. В Европе уже разработана и представлена Европейская облачная стратегия. В США пошли еще дальше, намереваясь перенести часть государственных информационных систем в «облако».

В России облачные технологии рассматривают все более пристально - провайдеры предлагают самые разные услуги, доступные частным лицам и необходимые серьезному бизнесу. Однако именно корпорации, которые могли бы получать выгоду от использования облачных вычислений, не торопятся отдавать «на сторону» критически важные приложения или бизнес-информацию, а если и признают пользу от технологии, то строят частное «облако», которое долгое время используют лишь в тестовом режиме.

Одна из основных причин осторожного отношения к концепции облачных вычислений — проблема сохранности данных.

Зачастую возникает вопрос о конфиденциальности и сохранности персональных данных и о распределении ответственности между провайдером и заказчиком. Разграничение прав и обязанностей зависит от предоставляемого типа услуг.

В России существует только один закон, касающийся персональных данных, но он достаточно четкий, в последние годы появились подзаконные акты, которые конкретизируют практику его применения. В частности, есть приказ ФСТЭК №21 формулирующий рамки и организационные требования, которым должна соответствовать информационная система провайдера, чтобы работать с тем или иным классом персональных данных. Так что законодательство проработано, осталось только выполнять его требования.

Перспективы развития облачных вычислений.

К 2014 году доля облачных вычислений в рабочей нагрузке ЦОД достигла 51%. По прогнозам, к концу 2015 году мировой объем трафика, связанного с облачными вычислениями, составит 1,6 зеттабайт .

Зеттабайт равен одному секстиллиону байт или одному триллиону гигабайт. Объем трафика в 1,6 зеттабайт - это:

- 22 триллиона часов потоковой музыки;
- 5 триллионов часов деловых веб-конференций с веб-камерами;
- 1,6 триллиона часов онлайновых видеопотоков высокого разрешения (HD).

Облако стало самым быстрорастущим сегментом трафика в центрах обработки данных. К концу 2015 года совокупный годовой объем трафика ЦОД вырастет в 4 раза до 4,8 зеттабайт, а среднегодовые темпы роста этого трафика составят 33 процента. В настоящее время доля "облачного" трафика в общем трафике ЦОД составляет 11 процентов. К 2016 году она должна

превысить 33 процента. Таким образом, облако приобретает критически важное значение для будущего информационных технологий, а также для доставки видео и контента.

Чтобы оценить мировую готовность к облачным вычислениям, исследователи проанализировали в разных географических регионах такие параметры, как распространение широкополосных технологий, средняя скорость во входящих и исходящих каналах и средний уровень задержки (латентности). Исследователи пришли к выводу, что в настоящее время все регионы, где проводился такой анализ: Азиатско-Тихоокеанский регион, Ближний Восток и Африка, Западная Европа, Центральная и Восточная Европа, Латинская Америка и Северная Америка, - готовы к внедрению облачных приложений для социальных сетей и веб-конференций. Что же касается облачных приложений более высокого уровня (видеочаты, видеопотоки высокого разрешения и т.п.), то сетевые ресурсы для их поддержки имеются в Азиатско-Тихоокеанском регионе, Западной Европе, Центральной и Восточной Европе и Северной Америке.

Литература:

1. http://www.croc.ru/solution/virtualization/
2. http://www.cisco.com/web/RU/news/releases/txt/2011/113011.html/
3. http://www.cnews.ru/

***В.Г. Кобак, *А.С. Мерзленко, А.Г. Жуковский**

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ПОИСКА ВСЕХ МАКСИМАЛЬНО ВНУТРЕННЕ УСТОЙЧИВЫХ ПОДМНОЖЕСТВ В РАМКАХ РЕШЕНИЯ ЗАДАЧИ ПОИСКА «МИНИМАКСНОЙ» РАСКРАСКИ ОБЫКНОВЕННОГО ВЗВЕШЕННОГО ГРАФА

*Донской государственный технический университет, г. Ростов-на-Дону, Россия
Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: метод Магу, алгоритм Брона-Кербоша, раскраска взвешенного графа.

В статье рассматриваются и сравниваются алгоритмы Магу и Брона-Кербоша поиска всех максимально внутренне устойчивых подмножеств графа. Алгоритмы сравниваются в контексте решения задачи поиска раскраски по минимаксному критерию. Сравнение производится по времени выполнения на графах разных размеров.

***V.G. Kobak, A.S. *Merzlenko, A.G. Zhukovskiy**

COMPARATIVE ANALYSIS OF ALGORITHMS FOR SEARCHING ALL MAXIMUM INDEPENDENT SUBSETS IN CASE OF THE «MINIMAX» COLORING OF ORDINARY WEIGHTED GRAPH

*Don state technical university, Rostov-on-Don, Russia
North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: Maghout method, Bron–Kerbosch algorithm, weighted graph coloring problem.

This paper represent specification and comparison of Maghout method and Bron–Kerbosch algorithm in context of weighted graph coloring problem. Algorithms compare in terms of speed on several sizes graphs.

Введение. Задача раскраски взвешенного графа – это модификация обычной задачи раскраски графа, в которой на отыскиваемую раскраску накладывается некоторое ограничение, связанное с весами вершин. В этой статье будет рассматриваться «минимаксная» раскраска, т.е. правильная раскраска, по возможности минимизирующая максимальную сумму весов вершин

одного цвета. Подобная задача возникает, например, при необходимости распределения команд (задач, операторов) в многопроцессорной системе, когда требуется минимизировать загрузку каждого процессора. Команды представляются вершинами графа, связи определяют зависимость одной команды от другой – в случае наличия зависимости, они не могут быть выполнены одновременно на разных процессорах. Эта задача является NP-полной [1, 2].

Один из подходов к решения задачи [3] содержит на первом этапе решения поиск всех максимально внутренне устойчивых подмножеств. От эффективности алгоритма поиска всех максимально внутренне устойчивых подмножеств, таким образом, напрямую зависит эффективность решения задачи вообще. В работе [3] для отыскания всех максимально внутренне устойчивых подмножеств использовался метод Магу [4]. Были проведены испытания, выявившие значительное падение скорости решения, начиная с 12 и более вершин при раскраске взвешенного графа [3]. С целью возможного улучшения эффективности решения задачи, в этой статье будет рассмотрен алгоритм Брона-Кербоша (метод ветвей и границ) [5] и его сравнение с методом Магу.

1. **Математическая постановка задачи.**

Имеется неориентированный связный взвешенный граф $G=(V,E)$, где V — множество вершин, E — множество ребер, $W(V_i)$ — вес i-й вершины. Необходимо раскрасить вершины графа таким образом, чтобы никакие две смежные вершины не были окрашены в один цвет, и при этом максимальная сумма весов вершин одного цвета стремилась к минимуму:

$$\max_{i\in(1..P)} \sum_{j\in B_i} W(v_j) \to \min \quad , \qquad (1.1)$$

где B_i — подмножество несмежных вершин графа, окрашенных в i-й цвет.

Формально:

$$\max T_j \to \min,$$

$$T_j = \sum_{i\in N_j} t_{i,j}$$

при условиях

$$t_{i,j} \ge 0; i = 1..m,\ j = 1..n, N_k \cap N_l = \varnothing; k,l \ne 1..n, k \ne l.\ \bigcup_{j=1}^{n} N_j = M \quad , \qquad (1.2)$$

где M — множество вершин, которые необходимо распределить по цветам;

N — количество цветов; $t_{i,j}$ — вес вершины i при цвете j.

Упомянутый во введении способ решения задачи разбивает ее на 3 этапа. Первые два этапа решают задачу поиска правильной раскраски графа: на первом ищутся все максимально внутренне устойчивые подмножества, на втором этапе выбираются кортежи T_e, длина которых равна хроматическому числу, а элементами являются максимально внутренне устойчивые подмножества, охватывающие все вершины (т.е. их объединение дает множество V). Второй этап может решаться с помощью метода Магу [4]. На третьем этапе l раз (l — число кортежей T_e) решается задача распределения программ по однородным вычислительным системам. Матрица загрузки приборов (процессоров) формируется следующим образом: строки соответствуют вершинам графа, столбцы — цветам раскраски. Если вершина $a_m \in C_l$, а C_l является элементом кортежа T_e, то на пересечении m-й строки и номера, под которым C_l стоит в кортеже T_e, ставится вес вершины $W(a_m)$. В противном случае ставится заведомо большее число («бесконечность»), чтобы вершина не могла быть назначена другому цвету.

2. Метод Магу. Этот метод основан на построении булевого уравнения, содержащего все вершины графа, и последующем сокращении слагаемых. Уравнение представляет собой произведение сумм смежных вершин. Формула упрощается по законам A&A=A и A+(A&B)=A. Вершины, отсутствующие в элементах получившегося многочлена, образуют максимально внутренне устойчивые подмножества.

Например, для графа (рис. 1) матрица смежности представлена в таблице 1.

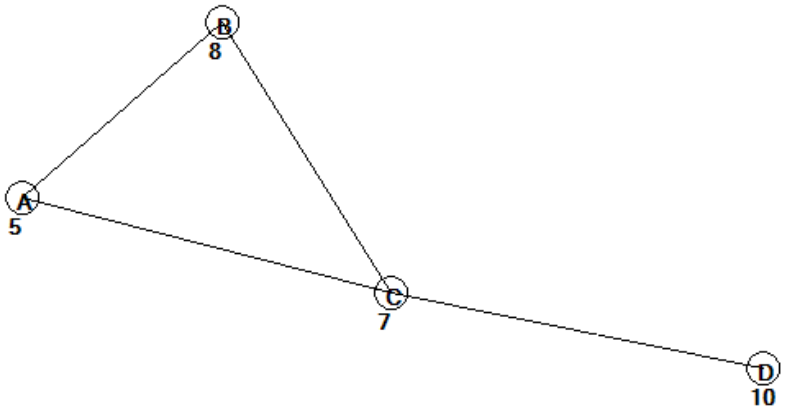


Рисунок 1. Граф

Таблица 1. Матрица смежности графа

	A	B	C	D
A	0	1	1	0
B	1	0	1	0
C	1	1	0	1
D	0	0	1	0

Уравнение, соответственно, будет иметь вид:

$$F_s = (\bar{a}+\bar{b})(\bar{a}+\bar{c})(\bar{b}+\bar{c})(\bar{c}+\bar{d}) = (\bar{a}+\bar{b}\bar{c})(\bar{c}+\bar{b}\bar{d}) = \bar{a}\bar{c}+\bar{b}\bar{c}+\bar{a}\bar{b}\bar{d}, \quad (2.1)$$

следовательно, максимально внутренне устойчивые подмножества:

{B,D}, {A,D}, {C}.

3. Алгоритм Брона-Кербоша. Алгоритм Брона-Кербоша – это, изначально, метод ветвей и границ для поиска всех клик графа. Напомним, что клика – это такое подмножество вершин графа, в котором любая пара вершин смежна, т.е. клика является противоположностью максимально внутренне устойчивому подмножеству. Поэтому алгоритм Брона-Кербоша очень легко модифицировать для поиска всех независимых множеств графа.

Алгоритм оперирует тремя множествами:

S_k – вершины формируемого независимого множества,

Q_k^+ – подмножество возможных вершин на включение в S_{k+1},

Q_k^- – подмножество вершин, которые использовались для расширения Sk.

На каждом шаге алгоритм пытается расширить множество Sk. Sk является максимально независимым множеством, если невозможно его дальнейшее расширение, т.е. когда $Q_k^+ = Ø$, при этом если $Q_k^- \neq Ø$, то множество S_k было расширено на некотором предыдущем этапе работы алгоритма и оно не является максимально независимым. Таким образом, необходимым и достаточным условием того, что S_k – максимально независимое множество, является выполнение равенства:

$$Q_k^+ = Q_k^- = Ø. \quad (3.1)$$

Условие:

$$\exists x \in Q_k^-, \ \textit{такая, что} \ \ \Gamma(x) \cap Q_k^+ = \varnothing, \quad (3.2)$$

является достаточным для осуществления шага возвращения. При возвращении происходит следующее: вершина x_{ih} удаляется из S_{k+1}, чтобы вернуться в S_k, удаляется из Q_k^+ и добавляется к старому множеству Q_k^- для формирования новых множеств Q_k^+ и Q_k^-.

4. Вычислительный эксперимент. Для определения какой алгоритм эффективнее справляется с 1-м этапом решения задачи поиска «минимаксной» раскраски, был поставлен вычислительный эксперимент на 100 случайно сгенерированных графах по 6, 12 и 14 вершин. В таблице 2 приведены средние значения времени решения всей задачи.

Таблица 2. Время работы алгоритмов.

Число вершин	Время работы с методом Магу, мс	Время работы с алгоритмом Брона-Кербоша, мс
6	1,010	1,170
12	519,08	148, 54
14	40940,303	4238,07

Таблица 3. Сравнение алгоритмов

Число вершин	Время работы алгоритма Магу, мс	Время работы алгоритма Брона-Кербошна, мс
5	11	20
15	3898	357
25	323,908	4,688
40	18510,403	39,94

Вывод.

Как видно, алгоритм Брона-Кербоша оказывается примерно в 3,5 раза эффективнее на 12-вершинных графах и почти в 10 раз эффективнее на 14-вершинных, т.е. сложность метода Магу, видимо, возрастает гораздо быстрее, чем алгоритма Брона-Кербоша. Чтобы точнее установить это свойство, алгоритмы были протестированы отдельно на 500 случайно сгенерированных графах. В связи со сложностью регистрации временных интервалов меньше одной миллисекунды (а именно столько алгоритмы работают на маленьких графах), для числа вершин 5 и 15 считалось общее время выполнения алгоритмов на всех 500 графах, а на 25 и 40 вершинах – среднее. Результаты приведены в таблице 3, из которой явно видно, что сложность метода Магу действительно растет гораздо быстрее.

В то же время, для совсем маленьких графов (5, 6 вершин) метод Магу оказывается эффективнее.

Литература:

1. Карп, Р. М. Сводимость комбинаторных проблем / Р. М. Карп // Кибернетический сборник, вып. 12. - Москва : Мир, 1975, С.16-38.

2. Гэри, М. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон. - Москва : Мир, 1982. - 416 с.

3. Кобак, В. Г. Алгоритм раскраски взвешенного графа / В. В. Букин, В. Г. Кобак // Известия СКНЦ ВШ. Технические науки. – 1998. – № 3(63). – С. 42-46.

4. Кофман, А. Введение в прикладную комбинаторику / А. Кофман. - Москва : Наука, 1975. - 480 с.

5. Кобак, В. Г. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций/ И. Ш. Кавтарадзе, В.В. Бормотов, С.А. Швидченко, В.Г. Кобак // СКФ МТУСИ «Инфоком-2014» - Ростов н/Д, СКФ МТУСИ, 2014. - 522с.

6. Кристофидес, Н. Теория графов. Алгоритмический подход / Н. Кристофидес. - Москва : Мир, 1988. - 432 с.

В.Г. Кобак, И.Ш. Кавтарадзе, С.А. Швидченко

СРАВНЕНИЕ РАЗЛИЧНЫХ МУТАЦИЙ ПРИ РЕШЕНИИ ЗАДАЧИ КОММИВОЯЖЕРА МОДЕЛЬЮ ГОЛДБЕРГА

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: Эволюционные вычисления, генетические алгоритмы, мутации, взвешенный полный граф, вычислительный эксперимент, среднее время выполнения.

Данная работа рассматривает решение одной из старейших задач (задачу коммивояжера) с помощью генетического алгоритма. Существенное отличие от других работ – использование различных видов мутаций, что приводит к интересным результатам.

V.G. Kobak, I.S. Kavtaradze, S.A. Shvidchenko

COMPARISON OF VARIOUS MUTATIONS AT THE SOLUTION OF THE TASK OF THE DIRECT-SALES REPRESENTATIVE GOLDBERG'S MODEL

Don state technical university, Rostov-on-Don, Russia

Keywords: evolutionary computation, genetic algorithms, mutation, weighted complete graph, numerical experiment, the average execution time.

This article examines a solution to one of the oldest problems (traveling salesman problem) using a genetic algorithm. The essential difference from the other works - use at different types of mutations that can lead to interesting results.

Введение. Задача о коммивояжёре – traveling salesman problem (TSP, ЗКВ) – является NP-сложной задачей дискретной оптимизации. На графах она формулируется следующим образом: требуется найти гамильтонов цикл наименьшей стоимости во взвешенном полном графе.

В последние годы интенсивно разрабатывается научное направление Natural Computing — «Природные вычисления», объединяющее математические методы, в которых заложены принципы природных механизмов принятия решений. Эти механизмы обеспечивают эффективную адаптацию флоры и фауны к окружающей среде на протяжении миллионов лет.

Генетические алгоритмы являются одним из видов эволюционных вычислений. Они применяются для поиска решений в задачах с большой комбинаторной сложностью, для которых трудно найти точное решение аналитическим путем. Принцип работы генетического алгоритма основан на теории эволюции Чарльза Дарвина. Основателем генетических алгоритмов считается Джон Холланд (John Holland), опубликовавший в 1975 году первую книгу в этой области исследований под названием «Адаптация в естественных и искусственных системах» («Adaptation in Natural and Articial Systems») [1].

Существует огромное разнообразие генетических алгоритмов:

- канонический генетический алгоритм появился в результате работ Холланда и его коллег. Формируем популяции, каждая из которых состоит из N хромосом с фиксированной разрядностью генов, далее создаем промежуточный массив, из которого случайным образом выбираются два родителя, производим одноточечный кроссинговер, и созданные два потомка мутируют с заданной вероятностью [2];
- модель Голденберга была впервые описана Д. Голденбергом на основе работ Д. Холланда. Вначале случайным образом генерируется популяция хромосом. Далее в качестве инструментов выделяются три вида операций: репродукция, скрещивание и мутация. Понятие репродукции связано с созданием копий родительских хромосом или обозначает процесс формирования новых особей, происходящих от конкретных родителей. Традиционно используется одноточечный кроссинговер, в котором две скрещивающиеся хромосомы разрезаются один раз в случайно выбранной точке, и производится обмен полученными частями;
- модель генитор (Genitor) - начале популяция инициализируется случайным образом, и ее особи оцениваются. Затем, также случайно, выбираются две особи, которые подвергаются скрещиванию, в результате которого получается только один потомок, который оценивается и занимает место менее приспособленной особи в популяции;
- гибридная модель ГА (Hybrid algorithms) сочетает в себе применение генетического алгоритма в союзе с другим классическим методами поиска, подходящими в контексте данной задачи.

Для исследования ЗКВ была выбрана модель Голденберга, подробно описанная в работе, при чем использовались только описанные ниже мутации [3,5].

Модифицированная модель Голденберга.

1. Формирование начальной популяции;

2. Определение вероятности мутации p_m;
3. Выбор точки отсчета особей: t=0;
4. Применяем к t- той особи популяции оператор мутации;
5. Вычисляем значение целевой функции для мутирующей t-ой особи и сравниваем его со значением целевой функции случайно выбранной особи из поколения, особь с наилучшем значением целевой функции добавляется в следующие поколение;
6. Устанавливаем t=t+1;
7. Определение особи с наилучшей приспособленностью (значением целевой функции) $f_{опт}$;
6. Если t = количеству особей в поколении, то проверяем сколько итераций алгоритма. $f_{опт}$ было неизменно. Если $f_{опт}$ было неизменным Nu итераций подряд, то конец работы, если меньше чем Nu, то переходим к шагу 3.

Мутация — случайное изменение одной или нескольких позиций в хромосоме. Оператор мутации (ОМ) помогает избежать «застревания» в ловушке локальных экстремумов и, следовательно, повышается возможность поиска с наибольшей точностью. Вероятность мутации p_m является фиксированным случайным числом на отрезке [0; 1].

Модифицированные виды мутаций:

– симметричный двухточечный ОМ сначала выбирает случайный ген в хромосоме, а далее обменивает местами гены, расположенные справа и слева от выбранного.

Например:

P:	1	2	|3	4	5	6	1	до ОМ
P':	1	4	|3	2	5	6	1	после ОМ

Симметричный двухточечный ОМ выполняется следующим образом:

1. В хромосоме P = (a_1,a_2,a_3,a_4 ... ,a_{n-1},a_n) случайным образом определяется позиция (например, a_3).
2. Гены, находящиеся справа и слева от выбранной позиции, переставляются, и формируется новая хромосома. P' = (a_1,a_4,a_3,a_2 ... ,a_{n-1},a_n).

– несимметричный двухточечный ОМ заключается в перестановке местами двух любых выбранных ген в хромосоме.

Например:

P:	1	|2	3	4	|5	6	до ОМ
P':	1	|5	3	4	|2	6	после ОМ

Несимметричный двухточечный ОМ выполняется следующим образом:

1. В хромосоме P = (a_1,a_2,a_3,... ,a_{n-2},a_{n-1},a_n) определяются случайным образом две позиции (например, a_2 и a_{n-1}).
2. Гены, соответствующие выбранным позициям, переставляются, и формируется новая хромосома. P' = (a_1, a_{n-1}, a_3,..., a_{n-2},a_2,a_n).

– четырехточечный ОМ.

Четырехточечный ОМ выполняется следующим образом:

1. В хромосоме P = (a_1,a_2,a_3,... ,a_{n-2},a_{n-1},a_n) определяются случайным образом две позиции (например, a_2 и a_{n-2}).
2. Гены, соответствующие выбранным позициям и стоящие справа от этих позиций, переставляются, и формируется новая хромосома. P' = (a_1, a_{n-2}, a_{n-1},..., a_2,a_3,a_n).

– несимметричный четырехточечный ОМ.

Несимметричный четырехточечный ОМ выполняется следующим образом:

1. В хромосоме P = (a_1,a_2,a_3,a_4,a_5,a_6,... ,a_{n-2},a_{n-1},a_n) случайным образом определяется одна позиция (например, a_4).
2. Гены, соответствующие выбранным позициям и стоящие справа от этих позиций, переставляются, и формируется новая хромосома. P' =(a_1,a_6,a_5,a_4,a_3,a_2,...,a_{n-2},a_{n-1}, a_n)

Для решения задачи коммивояжера в работе [4] в основном используются опера-торы кроссовера. В данной работе решение этой задачи предполагает использование только модифицированных операций мутации для симметричного графа. Аналитически определить какая из мутаций лучше практически невозможно, и потому был поставлен вычислительный эксперимент. Эксперимент проводился на графе описанном в [4] при различных весах (рис 1). А также на случайно сгенерированных графах, размерности 10,13,15,17,20,23,25,27,30.

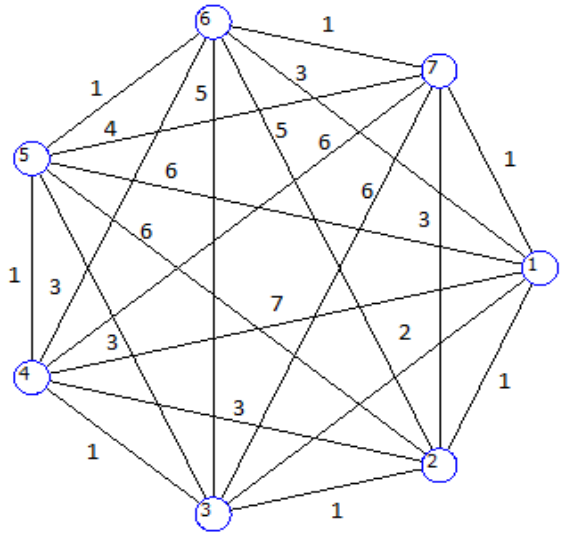


Рисунок 1. Взвешенный полный граф

Веса изменялись в пределах 1.7 случайным образом. Количество различных множеств весов равнялось 10. Сравнительные результаты тестирования модифицированной модели Голденберга в таблице 1, а также на рисунках 2-5.

Таблица 1. Результаты вычислительного эксперимента

граф	Симметричный двухточечный ОМ		Несимметричный двухточечный ОМ		Четырехточечный ОМ		Несимметричный четырехточечный ОМ	
	Ср. путь	Ср. время	Ср. путь	Ср. время	Ср. путь	Ср. время	Ср. путь	Ср. время
G7	14,70	0,66	14,50	0,30	14,50	1,40	14,40	0,56
G10	18,80	2,60	18,00	1,86	17,40	7,42	16,80	3,02
G13	24,00	5,80	21,80	3,05	21,20	2,61	21,60	5,90
G15	26,57	4,14	25,71	3,82	25,71	2,79	26,43	5,99
G17	30,83	9,37	28,17	6,01	28,33	4,05	28,17	7,63
G20	40,33	7,72	37,50	7,16	38,17	4,37	35,67	9,60
G23	45,00	10,33	41,33	7,71	41,00	3,27	41,50	5,76
G25	54,00	12,12	46,33	8,08	45,83	3,14	50,67	15,47
G27	56,80	8,21	50,00	13,59	50,20	3,41	50,00	12,13
G30	60,40	15,27	56,20	5,81	56,80	3,52	58,60	8,78

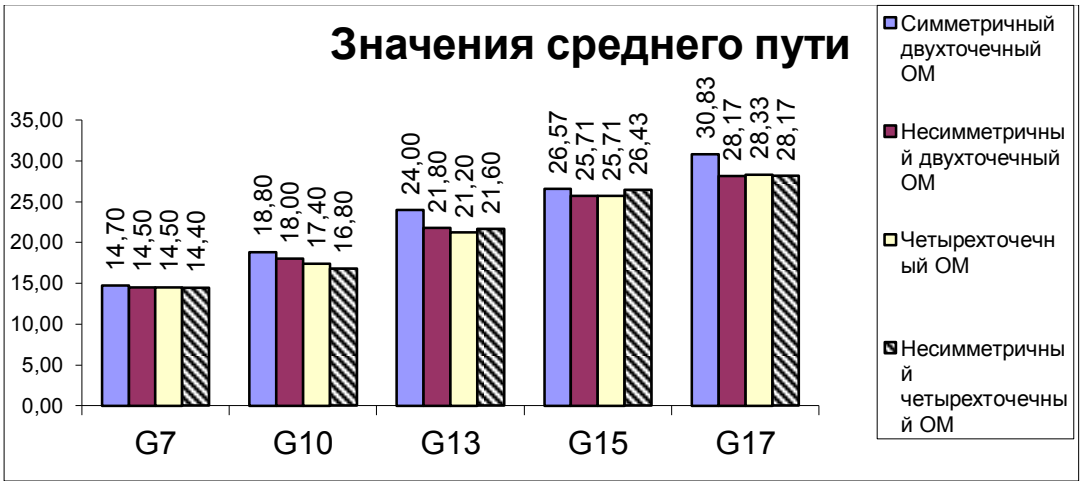


Рисунок 2. Значения среднего пути в графах с размерностями: 7,10,15,17

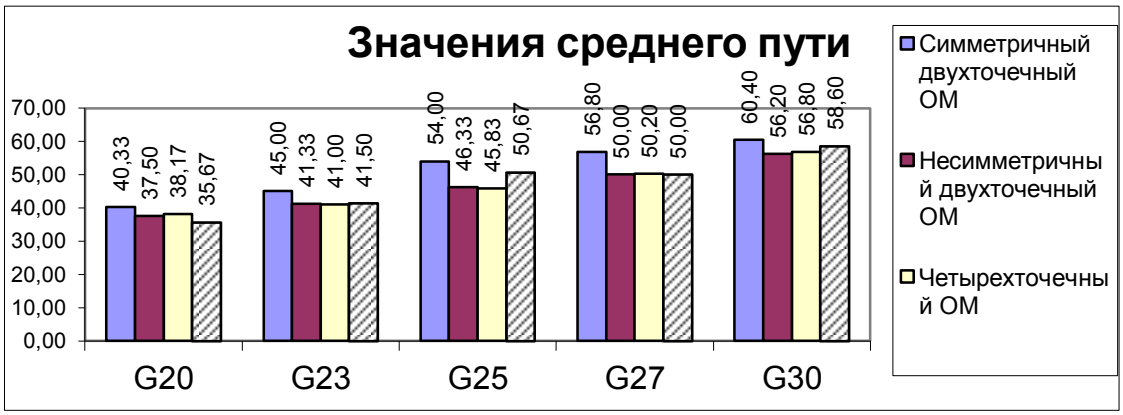


Рисунок 3. Значения среднего пути в графах с размерностями: 20,23,25,27,30

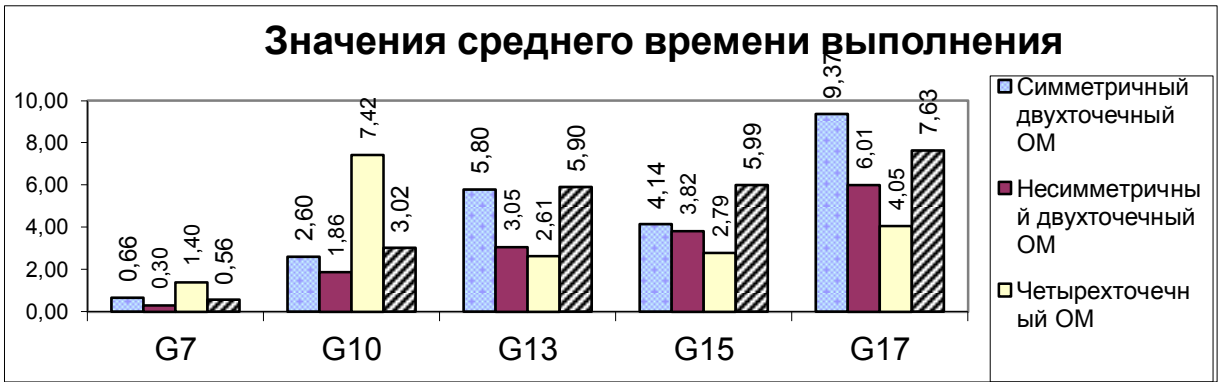


Рисунок 4. Значения среднего времени выполнения в графах с размерностями: 7,10,15,17

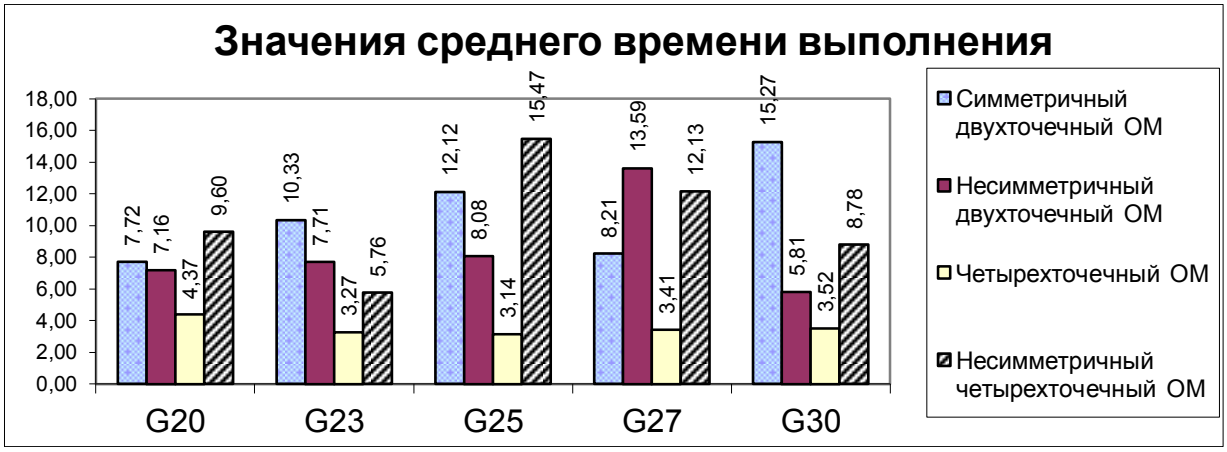


Рисунок 5. Значения среднего времени выполнения в графах с размерностями: 20,23,25,27,30

Вывод.

По результатам численных экспериментов можно сделать вывод, что наилучшее значение пути было получено при помощи модифицированной модели Голденберга с использованием четырехточечного ОМ и несимметричного двухточечного ОМ. Но время работы четырехточечного ОМ меньше почти в 2 раза. Значение среднего пути полученного при использовании несимметричного четырехточечного ОМ почти совпадает со значением пути найденного при помощи несимметричного двухточечного ОМ, но время его работы почти в 1,5 раза выше. Худшие результаты были получены с помощью симметричного двухточечного ОМ.

Литература:

1. Гладков Л. А., Курейчик В. В., Курейчик В. М. Генетические алгоритмы: Учебное пособие. — М: Физматлит, 2006.

2. Панченко Т.В. Генетические алгоритмы.: Учебное пособие - «Астраханский университет», 2007.

3. Титов Д.В., Кобак В.Г. Исследование способа формирования элитной особи генетического алгоритма для однородных систем. Математические методы в технике и технологиях - ММТТ-22: сб. тр. XXII Междунар. науч. конф. и IV Междунар. науч. - метод. симп. / ДГТУ. – Ростов н/Д, 2009.

4. Емельянов В.В., Курейчик В.М., Курейчик В.В. Теория и практика эволюционного моделирования. – М.: Физматлит, 2003.

5. Кобак, В. Г. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций/ И. Ш. Кавтарадзе, В.В. Бормотов, С.А. Швидченко, В.Г. Кобак // СКФ МТУСИ «Инфоком-2014» - Ростов н/Д, СКФ МТУСИ, 2014. - 522с.

***В.Г. Кобак, *Н.И. Троцюк, А.Г. Жуковский**

СРАВНЕНИЕ РАЗЛИЧНЫХ ПОДХОДОВ ПРИ ФОРМИРОВАНИИ ПОКОЛЕНИЯ В МОДЕЛИ ГОЛДБЕРГА

*Донской государственный технический университет, г. Ростов-на-Дону, Россия
Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: генетические алгоритмы, модель Голдберга, NP-полные задачи, поколенческая стратегия, теория расписаний.

В классических генетических алгоритмах используется концепция, предполагающая, что количество особей в поколении не изменяется. Рассмотрен подход, который позволяет повысить эффективность работы стандартной модели Голдберга за счет изменения количества особей в поколении. Представлен сравнительный анализ эффективности классической модели Голдберга и ее модификаций, использующих различные варианты поколенческой стратегии, для решения однородной минимаксной задачи теории расписаний, относящейся к классу NP-полных задач.

***V.G. Kobak, N.I. Trotsyuk, A.G. Zhukovskiy**

COMPARISON OF DIFFERENT APPROACHES AT THE FORMATION OF GENERATION IN THE GOLDBERG MODEL

*Don state technical university, Rostov-on-Don, Russia
North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: genetic algorithms, the model of Goldberg, NP-complete problems, generational strategy, scheduling theory.

In the classical genetic algorithm uses the concept, which assumes that the number of indi-viduals in a generation does not change. An approach that allows you to improve the efficiency of the standard model of Goldberg due to changes in the number of individuals in a generation was examined. The comparative analysis of the effectiveness of the classical model of Goldberg and its modifications using various options generational strategies for solving a homogeneous minimax scheduling problems related to the class of NP-complete problems was submitted.

Введение. При решении ряда задач в теории расписаний требуется найти оптимальное (субоптимальное) решение по одному из выбранных критериев.

В данной работе рассмотрена однородная минимаксная задача, принадлежащая к классу NP-полных задач. Для ее решения существуют различные алгоритмы – списочные, эволюционные и точные, основанные на идее метода ветвей и границ. Получение точного решения возможно только для малого количества заданий и приборов, а при большом количестве использование

данного метода крайне затруднительно. Поэтому большое значение приобретает нахождение субоптимальных решений, которые получаются с помощью различных генетических моделей, в том числе и модели Голдберга. Модель Голдберга отличается от классической модели – модели Холланда, тем, что использует турнирный отбор особей в новое поколение, который улучшает результаты алгоритма. Турнирный отбор может быть описан следующим образом: лучший потомок, полученный при кроссовере, сравнивается с особями в поколении, и если существует особь, значение которой хуже, то потомок занимает ее место [3,4,5]. Если же такой особи нет, то потомок уничтожается. Преимуществом данной стратегии является то, что она не требует дополнительных вычислений и упорядочивания особей в популяции по возрастанию приспособленности. Также, на мой взгляд, такой вариант селекции ближе к реальности, т.к. успешность той или иной особи во многом определяется ее окружением, насколько оно лучше или хуже ее.

1. Постановка задачи.

Имеется неориентированный связный взвешенный граф $G=(V,E)$, где V — множество вершин, E — множество ребер, $W(V_i)$ — вес i-й вершины. Необходимо раскрасить вершины графа таким образом, чтобы никакие две смежные вершины не были окрашены в один цвет, и при этом максимальная сумма весов вершин одного цвета стремилась к минимуму:

$$\max_{i\in(1..P)} \sum_{j\in B_i} W(v_j) \to \min \quad , \qquad (1.1)$$

где B_i — подмножество несмежных вершин графа, окрашенных в i-й цвет.

Формально:

$$\max T_j \to \min,$$

$$T_j = \sum_{i\in N_j} t_{i,j}$$

при условиях

$$t_{i,j} \ge 0; i = 1..m,\ j = 1..n, N_k \cap N_l = \varnothing; k,l \ne 1..n, k \ne l. \bigcup_{j=1}^{n} N_j = M \quad , \qquad (1.2)$$

где M — множество вершин, которые необходимо распределить по цветам;

N — количество цветов; $t_{i,j}$ — вес вершины i при цвете j.

Упомянутый во введении способ решения задачи разбивает ее на 3 этапа. Первые два этапа решают задачу поиска правильной раскраски графа: на первом ищутся все максимально внутренне устойчивые подмножества, на втором этапе выбираются кортежи T_e, длина которых равна хроматическому числу, а элементами являются максимально внутренне устойчивые подмножества, охватывающие все вершины (т.е. их объединение дает множество V). Второй этап может решаться с помощью метода Магу [4]. На третьем этапе l раз (l — число кортежей T_e) решается задача распределения программ по однородным вычислительным системам. Матрица загрузки приборов (процессоров) формируется следующим образом: строки соответствуют вершинам графа, столбцы — цветам раскраски. Если вершина $a_m \in C_l$, а C_l является элементом кортежа T_e, то на пересечении m-й строки и номера, под которым C_l стоит в кортеже T_e, ставится вес вершины $W(a_m)$. В противном случае ставится заведомо большее число («бесконечность»), чтобы вершина не могла быть назначена другому цвету.

2. Решение. Используемые генетические алгоритмы (ГА):

Алгоритм 1 – модель Голдберга:

Шаг 1. Формируется начальное поколение, состоящее из заданного числа особей.

Шаг 2. Отбор особей и применение ГА операторов кроссовера и мутации с заданной вероятностью для создания нового поколения.

Шаг 3. Проверка условия останова, которая обычно заключается в неизменности лучшего решения в течение заданного числа поколений. Если проверка прошла не успешно, то переход на Шаг 2.

Шаг 4. Лучшая особь выбирается как найденное решение.

Из [2] известно, что иногда полезно варьировать размер популяции, то есть количество особей может быть не только постоянным, но и переменным. Применительно к рассматриваемой

задаче в модификациях модели Голдберга «Алгоритм 2» и «Алгоритм 3» используется поколенческая стратегия отбора особей в новое поколение. В данной работе были использованы следующие схемы:

Для модификации «Алгоритм 2»:

1. В первом поколении задавалось количество особей k;
2. Во втором поколении генерировалось в два раза больше особей, чем в первом поколении;
3. В третьем поколении происходил возврат к исходному количеству особей k.

Для модификации «Алгоритм 3»:

1. В первом поколении задавалось количество особей k;
2. Во втором поколении генерировалось в два раза больше особей, чем в первом поколении;
3. В третьем поколении генерировалось в три раза больше особей, чем в первом поколении;
4. В четвертом поколении происходил возврат к исходному количеству особей k.

При усечении поколения оставались лучшие k особей.

Процесс продолжался до тех пор, пока значение критерия не повторится заданное количество раз.

Так как аналитически доказать, какой из алгоритмов в среднем лучше практически невозможно, то для оценки алгоритмов был проведен вычислительный эксперимент для различного количества приборов. Количество разных матриц для получения средних значений было выбрано равным 100. Диапазон работ один из самых используемых – 20-30. Результаты эксперимента приведены в Таблице 1.

Таблица 1 - Результаты эксперимента

N	M	Алгоритм 1		Алгоритм 2		Алгоритм 3	
		T_{max} среднее	t (c)	T_{max} среднее	t (c)	T_{max} среднее	t (c)
2	23	284,68	0,648	284,11	0,878	283,79	1,108
	71	872,48	0,856	871,56	1,176	871,20	1,565
	131	1606,01	1,024	1605,52	1,467	1605,04	2,003
3	23	194,12	0,739	193,12	0,956	193,34	1,244
	71	587,22	0,976	586,65	1,359	585,86	1,765
	131	1075,95	1,330	1075,75	1,857	1057,06	2,526
4	23	148,24	0,812	148,04	1,125	148,17	1,443
	71	445,78	1,119	445,19	1,539	445,20	2,004
	131	814,68	1,708	813,08	2,309	812,18	3,188
…							
7	131	476,18	2,461	474,68	2,938	472,71	4,636
	231	831,75	3,316	826,82	4,858	825,53	6,474
11	131	318,00	3,056	317,75	4,084	315,27	5,711
	231	553,13	3,972	546,75	5,993	545,69	8,706

Вывод.

По результатам проведенных экспериментов можно сделать вывод, что с увеличением количества процессоров и количества работ предложенная модификация модели Голдберга «Алгоритм 3» дает все более лучшие результаты с точки зрения минимаксного критерия чем предложенная модификация «Алгоритм 2» и классическая модель Голдберга, но тратит больше времени на поиск результата. Самым быстрым алгоритмом является классическая модель, но ее результаты хуже, чем у модификаций. Модификация «Алгоритм 2» показывает средние результаты и по времени выполнения, и по минимаксному критерию.

Литература:

1. Кобак В.Г., Троцюк Н.И. Сравнительный анализ алгоритмов: генетического с элитой и Крона с генетическим начальным распределением (статья) - Математические методы в технике и технологиях - ММТТ-26: сб. тр. Междунар. науч. конф. / СГТУ. - Саратов, 2013. - Ч.2.

2. Корнеев В.В., Гареев А.Ф., Васютин С.В., Райх В.В. Базы данных. Интеллектуальная обработка информации. – М.: «Нолидж», 2000.

3. Кобак В.Г., Титов Д.В. Исследование турнирного отбора в генетическом алгоритме для решения однородной минимаксной задачи (статья) – Математические методы в технике и технологиях - ММТТ-21: сб. тр. Междунар. науч. конф. - Саратов, 2008. – Т.5

4. Курейчик В.М. Генетические алгоритмы и их применение. – Таганрог:Изд-во ТРТУ, издание второе, дополненное, 2002.

5. Кобак, В. Г. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций/ И. Ш. Кавтарадзе, В.В. Бормотов, С.А. Швидченко, В.Г. Кобак // СКФ МТУСИ «Инфоком-2014» - Ростов н/Д, СКФ МТУСИ, 2014. - 522с.

В.А. Погорелов, А.О. Семилеткин, *С. А. Швидченко

РЕШЕНИЕ ЗАДАЧИ ИДЕНТИФИКАЦИИ НА ОСНОВЕ НЕГАУССОВСКОЙ АППРОКСИМАЦИИ АПОСТЕРИОРНОЙ ПЛОТНОСТИ ВЕРОЯТНОСТИ

ФГУП «Ростовский-на-Дону НИИ радиосвязи» ФНПЦ, г. Ростов-на-Дону, Россия
**Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: распределение Пирсона, идентификация, стохастическая фильтрация.

Рассмотрен метод, позволяющий осуществить идентификацию параметров вектора состояния динамической системы (ДС) в условиях действия помех. В качестве минимизируемого функционала выбран функционал, нелинейно зависящий от апостериорной плотности вероятности стохастической модели состояния ДС.

V.A. Pogorelov, A.O. Semiletkin, *S.A. Shvidchenko

SOLVING THE IDENTIFICATION TASK ON THE BASIS OF NON-GAUSSIAN APPROXIMATION OF A POSTERIORI PROBABILITY DENSITY

Federal State Unitarian Enterprise Scientific Research Institute of Radio Communication – Federal Scientific Production Center
*Don state technical university, Rostov-on-Don, Russia

Keywords: Pearson distribution, identification, stochastic filtering.

Reviewed herein is a technique that allows to identify the parameters of the vector of state of a dynamic system (DS) in a noisy environment. As the minimized functional a functional with a non-linear dependence on the a posteriori probability density of the stochastic model of the DS state has been selected.

Введение. Эффективность работы ДС во многом зависит от адекватности ее модели реальным условиям функционирования [1]. Очевидно, что синтезировать модель, абсолютно точно описывающую динамику ДС, в силу априорной неопределенности начальных условий и возмущающих факторов практически не возможно. В некоторой степени проблему решает использование в ДС робастных алгоритмов, которые позволяют гарантировать определенный уровень точности управления динамической системой в условиях отсутствия точной априорной информации о параметрах модели ДС [2, 3]. Однако грубость робастных алгоритмов не позволяет обеспечить главного требования, предъявляемого к ДС − обеспечение максимальной информацией потребителей в условиях действия внешних и внутренних возмущений различной физической природы.

В связи с этим более релевантным является использование в ДС современных методов стохастической фильтрации [4-7]. Применение этих методов позволяет получить оценки параметров модели ДС с требуемой точностью, обеспечивая при этом продолжительную автономность ее функционирования. На сегодняшний день существенным недостатком, ограничивающим область практического применения методов стохастической фильтрации, является нерешенная окончательно проблема их применения в случае отсутствия точной априорной информации о параметрах модели ДС. Вместе с тем, в практических приложениях часто отсутствует точная информация о параметрах ДС или они существенно меняются в процессе ее функционирования [1, 9]. Вследствие этого алгоритмы фильтрации становятся неустойчивыми, возникает рост энтропии и необходимость использования дополнительной внешней информации [4, 9, 12]. В определенной мере уменьшить погрешности оценивания, обусловленные дрейфом параметров, можно, применив в ДС алгоритмы идентификации на основе теории оценивания (АИТО) [7]. Эти методы позволяют оценивать как параметры модели, так и требуемые фазовые переменные ДС. Несмотря на то, что использование АИТО обеспечивает устойчивость процедуры оценивания, их использование для многосвязанных объектов в общем случае невозможно [7].

В связи с эти целью статьи является повышение точности оценивания состояния ДС в условиях действия возмущающих факторов различной физической природы и отсутствия точной информации о параметрах стохастической модели ДС.

1. Постановка задачи

Пусть объект описывается нелинейным дифференциальным уравнением в симметризованной форме

$$\dot{Y}(t) = f(Y,t) + Q(Y,t) + f_0(Y,t)V_t, \tag{1.1}$$

где $Y(t)$ – фазовая переменная;

$f(Y,t), f_0(Y,t)$ – известные нелинейные функции, удовлетворяющие условию Липшца $\forall Y,t$ и дифференцируемые на интервале времени $(0;t)$ N раз;

$Q(Y,t)$ – неизвестная функция, определяемая физическими свойствами объекта и подлежащая идентификации по показаниям измерителя;

V_t – белый гауссовский шум с нулевым средним и интенсивностью D_v.

Уравнение наблюдателя за вектором состояния (1) имеет вид

$$Z(t) = h(Y,t) + W_t, \tag{1.2}$$

где $Z(t)$ – выходной сигнал наблюдателя,

$h(Y,t)$ – известная нелинейная функция,

W_t – гауссовский шум с нулевым средним и известной интенсивностью D_W.

Апостериорная плотность вероятности ρ_z такого процесса, удовлетворяющего приведенным выше условиям, описывается интегро-дифференциальным уравнением с частными производными Стратоновича [8]:

$$\frac{\partial \rho_z}{\partial t} = L\{q,b,\rho_z\} + \frac{\partial}{\partial Y}[Q\rho_z] + [R - R_0]\rho_z, \tag{1.3}$$

где

$$L\{q,b,\rho_z\} = -\frac{\partial}{\partial Y}[q(Y,t)\rho_z] + \frac{1}{2}\frac{\partial^2}{\partial Y^2}[b(Y,t)\rho_z],$$

$$q(Y,t) = f_1(Y,t) + \frac{1}{2}\frac{\partial}{\partial Y} f_0^2(Y,t), \qquad b(Y,t) = f_0^2(Y,t),$$

$$R = R(Y,t) = -\frac{1}{2}[Z - h(Y,t)]^T D_W^{-1}[Z - h(Y,t)], \quad R_0 = \int_{-\infty}^{\infty} R(Y,t)\rho_z(Y,t)dY.$$

Поставленную задачу идентификации априорно неизвестной функции Q при наличии текущих наблюдений за состоянием объекта будем рассматривать далее как задачу поиска функции Q в реальном масштабе времени. Иными словами, задачу синтеза функции Q сформулируем далее как задачу синтеза такой Q, которая доставляла бы минимум функционалу J, характеризующему качество функционирования стохастического объекта (1) и зависящему в общем случае от плотности ρ_z:

$$J = -\int_T \int_{Y_*} \mathbf{\Phi}[\rho_z(Y, Q, t / Z(t))] dY dt \quad , \tag{1.4}$$

где $Y_* -$ область существования Y, в которой ищется оптимум;

$\mathbf{\Phi}[\rho_z(Y, Q, t / Z(t))]$ – заданная нелинейная аналитическая функция;

T – интервал времени функционирования системы.

В большинстве практических случаев функцию $\mathbf{\Phi}$ можно представить в виде двух независимых составляющих $\mathbf{\Phi}[\rho_z(Y, Q, t / Z(t))] = \mathbf{\Phi}_1[\rho_z] + \mathbf{\Phi}_2[Q]$. Учитывая тот факт, что исчерпывающей характеристикой случайного процесса является его апостериорная плотность вероятности (АПВ), в качестве $\mathbf{\Phi}_1$ целесообразно выбрать функционалы Фишера, Шеннона, Кульбака и др. Эти функционалы позволяют получить потенциально более точные оценки Y вследствие оптимизации всего процесса $Y(t)$, а не его локальной характеристики – дисперсии, как в традиционном среднеквадратическом критерии.

Отсутствие информации о функции *Q* увеличивает энтропию состояния системы. Поэтому процесс её идентификации должен, прежде всего, осуществляться с целью минимизации неопределенности (1.1), и при этом, требовать минимума энергетических затрат, т. е. минимума квадратичной формы Q^2.

Резюмируя выше изложенное можно сделать вывод, что для решения задачи параметрической идентификации объекта (1.1) необходимо минимизировать функционал (1.4) по Q.

2. Решение задачи совместного управления и идентификации.

Анализ современных методов синтеза ДС показывает, что в большинстве практических случаев входящие в (1.1) нелинейные функции, в конечном итоге, аппроксимируются различными функциональными рядами Тейлора, Фурье, сплайнами, интерполяционными многочленами Лагранжа и т.д. [6]. Учитывая это, представим правую часть (1.1) в следующем виде:

$$\dot{Y} = \sum_{i=0}^{N_0} f_{1_i}(t) Y^i + \sum_{i=0}^{N_1} Q_i Y^i + \left[\sum_{i=0}^{N_2} f_{0_i}(t) Y^i \right] V_t \quad , \tag{2.1}$$

где $N_i, i = \overline{0,2}$ – степень ряда, определяемая требуемой точностью аппроксимации функций,

f_{1_i}, Q_i, f_{0_i} – коэффициенты разложения в соответствующий ряд.

Так как в общем случае не существует аналитического решения уравнения (1.3), то для возможности дальнейшего поиска функции Q будем использовать параметрическую аппроксимацию ρ_z. Для этого сформируем систему дифференциальных уравнений, определяющих искомую плотность распределения.

Для определения апостериорных моментов m_j подставим (2.1) в (1.3) и воспользуемся методикой, разработанной в [9], получим дифференциальное уравнение j-го момента АПВ в следующем виде:

$$\dot{m}_j = j\sum_{i=0}^{N_0}\left[f_{1_i} + \frac{D_v}{2}\sum_{k=0}^{i} f_{0k} f_{0(i-k+1)}(i+1-k)\right]m_{i+j-1} + \frac{D_v}{2} j(j-1)\sum_{i=0}^{N_2}\left[\sum_{k=0}^{i} f_{0k} f_{0(i-k)}\right]m_{i+j-2} + \\ + \sum_{i=1}^{N_0} h_i\left(m_{i+j} - m_i m_j\right) + j\sum_{i=0}^{N_1} Q_i m_{i+j-1}, \tag{2.2}$$

где $j = 1,2,...;\ m_0 = 1$.

Анализ (2.2) показывает, что полученная система апостериорных моментов не замкнута. Будем считать, что из анализа процессов, протекающих в объекте управления, класс аппроксимирующей плотности известен и является распределением Пирсона [10]

$$\frac{\partial \rho_z}{\partial Y} = \frac{Y + a_0}{b_2 Y^2 + b_1 Y + b_0}\rho_z(Y),$$

где a_0, b_0, b_1, b_2 – параметры распределения, однозначно определяемые первыми четырьмя центральными, а, следовательно, и начальными моментами $m_j, j = \overline{1,4}$ [10].

Высказанное предположение о принадлежности ρ_Z к классу распределений Пирсона, позволяет преобразовать бесконечную систему в замкнутую систему уравнений с помощью рекурсии, связывающей первые четыре момента распределения с высшими моментами распределения [10]

$$m_{j+1} = -\frac{m_j\left(b_1(j+1) + a_0\right) + b_0 n m_{j-1}}{b_2(j+2) + 1}. \tag{2.3}$$

Воспользовавшись рекурсией (2.3) получим замкнутую систему уравнений моментов, которую представим в векторном виде

$$\dot{M} = G(M, F_1, F_0) + N(M)Q, \tag{2.4}$$

где $M = |m_1 \ \ ... \ \ m_l|^T$, $F_1 = |f_{1_0} \ \ \cdots \ \ f_{1_N}|$, $F_0 = |f_{0_0} \ \ \cdots \ \ f_{0_N}|$, $G(M, F_1, F_0)$ – известная нелинейная вектор-функция компоненты, которой определяются из (2.5), $N(M) = |im_{i+j-1}|\left(i = \overline{1,l};\ j = \overline{0,N}\right)$ – матрица размерности $l \times (N+1)$.

Для синтеза Q воспользуемся принципом максимума Понтрягина, для чего запишем соответствующий гамильтониан в виде [11]

$$H(M, P, t) = -\int_{Y*}\left[\Phi_1\left[\rho_Z(Y, M, t)\right] + \Phi_2[Q]\right]dY + \lambda^T\left[G(M, F_1, F_0) + N(M)Q\right] \tag{2.6}$$

где λ – вектор сопряженных переменных.

Компоненты вектора Q, определенные из условия стационарности гамильтониана, в случае использования квадратичных функций $Q^T k_Q Q$ имеют вид

$$Q = -\left(\int_{Y*}\left(k_Q^T + k_Q\right)dY\right)^{-1} N^T\lambda, \tag{2.7}$$

где k_Q – известные матрицы, выбранные исходя из конструктивных особенностей тракта управления.

Окончательное решение поставленной проблемы сводится в дальнейшем к решению двухточечной краевой задачи (ДТКЗ), система канонических уравнений которой определяется уравнением

$$\dot{M} = G(M, F_1, F_0) - N(M)Q, \tag{2.8}$$

и, сопряженным к нему

$$\dot{\lambda}(t) = -\left[\frac{\partial}{\partial M}\int_{Y*}\mathbf{\Phi}_1\left[\rho_z(Y,M,t)\right]dY\right]^T - \left[\frac{\partial G(M,F_1,F_0)}{\partial M} + \frac{\partial N(M)}{\partial M}Q\right]^T\lambda, \quad (2.9)$$

при краевых условиях $M(t_0) = M_0,\ \lambda(t_k) = 0$.

Решение сопряженной системы (2.7), (2.8) в бортовых цифровых вычислительных машинах с современным быстродействием оказывается трудно реализуемой задачей. Поэтому, с целью возможности идентификации параметров вектора состояния объекта в реальном масштабе времени, используем далее методику синтеза приближенного решения ДТКЗ на основе метода инвариантного погружения [5], позволяющего сформировать приближенное значение вектора состояния $\tilde{M}$ как систему уравнений, имеющую в данном случае вид

$$\dot{\tilde{M}} = G(\tilde{M},F_1,F_0) - D\left[\frac{\partial}{\partial\tilde{M}}\int_{Y*}\mathbf{\Phi}_1\left[\rho_z(Y,\tilde{M},t)\right]dY\right]^T, \quad (2.10)$$

$$\dot{D} = 2\left[\frac{\partial G}{\partial\tilde{M}} + \frac{\partial N}{\partial\tilde{M}}Q(\tilde{M},0) + N(\tilde{M})\frac{\partial Q(\tilde{M},0)}{\partial\lambda}\right]D +$$

$$+ D\left[\frac{\partial G}{\partial\tilde{M}} + \frac{\partial N}{\partial\tilde{M}}Q(\tilde{M},0)\right] - N(\tilde{M})\frac{\partial Q(\tilde{M},0)}{\partial\lambda} - 2D\left[\frac{\partial}{\partial\tilde{M}}\left[\frac{\partial}{\partial\tilde{M}}\int_{Y*}\mathbf{\Phi}_1\left[\rho_z(Y,\tilde{M},t)\right]dY\right]^T\right]D,$$

где матрица D играет роль весовой матрицы при отклонении оптимального вектора от его аппроксимации [5]. Значение матрицы $D(t_0)$ определяется экспериментальным путем, исходя из требуемой скорости сходимости решения при обеспечении устойчивости системы нелинейных дифференциальных уравнений.

Для оценки точности и вычислительной эффективности разработанного подхода было проведено численное моделирование системы (2.10) при $D_n = 1{,}7$, $Y(0) = 0$, $Y_* = [-2.1;3.5]$, $T = [0;1000]$ с, реализованного для 40 стохастических траекторий движения объекта. Интегрирование уравнений осуществлялось методом Рунге-Кутты четвертого порядка с шагом 0,01 с. Оценка точности управления осуществлялась путем усреднения по ансамблю реализаций среднемодульных отклонений отдельно взятых траекторий движения от границы интервала Y_* в течение времени T. По окончании моделирования было установлено, что точность оценивания увеличилась на 40 % по сравнению с традиционным методом, а объем вычислительных затрат увеличился только на 10%.

Выводы.

Разработанный метод идентификации параметров стохастической модели состояния ДС позволяет в условиях действия возмущающих факторов повысить точность функционирования ДС (в условиях примера на 40 %). При этом он не требует существенного увеличения объема вычислительных затрат по сравнению с традиционными методами [7], а, следовательно, его можно легко реализовать в вычислителях с современным быстродействием.

Полученный метод может найти применение в системах радиолокации, навигации, связи и управления динамическими системами самого широкого назначения.

Литература:

1. Информационные технологии в радиотехнических системах / Под ред. И. Б. Федорова. М.: Изд. МГТУ им. Н. Э. Баумана. 2003. 672 с.

2. Никифоров В. О. Адаптивное и робастное управление с компенсацией возмущений. СПб: Наука. 2003.

3. Небылов А. В. Гарантирование точности управления. М.: Наука. 1998.

4. Тертычный-Даури В. Ю. Стохастическая механика. М.: Факториал Пресс. 2001.

5. Хуторцев В. В., Соколов С. В., Шевчук П. С. Современные принципы управления и фильтрации в стохастических системах. М.: Радио и связь. 2001.

6. Пугачев В. С., Синицын И. Н. Теория стохастических систем. М.: Логос. 2004. 1000 с.

7. Синицын И. Н. Фильтры Калмана и Пугачева. М.: Логос. 2006. 640 с.

8. Стратонович Р. Л. Условные Марковские процессы и их применение к теории оптимального управления. М.: Изд. МГУ. 1966. 350 с.

9. Тихонов В. И. Марковские процессы. М.: Сов. радио. 1977. 300 с.

10.Тихонов В. И. Статистическая радиотехника. М.: Радио и связь. 1982. 2470 с.

11. Разоренов Г. Н., Бахрамов Э. А., Титов Ю. Ф. Системы управления летательными аппаратами. М.: Машиностроение. 2003. 582 с.

12. Погорелов В.А., Митькин А.С., Швидченко С.А. Управление объектом с параметрически неопределенной структурой вектора состояния. Научно-технический журнал. Труды рост. гос. унив. путей сообщения. № 4(25) 2013г.

***А.В. Елисеев, А.Г. Жуковский, *С.Н. Овсянников**

ОБОСНОВАНИЕ КРИТЕРИЯ ОБНАРУЖЕНИЯ МАНЕВРА В ЗАДАЧЕ ДИНАМИЧЕСКОЙ ФИЛЬТРАЦИИ ИНФОРМАЦИОННОГО ПРОЦЕССА

*Донской государственный технический университет, г. Ростов-на-Дону, Россия
Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: динамическая фильтрация, фильтр Калмана, критерий обнаружения маневра, имитационное моделирование.

Рассмотрена задача обоснования параметров критерия обнаружения маневра в задаче синтеза алгоритма адаптивной фильтрации. При этом под маневром понимается значительное изменение динамики информационного процесса, сопровождаемое изменением его математической модели. Проведен краткий анализ известных способов преодоления расходимости фильтра Калмана. Приведена математическая постановка задачи. Формализован критерий обнаружения маневра. Проведено имитационное моделирование, позволившее построить графики зависимостей показателей эффективности функционирования радиотехнической системы от параметров критерия обнаружения. Проведен краткий анализ результатов моделирования.

***A.V. Eliseev, A.G. Zhukovskiy, *S.N. Ovsyannikov**

RATIONALE DETECTION CRITERIA MANEUVER IN THE PROBLEM DYNAMIC FILTERING OF INFORMATION PROCESSES

*Don state technical university, Rostov-on-Don, Russia
North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: dynamic filtering, Kalman filter, the criterion of detection maneuver simulation.

The problem of justification test for detecting parameters of maneuver in the problem of synthesis of adaptive filtering algorithm. In this maneuver is meant by a significant change in the dynamics of the information process, followed by a change of its mathematical model. The brief analysis of the known methods to overcome the divergence of the Kalman filter. The mathematical formulation of the problem. Formal criteria detection maneuver. A simulation that allowed plotted the performance within the electronic system on the parameters of the detection criterion. The brief analysis of simulation results.

Введение. Известно [1], что в радиотехнических системах (РТС) различного назначения для оценивания параметров динамических информационных процессов широко используется фильтр Калмана и его модификации [2–5].

Наряду с такими достоинствами фильтра Калмана как использование для формирования оценки нарастающего объема измерений, а также учет динамики информационного процесса, ему свойственны и недостатки, одним из которых является склонность фильтра к расходимости. Расходимость приводит к значительному увеличению погрешности оценивания по отношению к прогнозируемой, характеризуемой ковариационной матрицей ошибок фильтрации. Одной из причин расходимости является неадекватность используемой в фильтре математической модели реальному информационному процессу. Подобная ситуация наиболее часто возникает при оценивании параметров положения и движения маневрирующих объектов, например, летательных аппаратов различного назначения. Для недопущения расходимости оценки, обусловленной неадекватностью математической модели исследуемого процесса, используются различные модификации алгоритма фильтра Калмана, которые условно можно разделить на три группы [1]: алгоритмы без обнаружителя маневра [6; 7], требующие знания статистических характеристик маневра цели; алгоритмы с обнаружителем маневра, предусматривающие как минимум два фильтра, один из которых настроен на маневр известного типа [8], разновидностью данных алгоритмов являются адаптивные фильтры, подстраивающие свои параметры на основе анализа показателя расходимости [9] или полученной оценки ускорения объекта; многомодельные алгоритмы, используемые в случае, когда маневр цели является неизвестным, но принадлежащим некоторому множеству возможных маневров [9].

Следует отметить, что выделить из всего многообразия однозначно лучший алгоритм фильтрации невозможно, так как эффективность применения конкретного фильтра зависит од многих факторов. Так, например, в условиях ограничений на вычислительные ресурсы РТС эффективными являются адаптивные фильтры с обнаружителем маневра [1; 8].

Цель данной работы – повышение эффективности динамической фильтрации в условиях параметрической неопределенности модели информационного процесса.

Для достижения данной цели в статье решена следующая *научная задача*: обоснование параметров критерия обнаружения маневра в задаче синтеза адаптивного фильтра Калмана.

Математическая постановка и решение задачи. Пусть информационный процесс на интервале времени $[t_0, T]$ описывается разностным уравнением

$$\mathbf{X}(j+1) = \mathbf{\Phi}(j+1, j)\mathbf{X}(j) + \mathbf{\Gamma}(j+1, j)\left(\mathbf{A}_x(j) + \mathbf{N}_x(j)\right),\ j = 0, 1, 2, \ldots \quad (1)$$

а уравнение наблюдения имеет вид

$$\mathbf{Z}(j) = \mathbf{H}(j)\mathbf{X}(j) + \mathbf{N}_z(j),\ j = 0, 1, 2, \ldots \quad (2)$$

где $\mathbf{X}(j)$ – вектор параметров процесса, $\mathbf{Z}(j)$ – вектор измерений, $\mathbf{\Phi}(j+1, j)$ $\mathbf{\Gamma}(j+1, j)$, $\mathbf{H}(j)$ – известные функциональные матрицы, $\mathbf{A}_x(j)$ – априорно неизвестный вектор интенсивностей изменения процесса $a_{x\,s}(j) \in \left[a_{x\min s}, a_{x\max s}\right]$, $s = \overline{1, m}$, $\mathbf{N}_x(j)$, $\mathbf{N}_z(j)$ – случайные шумы объекта (1) и канала наблюдения (2) соответственно, имеющие нулевые математические ожидания и корреляционные матрицы $\mathbf{Q}(j)$, $\mathbf{R}(j)$.

Полагаем, что для формирования оценки $\hat{\mathbf{X}}(j)$ вектора параметров используется два фильтра Калмана: первый настроен для сопровождения неманеврирующей цели, а второй – для маневрирующей цели. Выбор конкретного фильтра осуществляется на основе критерия обнаружения маневра.

Для решения задачи обнаружения маневра введем, по аналогии с работой [8], показатели невязки: мгновенная невязка $\varepsilon(j)$, модуль среднего арифметического значения невязки $\left|\bar{\varepsilon}(j)\right|$,

среднее арифметическое модуля значения невязки $\overline{|\varepsilon(j)|}$, при этом для простоты изложения без потери общности примем, что невязка является скалярной:

$$\boldsymbol{\varepsilon}(j)=Z(j)-H(j)\hat{X}(j|j-1), \text{ где } \hat{X}(j+1|j)=\Phi(j+1,j)\hat{X}(j) \quad (3)$$

$$|\bar{\varepsilon}(j)|=\frac{\left|\sum_{i=0}^{n-1}\varepsilon(j-i)\right|}{n};\ \overline{|\varepsilon(j)|}=\frac{\sum_{i=0}^{n-1}|\varepsilon(j-i)|}{n}. \quad (4)$$

С учетом принятых показателей невязки и полагая для простоты изложения, что $\mathbf{Q}_x=\left[\sigma_x^2\right]$ и $\mathbf{R}(j)=\left[\sigma_R^2\right]$ критерий обнаружения маневра будет иметь вид:

$$\mathrm{Y}(j)\equiv\begin{cases}\overline{|\varepsilon(j)|}>|\bar{\varepsilon}(j)|-\text{нет маневра},\\ \overline{|\varepsilon(j)|}=|\bar{\varepsilon}(j)|-\text{есть маневр}.\end{cases} \quad (5)$$

При задании показателей (4) важным вопросом является обоснование числа измерений (n), используемых при нахождении средних арифметических значений. Число измерений будет определять такие показатели качества функционирования алгоритма адаптации, как вероятность ложного обнаружения изменения модели процесса $(P_{\text{лт}})$, вероятность правильного обнаружения изменения модели процесса $(P_{\text{пр.обн.}})$, число измерений, выполненных после изменения модели процесса, необходимых для его обнаружения (m). Таким образом, для выбора значения (n) желательно иметь зависимость вида $n=f\left(P_{\text{лт}},P_{\text{пр.обн.}},m\right)$, позволяющую по заданным требованиям к $P_{\text{лт}},P_{\text{пр.обн.}},m$ произвести его обоснование. Нахождение подобной зависимости в аналитическом виде является довольно трудной задачей. По этой причине целесообразно проведение имитационного моделирования, позволяющего получить графики зависимостей $P_{\text{лт}}=f(n)$, $P_{\text{пр.обн.}}=f(m)\big|_{n=\text{const}}$. В статье проведено имитационное моделирование на примере обнаружения изменения модели, обусловленной маневрированием динамического объекта, например, самолета гражданской авиации, заходящего на посадку в нештатной ситуации. Результаты такого моделирования для частных случаев, характеризующихся конкретными значениями среднеквадратического отклонения (σ_R) ошибок измерений и ускорений маневра (a), представлены на рисунках 1 и 2. Комплексный анализ полученных зависимостей позволяет произвести обоснованный выбор значения (n) на основе применения следующего критерия пригодности:

$$K(n)=\begin{cases}"n-\text{пригодно}" \text{ при } P_{\text{лт}}\le P_{\text{лт.требуемое}}, P_{\text{пр.обн.}}\ge P_{\text{пр.обн.требуемое}}, m\le m_{\text{требуемое}},\\ "n-\text{не пригодно}" \text{ при } P_{\text{лт}}>P_{\text{лт.требуемое}}, P_{\text{пр.обн.}}<P_{\text{пр.обн.требуемое}}, m>m_{\text{требуемое}}.\end{cases} \quad (6)$$

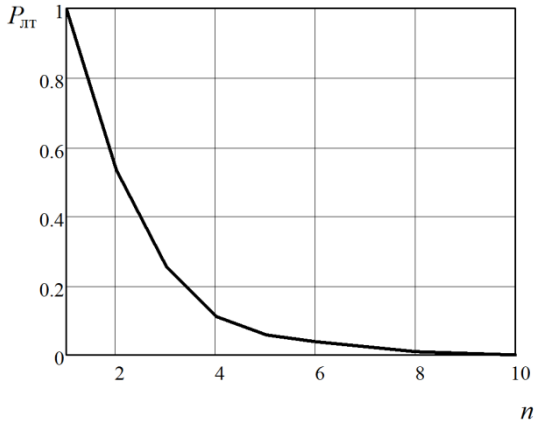


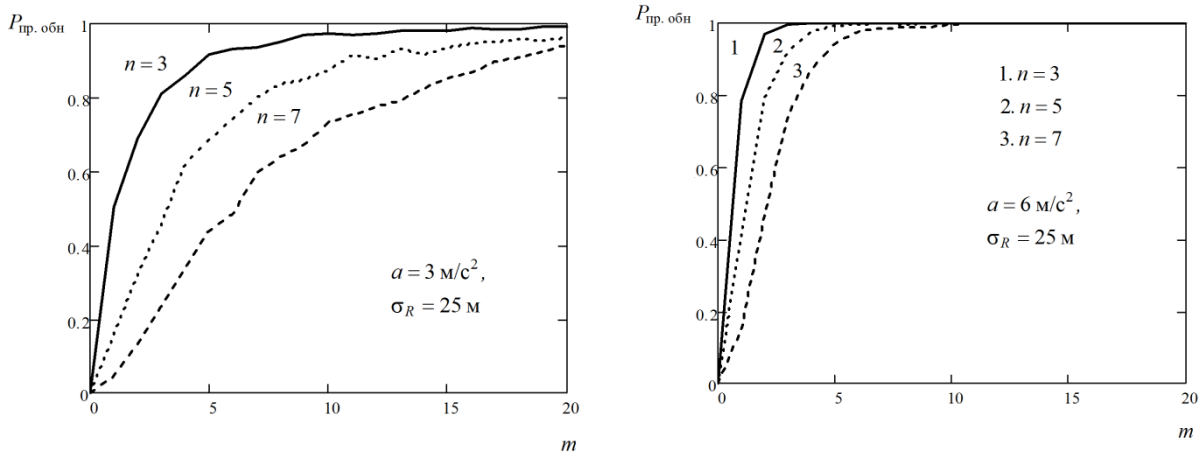
Рисунок 1. Зависимость вероятности ложной тревоги от числа измерений, используемых для нахождения показателей (4)

Так, например, если конкретизировать критерий (12) в следующем виде:

$$K(n)=\begin{cases}"n-\text{пригодно}" \text{ при } P_{лт}\le 0.1,\ P_{пр.обн.}\ge 0.8,\ m\le 10,\\ "n-\text{не пригодно}" \text{ при } P_{лт}>0.1,\ P_{пр.обн.}<0.8,\ m>10,\end{cases}$$

то для ускорений от $6\ \text{м/с}^2$ и выше пригодными, как следует из рисунков 1 и 2, будут $n\ge 5$.

Следует отметить, что при больших (n) и значительных ускорениях возможно снижение устойчивости фильтра, обусловленное увеличением времени обнаружения маневра, однако, как показали результаты моделирования, при ускорениях движения до 6 м/с^2 и $n\le 7$ такого эффекта не наблюдалось.



а) б)

Рисунок 2. Зависимость вероятности правильного обнаружения маневра от числа выполненных после начала маневра измерений (m) при различных ускорениях:
а) $a=3\ \text{м/с}^2$; б) $a=6\ \text{м/с}^2$

Заключение. Таким образом, в настоящей статье на основе имитационного моделирования обоснованы параметры критерия обнаружения маневра. Полученные результаты позволяют обоснованно задавать критерий обнаружения маневра, обеспечивающий заданные вероятности ложной тревоги и пропуска цели.

Литература:

1. Радиотехнические системы / [Ю. М. Казаринов и др.]; под ред. Ю. М. Казаринова. – М.: Изд. центр «Академия», 2008. –592с.

2. Елисеев А.В., Калашников Р.М., Тюрин Д.А. Алгоритм дискретной фильтрации в условиях динамических помех наблюдения // Автоматизация и современные технологии, 2014, №5, с. 26–34.

3. Елисеев А.В., Крылов А.А., Остапенко А.В. Алгоритмы обработки измерений параметров движения маневрирующего объекта в условиях неравноточных измерений // Радиотехника, 2014, №8, с. 29–38.

4. Булычев Ю. Г., Елисеев А.В. Проблемы жесткости уравнений приближенной нелинейной фильтрации // Автоматика и телемеханика, 1999, №1, с. 35–45.

5. Елисеев А.В. Оценивание вектора состояния объекта на основе фильтра с нечеткой логикой // Авиакосмическое приборостроение, 2006, №4, с. 30–38.

6. Зингер Р.А. Оценка характеристик оптимального фильтра для слежения за пилотируемой целью // Зарубежная радиоэлектроника, 1971, № 8, с. 40–57.

7. Hasan A.H., Grachev A.N. Adaptive $\alpha-\beta$-filter for target tracking using real time genetic algorithm // Journal of electrical and control engineering, 2013, №4, с. 32–38.

8. Родкин М.М. Адаптивный метод настройки фильтра Калмана // VI Всероссийская конференция «Радиолокация и радиосвязь», ИРЭ им Котельникова РАН, 19–22 ноября 2012, с. 125–128

9. Перов А.И. Адаптивные алгоритмы сопровождения маневрирующих целей // Радиотехника, 2002, №7, с. 73–81.

***В.Г. Кобак, *И.Ш. Рудова, А.Г. Жуковский**

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДИФИЦИРОВАННОЙ МОДЕЛИ ГОЛДЕНБЕРГА И МУРАВЬИНОГО АЛГОРИТМА ПРИ РЕШЕНИИ ЗАДАЧИ КОММИВОЯЖЕРА

*Донской государственный технический университет, г. Ростов-на-Дону, Россия
Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: задача коммивояжера, генетический алгоритм, модель голденберга, мутация, кроссовер, муравьиный алгоритм.

В работе рассмотрены различные модифицированные виды мутаций и их влияние на результат работы генетического алгоритма на основе модели Голденберга. Особенностью предложенного генетического алгоритма является то, что задача коммивояжера решается только с помощью различных мутаций. (без кроссовера). Сравнивается эффективность муравьиного и генетического алгоритмов по весам найденных маршрутов. Показано, что эффективность генетического алгоритма напрямую зависит от количества особей в поколении и количества итераций алгоритма.

***V.G. Kobak, *I.S. Rudova, A.G. Zhukovskiy**

COMPARATIVE ANALYSIS OF THE MODIFIED GOLDENBERG MODEL AND FORMIC ALGORITHMS FOR SOLVING THE TRAVELING SALESMAN PROBLEM

*Don state technical university, Rostov-on-Don, Russia
North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: traveling salesman problem, genetic algorithm, the Goldenberg model, mutation, crossover, ant algorithm.

In this article discusses the various modified forms of mutations and their impact on the result of a genetic algorithm based on the model Goldenberg. Feature of the proposed genetic algorithm is that the traveling salesman problem solved using only mutations of various types (without crossover). Efficiency of ant colony algorithm and genetic algorithms on weights of the found routes is compared. The efficiency of genetic algorithm depends on the number of individuals in generation, and the number of iterations of the algorithm.

Введение.

Задача о коммивояжёре – traveling salesman problem (TSP, ЗКВ) – является NP-сложной задачей дискретной оптимизации. Ее обычно формулируют на графах и звучит она следующим образом: найдите гамильтонов цикл наименьшей стоимости во взвешенном полном графе. Т.е. необходимо выйдя из начальной вершины, посетить каждую вершину графа ровно один раз и вернуться в начальную по кратчайшему пути. Для решения задачи коммивояжера существует множество алгоритмов, как точных так и приближенных, однако необходимо отметить, что даже для средней размерности задачи, решение точным методом практически невозможно. Для простого варианта симметричной задачи коммивояжера с n городами существует $\frac{(n-1)!}{2}$ всевозможных маршрутов. Иными словами для задачи из 13 городов необходимо найти оптимальный путь из более чем 3-х миллиардов маршрутов, а для 30 городов число маршрутов возрастает до $4{,}420880997\times10^{30}$. Поэтому вместо точных обычно пользуются приближенными алгоритмами, которые позволяют найти близкое к точному решение задачи за приемлемое время.

Обзор алгоритмов решения.

В данной статье решение задачи коммивояжера произведено генетическим и муравьиным алгоритмами, которые являются приближенными и существуют в рамках научного направления Natural Computing — «Природные вычисления», которое объединяет математические методы и основы принятия решений в живой природе.

Особенностью генетического алгоритма, приведенного в данной статье является то, что поиск оптимального маршрута происходит моделью Голденберга с использованием только лишь модифицированных операторов мутации (ОМ) без применения кроссовера. Мутация — случайное изменение одного или нескольких генов в хромосоме [1]. Оператор мутации (ОМ) помогает избежать «застревания» в ловушке локальных минимумов и, следовательно, повышается возможность поиска с наибольшей точностью. Вероятность мутации p_m является фиксированным случайным числом на отрезке [0; 1].

Виды операторов мутации, использованных в данной статье:

– Симметричный двухточечный ОМ сначала выбирает случайный ген в хромосоме, а далее обменивает местами гены, расположенные справа и слева от выбранного.

Например:

P:	1	2	|3	4	5	6	1	до ОМ
P':	1	4	|3	2	5	6	1	после ОМ

Симметричный двухточечный ОМ выполняется следующим образом:

1. В хромосоме $P = (a_1,a_2,a_3,a_4 \dots ,a_{n-1},a_n)$ случайным образом определяется позиция (например, a_3).
2. Гены, находящиеся справа и слева от выбранной позиции, переставляются, и формируется новая хромосома. $P' = (a_1,a_4,a_3,a_2 \dots ,a_{n-1},a_n)$.

– Несимметричный двухточечный ОМ заключается в перестановке местами двух любых выбранных ген в хромосоме.

Например:

P:	1	|2	3	4	|5	6	до ОМ
P':	1	|5	3	4	|2	6	после ОМ

Несимметричный двухточечный ОМ выполняется следующим образом:

1. В хромосоме $P = (a_1,a_2,a_3,\dots ,a_{n-2},a_{n-1},a_n)$ определяются случайным образом две позиции (например, a_2 и a_{n-1}).

2. Гены, соответствующие выбранным позициям, переставляются, и формируется новая хромосома. $P' = (a_1, a_{n-1}, a_3,..., a_{n-2}, a_2, a_n)$.

– Четырехточечный ОМ

Четырехточечный ОМ выполняется следующим образом:

1. В хромосоме $P = (a_1, a_2, a_3,... , a_{n-2}, a_{n-1}, a_n)$ определяются случайным образом две позиции (например, a_2 и a_{n-2}).
2. Гены, соответствующие выбранным позициям и стоящие справа от этих позиций, переставляются, и формируется новая хромосома. $P' = (a_1, a_{n-2}, a_{n-1},..., a_2, a_3, a_n)$.

– Несимметричный четырехточечный ОМ

Несимметричный четырехточечный ОМ выполняется следующим образом:

1. В хромосоме $P = (a_1, a_2, a_3, a_4, a_5, a_6,... , a_{n-2}, a_{n-1}, a_n)$ случайным образом определяется одна позиция (например, a_4).
2. Гены, соответствующие выбранным позициям и стоящие справа от этих позиций, переставляются, и формируется новая хромосома. $P' = (a_1, a_6, a_5, a_4, a_3, a_2,... , a_{n-2}, a_{n-1}, a_n)$.

Алгоритм работы модифицированной модели Голденберга:

1. Формирование начальной популяции.
2. Определение вероятности мутации p_m.
3. Выбор точки отсчета особей: t=0;
4. Применяем к t- той особи популяции оператор мутации.
5. Вычисляем значение целевой функции для мутирующей t-ой особи и сравниваем его со значением целевой функции предка, а затем лучшее из них сравниваем со значением целевой функции случайно выбранной особи из поколения. Особь с наилучшем значением целевой функции добавляется в следующие поколение.
6. Устанавливаем t=t+1.
7. Определение особи с наилучшей приспособленностью (значением целевой функции) $f_{опт}$.
8. Если t = количеству особей в поколении, то проверяем сколько итераций алгоритма $f_{опт}$ было неизменно. Если $f_{опт}$ было неизменным Nu итераций подряд, то конец работы, если меньше чем Nu, то переходим к шагу 3.

Помимо сильных мутаций была применена также элитарная стратегия, которая заключается в том, что лучшая особь из текущего поколения автоматически переходит в следующее.

Определить аналитически, какой из операторов мутации является наиболее эффективным невозможно, поэтому был поставлен вычислительный эксперимент. Был рассмотрен граф nBaeg29, средней размерности. Значение оптимально пути которого 1610. Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты вычислительного эксперимента для графа nBaeg29

Повторы	Простой Симметричный двухточечный ОМ		Симметричный двухточечный ОМ с одной элитной особью		Простой Несимметричный двухточечный ОМ		Несимметричный двухточечный ОМ с одной элитной особью		Простой Четырехточечный ОМ		Четырехточечный ОМ с элитной особью		Простой Несимметричный четырехточечный ОМ		Несимметричный четырехточечный ОМ с элитной особью	
	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т	ср. путь	лучший р-т
10	2200.1	1903	3099.63	2652	2015.4	1807	3375.4	2768	2277.9	1881	3149.8	2730	2073	1881	3347.2	2611

Продолжение таблицы 1.

50	1846.7	1656	2038.4	1761	1992.5	1794	2908.2	2352	1979.4	1780	2179.9	1966	1969.7	1762	2698.5	2425
100	1792.8	1628	1885.37	1670	1978.9	1830	2834.	2484	1917.6	1746	2017.8	1777	1971	1777	2520.6	2081

Из таблицы 1 видно, что наилучший результат получен при использовании простого симметричного двухточечного ОМ. Поэтому именно он и был выбран для дальнейшего исследования (таблица 2). Число повторов было выбрано также 50 и 100.

Таблица 2. Результаты работы простого симметричного двухточечного ОМ

граф nBaeg29 число повторов	20 запусков алгоритма		35 запусков алгоритма		50 запусков алгоритма	
	среднее из 10-ти лучших	лучшее из 10-ти лучших	среднее из 10-ти лучших	лучшее из 10-ти лучших	среднее из 10-ти лучших	лучшее из 10-ти лучших
50	1744,1	1660	1723,8	1663	1700,1	1643
100	1716,4	1654	1677,9	1618	1674	1622

Для сравнения с генетическим был выбран муравьиный алгоритм улучшенный применением элитарной стратегии [2]. Идея муравьиного алгоритма – имитация поведения колонии муравьёв, которая легко может отыскать кратчайший путь от муравейника к источнику пищи и адаптироваться к изменяющимся условиям флоры и фауны, находя новый кратчайший путь [3]. Аналитически нельзя сделать вывод о том какой из алгоритмов лучше. Поэтому был поставлен вычислительный эксперимент, результаты которого представлены в таблице 3.

Таблица 3. Результаты работы муравьиного алгоритма

граф nBaeg29 число повторов	20 запусков алгоритма		35 запусков алгоритма		50 запусков алгоритма	
	среднее из 10-ти лучших	лучшее из 10-ти лучших	среднее из 10-ти лучших	лучшее из 10-ти лучших	среднее из 10-ти лучших	лучшее из 10-ти лучших
50	1664,1	1639	1654	1627	1649,5	1634
100	1646,8	1625	1638,6	1628	1635,1	1623

Выводы:

Для размерностей графов 15-20 генетический алгоритм превосходит муравьиный [4]. Для графов большей размерности муравьиный алгоритм даже при малом количестве итераций находит решение ближе к оптимуму чем генетический алгоритм.

Литература:

1. Емельянов В.В., Курейчик В.М., Курейчик В.В. Теория и практика эволюционного моделирования. – М.: Физматлит, 2003.

2. И.Ш. Кавтарадзе, В.В. Бормотов Решение NP-сложных задач методом «муравьиного» алгоритма. Системный анализ, управление и обработка информации: сб. тр. II Междунар. науч. семинара, п. Дивноморское, 27 сент. – 2 окт. [Электронный ресурс] / ДГТУ – Ростов н/Д, 2011. – 1 электрон. опт. диск (CD-ROM). - № гос. Регистрации 0321103695

3. Бормотов В.В., Кавтарадзе И.Ш. Реализация алгоритма ортогональной муравьиной колонии для дискретного набора данных. Системный анализ, управление и обработка

информации: сб. тр. III Междунар. науч. семинара, п. Дивноморское, 27 сент. – 2 окт. [Электронный ресурс] / ДГТУ – Ростов н/Д, 2012. – 1 электрон. опт. диск (CD-ROM)

4. В.Г. Кобак, И.Ш. Кавтарадзе, В.В. Бормотов Решение задачи коммивояжера модифицированной моделью Голденберга с помощью различного вида мутаций. «Труды Северо-Кавказского филиала Московского технического университета связи и информатики».- Ростов-на-Дону: ДГТУ, 2014.

И.С. Коновалов, В.А. Фатхи, В.Г. Кобак

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАБОТЫ ЖАДНОГО АЛГОРИТМА ХВАТАЛА И МОДИФИЦИРОВАННОЙ МОДЕЛИ ГОЛДБЕРГА ПРИ РЕШЕНИИ ВЗВЕШЕННОЙ ЗАДАЧИ НАХОЖДЕНИЯ МИНИМАЛЬНОГО ПОКРЫТИЯ МНОЖЕСТВ

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: Генетический алгоритм, жадный алгоритм Хвatала, задача покрытия множеств, модель Голдберга, эвристический алгоритм, приближенный алгоритм

В статье описывается задача нахождения минимального покрытия множеств, ее формальное описание и применение для решения оптимизационных задач. Подробно рассмотрен принцип работы модели Голдберга генетического алгоритма и его применимость для решения задачи покрытия множеств. Дается описание жадного алгоритма Хвatала. Сравнивается эффективность жадного и генетического алгоритмов по времени работы и весам найденных покрытий. Показано, что эффективность генетического алгоритма напрямую зависит от количества особей в поколении.

I.S. Konovalov, V.A. Fathi, V.G. Kobak

COMPARATIVE ANALYSIS OF WORK GREEDY ALGORITHM OF CHVATAL AND MODIFIED GOLDBERG MODELS WEIGHTED IN SOLVING THE PROBLEM OF FINDING MINIMAL COVERINGS OF SETS

*Don state technical university, Rostov-on-Don, Russia

Keywords: genetic algorithm, greedy algorithm of Chvatal, the task is an open set, Goldberg model, a heuristic algorithm, approximate algorithm

In article set cover problem, its formal description and application for the solution of optimization tasks is described. Explicitly the principle of operation of model of Goldberg of the genetic algorithm and its applicability for the solution of the task of a covering of sets is considered. The description of greedy algorithm of Chvatal is given. Efficiency of greedy and genetic algorithms on an operating time and weights of the found coverings is compared. It is shown that efficiency of the genetic algorithm directly depends on quantity of individuals in generation.

1. Введение.

Задача о покрытии множества широко известна в дискретной оптимизации и имеет многочисленные приложения. Она является одной из основных задач информатики и теории сложности. Задача о покрытии множества относится к числу NP-трудных.

На практике задачи о покрытии возникают при размещении пунктов обслуживания, в системах информационного поиска, при назначении экипажей на транспорте, проектировании интегральных схем и конвейерных линий и т.д.

К задаче о покрытии можно свести многие задачи дискретной оптимизации: задачи стандартизации, упаковки и разбиения множества, задача о наибольшей клике, построения расписаний. Известна также и обратная сводимость задачи о покрытии к этим задачам.

2. Постановка задачи.

Дано множество U из n элементов, и набор подмножеств U, $S = \{S_1,\ldots, S_k\}$. Каждому подмножеству S_i сопоставлена некоторая неотрицательная стоимость c: $S \to Q^+$. $S' \subseteq S$ является покрытием, если любой элемент из U принадлежит хотя бы одному элементу из S'

Задача о покрытии множествами заключается в нахождении набора подмножеств, покрывающего все множество U и имеющего минимальный возможный вес.

Можно представить задачу в матричном виде [1]. Пусть A= (a_{ij}) — произвольная матрица размера m x n с элементами $a_{ij} \in \{0,1\}$ без нулевых строк и столбцов. Будем говорить, что в A строка i покрывается столбцом j , если a_{ij}=1. Подмножество столбцов называется покрытием, если в совокупности они покрывают все строки матрицы A. Пусть каждому столбцу поставлено в соответствие положительное число c_j, называемое весом столбца. Требуется найти покрытие минимального суммарного веса. Вводя переменные x_j, равные 1, если столбец j входит в искомое покрытие, и равные 0 в противном случае, приходим к следующей формулировке задачи о покрытии: минимизировать сумму

$$\sum_{j=1}^{n} c_j x_j \to min$$

при ограничениях

$$\sum_{j=1}^{n} a_{ij} x_j \geq 1, i = 1, \ldots m, x_j \in \{0,1\}, j = 1, \ldots, n$$

3. Обзор алгоритмов решения.

Для решения задачи покрытия множеств разработано множество алгоритмов, которые можно разделить на классы: приближенные алгоритмы с априорной оценкой, эвристические алгоритмы, точные алгоритмы.

Одним из первых приближенных алгоритмов является жадный алгоритм. Для задачи о покрытии с произвольными весами В. Хватал предложил модификацию жадного алгоритма. Эвристики носят вероятностный характер и поэтому их сложность невозможно оценить априорно. К ним можно отнести методы лагранжевой релаксации, генетические алгоритмы, поиск с запретами, алгоритмы муравьиной колонии, нейронные сети. Примером точных алгоритмов служит метод ветвей и границ [2]

В данной статье показаны результаты сравнения жадного алгоритма Хватала и модели Голдберга генетического алгоритма.

3.1 Жадный алгоритм.

В 1979 году Хватал предложил жадный алгоритм для задачи о покрытии множествами [3].

Алгоритм_Хватала (U, S, c: $S \to Q^+$)

1) $C \leftarrow \varnothing$, $Sol \leftarrow \varnothing$
2) While $C \neq U$ do:
   Найти SiÎ S – Sol, у которого
   αi=c(Si)/|Si - C| минимально.
   Sol ¬ Sol U{Si}
   C ¬ C U Si (Si – самое эффективное)
   price(e) = αi для всех eÎ Si – C
3) Output (Sol)

На каждой итерации выбираем самое эффективное множество, удаляем покрытые элементы и продолжаем до тех пор, пока не будут покрыты все элементы. Пусть C — это множество элементов, уже покрытых на предыдущих итерациях. Для каждого множества S_i определим его эффективность как $\alpha_i = c(S_i)/|S_i - C|$. Эффективность множества равна средней стоимости, с которой покрываются элементы этого множества, еще не покрытые на предыдущих итерациях.

3.2 Генетический алгоритм.

Предложенные в 1975 году Джоном Холландом генетические алгоритмы (ГА) основаны на принципах естественного отбора и наследования и относятся к стохастическим методам. Эти алгоритмы успешно применяются в различных областях деятельности (экономика, физика, технические науки и т.п.), также их используют для решения задач теории расписаний. Базовая схема работы ГА [4] следующая: на первом шаге формируется начальное поколение, состоящее из заданного числа особей; на втором шаге происходит отбор особей и применение операторов

кроссовера и мутации ГА с заданной вероятностью, формирование нового поколения; на шаге три происходит проверка условия останова, которая обычно заключается в неизменности лучшего решения в течение заданного числа поколений, если проверка прошла успешно, то лучшая особь выбирается как найденное решение, иначе происходит переход на второй шаг. Такая схема является общим алгоритмом для решения многих задач, и при применении её к конкретной задаче необходимо выбрать механизм кодирования параметров в гены особи. В данном случае, для решения задачи поиска минимального покрытия множеств, оптимизационной функцией будет являться минимизация веса покрытия, а условием останова будет неизменность лучшего решения в течение заданного числа поколений.

Рассмотрим механизм кодирования особи. Каждый индивид k представлен хромосомой, являющейся n-мерным вектором x^k, у которого j-й элемент x^k_j принимает значение 1, если подмножество Sj входит в покрытие, и принимает значение 0, если иначе. С таким представлением степень приспособленности f_k индивида x^k может быть рассчитана следующим образом:

$$f_k = \sum_{j=1}^{n} c_j x_j^k,$$

где c_j-стоимость подмножества S_j.

Таким образом, оптимизационная функция выглядит как $f_k \rightarrow min$.

В алгоритме используется тип мутации, основанный на изменении случайного гена на противоположное значение. Оператор скрещивания точечный. Выбираются пары хромосом из родительской популяции. Далее для каждой пары отобранных таким образом родителей разыгрывается позиция гена (локус) в хромосоме, определяющая так называемую точку скрещивания – l_k. В результате скрещивания пары родительских хромосом получается следующая пара потомков: P1 - потомок, хромосома которого на позициях от 1 до l_k состоит из генов первого родителя, а на позициях от $l_k + 1$ до L – из генов второго родителя; P2 - потомок, хромосома которого на позициях от 1 до l_k состоит из генов второго родителя, а на позициях от $l_k + 1$ до L– из генов первого родителя.

Начальное поколение формируется из особей, соответствующим найденным случайным образом покрытий с помощью алгоритма, подобному жадному алгоритму.

Очень важная деталь работы генетического алгоритма в том, что при скрещивании и мутации могут появиться особи, соответствующие покрытия которых не существуют, то есть получаются недопустимые решения. От этих решений нужно избавляться. Алгоритм проверяет, существует ли покрытие, и если нет, то пытается в случае скрещивания, выбрать другую вторую родительскую особь, а в случае мутации - выбрать другой ген для его инвертирования.

4. Анализ производительности жадного алгоритма и модифицированной модели Голдберга.

Модифицированная модель Голдберга генетического алгоритма относится к эвристическим алгоритмам, а поведение эвристик трудно описать аналитически и невозможно априорно оценить сложность, ведь они носят вероятностный характер. Поэтому эффективность модели Голдберга нужно проверять на практике с помощью эксперимента. Для этих целей создано программное средство на языке программирования C# с помощью среды разработки Microsoft Visual Studio Ultimate 2013. Запуск ПО производился на ПК со следующими характеристиками: ОС Microsoft Windows 8 Professional x64, процессор Intel Core i5-2500K, оперативная память 6 Гб. Предполагается зарегистрировать ПО на имя Донского государственного технического университета.

С помощью разработанного ПО было проведено по 100 экспериментов с различными матрицами размером n X m, где n- количество подмножеств множества U, m-мощность (количество элементов) множества U. Матрицы заполняются случайным образом "0" и "1".

- Коэффициент заполненности матрицы подмножеств единицами p=0.5.
- Интервал распределения весов подмножеств 1..50 (целые числа), формируются случайным образом.
- Количество подмножеств n принимает значения 10,25,50,75,150
- Количество элементов множества U принимает значения 10,25,50,75,150

Показаны результаты сравнения модифицированной модели Голдберга с различным числом особей (25,50,75,100,200) и жадного алгоритма Хватала. Параметры для модели Голдберга были заданы следующие:

– вероятность скрещивания = 0.9,
– вероятность мутации = 0.1,
– условие останова =100 поколений,
– тип оператора скрещивания - одноточечное,
– тип мутации - одноточечная

Результаты сравнения алгоритмов по точности решения представлены в таблице 1, а по времени работы - в таблице 2.

Таблица 1. Результаты экспериментов - точность решения задач

m \ n	Алгоритм	10	25	50	75	150
10	**ГА200**	34,98	53,66	76,97	88,66	111,16
	ГА100	35,14	53,89	77,04	88,7	111,38
	ГА75	35,19	54,8	78	89,05	111,86
	ГА50	35,58	54,71	78,83	89,99	112,67
	ГА25	37,03	57,72	80,27	93,69	114,2
	Жадный	38,89	60,18	88,79	101,8	134,86
25	**ГА200**	17,03	25,65	34,72	44,24	54,58
	ГА100	17,79	28,53	38,81	49,85	59,17
	ГА75	18,29	29,73	40,78	50,84	61,94
	ГА50	19,72	32,66	43,25	56,6	68,75
	ГА25	22,71	41,62	54,84	65,19	81,93
	Жадный	18,49	28,42	44,91	59,62	85,75
50	**ГА200**	9,95	17,71	22,03	27,82	34,58
	ГА100	11,42	20,15	27,59	34,26	39,64
	ГА75	13,3	24,29	32,19	38,36	46,43
	ГА50	13,5	28,06	38,06	43,33	51,88
	ГА25	18,73	37,86	48,12	60,34	69,06
	Жадный	10,28	19,25	30,82	43,82	68,15
75	**ГА200**	8,1	14,09	20,63	24,98	28,86
	ГА100	10	19,61	25,43	31,25	39,74
	ГА75	11,19	20,9	28,87	35,18	43,51
	ГА50	13,51	26,27	34,54	41,65	55,5
	ГА25	17,54	36,36	48,3	58,29	69,34
	Жадный	8,1	16,72	27,34	40,59	67,93
150	**ГА200**	6,93	11,48	16,34	18,04	26,69
	ГА100	8,95	16,12	25,45	27,23	35,13
	ГА75	10,98	18,79	28,35	31,04	40,21
	ГА50	14,17	24,13	33,37	39,37	49,03
	ГА25	21,33	35,08	48	50,92	69,02
	Жадный	6,13	13,67	25,68	37,66	63,04

Таблица 2. Результаты экспериментов - временные затраты работы алгоритмов (в мс)

m \ n	Алгоритм	10	25	50	75	150
10	**ГА200**	114,64	209,89	400,28	607,1109	1291,27
	ГА100	58,14	105,7	202,96	308,77	649,36
	ГА75	43,77	80,22	156,4	232,11	493,22
	ГА50	29,68	53,79	103,19	155,68	329,55
	ГА25	15,66	27,66	52,2	79,02	166,72
	Жадный	0,02	0,04	0,07	0,11	0,25

Продолжение таблицы 2.

25	**ГА200**	254,12	449,12	858,54	1279,61	2587,3
	ГА100	131,13	226,64	425,2	633,58	1283,99
	ГА75	98,9	171,58	318,57	478,8	959,27
	ГА50	67,6	116,74	213,08	323,03	640,55
	ГА25	36,9	57,901	107,16	160,79	329,68
	Жадный	0,02	0,05	0,13	0,21	0,48
50	**ГА200**	511,52	903,06	1643,08	2404,2275	4655,22
	ГА100	261,56	442,45	802,88	1182,04	2305,44
	ГА75	201,06	334,66	608,79	884,52	1705,08
	ГА50	140,69	222,06	396,82	597,86	1136,35
	ГА25	70,86	114,89	205,97	300,47	579,97
	Жадный	0,03	0,1	0,22	0,37	0,8
75	**ГА200**	765,29	1265,4	2396,39	3421,77	7250,63
	ГА100	389,3	632,96	1189,62	1714,2	3363,97
	ГА75	281,57	485,57	886,78	1269,09	2498,07
	ГА50	202,79	319,79	623,97	840,82	1689,46
	ГА25	100,36	169,2	301,84	428,03	854,91
	Жадный	0,05	0,14	0,31	0,49	1,1
150	**ГА200**	1391,92	2445,02	4511,82	6640,65	12681,57
	ГА100	676,29	1211,87	2174,45	3324,15	6458,85
	ГА75	524,54	909,8	1638,94	2480,83	4684,3
	ГА50	345,02	609,06	1121,28	1666,91	3226,66
	ГА25	180,04	313,5	570,07	844,68	1658,55
	Жадный	0,08	0,24	0,59	0,98	2,09

5. Заключение

Модифицированная модель Голдберга намного превосходит жадный алгоритм по точности решения, но проигрывает по времени выполнения.

Причем, чем больше особей в поколении использует модель Голдберга, тем точнее получившиеся решения, модель Голдберга с 200 особями лучший из рассмотренных. Но, естественно, чем больше особей, тем дольше работает алгоритм.

При малом количестве элементов (10, иногда до 25) разница между средней точностью решения задачи моделью Голдберга и жадным алгоритмом небольшая, но жадный работает намного быстрее, поэтому, в случаях, когда нам важно время работы программы, можно было бы воспользоваться жадным. А в задачах средней и большой размерности (количество подмножеств 50 и более), лучше использовать модель Голдберга с большим количеством особей, пожертвовав временем, но получив намного более точные решения.

Литература:

1. Еремеев, А.В. Генетический алгоритм для задачи о покрытии, Дискретн. анализ и исслед. опер., 2000, том 7, номер 1, 47–60

2. Еремеев, А.В. Задача о покрытии множества: сложность, алгоритмы, экспериментальные исследования. Дискретн. анализ и исслед. опер.// А.В. Еремеев, Л. А. Заозерская, А. А. Колоколов, 2000, том 7, номер 2, 22–46

3. Кононов, А. В. Приближенные алгоритмы для NP-трудных задач : учеб.-метод. пособие / А. В. Кононов, П. А. Кононова ; Новосиб. гос. ун-т. — Новосибирск: РИЦ НГУ, 2014. — 117 с

4. Титов Д.В., Коновалов И.С. Сравнение различных видов оператора мутации при работе генетического алгоритма в процессе решения однородной минимаксной задачи-Ростов н/Д: Аспирант.- 2014.-№2

5. Ханг , Н.М. Применение генетического алгоритма для задачи нахождения покрытия множества /М: Институт системного анализа РАН С.14

***Н.И. Троцюк, *В.Г. Кобак, И.П. Рыбалко**

СРАВНЕНИЕ МОДИФИКАЦИЙ МОДЕЛИ ГОЛДБЕРГА ПРИ РЕШЕНИИ ОДНОРОДНОЙ МИНИМАКСНОЙ ЗАДАЧИ

*Донской государственный технический университет, г. Ростов-на-Дону, Россия
Северо-Кавказский филиал Московского технического университета связи и информатики, г.Ростов-на-Дону, Россия

Ключевые слова: генетические алгоритмы, модель Голдберга, NP-полные задачи, поколенческая стратегия, теория расписаний, элитизм.

В статье рассматривается анализ эффективности различных модификаций классической модели Голдберга применительно к решению однородной минимаксной задачи, относящейся к классу NP-полных задач теории расписаний. Представлены модификации, использующие поколенческую стратегию отбора особей в новое поколение, а также формирование элиты с использованием алгоритма критического пути.

***N.I. Trotsyuk, *V.G. Kobak, I.P. Rybalko**

COMPARISON OF MODIFICATIONS GOLDBERG MODEL IN SOLVING THE HOMOGENEOUS MINIMAX PROBLEMS

*Don state technical university, Rostov-on-Don, Russia
North-Caucasus branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: genetic algorithms, Goldberg model, NP-complete problems, generational strategy, scheduling theory, the formation of the elite.

The article deals with the analysis of the effectiveness of various modifications of the classical model of Goldberg as applied to the homogeneous minimax problem related to the class of NP-complete problems in scheduling theory. Presented modifications using generational strategy selection of individuals in the next generation, as well as the formation of elite using algorithm critical path.

Одними из наиболее часто решаемых задач теории расписаний являются NP-полные задачи, которые отличаются тем, что для них практически невозможно подобрать решение за полиноминально быстрое время. К таким задачам относится также и однородная минимаксная задача. Постановка задачи представлена в работах [1,2]. Актуальным является разработка различных методов, позволяющих получить близкое к оптимальному приближенное решение. Такие решения получаются в том числе и с использованием генетических алгоритмов.

Рассмотрим в качестве базового генетического алгоритма модель Голдберга, которая отличается от классического генетического алгоритма – модели Холланда, тем, что использует турнирный отбор особей в новое поколение, что позволяет улучшить результаты алгоритма. Модель Голдберга можно отразить в виде последовательности следующих шагов:

Шаг 1. Формируется начальное поколение, состоящее из заданного числа особей.

Шаг 2. Турнирный отбор особей и применение ГА операторов кроссовера и мутации с заданной вероятностью для создания нового поколения.

Шаг 3. Проверка условия конца работы алгоритма, которая обычно заключается в неизменности лучшего решения в течение заданного числа поколений. Если проверка прошла неуспешно, то переход на шаг 2.

Шаг 4. Лучшая особь выбирается как найденное решение [2].

В классическом генетическом алгоритме количество особей является постоянным на протяжении всей работы алгоритма. Но из [3] известно, что количество особей может быть не только постоянным, но и переменным, то есть размер популяции может варьироваться на протяжении работы алгоритма. В данной работе для улучшения результата алгоритма Голдберга были использованы базовые изменения по следующим схемам:

Схема поколенческой стратегии формирования нового поколения 1–2:

1. В первом поколении задавалось количество особей *k*.
2. Во втором поколении генерировалось в два раза больше особей, чем в первом поколении.
3. В третьем поколении происходил возврат к исходному количеству особей *k*.

Процесс продолжался до тех пор, пока значение критерия не повторилось заданное количество раз [4].

Кроме того, для модификаций алгоритмов были использованы схемы поколенческой стратегии 1–2–3, 1–2–3–4–5 и 1–2–3–4–5–6–7–8–9, которые отличаются от рассмотренных тем, что возврат к исходному количеству особей происходил соответственно после пятикратного и девятикратного увеличения.

Для усиления полученных модификаций также был использован принцип элитизма. Элитой считается лучшая особь в поколении. Первоначально для формирования элитной особи был выбран списочный алгоритм – алгоритм критического пути, который можно отразить в виде последовательности шагов:

Шаг 1 Упорядочивается в порядке убывания веса множество заданий; $\tau(t_1) \geq \tau(t_2) \geq \ldots \geq \tau(t_m)$, где $t_i \in T$, $i = 1,2 \ldots M$

Шаг 2 Начальная загрузка всех устройств равна нулю, выбирается первое устройство (процессор) $k = 1$ и первое задание из множества заданий T, $f_j = 0;$ для всех $1 \leq j \leq N$.

Шаг 3. Выбирается устройство, на котором будет обрабатываться текущее задание, (процессор) p_j с наименьшим f_j среди всех процессоров (т.е. процессоров с минимальным временем загрузки на текущий момент).

Шаг 4. Назначается t_{i_k} следующим заданием на процессор p_j. $A_R(t_{i_k}) = p_j$, пересчитать $f_j = f_j + \tau(t_{j_k})$.

Шаг 5. Если $k \neq m,$ то увеличить $k = k + 1$ и перейти на Ш.3 Иначе алгоритм заканчивается с построенным расписанием $R,$ общая длина которого равняется $\max(f_j)$ [5].

Далее, если находится новая полученная особь, которая лучше элитной, то она ее заменяет. Элитная особь сразу переходит в новое поколение, что позволяет ускорить нахождение решения выбранной задачи.

Так как аналитически доказать, какой из алгоритмов в среднем лучше практически невозможно, то для оценки алгоритмов был проведен вычислительный эксперимент для различного количества приборов. Количество разных матриц для получения средних значений было выбрано равным 100. Диапазон параметров, который работа может принимать при выполнении на процессоре, — [25;30] (один из самых используемых). Массив работ генерируется случайно из заданного диапазона. Вероятность кроссовера и вероятность мутации – 1 (то есть происходит всегда). Количество поколений до конца работы алгоритма – 10. Начальный размер популяции – 10. Результаты вычислительного эксперимента приведены в таблицах 1–2, где N – количество процессоров, M – количество работ, T_{max} среднее – среднее значение критерия, t (мс) – время работы алгоритма в микросекундах.

Таблица 1. Результаты эксперимента (модификации модели Голдберга, использующие поколенческую стратегию)

N	M	Алгоритм 1		Алгоритм 2		Алгоритм 3		Алгоритм 4		Алгоритм 5	
		T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)
2	23	318,11	7,12	316,97	14,26	317,24	22,43	316,73	44,22	316,13	113,08
	71	961,78	12,69	960,48	24,26	959,56	38,44	958,84	68,92	959,23	146,96
	131	1771,00	17,44	1769,51	34,38	1769,21	52,41	1768,91	90,34	1768,82	184,25
	231	3121,39	26,22	3120,12	48,12	3119,80	70,63	3119,23	126,12	3119,23	242,80
	523	7063,88	46,35	7062,97	90,74	7061,96	138,35	7061,56	227,69	7061,49	407,81
	1013	13678, 86	84,78	13677, 66	158,73	13676,44	239,42	13675,76	388,79	13675,54	702,25
3	23	214,64	8,75	214,21	16,68	213,99	25,80	214,04	47,74	213,69	112,61
	71	646,85	16,40	646,22	30,28	645,53	45,77	645,02	81,98	644,79	179,75
	131	1187,70	24,40	1187,13	44,13	1186,50	66,21	1185,22	114,11	1185,65	224,33
	231	2086,97	34,92	2085,77	65,08	2085,71	93,74	2084,05	163,63	2084,24	325,22
	523	4716,13	72,66	4715, 86	124,50	4715,05	181,17	4713,67	304,86	4713,57	537,23
	1013	9126,96	132,14	9124,85	238,28	9124,31	337,17	9123,66	545,78	9122,95	1004,66
4	23	162,67	11,36	162,30	20,89	161,97	33,60	161,85	57,78	161,77	130,85
	71	489,47	21,83	487,18	39,98	487,05	61,97	486,51	103,55	486,01	201,76
	131	895,65	30,70	893,19	56,62	893,25	84,98	891,82	140,78	890,76	277,44
	231	1572,96	48,26	1568,56	83,74	1568,86	118,12	1568,24	195,28	1567,30	362,48
	523	3550,13	96,65	3543,87	164,34	3543,11	239,48	3542,42	392,91	3540,33	710,61
	1013	6858,55	178,19	6853,99	319,88	6851,31	437,37	6847,86	712,62	6846,57	1221,50

Таблица 2. Результаты эксперимента (модификации модели Голдберга, использующие элитизм и поколенческую стратегию)

N	M	Алгоритм 6		Алгоритм 67		Алгоритм 8		Алгоритм 9		Алгоритм 10	
		T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)	T_{max} среднее	t (мс)
2	23	318,01	6,90	317,29	14,30	316,78	22,49	317,18	42,43	316,38	113,81
	71	961,64	13,05	960,86	25,81	959,92	38,81	959,33	69,38	959,39	148,73
	131	1770,69	17,85	1769,60	35,40	1769,41	51,94	1769,19	91,85	1768,66	189,01
	231	3121,35	25,25	3120,61	50,36	3119,78	72,93	3119,57	120,62	3119,54	235,97
	523	7063,75	48,63	7062,93	95,71	7061,94	139,41	7061,82	236,75	7061,59	405,68
	1013	13678, 19	87,23	13677, 20	160,97	13676, 26	235,90	13676, 03	408,94	13675, 82	697,49
3	23	214,59	7,94	214,39	15,77	214,28	23,75	214,17	45,10	213,84	113,65
	71	646,69	13,54	646,15	26,75	645,66	42,14	645,36	76,41	645,11	163,80
	131	1187,61	18,99	1186,82	39,07	1186,95	56,68	1186,15	105,48	1186,03	209,40
	231	2079,80	25,61	2079,80	48,00	2079,80	69,49	2079,80	122,04	2079,80	228,48
	523	4719,89	56,98	4719,22	109,59	4717,00	167,11	4716,56	282,98	4715,09	529,87
	1013	9124,77	90,11	9124,77	165,35	9124,34	236,52	9124,11	411,79	9123,93	721,89
4	23	161,62	8,69	161,58	17,05	161,56	25,26	161,51	48,25	161,48	108,92
	71	485,67	14,94	485,68	28,51	485,65	41,66	485,64	76,38	485,56	156,28
	131	890,16	20,06	890,16	38,14	890,13	54,88	890,08	98,18	890,05	194,40
	231	1565,62	27,38	1565,63	51,30	1565,57	74,00	1565,57	129,73	1565,60	242,09
	523	3537,74	51,77	3537,75	96,00	3537,74	137,93	3537,74	237,14	3537,72	418,14
	1013	6854,71	99,33	6854,89	185,04	6855,31	240,43	6853,68	464,34	6853,87	763,66

Сравниваемые алгоритмы:

Модификации модели Голдберга, использующие поколенческую стратегию:

Алгоритм 1 – стандартная модель Голдберга.

Алгоритм 2 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2.

Алгоритм 3 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3.

Алгоритм 4 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3–4–5.

Алгоритм 5 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3–4–5–6–7–8–9.

Модификации модели Голдберга, использующие в качестве элиты алгоритм критического пути по убыванию и поколенческую стратегию:

Алгоритм 6 – стандартная модель Голдберга.

Алгоритм 7 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2.

Алгоритм 8 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3.

Алгоритм 9 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3–4–5.

Алгоритм 10 – модификация модели Голдберга, использующая схему поколенческой стратегии 1–2–3–4–5–6–7–8–9.

Исходя из результатов проведенного эксперимента можно сделать вывод, что с увеличением количества работ и процессоров модификации алгоритма Голдберга, использующие поколенческую стратегию и элитизм, работают в среднем быстрее, чем модификации, использующие только поколенческую стратегию, но показывают худший результат по минимаксному критерию.

Литература:

1. Кобак, В. Г. Сравнительный анализ алгоритмов : генетического с элитой и Крона с генетическим начальным распределением / В. Г. Кобак, Н. И. Троцюк // Математические методы в технике и технологиях. — ММТТ — 26 : сб. трудов Междунар. науч. конф. — Саратов, 2013. — Т.12, ч. 2. — С. 62–64.

2. Кобак, В. Г. Исследование турнирного отбора в генетическом алгоритме для решения однородной минимаксной задачи / В. Г. Кобак, Д. В. Титов // Математические методы в технике и технологиях — ММТТ — 21: сб. трудов Междунар. науч. конф. — Саратов, 2008. — Т.5.

3. Базы данных. Интеллектуальная обработка информации / В. В. Корнеев [и др.]. — М. : «Нолидж», 2000. — 352 с.

4. Троцюк, Н. И. Сравнение использования поколенческой стратегии в моделях Голдберга и Холланда при решении однородной минимаксной задачи / Н. И. Троцюк, В. Г. Кобак // Вестник Дон. гос. техн. ун-та. — 2014. — Т. 14, № 3. — С. 138–144.

5. Коффман, Э. Г. Теория расписания и вычислительные машины / Э. Г. Коффман — М.: «Наука», 1984. — 336 с

Н.В. Болдырихин, И.П. Рыбалко, И.А. Сосновский, А.В. Яровой

УПРАВЛЕНИЕ НАБЛЮДЕНИЯМИ ЗА ПОТОКОМ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ИЗМЕРИТЕЛЬНОЙ СИСТЕМЕ

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону

Ключевые слова: управление, измерительная система, итерационная процедура, случайный процесс

Рассматривается процедура синтеза закона управления для информационных процессов, появляющихся и исчезающих в случайные моменты времени.

N.V. Boldyrikhin, I.P. Rybalko, I.A. Sosnovskiy, A.V. Yarovoy

CONTROL OF OBSERVATIONS FOR THE FLOW OF INFORMATION PROCESSES IN THE MEASURING SYSTEM

North-Caucasian branch of the Moscow technical university relationship and informatics, Rostov-on-Don

Keywords: control, measurement system, an iterative procedure, a random process

Regarded the procedure for synthesizing the law of control for information processes, appearing and disappearing at random moments of time

1. Постановка задачи

Предположим, что наличие процесса на входе измерительной системы описывается закономерностями профильтрованного пуассоновского процесса вида

$$\overline{I}(t) = \sum_{i=1}^{I(t)} r(t, \tau_i, \beta_i), \tag{1}$$

где $\{I(t),\ t \geq 0\}$–стандартный пуассоновский поток с интенсивностью ν; $\{\beta_i\}$ – последовательность взаимно независимых и одинаково распределенных случайных величин, не зависящая от $\{I(t), t \geq 0\}$, и описывающая время нахождения i - го процесса на входе измерительной системы, $\beta_i > 0$;

$$r(t, \tau_i, \beta_i) = \begin{cases} 1, & \tau_i \leq t \leq \tau_i + \beta_i, \\ 0, & t < \tau_i,\ t > \tau_i + \beta_i. \end{cases} \tag{2}$$

При практических расчетах может использоваться любое распределение случайных величин β_i, при условии, что

$$\int_0^{\infty} W_{\beta}(\beta) = 1, \tag{3}$$

где $W_{\beta}(\beta)$ - плотность распределения случайной величины β_i.

Введем обозначение

$$\tau_i' = \tau_i + \beta_i, \tag{4}$$

где τ_i' – случайный момент времени исчезновения *i* – го информационного процесса.

Математическая постановка задачи для данного случая описывается следующими соотношениями:

$$\frac{dx_i}{dt} = A_i x_i + F_i \xi_i, \quad i = \overline{1, I(t_к)}, \quad x_i(\tau_i) = x_{iн}, \ \tau_i \in [0, t_к], \ t \in [\tau_i, \tau_i']; \tag{5}$$

$$\rho = \sum_{i=1}^{I(t_к)} \tilde{f}_i \gamma_i H_i x_i + \eta, \quad t \in [0, t_к], \ i = \overline{1, I(t_к)}, \tag{6}$$

где $\tilde{f}_i = \tilde{f}_i(\tau_i, \tilde{\tau}_i', t) = \begin{cases} 1, & \tau_i \leq t \leq \tilde{\tau}_i', \\ 0, & t < \tau_i, \ t > \tilde{\tau}_i', \end{cases} \quad \tilde{\tau}_i' = \begin{cases} \tau_i', & \tau_i' \leq t_к, \\ t_к, & \tau_i' > t_к; \end{cases} \quad x_i = x_i(t) \in R^{n_i}$ – вектор состояния $i-$го объекта; $x_{iн}-$ гауссовский вектор, $M[x_{iн}] = x^*_{iн}$, $M[(x_{iн} - x^*_{iн})(x_{iн} - x^*_{iн})^T] = K_{iн}$; τ_i - случайный момент появления $i-$го объекта,

подчиняющийся закономерностям потока случайных событий; $A_i = A_i(t) \in R^{n_i \times n_i}$; $F_i = F_i(t) \in R^{n_i \times r_i}$; $\xi_i = \xi_i(t) \in R^{r_i} - i-$й окрашенный шум, для которого $M[\xi_i(t)] = 0$; $M[\xi_i(t)\xi_i^T(t-\varsigma)] = Q_{i\xi}\delta(\varsigma)$, $Q_{i\xi} \in R^{r_i \times r_i}$ $\rho = \rho(t) \in R^m$; $f_i = f_i(\tau_i, t) = \begin{cases} 1, & \tau_i \le t \le t_к, \\ 0, & t < \tau_i, \ t > t_к; \end{cases}$ $\gamma_i = \gamma_i(t) - i$ –я управляющая функция; $H_i = H_i(t) \in R^{m \times n_i} -$ матричная функция, определяющая состав измеряемых параметров $i-$го объекта; $\eta = \eta(t) \in R^m -$ белый шум, для которого $M[\eta(t)] = 0$; $M[\eta(t)\eta^T(t-\varsigma)] = Q_\eta\delta(\varsigma)$, $Q_\eta \in R^{m \times m} -$ диагональная матрица; $I(t\,) -$ целочисленный дискретный случайный процесс; $I(t_к) -$ описывает количество процессов из совокупности (5), взятых на сопровождение в течение интервала наблюдения $[0, t_к]$.

Ограничения на управляющие функции $\gamma_i(t)$ и матрицы H_i, определяющие состав измеряемых параметров описываются выражениями

$$\gamma_i(t) \in \Gamma = \{0,1\}, \ \sum_{i=1}^{I(t_к)} \gamma_i(t) \in \Gamma, \ \int_0^{t_к} \sum_{i=1}^{I(t_к)} \gamma_i(t)dt = t_\Sigma < t_к, \ H_i(t) \in \overline{H}_i(t). \tag{7}$$

Точностные характеристики оценивания траекторий (5) на основании наблюдений (6) описывает совокупность дифференциальных уравнений Риккати относительно корреляционных матриц $K_i(t)$ ошибок фильтрации [1,2]

$$\frac{dK_i}{dt} = A_i K_i + K_i A_i^T + C_i - \gamma_i \tilde{f}_i K_i B_i K_i, \quad i = \overline{1, I(t_к)}, \ t \in [\tau_i, \tilde{\tau}_i'], \ K_i(\tau_i) = K_{i0}; \tag{8}$$

$C_i = F_i Q_{i\xi} F_i^T$; $B_i = H_i^T Q_\eta^{-1} H_i$.

Использование математической модели (7) для решения задачи оптимизации наблюдений является затруднительным в силу её высокой размерности и нелинейности [2]. Воспользуемся подходом, предложенным в [2], и перейдем к проекции гамильтоновой системы, соответствующей (8), на пространство R^{2n_i} переменных. Такая проекция имеет вид

$$\frac{dq_i}{dt} = -A_i^T q_i + \gamma_i \tilde{f}_i B_i p_i,$$

$$\frac{dp_i}{dt} = C_i q_i + A_i p_i, \qquad i = \overline{1, I(t_к)}, \ K_i q_i = p_i, \ t \in [\tau_i, \tilde{\tau}_i'], \tag{9}$$

$$K_{i0} q_{i0} = p_{i0}, \quad i = \overline{1, I(t_к)}. \tag{10}$$

Критерий качества в терминах (9)

$$J = \mathrm{M}[\sum_{i=1}^{I(t_к)} \omega_i^T p_i(\tilde{\tau}_i')] \to \min_{\Pi}; \tag{11}$$

при условии, что

$$q_i(\tilde{\tau}_i') = \omega_i. \tag{12}$$

2. Решение задачи

Рассмотрим решение задачи синтеза законов управления измерительными процессами в одноканальной измерительной системе при фильтрации группы процессов, появляющихся и исчезающих в соответствии с закономерностями случайного потока (1).

Гамильтониан для (9) имеет вид

$$\mathrm{H} = -\alpha \sum_{i=1}^{I(t_к)} \gamma_i + \sum_{i=1}^{I(t_к)} \left\{ \varphi_{iq}{}^T \left[-A_i{}^T q_i + \gamma_i \tilde{f}_i B_i p_i \right] + \varphi_{ip}{}^T \left[C_i q_i + A_i p_i \right] \right\}, \quad (13)$$

Решающее правило для определения оптимальной стратегии наблюдения имеет вид

$$\gamma_i{}^{on}(t) = \begin{cases} 1, & T_i^{on} \geq \alpha, \quad T_i^{on} \geq T_s^{on}, \quad (s = \overline{1, I(t_к)}, \ s \neq i), \\ 0, & T_i^{on} < \alpha, \quad T_i^{on} < T_s^{on}, \end{cases} \quad (14)$$

где T_i^{on} _i -я программная функция или функция переключения (индекс «*on*» означает, что план наблюдения соответствует оптимальной структуре).

Получим выражения для программных функций и матрицы, определяющей состав измеряемых параметров:

$$T_i^{on}(t) = \tilde{\psi}_i \int_0^{t_к} \int_{\tau}^{t_к} \tilde{f}_i p_i^T B_i^{on} p_i \ \bar{W}_{i\tau,\tau'}(\tau, \tau') d\tau d\tau', \quad (15)$$

$$H_i^{on}(t) = \arg \max_{H_i \in H_i} \tilde{\psi}_i \int_0^{t_к} \int_{\tau}^{t_к} \tilde{f}_i p_i^T B_i^{on} p_i \ \bar{W}_{i\tau,\tau'}(\tau, \tau') d\tau d\tau', \quad (16)$$

где $\tilde{\psi}_i$ - вероятность наличия информационного процесса на входе измерительной системы в течение интервала $[0, t_к]$, $\tilde{\psi}_i = \int_0^{t_к} \int_{\tilde{\tau}}^{t_к} W_{i\tau,\tau'}(\tau, \tau') d\tau d\tau'$; $W_{i\tau,\tau'}(\tau, \tau')$ - плотность распределения системы случайных величин τ и τ'; $\bar{W}_i(\tau) = W_{i\tau,\tau'}(\tau, \tau') / \tilde{\psi}_i$.

Покажем, что $W_{i\tau,\tau'}(\tau, \tau') = W_{i\tau}(\tau) W_{i\beta}(\tau' - \tau)$, где $W_{i\tau}(\tau)$ - плотность распределения случайной величины τ_i, описывающей время появления i - го процесса. В соответствии с плотность распределения случайной величины τ_i' с учетом равенства (4), где τ_i и β_i независимы, определяется выражением

$$W_{i\tau'}(\tau') = \int_{-\infty}^{\infty} W_{i\tau}(\tau) W_{\beta}(\tau' - \tau) d\tau. \quad (17)$$

С другой стороны

$$W_{i\tau'}(\tau') = \int_{-\infty}^{\infty} W_{i\tau,\tau'}(\tau, \tau') d\tau. \quad (18)$$

Приравнивая (16) и (17) получим

$$\int_{-\infty}^{\infty} W_{i\tau,\tau'}(\tau, \tau') d\tau = \int_{-\infty}^{\infty} W_{i\tau}(\tau) W_{\beta}(\tau' - \tau) d\tau, \quad (19)$$

следовательно $W_{i\tau,\tau'}(\tau, \tau') = W_{i\tau}(\tau) W_{\beta}(\tau' - \tau)$.

Плотность вероятности $W_{\beta}(\tau' - \tau)$ представляет собой условную плотность распределения момента исчезновения информационного процесса τ_i', т.е.

$$W_{\beta}(\tau' - \tau) = W_{\tau'}(\tau' / \tau) \quad (20)$$

Итерационная процедура последовательных приближений, за исключением пп. 2-4, аналогична процедуре, описанной [1].

Рассмотрим пп. 2-4.

2. Формирование для каждого i ($i=\overline{1,\chi}$) решения ДТКЗ (9), (10), (12) $p_i^0(\tau_i,\tilde{\tau}_i,t)$, зависящего от начального и конечного моментов как от параметра.

3. Определение состава измеряемых параметров

$$\tilde{H}_i^0(t)=\arg\max_{H_i\in H_i}\tilde{\psi}_i\int_0^{t_к}\int_\tau^{t_к}\tilde{f}_i[p_i^0]^T B_i^0 p_i^0\ \bar{W}_{i\tau,\tau'}(\tau,\tau')d\tau d\tau', \tag{21}$$

где $B_i^0=\left(H_i^0\right)^T Q_\eta^{-1}H_i^0$.

4. Формирование в соответствии с (15) программных функций

$$\tilde{T}_i^0(t)=\tilde{\psi}_i\int_0^{t_к}\int_\tau^{t_к}\tilde{f}_i[p_i^0]^T\tilde{B}_i^0 p^0{}_i\ \bar{W}_{i\tau,\tau'}(\tau,\tau')d\tau d\tau', \tag{22}$$

где $\tilde{B}_i^0=\left(\tilde{H}_i^0\right)^T Q_\eta^{-1}\tilde{H}_i^0$.

Реализацию второго пункта итерационной процедуры проведем следующим образом.

Введём на подпространстве $[0,t_к]$ пространства $[0,\infty]$ возможных значений случайной величины τ_i дискретизацию

$$\{\tau^0,\tau^1,...,\tau^{\mu}\} \tag{23}$$

с шагом

$$\tau^{j+1}-\tau^j=\Delta_\tau,\ j=\overline{0,\mu-1}. \tag{24}$$

На подпространстве $[\tau^j,t_к]$ пространства $[0,\infty]$ возможных значений случайной величины τ_i' введем дискретизацию

$$\{\tau'^0,\tau'^1,...,\tau'^{\mu'}\} \tag{25}$$

с шагом

$$\tau'^{j'+1}-\tau'^{j'}=\Delta_{\tau'},\ j'=\overline{0,\mu'-1}. \tag{26}$$

Рассмотрим i-ю ДТКЗ для τ^j, $\tau'^{j'}$ ($\tau'^{j'}>\tau^j$) и $\Pi=\Pi_i^k$

$$\frac{dq_i^k}{dt}=-A_i^T q_i^k+\gamma_i^k\tilde{f}_i^{jj'}B_i^k p_i^k,$$

$$\frac{dp_i^k}{dt}=C_i q_i^k+A_i p_i^k, \tag{27}$$

$$i=\overline{1,I(t_к)},\ j=\overline{0,\mu-1},\ j'=\overline{0,\mu'-1},\ t\in[\tau^j,\tau'^{j'}]$$

$$K_{i0}q_i(\tau^j)=p_i(\tau^j), \tag{28}$$

$$q_i(\tau'^{j'})=\omega_i, \tag{29}$$

где $B_i^k=\left(H_i^k\right)^T Q_\eta^{-1}H_i^k$, $\tilde{f}_i^{jj'}=\tilde{f}_i(\tau^j,\tau'^{j'},t)$.

Решение ДТКЗ (27)-(29) предполагает:

– решение уравнения Риккати

$$\frac{dK_i^k}{dt} = A_i K_i^k + K_i^k A_i^T + C_i - \gamma_i^k \tilde{f}_i^{jj'} K_i^k B_i^k K_i^k \quad , \tag{30}$$

соответствующего (27), с начальным условием

$$K_i(\tau^j) = K_{i0} \tag{31}$$

в прямом времени на интервале $[\tau^j, \tau'^{j'}]$, $\tau'^{j'} > \tau^j$, (результат такого решения для $t = \tau'^{j'}$ обозначим как $K_i^{jj'k}(\tau'^{j'}) = K_i^k(\tau^j, \tau'^{j'})$);

– формирование краевых условий для (27) при $t = \tau'^{j'}$

$$p_i^{jj'k}(\tau'^{j'}) = p_i^k(\tau^j, \tau'^{j'}) = K_i^{jj'k}(\tau'^{j'})\omega_i,$$
$$q_i(\tau'^{j'}) = \omega_i; \tag{32}$$

–решение уравнений (27) с краевыми условиями (32) в обратном времени.

В результате может быть сформировано множество решений

$$p_i^{jj'k}(t) = p_i^k(\tau^j, \tau'^{j'}, t), \quad t \in [\tau^j, \tau'^{j'}], \quad j = \overline{0, \mu - 1}, \quad j' = \overline{0, \mu' - 1}. \tag{33}$$

С учётом введенной дискретизации приближенные соотношения, соответствующие (21), (22), принимают следующий вид

$$\tilde{H}_i^k(t) = \arg \max_{H_i \in \overline{H_i}} \tilde{\psi}_i \sum_{j=0}^{\mu-1} \sum_{j'=0}^{\mu'-1} \tilde{f}_i^{jj'} [p_i^k(\tau^j, \tau^{j'}, t)]^T B_i^k p_i^k(\tau^j, \tau^{j'}, t) w_i^{jj'} \quad , \tag{34}$$

$$\tilde{T}_i^k(t) = \tilde{\psi}_i \sum_{j=0}^{\mu-1} \sum_{j'=0}^{\mu'-1} \tilde{f}_i^{jj'} [p_i^k(\tau^j, \tau^{j'}, t)]^T \tilde{B}_i^k p_i^k(\tau^j, \tau^{j'}, t) w_i^{jj'} \quad , \tag{35}$$

где $\tilde{B}_i^k = \left(\tilde{H}_i^k\right)^T Q_\eta^{-1} \tilde{H}_i^k$, $w_i^{jj'} = \bar{W}_{i\tau,\tau'}(\tau, \tau')\Delta_\tau \Delta_{\tau'}$.

Литература:

1. Болдырихин Н.В., Хуторцев В.В. Управление наблюдениями за потоками случайных процессов // Автоматика и телемеханика. 2006. № 12. С. 43-55.

2. Малышев В.В., Красильщиков М.Н., Карлов В.И. Оптимизация наблюдения и управления летательных аппаратов. М.: Машиностроение, 1989.

В.В. Бормотов, Г.Н. Бормотова

ЗАДАЧА КОММИВОЯЖЕРА - РЕШЕНИЕ МОДИФИЦИРОВАННЫМ МУРАВЬИНЫМ АЛГОРИТМОМ

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: Проблема комбинаторной оптимизации, проблема коммивояжера, оптимизация колонии муравьев; метод колонии муравьев.

Задача коммивояжёра представляет собой одну из самых известных задач комбинаторной оптимизации, заключающуюся в отыскании самого выгодного маршрута, проходящего через указанные города хотя бы по одному разу с последующим возвратом в исходный город. Для улучшения качества создаваемых маршрутов в работе использован алгоритм локального поиска 2-точечной оптимизации. Тестирование алгоритма производилось на задачах коммивояжёра из библиотеки TSPLIB, для которых известно наилучшее на данный момент решение.

V.V. Bormotov, G.N. Bormotova

TRAVELING SALESMAN PROBLEM IS SOLUTION MODIFIED ANT ALGORITHM

Keywords: Combinatorial Optimization Problem, The Traveling Salesman Problem, Ant colony optimization; Ant Colony Algorithm.

The traveling salesman problem is one of the most famous combinatorial optimization problems, is to find the most profitable route, passing through said city at least once, and then return to the starting city. To improve the quality of routes created in the local search algorithm used a 2-point optimization. Testing was carried out on the algorithm of traveling salesman problem library TSPLIB, for which the best known at the moment decision.

Введение.

Задача коммивояжёра представляет собой одну из самых известных задач комбинаторной оптимизации, заключающаяся в отыскании самого выгодного маршрута, проходящего через указанные города хотя бы по одному разу с последующим возвратом в исходный город.

Первые упоминания о математической постановке задачи как задачи оптимизации принадлежат Карлу Менгеру, который сформулировал её в 1930 году так:

«Мы называем проблемой посыльного (поскольку этот вопрос возникает у каждого почтальона, в частности, ее решают многие путешественники) задачу найти кратчайший путь между конечным множеством мест, расстояние между которыми известно.»[1]

Постановка задачи.

Задачу коммивояжёра обычно представляют в виде графа, вершины которого соответствуют городам, а ребра (i, j) между вершинами i и j — пути сообщения между этими городами. Задача заключается в отыскании кратчайшего маршрута.

Однако, существуют алгоритмы поиска приближенных решений для метрической задачи за полиномиальное время и нахождения маршрута близкого к оптимальному.

Решение поставленной задачи.

Муравьиный алгоритм [2] — один из эффективных полиномиальных алгоритмов для нахождения приближённых решений задачи коммивояжёра, а также аналогичных задач поиска маршрутов на графах. Суть подхода заключается в анализе и использовании модели поведения муравьёв, ищущих пути от колонии к источнику питания и представляет собой метаэвристическую оптимизацию. Первая версия алгоритма, предложенная доктором наук Марко Дориго в 1992 году [3], была направлена на поиск оптимального пути в графе.

Работа алгоритма начинается с размещения муравьёв в вершинах графа. Муравей выбирает следующего клиента из списка доступных клиентов и обновляет свою текущую загрузку перед выбором следующего. Выбор следующего пункта производится случайным образом на основе следующей зависимости:

$$p = \frac{(\tau_{ij})^{\alpha}(\mu_{ij})^{\beta}}{\sum_{u \notin Mk}(\tau_{iu})^{\alpha}(\mu_{ju})^{\beta}}$$, если $j \in Mk$, иначе 0,

где τ - количество феромона на пути между текущей позицией i и возможной позиции j;

$$\mu_{i,j} = 1/d_{ij};$$

α и β параметры означающие относительные значимости количества феромона и расстояния при выборе следующего клиента. При $\alpha = 0$ алгоритм вырождается в жадный, когда выбирается ближайший город без учета количества феромона. Суммарная длина L_k рассчитывается как значение объектной функции полного маршрута k-го искусственного муравья.

Обновление феромона состоит из двух этапов: имитация испарения и обновление следа в зависимости от качества получаемого решения. Имитация испарения феромона рассчитывается на основании зависимости:

$$\tau_{ij} = (1-p)\tau_{ij} + \sigma$$

где p — параметр контролирующий интенсивность испарения феромона;

σ — параметр, гарантирующий минимальную концентрацию феромона на ребре, который равен произвольному, достаточно небольшому значению.

Для дуги (i,j) и маршрута T_k количество откладываемого феромона задаётся в виде:

$$\Delta\tau_{ij,k} = \begin{cases} \dfrac{0}{L_k}, (i,j) \in T_k \\ 0, (i,j) \notin T_k \end{cases}$$

где O - параметр, имеющий значение порядка оптимальной длины всех маршрутов, тогда для ребра (i,j) общее количество феромона определяется:

$$\Delta\tau_{ij} = \sum_{k=0}^{m} \Delta\tau_{ij,k},$$

где m — количество муравьёв в колонии.

Таким образом, по сумме двух этапов количество феромона задаётся формулой:

$\tau_{ij} = (1-p)\tau_{ij} + \sigma + \Delta\tau_{ij}$.

Для улучшения качества создаваемых маршрутов применялся алгоритм локального поиска 2-точечной оптимизации. В этом алгоритме производятся последовательные замены двух несмежных рёбер маршрута новыми, и если значение целевой функции улучшается, то выбирается наиболее эффективная из них.

Анализ разработанного алгоритма муравьиных колоний позволяет выделить следующие этапы решения задачи:

- начальная подготовка, включающая в себя загрузку и начальную инициализацию данных;
- последовательное построение и улучшение маршрутов – непосредственно сам вычислительный этап;
- обработка и вывод полученных результатов.

Наибольшую сложность в вычислительном плане составляет построение и улучшение маршрутов. Этот этап можно разбить на следующие подэтапы: построение маршрута и его последующее улучшение для каждого муравья, затем обновление следа феромона.

Тестирование алгоритма.

Тестирование алгоритма производилось на задачах коммивояжёра из библиотеки TSPLIB [4] для которых известно наилучшее на данный момент решение.

Результаты тестирования, приведенные в таблице 1, сравнивались с результатами решения этих же задач другими методами, алгоритм «приближение кривой», алгоритм «иди к ближайшему» и генетический алгоритм [5].

Таблица 1. Сравнение разработанного алгоритма с другими алгоритмами решения задачи, такими как метод «приближение кривой», алгоритм «иди к ближайшему» и генетический алгоритм

Пример и число пунктов	Оптимальный результат, т.е. наиболее точный на сегодня	Результат алгоритма «приближение кривой»	Ошибка %	Результат алгоритма «иди к ближайшему»	Ошибка %	Генетический алгоритм	Ошибка %	Результат алгоритма МК с ЛП	Ошибка %	Время (сек.) работы алгоритма МК с ЛП
Berlin52	7542	8731	13,6	8980	16	7572,9	0,4	7542	0,0	1
Dsj1000	18660188	26231478	28,86	24395823	23,5	-	-	19216956	2,9	450 (7,5мин)
Eil101	629	734	14,3	832	24,4	654,3	4,0	630	0,2	37
Eil51	426	469	9,168	512	16,8	430,4	1,03	426	0,0	1
kroA100	21282	22498	5,4	26762	20,5	21937,5	3,08	21282	0,0	3
Fl1577	22249	30963	28,1	29091	23,5	-	-	22852	2,7	226 (3.8 мин)
Lin105	14379	16629	-	20213	-	14745,8	2,55	14379	0,0	1
Rat99	1211	-	-	-	-	1232,5	1,78	1211	0,0	1

Выводы.

Для решения задачи коммивояжера высокой размерности разработан модифицированный муравьиный алгоритм, позволяющий получать решение за полиноминальное время. Сравнение разработанного алгоритма с другими алгоритмами решения задачи показало более высокую

точность вычислений. Разработанный алгоритм может быть использован для решения реальных задач.

Литература:
1. Задача коммивояжера – URL: http://ru.wikipedia.org/wiki/.
2. Штовба С.Д. Муравьиные алгоритмы. Математика в приложениях – М.: Exponenta Pro, 2003.
3. M. Dorigo. Ottimizzazione, apprendimento automatico, ed algoritmi basati su metafora naturale – диссертация на соискание ученой степени: Milano, 1992 г.
4. TSPLIB – URL: http://www.akira.ruc.dk/.
5. Гуляницкий Л.Ф., Гобов Д.А. Применение Н-метода для решения задач комбинаторной оптимизации – Системные исследования и ИТ., 2007.

С.С. Остапенко, В.Г. Кобак, А.П. Кузин

РЕШЕНИЕ ОДНОРОДНОЙ МИНИМАКСНОЙ ЗАДАЧИ ПРИ УСЛОВИИ ИЗБИРАТЕЛЬНОСТИ ПРИБОРОВ МОДИФИЦИРОВАННОЙ МОДЕЛЬЮ ГОЛДБЕРГА

Донской государственный технический университет, г. Ростов-на-Дону, Россия

Ключевые слова: генетические алгоритмы, модель Голдберга, NP-полные задачи, поколенческая стратегия, теория расписаний.

В статье рассматривается анализ эффективности модификаций классической модели Голдберга применительно к решению однородной минимаксной задачи, относящейся к классу NP-полных задач теории расписаний. Также анализируется применимость рассматриваемых алгоритмов для неоднородной минимаксной задачи. Представлены модификации, использующие поколенческую стратегию отбора особей в новое поколение, а также рассмотрены модификации алгоритма критического пути.

S.S. Ostapenko, V.G. Kobak, A.P. Kuzin

MINIMAX SOLUTIONS OF THE HOMOGENEOUS PROBLEM PROVIDED SELECTIVITY DEVICES MODIFIED GOLDBERG MODEL

Don state technical university, Rostov-on-Don, Russia

Keywords: genetic algorithms, Goldberg model, NP-complete problems, generational strategy, scheduling theory.

The article deals with the analysis of the effectiveness of modifications of the classical model of Goldberg as applied to the homogeneous minimax problem related to the class of NP-complete problems in scheduling theory. Also analyzed applicabitlity of considered algorithms to the heterogeneous minimax problem. Presented modifications using generational strategy selection of individuals in the next generation, as well as the modifications of critical path algorithm.

Непрерывно ускоряющийся темп развития информационных технологий и научно-технического прогресса, наблюдаемый на протяжении всей истории не только вычислительной техники, но и технологий в целом, делает информационную область важным элементом практически всех сфер жизни современного общества. В связи с этим, неизбежно также развитие многих теоретических областей, в частности, такого раздела дискретной математики, как теория расписаний. Теория расписаний ставит проблемы упорядочения, описывая их как в абстрактных задачах (например, задача раскраски взвешенного графа), так и в более «приземленных» и имеющих практическое применение (таких, как распределение задач по вычислительным ядрам процессора или составления расписания движения поездов).

Ввиду комплексности и масштабности современных задач, требующих или имеющих возможность решения с помощью вычислительной техники, вопрос об оптимальном распределении ресурсов для нахождения решения, на сегодняшний день, остается открытым и актуальным.

Поскольку для пользователя самым ощутимым и, пожалуй, самым ценным ресурсом является время, оптимальным, в данном случае, следует считать такое решение, которое позволит выполнить заданный набор заданий на заданном наборе вычислительных устройств за минимальное время. То есть, необходимо минимизировать максимальное время, за которое на одном устройстве выполняется подмножество заданий. Такая задача называется минимаксной и она относится к классу NP-полных задач (то есть, задач, для которых на сегодняшний день не найдены алгоритмы, способные решить их за полиномиальное время). Однако, нахождение оптимального распределения также может потребовать большого количества времени, в следствие чего для решения этой проблемы часто используются приближенные алгоритмы.

В современной вычислительной технике (в операционных системах, в частности) используется множество алгоритмов распределения заданий по вычислительным устройствам. Однако, эти алгоритмы предполагают, что все вычислительные устройства идентичны и одно и то же задание будет выполняться на любом из них. Если предположить, что система состоит из разнородных вычислительных устройств или определенная задача ввиду некоторых причин не может быть выполнена на определенных устройствах, то данные алгоритмы либо неприменимы, либо требуют модификации.

В данной статье будут рассмотрены алгоритмы, учитывающие разнородность вычислительных устройств, входящих в одну систему, а также модифицированные алгоритмы для систем с однородными устройствами. Рассмотрим эти два случая: если каждое задание выполняется за одинаковое время на всех вычислительных устройствах, на которых оно может быть выполнено, и если для каждого устройства одно и то же задание может выполняться за разное время.

Первый случай кажется упрощенным, если речь идет о вычислительных устройствах. Так для чего же нужно решение такой постановки проблемы? Некоторые задачи из других областей могут быть сведены именно к таким условиям. Например, упомянутая ранее задача раскраски взвешенного графа (если принять за количество вычислительных устройств хроматическое число графа, а количество вершин за количество выполняемых заданий – поскольку вес вершины не может меняться, в какое бы подмножество она не входила, то в данной задаче устройства следует считать однородными).

Итак, имеется вычислительная система, состоящая из несвязанных однородных устройств, а также набор независимых заданий, каждое из которых выполняется на всех устройствах за одинаковое время либо не выполняется вообще. На каждом устройстве в каждый момент времени может выполняться только одно задание. Необходимо распределить задания по вычислительным устройствам таким образом, чтобы максимальное время выполнения на одном устройстве было минимальным из возможных.

Решим эту задачу несколькими алгоритмами и проанализируем их целесообразность использования в тех или иных условиях.

Рассмотрим алгоритм критического пути. Классический вид алгоритма заключается в следующем:

1. Упорядочение заданий по убыванию времени их выполнения;
2. На каждом шагу задание распределяется на то устройство, на котором в сумме после предыдущих шагов наименьшая загрузка [1].

Для сформулированной ранее задачи требуется еще один пункт – проверка, возможно ли выполнение данного задания на предполагаемом устройстве. В противном случае, необходимо выбрать устройство с наименьшей загрузкой среди тех, на которых выполнение задания возможно. Назовем это алгоритмом №1.

Очевидно, что множество заданий можно разделить на два класса: задания универсальные, которые могут выполняться на любом устройстве, и ограниченные, невыполнимые на некотрых устройствах. Логично предположить, что для ограниченных заданий следует определить больший приоритет в распределении, поскольку доступные для задания вычислительные устройства могут быть нагружены универсальными заданиями, а недоступные, наоборот, быть слабо нагруженными, что по определению не может быть оптимальным распределением. Поэтому

необходимо добавить к алгоритму еще один пункт – при сортировке упорядочить по убыванию сначала все ограниченные задания (время работы на недоступных для этих заданий устройствах будет обозначаться бесконечностью (∞)), а уже потом все универсальные. Такую модификацию назовем алгоритмом №2.

Также можно предположить, что чем больше для задания недоступных устройств, тем сложнее построить оптимальное распределение, поскольку единственные возможные варианты могут оказаться самыми загруженными. Поэтому добавим к предыдущему алгоритму поправку – при сортировке также учитывать число недоступных устройств для этого задания (то есть, число бесконечностей в его строке в матрице загрузки). Назовем это алгоритмом №3 и посмотрим, сильно ли повлияет такая поправка на работу алгоритма.

Метод критического пути – один из наиболее мощных алгоритмов для решения минимаксной задачи. Однако, появление в матрице загрузки бесконечностей накладывает ограничения на любые модификации алгоритма и лишает гарантий оптимального результата. Для сравнения обратимся к одному из эвристических алгоритмов – генетическому.

Генетический алгоритм получил свое название благодаря тому, что демонстрирует в какой-то степени естественный отбор и эволюцию и использует так называемую «поколенческую стратегию». Принцип работы выбранной модификации заключается в следующем:

1. Формируется первое поколение – совершенно случайный набор возможных решений (каждое решение называется особью).
2. Каждое следующее поколение формируется следующим образом. По очереди берется каждая особь в поколении и «скрещивается» со случайной особью в поколении. В результате скрещивания получаются две особи – каждый из родителей отдает одну часть своего решения первому ребенку, а другую второму. Из этих двух особей выбирается лучшая (решение с наименьшим максимумом). Затем эта особь сравнивается со случайной особью в родительском поколении, а также с самим родителем. И уже лучшая особь от этого сравнения идет в следующее поколение на место той особи, что рассматривалась в начале.
3. Определяется лучшая особь (с минимальным максимумом).
4. Образование следующих поколений продолжается до тех пор, пока лучший результат не меняется определенное количество раз (условие останова алгоритма) [2].

Следующее поколение формируется из потомков текущего поколения без "элитизма". Потомки занимают места своих родителей.

Такая модель алгоритма называется «моделью Голдберга». Она имеет следующие характеристики:

- Фиксированный размер популяции.
- Фиксированная разрядность генов.
- Пропорциональный отбор.
- Особи для скрещивания выбираются случайным образом.
- Одноточечный кроссовер (скрещивание) и одноточечная мутация.

Такой метод может показаться достаточно затратным как в плане ресурсов памяти, так и времени. Однако, при довольно большом количестве заданий и вычислительных устройств может показать куда более эффективную работу, о чем пойдет речь чуть позже.

Обозначим описанный алгоритм номером 4.

Другая модификация генетического алгоритма (алгоритм №5) заключается в том, что при формировании нового поколения особь-ребенок не сравнивается с родительской особью. Такой подход, с одной стороны, опасен тем, что можно в какой-то момент потерять лучшую особь и в дальнейшем не улучшить результат. С другой стороны, менее эффективные решения в дальнейшем при скрещивании могут дать результат лучше текущего, но они, зачастую, отсекаются за счет сравнения с лучшей особью из родительского поколения.

Также следуют упомянуть о таком важном механизме генетического алгоритма, как мутация. В технической реализации то, на каком устройстве будет выполняться задание, зависит от присвоенного этому заданию идентификатора (гена). В классическом случае мутация меняет в гене случайный бит. Получается совершенно другое число, и тогда задание может перейти на другое устройство, а может и остаться на текущем. Именно мутация гарантирует, что алгоритм продолжает поиск лучших решений, даже если в ходе выполнения алгоритма лучшая особь

вытеснила все остальные – такое может произойти при малом количестве особей в поколении или при неудачной реализации алгоритма генерации случайных или псевдослучайных чисел. Поэтому в алгоритмах 4 и 5 будем для оценки их работы будем использовать вероятность мутации, равную 1.

Итак, для начала возьмем для начала следующие начальные условия: 3 вычислительных устройства, 7 заданий и матрицу загрузки, представленную на рисунке 1.

	1	2	3
	19	19	19
	17	17	17
	=	17	17
	13	=	=
	=	14	=
	22	=	22
	=	23	=

Рисунок 1. Матрица загрузки для серии опытов №1.

Каждая строка на рисунке соответствует заданию, а столбец – вычислительному устройству.

Алгоритм критического пути определен однозначно и поэтому его модификации не требуют проведения больше одного опыта для одних и тех же данных.

Результат представлены в следующем виде. В графе «Решение» представлен массив заданий. Допустим, первый элемент массива равен 2 (10). Это означает, что первое задание будет выполняться на устройстве №2, а время его выполнения на этом устройстве равно 10. В графе «Нагрузки устройств» указано общее время выполнения всех заданий на данном устройстве.

Результат алгоритма №1 (критический путь, без учета бесконечностей):
Решение: [3 (19), 3 (17), 2 (17), 1 (13), 2 (14), 1 (22), 2 (23)]
Нагрузки процессоров: [1 (35), 2 (54), 3 (36)]
Максимальное значение: 54

Результат алгоритма №2 (критический путь, с учетом бесконечностей):
Решение: [3 (19), 1 (17), 3 (17), 1 (13), 2 (14), 1 (22), 2 (23)]
Нагрузки процессоров: [1 (52), 2 (37), 3 (36)]
Максимальное значение: 52

Результат алгоритма №3 (критический путь, с учетом числа бесконечностей)
Решение: [1 (19), 1 (17), 3 (17), 1 (13), 2 (14), 3 (22), 2 (23)]
Нагрузки процессоров: [1 (49), 2 (37), 3 (39)]
Максимальное значение: 49

Данный пример удачно показывает, как модификации алгоритма улучшают его результат. Однако, учитывая, что диапазон значений времени выполнения для одного задания варьируется от 10 до 25, то разница между худшим и лучшим результатами (5) слишком мала, чтобы говорить о кардинальном улучшении. Кроме того, в зависимости от нахождения и количества бесконечностей лучший результат может выдать любой из этих трех алгоритмов, что продемонстрировали опыты на других матрицах загрузки с теми же размерами и тем же диапазоном значений времени выполнения заданий.

Опыт с такими же входными параметрами был проведен еще на 47 различных вариантах матрицы загрузки. Ниже приведены некоторые из результатов, представлены только максимальные значения:

1. №1 – 67, №2 – 67, №3 – 46.
2. №1 – 51, №2 – 51, №3 – 51.

3. №1 – 43, №2 – 45, №3 – 45.
4. №1 – 65, №2 – 55, №3 – 55.
5. №1 – 50, №2 – 47, №3 – 47.
6. №1 – 62, №2 – 53, №3 – 53.
7. №1 – 52, №2 – 52, №3 – 52.
8. №1 – 49, №2 – 47, №3 – 46.
9. №1 – 65, №2 – 65, №3 – 59.
10. №1 – 53, №2 – 50, №3 – 53.
……

Итого, на 48 различных матрицах 22 раза лучший результат показал алгоритм №3, 20 раза – алгоритм №1 и 2 раза алгоритм №2 и четырежды все три выдали одинаковый результат.

Но вернемся к показанному на рисунке 1 примеру, чтобы оценить работу генетического алгоритма. Поскольку алгоритм во многом зависит от выбора случайных чисел, одного опыта для его оценки недостаточно. Было проведено по 10 опытов для каждого алгоритма и далее представлены только максимальные значения полученных решений.

Результаты алгоритма №4 (генетический, с учетом родительской особи):
Максимальные значения: 52, 52, 49, 49, 52, 49, 52, 49, 52, 49.
Лучший результат: 49.
Худший результат: 52.

Результаты алгоритма №5 (генетический, без учета родительской особи):
Максимальные значения: 49, 52, 49, 49, 49, 52, 52, 52, 52, 49.
Лучший результат: 49.
Худший результат: 52.

Для других матриц загрузки с такими же входными параметрами генетический алгоритм ни разу показал результат, лучший, чем алгоритм критического пути, а 6 раз из 48 показал худший.

Полученные результаты весьма красноречивы и означают, что при малых количествах заданий и вычислительных устройств и модификации алгоритма критического пути, и модификации генетического алгоритма работают практически с одинаковой эффективностью и, в данном случае, может быть выбран любой. Для разработчика программного средства предпочтительней окажется, скорее всего, тот, что проще в реализации, то есть, классический алгоритм критического пути.

Чтобы оценить эффективность алгоритмов, необходимо поставить перед ними более сложную задачу. Для опыта №2 были выбраны следующие параметры: 7 вычислительных устройств, 30 заданий, диапазон времени выполнения – 50-150. На рисунке 2 изображена матрица загрузки, введенная в программное средство, реализующее рассматриваемые алгоритмы.

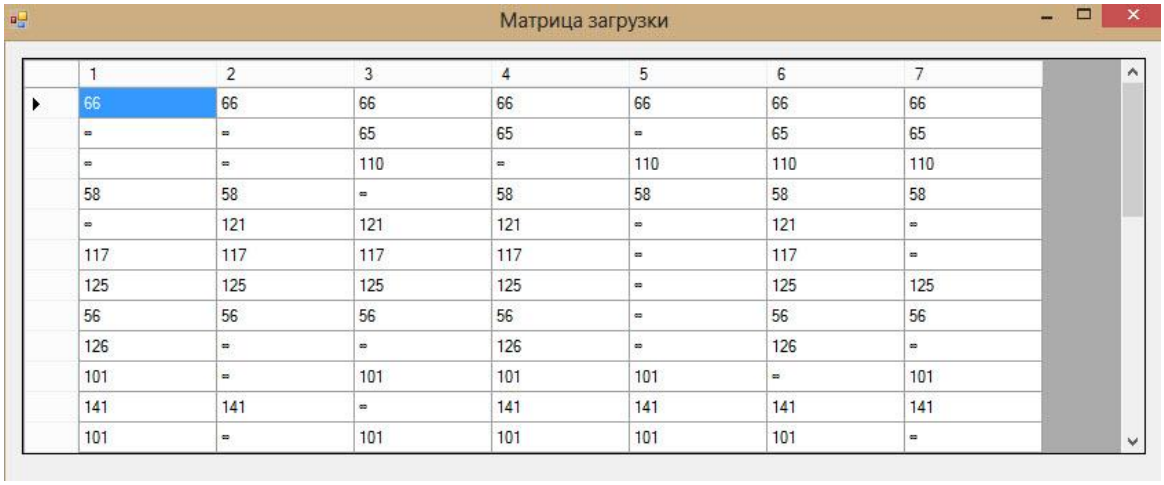


Рисунок 2. Матрица загрузки для серии опытов №2.

Рассматриваемые алгоритмы показали себя следующим образом.

Результат алгоритма №1:
Максимальное значение: 452

Результат алгоритма №2:
Максимальное значение: 461

Результат алгоритма №3:
Максимальное значение: 459

Результат алгоритма №4:
Максимальные значения: 447, 439, 439, 446, 438, 441, 442, 437, 469, 439
Лучший результат: 437
Худший результат: 469

Результат алгоритма №5:
Максимальные значения: 448, 441, 449, 461, 450, 446, 447, 453, 439, 442
Лучший результат: 439
Худший результат: 461

Было проведено 19 дополнительных опытов на других матрицах загрузки с такими же параметрами. Во всех 20 опытах генетический алгоритм находил лучшие результаты, но в 14 из них также находил и худшие.

Как видно из полученных результатов, на большем количестве заданий и вычислительных устройств, генетический алгоритм, в среднем, показал себя лучше алгоритма критического пути. Однако, есть вероятность, что он даст и худшее значение. Но стоит понимать, что разница между лучшим и худшим результатами во всех опытах снова меньше минимального значения времени выполнения задания. А разница между лучшими результатами обоих алгоритмов независимо от модификаций также не дает повода для каких-либо категоричных выводов в пользу или против какого-то из методов.

В серии опытов №3 возьмем еще более сложные условия: 20 вычислительных устройств, 150 заданий, диапазон времени выполнения – 100-2000.

1	2	3	4	5	6	7	8
362	"	"	"	362	"	"	362
"	1042	"	1042	1042	1042	1042	"
489	489	"	489	489	"	489	"
"	"	"	"	118	"	118	118
493	493	493	"	493	493	"	"
572	"	572	572	"	572	572	"
1365	1365	1365	1365	"	"	1365	1365
"	192	192	192	"	"	"	192
"	1088	"	1088	1088	1088	1088	1088
"	556	556	556	"	556	556	556
1041	1041	1041	1041	1041	1041	1041	1041

Рисунок 3. Матрица загрузки для серии опытов №3.

На выходе в примере, показанном на рисунке 3, получилось следующее.

Результат алгоритма №1:
Максимальное значение: 7313

Результат алгоритма №2:
Максимальное значение: 7313

Результат алгоритма №3:
Максимальное значение: 8298

Результат алгоритма №4:
Максимальные значения: 7390, 7440, 7614, 7417, 7509, 7464, 7417, 7413, 7383, 7533
Лучший результат: 7383
Худший результат: 7614

Результат алгоритма №5:
Максимальные значения: 7727, 8107, 7526, 7389, 7551, 7535, 7519, 7380, 7445, 7448
Лучший результат: 7380
Худший результат: 8107

Результат серии опытов №3 (также их было 20) – картина, противоположная той, что наблюдалась в опыте №2. Теперь и лучший, и худший результат показал алгоритм критического пути (в 17 из 20, в трех остальных - наоборот), но генетический по-прежнему, если сравнивать по средним показателям, выдает результат лучше.

Какие же напрашиваются выводы? Значат ли полученные результаты, что генетические алгоритмы предпочтительнее для подобного рода задач, поскольку при малом количестве заданий и устройств разницы между ними и алгоритмами критического пути практически нет, а при большом – средние показатели ближе к оптимальным? К сожалению, нет. Генетические алгоритмы требуют гораздо большее количество операций при исполнении и, в зависимости от начальных параметров (условие останова, количество особей в поколении), оно может сильно варьироваться. Поэтому при увеличении входных данных время работы алгоритма ощутимо увеличивается. И если отчеты о работе алгоритма критического пути в последнем опыте занимали всего по 14 КБ на жестком диске, то отчеты генетических алгоритмов со всеми образованными в процессе поколениями занимали от 5 до 13 МБ.

Таким образом, необходимо определиться, что важнее при решении поставленной задачи распределения – время ее выполнения или как можно более близкий к оптимальному результат. Генетический алгоритм – это поиск среди множества решений, поэтому для нахождения оптимального результата независимо от времени его выбор выглядит более целесообразно.

Если же решение должно быть найдено максимально быстро, то здесь более выигрышно смотрится алгоритм критического пути, средние показатели которого ненамного отстают от показателей генетического алгоритма. Но проблема в том, что три модификации, использованные в проведенных опытах, во всех случаях вели себя по-разному, и невозможно сделать вывод о том, какая модификация лучше. Все зависит от самой матрицы загрузки, но даже если вывести закономерности, позволяющие выбрать тот или иной вариант алгоритма, - дополнительный анализ, в данном случае, непозволительная роскошь.

Что же касается случая, когда система состоит из разнородных вычислительных устройств и время выполнения одной задачи на разных устройствах может быть разным? Здесь ситуация выглядит более прозрачно. Важным пунктом алгоритма критического пути является упорядочение по убыванию. Но, в данном случае, для каждого устройства отсортированный массив времени выполнения заданий будет выглядеть совершенно по-разному. То есть, в технической реализации необходимо создавать для каждого устройства такой массив, что является нецелесообразным. Получается, что в такой системе можно однозначно сделать выбор в пользу генетического алгоритма.

Подтвердим это утверждение опытом, в котором для сортировки в алгоритме критического пути используем сортировку по максимальному элементу в строке. В качестве начальных условий выберем следующие: 7 вычислительных устройств, 30 заданий, диапазон времени выполнения – 100-250.

	1	2	3	4	5	6	7
▶	∞	117	∞	∞	∞	194	249
	115	∞	183	242	104	∞	104
	∞	∞	237	∞	175	∞	144
	∞	114	∞	131	151	∞	235
	∞	∞	∞	235	226	231	167
	129	146	∞	197	222	209	171
	∞	142	∞	116	∞	172	247
	187	210	∞	135	143	∞	∞
	∞	238	∞	168	170	∞	∞
	∞	∞	190	∞	∞	208	∞
	∞	110	111	109	202	229	201
	∞	∞	∞	∞	∞	∞	218

Рисунок 4. Матрица загрузки для опыта с неоднородной системой.

Результат алгоритма №1:
Максимальное значение: 910

Результат алгоритма №2:
Максимальное значение: 910

Результат алгоритма №3:
Максимальное значение: 905

Результат алгоритма №4:
Максимальные значения: 787, 775, 749, 806, 676, 777, 771, 853, 746, 762
Лучший результат: 676
Худший результат: 853

Результат алгоритма №5:
Максимальные значения: 786, 755, 821, 770, 791, 752, 739, 809, 781, 831
Лучший результат: 739
Худший результат: 831

Как и было предсказано, генетический алгоритм в таких условиях показал себя лучше, поскольку является более гибким. Его гибкость заключается в том, что результат его работы не зависит напрямую от значений, введенных в матрицу загрузки – он просто перебирает возможные решения. Таким образом, на выходе он дает близкое к оптимальному и, по сравнению с точными методами, быстрое решение.

Поиск новых алгоритмов, а также совершенствование старых не прекращается. Рассмотренные в данной статье два алгоритма демонстрируют совершенно разные взгляды на решение одной и той же задачи, что лишь вдохновляет на поиски новых методов решения. Более точных или более универсальных.

Литература:

1. Кобак В.Г. “Модификация алгоритма обслуживания по «Критическому пути» для систем с избирательными свойствами приборов”– “Микропроцессорные и цифровые системы”, 2003 №2.

2. Кобак, В. Г. Исследование турнирного отбора в генетическом алгоритме для решения однородной минимаксной задачи / В. Г. Кобак, Д. В. Титов // Математические методы в технике и технологиях — ММТТ — 21: сб. трудов Междунар. науч. конф. — Саратов, 2008. — Т.5.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А.К. Абрамов

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ В БЕСПРОВОДНОЙ СЕТИ СТАНДАРТА 802.11

Академия ФСО России, г. Орёл, Россия

Ключевые слова: несанкционированный доступ, конфиденциальная информация, среда передачи, защищенность, способ шифрования.

Описана проблема несанкционированного доступа к конфиденциальной информации, передаваемой в сети стандарта 802.11. Обоснован выбор режима работы блочного шифра, рекомендованного отечественным стандартом ГОСТ 28147-89 и обеспечивающего требуемый уровень защищенности передаваемой информации. Приведена функциональная модель программного обеспечения, реализующего выбранный режим, а также последовательность операций, предусмотренная в процессе работы программы.

A.K. Abramov

SECURITY INCREASE OF CONFIDENTIAL INFORMATION TRANSMITTED THROUGH WIRELESS NETWORK OF 802.11 STANDARD

FGS Academy of Russia, Orel, Russia

Key words: unauthorized access, confidential information, communication media, security, ciphering technique.

The problem of unauthorized access to the confidential information transmitted through the network of 802.11 Standard is described. It is proved the choice of the block cipher operating mode recommended by the domestic 28147-89 State Standard and providing required security level of transmitted information. It is presented software functional simulator implementing the chosen mode as well as operations sequence foreseen in the program performance process.

Основными составляющими безопасности информации являются ее доступность, целостность и конфиденциальность [1]. Безопасность информации определяется состоянием защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.

Стандарт 802.11 в качестве среды передачи использует беспроводную среду передачи данных. Таким образом, появляется возможность скрытно подключиться к сети или просто перехватывать трафик, идущий от абонентов к точке доступа и обратно, имея в распоряжении стандартный модуль и необходимое программное обеспечение. В связи с этим возникает проблема несанкционированного доступа к информации, содержание которой может носить конфиденциальный характер.

В качестве альтернативного варианта предлагается использование отечественного стандарта ГОСТ 28147-89 [2], которым рекомендованы три режима работы блочного шифра, обеспечивающего конфиденциальность: режим простой замены, режим гаммирования и режим гаммирования с обратной связью. Рассмотрим особенности применения указанных режимов.

Режим «простой замены» имеет достаточно существенный недостаток, заключающийся в возможности проникновения статистики открытого сообщения в криптограмму, поэтому применение данного режима для шифрования в беспроводных сетях стандарта 802.11 представляется нецелесообразным.

Режим «гаммирования» лишен этого недостатка, но менее устойчив к перекрытию шифра, то есть зашифрования разных сообщений одной гаммой. В режиме «гаммирования» блоки шифрующей гаммы вырабатываются путем преобразования синхропосылки, затем гамма

накладывается на открытую информацию. В данной ситуации, при использовании псевдослучайных синхропосылок, вероятность их повторения в различных сеансах связи, но при работе на одном и том же ключе, возрастает, что может привести к перекрытию шифра. В такой же ситуации, но в режиме «гаммирования с обратной связью» перекрытие шифра произойдет только в первом блоке открытой информации, что составляет 64 бита. Далее шифрующая гамма будет вырабатываться преобразованием предыдущего блока зашифрованной информации, остальная часть криптограммы перекрытию шифра подвержена не будет. Таким образом, режим «гаммирования с обратной связью» практически не подвержен перекрытию шифра, что особенно важно при его программной реализации и, таким образом, выгодно отличает его от режима «гаммирования».

Рассмотренные режимы относятся к симметричным способам шифрования, то есть для зашифрования и расшифрования используется один и тот же ключ. Длина ключа составляет 256 бит, что делает алгоритм более стойким по сравнению с зарубежными алгоритмами шифрования, используемыми в частности, в протоколе *WPA*2 [1,3].

С учетом характера решаемой задачи – обеспечения конфиденциальности передаваемых сообщений в беспроводных сетях стандарта 802.11, для последующей программной реализации был выбран режим «гаммирования с обратной связью». Данное решение было принято на основании того, что указанный режим более устойчив к перекрытию шифра из-за малой вероятности одновременного совпадения ключей, синхропосылок и защищаемой информации.

Особенности программной реализации выбранного режима шифра заключаются в следующем. Для получения синхропосылки используются стандартные функции выработки случайных чисел. Последовательности, вырабатываемые стандартными датчиками случайных чисел, являются псевдослучайными, потому что для их получения применяются алгоритмические способы генерации случайных чисел. Для зашифрования при передаче, файл, в соответствии с ГОСТ 28147-89 разбивается на блоки по 64 бита, происходит блочное криптографическое преобразование информации. На выходе программного модуля получается файл с таким же именем и расширением, только в зашифрованном виде. Выработанная синхропосылка в открытом виде дописывается в конец передаваемого файла, из-за чего его объем увеличивается на 8 байт. При расшифровании синхропосылка считывается, происходит ее преобразование и расшифрование информации, в результате получается исходный файл.

Следует отметить, что криптографическая защита на прикладном уровне эталонной модели взаимодействия открытых систем (ЭМВОС) является наиболее предпочтительным вариантом с точки зрения ее гибкости. Шифрование на прикладном уровне обеспечивает отсутствие конфиденциальной информации в сети, так как в *IP*-пакеты инкапсулируются уже зашифрованные данные. Таким образом, злоумышленник не сможет использовать известные уязвимости стека протоколов *TCP/IP*, которые могут привести к нарушению конфиденциальности передаваемой информации, например: чтение поля данных пакета или внесение подложных данных.

Информация, находящаяся на нижестоящих иерархических уровнях ЭМВОС, относительно объекта прикладного уровня представляет собой подобъекты данного объекта, рассматриваемые, как правило, изолированно друг от друга. В связи с этим на нижестоящих уровнях невозможно достоверно распознавать а, следовательно, и защищать криптографическими методами объекты сложной структуры типа "электронный документ" в виде файла.

Другим преимуществом шифрования на прикладном уровне является то, что для осуществления несанкционированного доступа к передаваемым данным необходимо перехватить и выделить только те пакеты, в которые инкапсулированы защищаемые данные, представляющие интерес для злоумышленника. Но в случае отсутствия одного из пакетов и даже при наличии сеансового ключа у злоумышленника, расшифрование перехваченных данных невозможно. Следовательно, криптографическая защита данных прикладного уровня является наиболее приоритетной для всех нижестоящих уровней. Функциональная модель программного обеспечения, реализующего режим «гаммирования с обратной связью» представлена на рисунке 1.

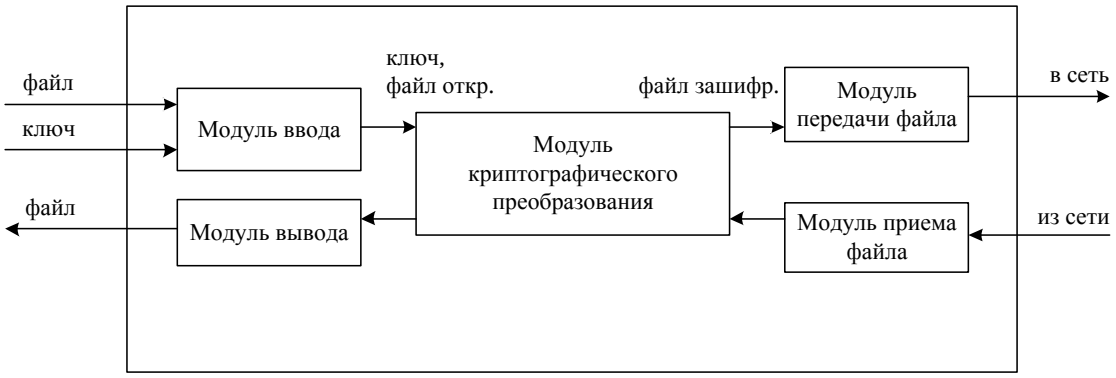


Рисунок 1. Функциональная модель программного обеспечения

Следует отметить, что для функционирования программы необходимо наличие ключа шифрования. Ключ представляет собой последовательность длиной 256 бит и должен отвечать соответствующим требованиям, предъявляемым к ключам [1]. Ключ может вводиться с любого переносного цифрового машинного носителя информации, например: с учтенной флэш-карты или токена.

Последовательность операций, предусмотренная в процессе работы программы, заключается в следующем.

При вводе ключа и выборе файла для передачи открывается диалоговое окно «Проводник» операционной системы *Windows*. Функции выбора файла и введения ключа осуществляются в модуле ввода. Передача файла при отсутствии ключа блокируется. На передающей стороне зашифрованный экземпляр файла вместе с синхропосылкой сохраняется в специальной папке на жестком диске ПЭВМ, что дает возможность учета и мониторинга файлового обмена встроенными средствами используемой операционной системы.

Операция зашифрования осуществляются в модуле криптографического преобразования, а операция передачи и приема файла – в модулях передачи и приема соответственно.

На приемной стороне зашифрованный файл сохраняется на жестком диске ПЭВМ, затем расшифровывается и также сохраняется. За сохранение файла на жестком диске отвечает модуль вывода.

Операция расшифрования файла осуществляется в модуле криптографического преобразования. Наличие файла в зашифрованном виде дает возможность его повторного расшифрования, если его хранение в открытом виде нежелательно.

Выводы:

1. Шифрование на прикладном уровне ЭМВОС исключает возможность выхода открытой информации в сеть. Целостность информации обеспечивается стандартными возможностями стека протоколов *TCP/IP* и алгоритмами, применяемыми в протоколах *WEP, WPA, WPA*2, в зависимости от того, какое оборудование применяется для построения беспроводной сети стандарта 802.11.

2. Использование отечественного стандарта ГОСТ 28147-89, не накладывает никаких ограничений на степень секретности защищаемой информации.

3. Обеспечение удобства внедрения программного обеспечения, так как при использовании программы отсутствует необходимость изменения стандартных установок используемой ОС, а сама программа не требует никаких дополнительных настроек.

Литература:

1. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 2 – Средства защиты в сетях/ С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия–Телеком, 2008. – 558 с.

3. ГОСТ 28147-89 – Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Издательство стандартов, 1989.

2. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. – М.: Горячая линия–Телеком, 2008.– 288 с.

А.В. Ашихина

ИССЛЕДОВАНИЕ АТАК НА БЕСПРОВОДНЫЕ СЕТИ СТАНДАРТА IEEE 802.11 С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

Северо-Кавказский федеральный университет, г. Ставрополь, Россия

Ключевые слова: стандарт IEEE 802.11, операционная система Android, sniffing-атаки, spoofing-атаки, взлом пароля Wi-Fi, мобильные приложения.

В статье описана проблема защищенности информации в беспроводных сетях стандарта IEEE 802.11. Проведен анализ актуальных на данный момент атак на сети стандарта IEEE 802.11 с использованием мобильных приложений на операционной системе Android, с помощью которого выявлены наиболее опасные из них. На основе проведенного исследования предлагается рассмотреть вопрос необходимости усовершенствования способов и механизмов защиты передаваемой по беспроводным сетям стандарта IEEE 802.11 информации от мобильных приложений на операционной системе Android и предприятия мер по борьбе с распространением этих программ.

A.V. Ashikhina

RESEARCH OF ATTACKS ON IEEE 802.11 STANDARD WIRELESS NETWORKS USING MOBILE APPLICATIONS FOR ANDROID OPERATION SYSTEM

North-Caucasian Federal University, Stavropol, Russia

Keywords: IEEE 802.11 standard, Android operating system, sniffing-attacks, spoofing-attacks, Wi-Fi password cracking, mobile applications.

The article describes the security problem of IEEE 802.11 wireless network. Given the analysis of attacks, that are actual for the IEEE 802.11 networks, which use mobile applications based on Android operating system, revealed the most dangerous of them. On the basis of the research it's offered to consider the need to improve protection methods and mechanisms for information transmitted over IEEE 802.11 wireless networks for mobile applications based on the Android OS and developing steps to reduce the spread of these programs.

Беспроводные сети, одна из самых актуальных новинок IT-технологий. Заманчивая перспектива уйти от проводных соединений и транспортировать информацию по радио-телекоммуникациям породила целый бум научно-технических изысканий в области подобных сетевых решений. Однако вышеупомянутое удобство параллельно открыло широчайшие возможности для злоумышленников, и реализации их атак на беспроводные сети связи.

Целью статьи является анализ известных атак на беспроводные сети стандартов IEEE 802.11 и выявление наиболее опасных из них.

Стандарты IEEE 802.11 (Wi-Fi) для сетей были разработаны по инициативе IEEE с целью создания беспроводного расширения существующих стандартов локальных вычислительных сетях 802 серии. Wi-Fi – это беспроводное соединение, которое пользуется большой популярностью, особенно среди владельцев планшетов и смартфонов. Принцип работы таких сетей базируется на точках доступа, которые преимущественно защищаются паролем [1; 2; 3; 4].

На данный момент актуальными являются 2 вида атак на Wi-Fi с использованием мобильных средств на операционной системе Android:

1. взлом пароля Wi-Fi;
2. перехват трафика:
   - sniffing-атаки;
   - spoofing-атаки.

Проанализируем каждый из этих способов.

Известны следующие приложения, реализующие взлом пароля Wi-Fi [5; 6; 7]:

- Wi-fi Pirate – это бесплатная программа для взлома Wi-Fi для Android. Основное ее назначение – это взлом Wi-Fi для того, чтобы получить доступ в Интернет и бесплатно использовать чужой трафик. На сегодня, Wi-Fi Pirate считается одной из лучших программ, разработанных для Android устройств. Используя ее, вероятность успешного получения пароля составляет 99,8 %. Такой статистики больше, чем достаточно, чтобы доверять программе Wi-Fi Pirate;
- WiHack Mobile – это мобильная версия программы для взлома Wi-Fi. Данная программа подбирает пароли к закрытым беспроводным сетям методом полного перебора (BruteForce), используя основные компоненты программы AirCrack. Взлом Wi-Fi на Android занимает не так много времени (от 3 до 10 минут);
- WiCrack – это программа для взлома паролей от Wi-Fi, строго говоря, это программа для подбора паролей к защищенным (запароленным Wi-Fi соединениям), программа объединяет в себе функции sniffer (сбор пакетов для дальнейшего взлома) и полного перебора (BruteForce) Wi-Fi ключей (подбор пароля к соединению по существующим пакетам). Таким образом, если раньше, чтобы взломать Wi-Fi нужны были использовать две программы: sniffer + BruteForce, то WiCrack объединяет все в одну программу.

Однако в сетях стандартов IEEE 802.11 используются не только атаки для взлома пароля, но и реализуется перехват аккаунтов пользователей в Wi-Fi сетях с Android. Известен sniffer (анализатор трафика) под любой смартфон или планшет на Android.

Слово sniffer (дословно с английского это можно перевести как "нюхач" или "вынюхиватель"). То есть, sniffer – это, по сути, программа, которая перехватывает сетевые пакеты.

Виды снифферов и сниффинга классифицируются:

1. По месторасположению сниффер может работать:
   - на маршрутизаторе (шлюзе) – при таком раскладе перехватывается трафик, проходящий через интерфейсы этого шлюза;
   - на оконечном узле сети.
2. По функциональным возможностям:
   - поддерживаемые физические интерфейсы и протоколы канального уровня;
   - качество декодирования и количество известных протоколов;
   - пользовательский интерфейс и удобство отображения;
   - дополнительные возможности:
     a) статистика;
     b) просмотр в реальном времени;
     c) генерирование или модификация пакетов.

Сниффер позволяет заходить под чужими аккаунтами на многие веб-сайты в общественных сетях Wi-Fi. Пример сниффинга – программа DroidSheep, которая перехватывает пакеты, проходящие в Wi-Fi сети, одним нажатием кнопки на Android-устройстве [8].

Допустим, некий пользователь заходит на свою страницу веб-сайта, используя свой смартфон или планшет через Wi-Fi, который раздается бесплатно в общественном месте (например, кафе). Злоумышленник запускает DroidSheep и через некоторое время начинает просматривать веб-страницу пользователя, читать его сообщения, писать сообщения от его имени. То есть, получает права полного администратора.

Механизм работы программы DroidSheep:

Когда Пользователь использует Wi-Fi-сеть, его планшет или смартфон отправляет все данные, предназначенные для веб-сайта, по воздуху на беспроводной маршрутизатор кафе. Иными словами «по воздуху» означает «видимые всеми».

Злоумышленник может прочитать все данные, передаваемые пользователем. Поскольку некоторые данные шифруются перед отправкой, пароль от веб-сайта он прочитать не сможет, но чтобы пользователь не вводил свой пароль после каждого клика, веб-сайт посылает пользователю так называемый «идентификатор сессии» после входа в систему, который он посылает сайту при взаимодействии с ним. Как правило, только сам пользователь знает этот идентификатор, так как он получает его в зашифрованном виде. Но когда он использует Wi-Fi в кафе, то распространяет свой идентификатор сессии по Wi-Fi для всех. Злоумышленник принимает этот идентификатор

сессии и использует его, веб-сайт не может определить, кто использует идентификатор: пользователь или злоумышленник и дает доступ обоим.

DroidSheep делает этот механизм простым в использовании, нужно просто запустить DroidSheep, нажать «Пуск» и подождать, пока кто-то начнет пользоваться одним из поддерживаемых веб-сайтов. «Прыгнуть» в чужую сессию можно лишь одним кликом по экрану.

Spoofing – общее название для сетевых атак, когда один участник маскируется под другого.

В большинстве своём spoofing-атаки направлены на то, чтобы заставить жертву отправлять трафик не законному получателю напрямую, а злоумышленнику, который затем уже ретранслирует трафик дальше. При этом злоумышленник получает возможность модификации трафика или, как минимум, его просмотра.

К наиболее распространённые spoofing-атакам относятся:

- MAC-spoofing – атака канального уровня, заключающаяся в том, что на сетевой карте изменяется MAC-адрес, что заставляет коммутатор отправлять на порт, к которому подключен злоумышленник, пакеты, которые до этого он видеть не мог;
- ARP-spoofing – атака, эксплуатирующая слабость протокола ARP, позволяющая разместить в ARP-кэше пользователя ложную запись о соответствии IP-адреса другого пользователя MAC-адресу злоумышленнику;
- IP-spoofing – атака, заключающаяся в использовании в IP-пакетах, отправляемых пользователю, IP-адресов хоста, которому она доверяет; легко осуществима в UDP, в некоторых случаях возможна в TCP-соединениях;
- DNS-spoofing – атака, базирующаяся на заражении кэша DNS-сервера пользователя ложной записью о соответствии DNS-имени хоста, которому пользователь доверяет, и IP-адреса злоумышленника.

Для защищенных WPA/WPA2 Wi-Fi-сетей программа использует DNS-Spoofing атаки [9].

В работе рассмотрены виды актуальных атак на Wi-Fi с использованием мобильных средств на операционной системе Android, а так же программы, с помощью которых можно реализовать эти атаки. За счет того, что программы, реализующие атаки на Wi-Fi легко можно скачать из Интернета и зачастую они являются бесплатными, то каждый пользователь при желании может воспользоваться одной из них.

Как показал проведенный анализ исследуемых атак на беспроводные сети стандартов IEEE 802.11, наиболее опасным является перехват трафика в виде sniffing- и spoofing-атак, так как с их помощью злоумышленник может получить информацию, которая ему не предназначалась, но в получении которой он были заинтересованы.

Таким образом, вопросы совершенствования способов и механизмов защиты от подобных программ беспроводных сетей стандартов IEEE 802.11 являются весьма актуальными. Кроме того, важным является вопрос развития способов борьбы с распространением выше упомянутых программ.

Список литературы

1. Петренко С.А., Симонов СВ. Управление информационными рисками: Экономически оправданная безопасность. - М.: АйТи-Пресс, 2014. -35-39 с.

2. Жалыбина Ю.В., Жук А.П. Анализ и перспективы развития беспроводных инфокоммуникационных технологий в сельской местности. Материалы 78-й научно-практической конференция "Актуальные проблемы социально-экономического развития СКФО". – Ставрополь: Издательство «Агрус», 2014. -56-61 с.

3. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие - М.: РИОР ИНФРА-М, 2013. – 282-284 с.

4. Щербаков В.Б., Ермаков С.А.: Безопасность беспроводных сетей стандарта IEEE 802.11.–М.: РадиоСофт, 2010 – 13-15с.

5. https://wi-fi-pirate.ru/programma-dlya-vzloma-wifi-dlya-android-wi-fi-pirate#.VIgt-O7p_HT9

6. https://mobile.wihack.com/

7. http://geektimes.ru/post/127566/

8. Симонов СВ. Методология анализа рисков в информационных системах.//Защита информации, 2012, №2, с.12-18.

9. Мучлер Ш. Беспроводные сетевые инфраструктуры.// Журнал сетевых решений LAN, 2013, №11, с.14-17.

Н.Н. Баранова, В.В. Шишкин

ОБОБЩЕННАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРЕДПРИЯТИЯ

Ульяновский государственный технический университет, г. Ульяновск, Россия

Ключевые слова: единое информационное пространство, объект защиты, классификация угроз безопасности, уязвимость объекта защиты.

В данной статье представлена обобщенная классификация угроз безопасности единого информационного пространства, учитывающая деструктивное воздействие прямых и косвенных угроз безопасности на защищаемую информацию. Приведена модель деструктивных воздействий на объекты защиты единого информационного пространства предприятия, а также формула для расчета вероятности реализации косвенных угроз безопасности информации.

N.N. Baranova, V.V. Shishkin

GENERALIZED CLASSIFICATION OF INFORMATION SECURITY THREATS OF COMMON INFORMATION SPACE ENTERPRISE

Ulyanovsk State Technical University, Ulyanovsk, Russia

Key words: common information space, object of protection, classification of security threats, vulnerabilities of the object of protection.

This article presents a generalized classification of threats to the security of a common information space, taking into account the destructive impact of direct and indirect security threats to the protected information. Here describes the model of the destructive effects on the objects of protection of the common information space enterprise, as well as the formula for calculating the probability of indirect threats to the information security.

Единое информационное пространство (ЕИП) предприятия – это совокупность информационных ресурсов, используемых программно-технических средств и технологий, необходимых для обеспечения взаимодействия пользователей пространства.

Безопасность информации, циркулирующей в едином информационном пространстве, достигается путем реализации механизмов защиты, способных противодействовать потенциально опасным видам угроз.

Модель угроз безопасности информации представляет собой систематизированный перечень угроз, присущих данному информационному пространству. Для формирования данного перечня необходимо произвести классификацию угроз.

Построение модели угроз безопасности информации играет важную роль в создании системы защиты и, как правило, предшествует ей. Такой подход дает гарантию того, что система защиты будет противодействовать только тем угрозам, которые действительно являются опасными для информационного пространства.

При рассмотрении вопроса о построении модели угроз безопасности для единого информационного пространства, следует говорить об угрозах, присущих элементам ЕИП, используемым для обработки защищаемой информации. К таким элементам относятся: операционная система пользователя, программное обеспечение, носитель информации, средства коммуникации пользователей ЕИП, линии связи и т.д.

Реализация воздействий на элементы осуществляется злоумышленником посредством имеющихся в них уязвимостей.

Совокупность элементов, представляющих автоматизированное рабочее место (АРМ) в ЕИП, используемое для работы с требующей защиты информацией, представляет собой объект защиты. Однако поскольку целью нарушителя может являться не только получение, модификация или уничтожение информации, но и выведение из строя средств её хранения, обработки, передачи и отображения, то для её реализации существуют различные методы и средства.

Множество деструктивных воздействий на объект защиты является декартовым произведением множества целей нарушителя $O = \{o_i\}_{i=1}^{n}$, множества угроз безопасности $T = \{t_j\}_{j=1}^{m}$ и множества уязвимостей объекта защиты, позволяющих реализовать угрозу $V = \{v_k\}_{k=1}^{s}$:

$$E = O * T * V.$$

При построении модели угроз безопасности, ввиду гетерогенности структуры ЕИП, необходимо рассмотреть следующие угрозы:

- угрозы, связанные со средствами хранения информации;
- угрозы, связанные со средствами обработки информации;
- угрозы, связанные со средствами отображения информации;
- угрозы, связанные со средствами передачи информации.

В зависимости от месторасположения нарушителя объект защиты может подвергаться внешним и внутренним угрозам безопасности [1]. При этом, учитывая взаимосвязь объектов защиты единого информационного пространства, они могут быть подвержены не только прямому внешнему или внутреннему воздействию нарушителя, которое рассмотрено в моделях ФСТЭК России, ФСБ, Банка России, модели Digital Security, модели угроз Microsoft и т. д. [2;3], но и косвенному – исходящему от соседних менее защищенных объектов пространства.

Прямые угрозы – угрозы, направленные на объект защиты, реализованные с использованием уязвимости самого объекта защиты.

Косвенные угрозы – угрозы, направленные на объект защиты, но реализованные посредством уязвимостей других объектов, находящихся с ним в одном сегменте сети.

Примером реализации косвенной угрозы является случай отсутствия средства антивирусной защиты на АРМ пользователя, расположенного в одном сегменте локальной вычислительной сети предприятия с АРМ, обрабатывающим защищаемую информацию. Наличие данной уязвимости может привести к заражению данного АРМ вредоносным программным обеспечением и использовании его для выполнения DDos-атаки, либо распространение с зараженного АРМ спама и так далее. Косвенная угроза может быть реализована как санкционированным пользователем сети, так и несанкционированным, в случае отсутствия в автоматизированной системе подсистемы контроля доступа к средствам вычислительной техники (СВТ).

На рисунке 1 представлена классификация угроз безопасности ЕИП.

Рисунок 1. Обобщенная классификация угроз безопасности информации

Представленная схема содержит описание наиболее опасных видов угроз для речевой, видовой информации и информации, обрабатываемой техническими средствами классифицируемых по следующим признакам:

- по источнику угрозы;
- по цели воздействия;
- по типу угрозы;
- по уязвимости объекта воздействия;
- по объекту воздействия.

Применение предложенной обобщенной классификации угроз безопасности для построения модели угроз позволит рассмотреть более полный перечень угроз безопасности влияющих на информацию, обрабатываемую в ЕИП. Учёт влияния угроз со стороны других объектов ЕИП позволит повысить уровень защищенности сегмента сети аттестованного по требованиям безопасности информации или защищенного собственными силами предприятия.

Литература:

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

2. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учеб. пособие / В. А. Сердюк.– Москва: ВШЭ, 2011.– 573 с.

3. Медведовский И.Д., Семьянов П.В., Платонов В.В. АТАКА ЧЕРЕЗ INTERNET/ Под научной редакцией проф. П. Д. Зегжды. – СПб.: НПО «Мир и семья-95», 1997 г.

4. Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: МИФИ, 1997. – 537 с.

Н.В. Белан

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИИ

Северо-Кавказский федеральный университет, г. Ставрополь, Россия

Ключевые слова: стеганография, метод LSB, метод псевдослучайного интервала, метод замены палитры, метод встраивания цифровых водяных знаков, файл-контейнер.

В статье рассмотрены четыре метода стеганографии: метод LSB, метод псевдослучайного интервала, метод замены палитры и метод встраивания цифровых водяных знаков, выявлены преимущества и недостатки каждого метода, проведен их сравнительный анализ. Эффективность каждого метода оценивалась по следующим критериям: наибольшее количество информации, которое можно скрыть с использованием метода, возможность визуального обнаружения внедренной информации и возможность обнаружения факта внедрения информации в сообщение путем использования статистического анализа.

N.V. Belan

COMPARATIVE ANALYSIS OF METHODS OF STEGANOGRAPHY

North-Caucasus Federal University, Stavropol, Russia

Keywords: steganography, method LSB, method of pseudorandom interval, method of palette replacement, method of embedding a digital watermark, container file.

In the article have examined four methods of steganography: method LSB, method of pseudorandom interval, method of palette replacement and method of embedding a digital watermark, have detected advantages and disadvantages of every method, have done their comparative analysis. The effectiveness of every method has evaluated by the following criteria: the largest quantity of information that can be hidden by using the method, the opportunity of visual detection of hidden information and the opportunity of detection the fact of hidden information in the message by using statistical analysis.

Стеганография – один из методов обеспечения информационной безопасности. Методы стеганографии обеспечивают защиту информации от несанкционированного доступа, защищают авторское право и, что не маловажно скрывают факт внедрения информации в передаваемое сообщение. Стеганография динамично развивается, так как она реализует вышеперечисленные функции защиты информации, а также в связи с тенденцией на ввод ограничений на использование криптографических методов и средств защиты информации в некоторых странах [1, 2, 6, 8].

Актуальность исследования и сравнительного анализа методов стеганографии обусловлена тем, что их для скрытия факта передачи конфиденциальной информации используют не только «продвинутые» пользователи, но и злоумышленники. Так как проблема несанкционированной скрытой передачи информации является актуальной в России, необходимо с ней бороться путем раскрытия факта использования злоумышленниками наиболее эффективных методов стеганографии.

Цель статьи – получение сравнительной характеристики различных методов стеганографии для выявления наиболее эффективных методов.

Задачи, решаемые для достижения поставленной цели:

- выявить преимущества и недостатки исследуемых методов стеганографии;
- на основе выявленных преимуществ и недостатков определить наиболее эффективный метод.

Метод LSB (Least Significant Bits) – метод замены наименее значимых битов, использующий погрешности дискретизации, которые присутствуют в оцифрованных изображениях [3, 6, 8].

Суть метода заключается в незаметном изменении нескольких младших битов в каждом из цветов модели RGB. Например, в 24-битном растровом RGB-изображении одна точка кодируется тремя байтам. Каждый байт отвечает за интенсивность одного из цветов модели RGB (в

соответствии с таблицей 1). При смешении цветов пиксель получает нужный оттенок. При замене в красном цвете (R) одного бита, двух битов в зеленом (G) и одного в синем (B) оттенок изображения немного изменяется, но в целом это изменение незаметно.

Таблица 1. Исходные компоненты цвета

1	1	0	0	0	0	1	1	R-195
0	0	1	0	0	0	0	0	G-32
0	1	1	0	0	1	1	0	B-102

Таблица 2. Измененные компоненты цвета

1	1	0	0	0	0	1	0	R-194
0	0	1	0	0	0	1	1	G-35
0	1	1	0	0	1	0	0	B-100

Следует заметить, что если занять два бита из восьми на каждый канал, то можно спрятать три байта полезной информации на каждые четыре пикселя изображения, что соответствует 25 % объема картинки. Таким образом, имея файл изображения размером 200 Кбайт, можно скрыть в нем до 50 Кбайт произвольных данных так, что невооруженному глазу эти изменения не будут заметны.

Преимущества метода:

- размер файла-контейнера не изменяется;
- при замене одного бита в канале синего цвета внедрение невозможно заметить визуально;
- возможность изменять пропускную способность при изменении количества заменяемых бит.

Недостатки метода:

- при просмотре битовых срезов легко обнаруживается внедрение сообщения.

Метод псевдослучайного интервала заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Эта методика особенно эффективна в случае, когда битовая длина секретного сообщения существенно меньше количества пикселей изображения [4].

Недостатки метода:

- биты сообщения в контейнере размещены в той же последовательности, что и в сообщении, только интервал между ними изменяется псевдослучайно.

Метод замены палитры заключается в присваивании каждому пикселю изображения (в зависимости от его цвета) символа передаваемого сообщения. Следовательно, метод замены палитры предусматривает создание алфавита, содержащего символы передаваемого сообщения, и палитры цветов.

Для скрытия данных можно использовать палитру цветов, присутствующих в изображении. Палитра представляет собой некоторое число триад байт (не более 256), которые описывают цвет точки. Следует заметить, что за палитрой расположен массив байт, описывающий одну точку изображения и содержащий номер цвета в палитре [5].

Примеры алфавита и палитр цветов для черного и белого цвета представлены в таблицах 3-5.

Таблица 3. Алфавит для передаваемого сообщения

Код	0	1	2	…	49	50
Символ	А	Б	В	…	:	,

Таблица 4. Палитра цветов для черного цвета

Код	0	1	2	…	49	50
Цвет	000000	000000	000000	…	000000	000000

Таблица 5. Палитра цветов для белого цвета

Код	51	52	53	…	100	101
Цвет	FFFFFF	FFFFFF	FFFFFF	…	FFFFFF	FFFFFF

Алгоритм метода замены палитры заключается в следующем: для скрытия информации берут первую точку изображения, анализируют ее принадлежность к определенной группе цвета, затем этой точке присваивается код текущего символа из файла-сообщения с учетом выбранной цветовой группы.

Преимущества метода:

- самый емкий метод для скрытия информации в графических файлах;
- позволяет оставлять изображение неизменным.

Недостатки метода:

- скрытая информация быстро выявляется статистическим анализом.

Метод встраивания цифровых водяных знаков

Цифровой водяной знак (ЦВЗ) – технология, созданная для защиты авторских прав [3, 7, 8, 9]. Цифровые водяные знаки делятся на два типа: видимые и невидимые [3, 8, 9]. К видимым ЦВЗ относят логотипы и надписи. Такой ЦВЗ достаточно просто удалить или заменить другим, используя графические или текстовые редакторы. Видимый ЦВЗ не выдерживает изменения самого контейнера. Невидимые ЦВЗ представляют собой встраиваемые искажения, незаметные человеческому глазу. Цифровой водяной знак – двоичный код логотипа или текста с указанием организации или автора, защищающих документ. ЦВЗ также может содержать управляющую информацию о конфиденциальности и ограничениях использования документа.

Преимущества метода:

- метод не требует дополнительных процедур предобработки изображения ЦВЗ;
- метод не требует использования фиксированного ЦВЗ для обнаружения модификаций, что обеспечивает стойкость ЦВЗ к различным атакам.

Недостатки метода:

- ЦВЗ могут позволять сжимать изображения, но запрещать вырезку из него или вставку в него фрагмента.

В данной статье были рассмотрены четыре метода стеганографии, в результате их сравнительного анализа сделаны следующие выводы:

- визуально определить была ли внедрена информация в изображение невозможно с использованием всех методов;
- наибольшее количество информации можно скрыть в изображении с использованием метода замены палитры;
- факт внедрения информации в изображение при использовании всех методов легко выявляется при использовании статистического анализа в специальных графических редакторах для всех методов.

Литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. – М.: РИОР ИНФРА-М, 2013. – 392 с.

2. Лепешкин О.М., Копытов В.В., Жук А.П. Комплексные средства безопасности и технические средства охранно-пожарной сигнализации: Учебное пособие. – М.: Гелиос АРВ, 2009. – 288 с.

3. Васина Т.С. Обзор современных алгоритмов стеганографии. – М.: НИО,2012. – 8 с.

4. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика.– К.: МК-Пресс, 2006. – 288 с.

5. Иванов В. Игры с цветами: метод замены цветовой палитры.–http://www.nestego.ru/.

6. Рябко Б.Я., Фионов А.Н.Основы современной криптографии и стеганографии. – М.: Горячая линия-Телеком, 2010. – 232 с.

7. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. – М.: ОГИЗ, 2009. – 220 с.

8. Грибунин В.Г. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.

9. Хорошко В.О. Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов. – Винница: ВДТУ, 2003. – 143 с.

А.А. Агафонов, В.А. Бурмистров,
А.А. Гавришев, Л.А. Луганская, А.А. Лысенко

О КОНФИДЕНЦИАЛЬНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ ТРЕТЬЕГО И ЧЕТВЁРТОГО ПОКОЛЕНИЙ

Северо – Кавказский федеральный университет, г. Ставрополь, Россия

Ключевые слова: системы мобильной связи, конфиденциальность информации, генератор стохастических ортогональных сигналов.

Описаны перспективы развития систем мобильной связи третьего и четвёртого поколений, примерный объём доходов рынка мобильной передачи данных и доли технологий мобильного широкополосного доступа в Интернет на конец 2017 – начало 2018 года. Описаны области использования систем мобильной связи второго и третьего поколений для передачи информации, которая очень чувствительна к уровню конфиденциальности. Указана актуальность проблемы обеспечения конфиденциальности критически важной информации. Разработаны предложения по повышению защищённости передачи информации по каналу сотовой связи в системах мобильной связи, основанных на использовании технологии передачи информации CDMA, и предложен вариант повышения защищённости.

A.A. Agafonov, V.A. Burmistrov,
A.A. Gavrishev, L.A. Luganskaya, A.A. Lysenko

ABOUT PRIVACY OF TRANSMITTING DATA IN MOBILE COMMUNICATION SYSTEMS OF THE THIRD AND FOURTH GENERATIONS

North-Caucasian federal university, Stavropol, Russia

Keywords: mobile communication systems, information privacy, generator of stochastic orthogonal signals.

Development prospects of mobile communication systems of third and fourth generation, suggested amount of mobile data transmission market and parts of wideband Internet access technologies are described at the end of 2017 – beginning of 2018. Areas of use of systems of mobile communication of the second and third generations for information transfer which is very sensitive to confidentiality level are described. Relevance of a problem of ensuring confidentiality of crucial information is specified. Offers on increase of security of transfer of information on the channel of cellular communication in the systems of mobile communication based on use of technology of information transfer of CDMA are developed and the security increase option is offered.

Стремительное развитие сетей мобильной радиосвязи наблюдается во всём мире. Активно развиваются сотовые, транкинговые, пейджинговые сети, а также сети абонентского радиодоступа.

Основной тенденцией на рынке беспроводных инфокоммуникационных технологий на сегодня является широкополосный доступ LTE. Эта технология сейчас имеет самые высокие показатели эффективности использования радиочастотного спектра, что позволяет при том же количестве базовых станций увеличить емкость сети в 2-4 раза по сравнению с технологиями предыдущего поколения [2].

По итогам третьего квартала 2013 г. число активных SIM-карт мобильной связи в мире составило 6,6 млрд, и по прогнозам Ericsson, к 2017 г. превысит 8,4 млрд. В настоящее время активно развиваются сети 3G и 4G/LTE; ожидается, что к концу 2017 г. мировые доходы от мобильной передачи данных достигнут $200 млрд [5]. Операторы все активнее используют фемтосоты, разгружают мобильный трафик через сети Wi-Fi, начинают использовать WiMAX и TDD-LTE в качестве распределительных сетей backhaul для малых сот и пр. Все эти факторы являются драйверами для развития данных сегментов рынка [5].

С другой стороны, можно выделить следующие основные проблемы [5] для перехода к сетям нового поколения: дефицит доступного спектра в большинстве регионов; неопределенность архитектуры оказания голосовых услуг в сетях LTE и гетерогенных сетях (беспроводные сети, состоящие из классических базовых станций (макросот), малых сот (фемто-, пико- и микросоты) и точек доступа Wi-Fi операторского класса); ожидание возврата инвестиций в 3G.

В целом, 3G-покрытие (доля населения, проживающего на территории, охваченной сетями 3G), по оценке J'son & Partners Consulting, на конец 2012 г. превысило 75%, в то время как в 2010 г. этот показатель составлял около 65% [6].

По прогнозу Ericsson, в 2018 г. в мире технология WCDMA/HSPA будет доминировать на мировом рынке (Рисунок 1). В 2015 г. ожидается появление технологий HSPA+Advanced и WCDMA+. Согласно прогнозу Informa Telecoms & Media, количество подключений к HSPA в мире к концу 2017 года вырастет до 4,2 млрд., в то время как число LTE-подключений составит 940 млн [6].

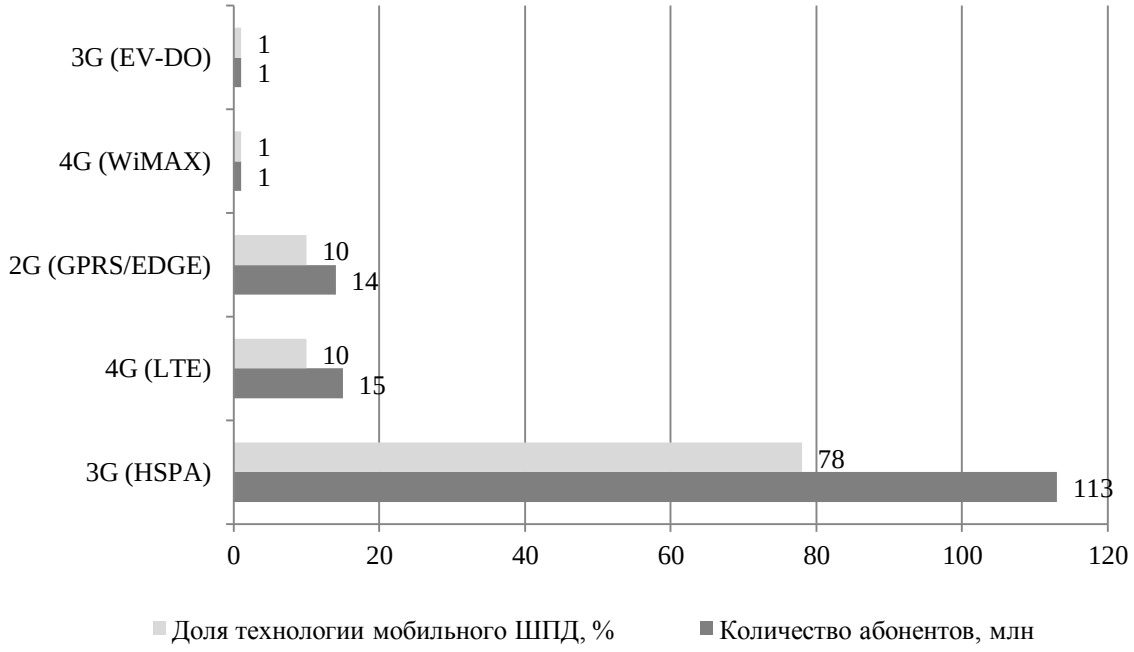


Рисунок 1. Прогноз количества абонентов (млн) и долей (%) различных технологий мобильного ШПД в России на 2018 г.

На сегодняшний день GSM и 3G используются для связи между автоматическими устройствами типа «машина-машина» (M2M). Такая связь требует небольшой емкости сети, а нужные для нее устройства — модемы — гораздо дешевле модемов LTE. Поэтому на базе GSM и 3G целесообразно организовывать сервисы удаленного мониторинга состояния объектов (радиоканальные системы охраны), транспорта (навигационные программно – аппаратные комплексы и тахографы), передвижения грузов и так далее [2].

Развитие 4G дает мощный толчок к развитию технологии LTE Connected Car, в результате реализации которой транспортное средство (в первую очередь, личный автомобиль) оборудуется радиоаппаратурой LTE мобильного широкополосного доступа к Интернет и соответствующей операционной системой (на сегодняшний день известна платформа QNX CAR) [1; 3; 7],

предоставляющей владельцу доступ к развлекательным, навигационным, коммуникационным сервисам и средствам дистанционного управления (например, умным домом) и контроля за транспортным средством.

Несмотря на стремительный старт технологии 4G/LTE, третье поколение мобильной связи еще как минимум несколько лет будет оставаться основным источником доходов операторов мобильной связи. Рост скоростей передачи данных в сетях 3G, увеличение проникновение смартфонов и других устройств с поддержкой этой технологии и расширение зоны покрытия сетей третьего поколения станут основными драйверами инвестиций в такие сети [6].

В связи с ростом использования радиоканальных систем связи для передачи критически важной информации (управляющие команды, информация о местоположении и состоянии транспортного средства, сигналы экстренных вызовов и ДТП), не говоря о коммуникационной информации вообще, возникает вопрос о ее конфиденциальности [6].

Наиболее вероятны следующие варианты повышения уровня конфиденциальности передаваемой информации.

Первый вариант – криптографическая защита информации. Криптографическая защита информации, которая предполагает наличие аппаратной, программной или аппаратно – программной реализации выбранного алгоритма шифрования как на оконечных устройствах, так и на серверном оборудовании. Ключевым является вопрос криптографической стойкости выбранного алгоритма. Также варьируется стоимость: наличие криптоалгоритма увеличивает стоимость радиоканальной системы связи по сравнению с радиоканальными системами идентичного функционала без криптоалгоритма. Кроме того, логично использование криптоалгоритма силовыми структурами и спецподразделениями (ВС РФ, ФСБ, ГРУ, МВД), но его использование иными пользователями (кроме стандартных криптоалгоритмов, предлагаемых производителями защищенных радиоканальных систем связи), скорее всего, будет затруднено.

Вторым вариантом повышения защищённости информации является возложение обеспечения её конфиденциальности на оператора сотовой связи. Однако при его реализации существуют следующие трудности: увеличение абонентской платы – помимо оплаты трафика для передачи собственно информации оператор, скорее всего, будет взимать оплату за пользование сервисом защищённой передачи информации; существует ряд сложностей с использованием канала сотовой связи, которые зависят от степени развития зоны покрытия оператора в конкретном регионе РФ или конкретной стране.

Третьим вариантом повышения защищённости информации в системах мобильной связи, основанных на использовании технологии передачи информации CDMA, является применение генераторов стохастических ортогональных сигналов, теория и практика построения которых в настоящее время глубоко не проработана. Тем не менее, путём добавления небольшого (и недорого) модуля в оконечные устройства и на серверное оборудование можно добиться повышения структурной скрытности передаваемой информации в канале сотовой связи, использующем 3G, что ведёт к повышению уровня конфиденциальности передачи и достоверности информации.

Таким образом, авторами исследованы тенденции развития рынка беспроводных информационных технологий и установлено, что, несмотря развитие и внедрение LTE технологии сотовой связи 3G будут превалировать; разработаны предложения по повышению защищённости передачи информации по каналу сотовой связи в системах мобильной связи, основанных на использовании технологии передачи информации CDMA, и предложен вариант повышения защищённости информации в рассматриваемых системах мобильной связи третьего и четвертого поколений.

Литература:

1. LTE Connected Car: широкополосный Интернет на колёсах [Электронный ресурс]. – Режим доступа: http://www.3dnews.ru/auto/609864, свободный.

2. Глава Bell Labs: Связью GSM будут пользоваться только машины [Электронный ресурс]. – Режим доступа: http://digit.ru/telecom/20131203/408941666.html, свободный.

3. Жалыбина Ю.В., Жук А.П. Анализ и перспективы развития беспроводных инфокоммуникационных технологий в сельской местности. Материалы 78-й научно-практической конференция "Актуальные проблемы социально-экономического развития СКФО". – Ставрополь: Издательство «Агрус», 2014. -56-61 с.

4. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие - М.: РИОР ИНФРА-М, 2013. – 282-284 с.

5. Тенденции и перспективы развития мирового рынка инфраструктуры беспроводной связи (2G, 3G, LTE, WiMAX, Wi-Fi), 2012-2017 гг. [Электронный ресурс]. – Режим доступа: http://web.json.ru/files/news/2014-01-30_Wireless%20Infrastructure_MW_RU.pdf, свободный.

6. Перспективы развития 3G в России и мире [Электронный ресурс]. – Режим доступа: http://telekomza.ru/2013/12/11/perspektivy-razvitiya-3g-v-rossii-i-mire/, свободный.

7. Подключенный автомобиль» (Connected Car): автомобильная телематика и информационно-развлекательные автомобильные системы, 2013-2017 [Электронный ресурс]. – Режим доступа:
http://web.json.ru/poleznye_materialy/free_market_watches/analytics/podklyuchennyj_avtomobil_connected_car_avtomobilnaya_telematika_i_informacionno-razvlekatelnye_avtomobilnye_sistemy_2013-2017/, свободный

С.А. Быстров, *Е.И. Ковалев

ИСПОЛЬЗОВАНИЕ ШУМОПОДОБНОГО СИГНАЛА В СИСТЕМЕ С УСТРОЙСТВОМ ВЕСОВОЙ ОБРАБОТКИ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Уральский технический институт связи и информатики (филиал) федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Сибирский государственный университет телекоммуникаций и информатики», г. Екатеринбург, Россия
*Уральский Федеральный университет имени первого Президента России Б.Н. Ельцина, г. Екатеринбург, Россия

Ключевые слова: шумоподобный сигнал, устройство весовой обработки, преобразование Гилберта, шум.

Традиционно в системах обработки информации в качестве несущего колебания рассматривается квазигармоническое колебание, у которого один или несколько параметров изменяются по закону модулирующего процесса. Однако имеется ряд задач, когда в качестве несущей может использоваться либо псевдослучайный сигнал, либо шумоподобный случайный процесс. [1] В современных условиях все большее значение придается вопросам скрытной передаче информации по радиоканалу и проводным каналам связи. В данной статье приводится один из примеров использования шумоподобного сигнала для скрытой передачи информации.

S.A. Bystrov, *E.I. Kovalev

THE USE OF NOISE-LIKE SIGNAL WITH WEIGHING SYSTEM FOR SECURE COMMUNICATION DEVICES

Ural Technical Institute of Communications and Informatics (branch) of the Federal State budget institution of higher education «Siberian State University of Telecommunications and Informatics», Ekaterinburg , Russia
*Ural Federal University named after the first President of Russia B.N.Yeltsin, Ekaterinburg, Russia

Keywords: noise-like signal, weighting device, Hilbert transform, the noise

Traditionally, the information processing systems as the carrier wave is considered quasi-harmonic oscillation, which has one or more parameters vary according to the modulation process. However, there are a number of problems when, as a carrier can be used either pseudorandom signal or noise-random process. [1] In modern conditions increasing emphasis on the information hiding via radio

and wire communication channels. This article provides an example of the use of noise-like signal for secure communication

При рассмотрении системы передачи информации с использованием шумоподобного сигнала, в качестве источника информации можно использовать различные сигналы. Для простоты примера представим сигнал x_1 как обычный синусоидальный сигнал с некоторой частотой и начальной фазой:

$$x_1(t) = A_1 \cdot \sin(\omega_1 t + \varphi_0), \quad (1)$$

где A_1 - амплитуда сигнала, несущего информацию, ω_1 - частота, φ_0 - начальная фаза.

Таким образом, сигнал x_1, будет являться основным переносчиком информации. Для дальнейшей скрытой передачи, необходимо его замаскировать шумовым сигналом, превосходящим сигнал x_1 по амплитуде и имеющий нормальное распределение:

Шумовые колебания, занимающие некоторую полосу частот от нижней граничной частоты f_1 до верхней граничной частоты f_2, могут быть представлены нормальным узкополосным случайным процессом:

$$x_2(t) = E(t)\,cos\big(\omega_0 t + \varphi(t)\big) \quad (2)$$

где: E(t) - огибающая с ненулевым средним, φ(t) – случайная начальная фаза, ω_0 – средняя частота случайного процесса.

Для работы такой системы необходимо, чтобы на приеме сигналы x_1 и x_2 разделялись между собой. Таким образом, основной задачей можно считать выделение сигнала x_1 из суммы сигналов x_1 и x_2. Этого можно добиться путем использования обычного устройства весовой обработки, состоящей из фазовращателя, умножителя и сумматора.

Сигнал, поступающий от источника информации и представленный, в нашем случае, обычным синусоидальным сигналом умножается на $\cos(\alpha_1)$, а шумовой сигнал, генерируемый передатчиком, умножается на $\cos(\alpha_2)$. В данном случае α_1 и α_2 - это углы линейной модуляции.

Таким образом, на выходе передатчика будет формироваться сигнал следующего вида:

$$S(t) = x_1(t) \cdot \cos(\alpha_1) + x_2(t) \cdot \cos(\alpha_2) \quad (3)$$

Данный сигнал после прохождения через канал связи, попадая на приемник, будет проходить ряд модификаций. На первом этапе сигнал S(t) разделяется на 2 части. Первая часть остается неизменной и будет обозначаться как $S_1(t)$, тогда как вторая часть проходит через преобразование Гилберта. Взяв мнимую часть от данного преобразования, можно получить сигнал следующего вида:

$$S_2(t) = x_1(t) \cdot \sin(\alpha_1) + x_2(t) \cdot \sin(\alpha_2) \quad (4)$$

Далее, сигналы $S_1(t)$ и $S_2(t)$ умножаются на $\cos(\beta)$ и $\sin(\beta)$ соответственно и находится сумма двух сигналов:

$$\begin{aligned} S'(t) = {} & x_1(t) \cdot \cos(\alpha_1) \cdot \cos(\beta) + x_2(t) \cdot \cos(\alpha_2) \cdot \cos(\beta) + \\ & + x_1(t) \cdot \sin(\alpha_1) \cdot \sin(\beta) + x_2(t) \cdot \sin(\alpha_2) \cdot \sin(\beta) = \\ & = x_1(t) \cdot \cos(\alpha_1 - \beta) + x_2(t) \cdot \cos(\alpha_2 - \beta) \end{aligned} \quad (5)$$

При условии, что $\beta=\alpha_2 \pm \pi/2$, будет происходить выделения из суммы первой части сигнала, а именно первоначального сигнала, несущего информацию. Таким образом, можно осуществить скрытую передачу сообщения. Данная обработка сигналов хорошо себя зарекомендовала в акустических системах при выделении зашумленных сигналов. Сама обработка является программной. [2,3]

Если получатель не знает углов линейной модуляции или же методов обработки сигнала, то получить полезную информацию из сообщения становится невозможным. Остается лишь проблема реальных помех в канале связи, из-за которых сигнал S(t) должен быть достаточно большим, а это в свою очередь приведет к тому, что сигнал будет выделяться на фоне естественных помех, хоть и его содержание будет скрытым от посторонних получателей. Еще одним недостатком такой передачи является использование широкополосного случайного сигнала, ведь не всегда имеется широкий диапазон частот, которые можно использовать и передать по каналу связи. [4,5]

Следовательно, следующим шагом улучшения такой системы будет привязывания ее к какому-либо конкретному несущему сигналу. За счет этого, сигнал S(t) можно будет сделать достаточно высоким, чтобы уменьшить влияние различных помех. А также даст возможность использовать модель реальных шумов, в качестве скрывающего сигнала $S_2(t)$.

Литература:
1. Максимов М.В. и др. Защита от радиопомех./ под ред. Максимова М.В., М.: Сов.радио, 1976, 496 с.
2. А.С. № 331927 от 01.11.91 Система связи с малоиндексной амплитудно – фазовой модуляцией, Ковалев Е.И., Астрецов Д.В., Лучинин А.С., Леонтьев А.А., Щепеткин Ф.В.
3. Патент РФ №2019039 от 05.05.94 Система для передачи и приема сигналов с одновременной амплитудной и частотной модуляцией. Ковалев Е.И., Астрецов Д.В., Лучинин А.С.
4. Ковалев Е.И., Моделирование алгоритма обработки сигналов с модуляцией по амплитуде и частоте (АЧМ) в присутствии широкого класса помех. Сб. региональной НПК «Безопасность информационного пространства», Екатеринбург, 2011. Тезисы доклада. 2 с.
5. Д.В. Астрецов. Помехоустойчивость некогерентной обработки флуктуирующего сигнала с амплитудно-угловой модуляцией двумя сообщениями при действии аддитивной широкополосной помехи// Теория, техника и экономика сетей связи. Сборник научно-технических и методических трудов. Выпуск 3. Екатеринбург, ГОУ ВПО «СибГУТИ», 2004.

А.А. Варисов, М.С Якубов

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗЛОУМЫШЛЕННИКА В ИНФОРМАЦИОННЫХ РЕСУРСАХ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Ташкентский университет информационных технологии г. Ташкент, Узбекистан

Ключевые слова: безопасность, информационные ресурсы, сеть, дерево, уязвимостей, ветвящиеся процессы.

Рассматриваются вопросы математическая модель злоумышленника для проникновение к информационным ресурсам правительства. Кроме этого, обсуждается вопросы об ошибках персонала предприятий при обработки данных. Рассмотрены проблемы источников информации в государстве их интерактивные услуги, системы обеспечение безопасности.

A.A. Varisov, M.S. Yakubov

MATHEMATICAL MODEL OF THE ATTACKER IN THE INFORMATION RESOURCES E-GOVERNMENT

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: security, information resources, network, wood, vulnerabilities, branching processes.

The problems of the mathematical model for the penetration of the attacker to the information resources of the government. In addition, the issues of human errors during data processing companies. The problems of information sources in their State of interactive services, system security.

В компьютеризации население без условно выигрывают весь сектор государства, но кроме этого возникают новые проблемы по поводу обмена потоками информации местного, а также регионального характера. И в решении таких задач нужно учитывать все важные стороны в обмене, обработки, а также передачи данных по важностью. Для исследования проблем безопасности и защищённости информационных ресурсов предлагается использовать модель действий злоумышленника, построенную на основе марковских ветвящихся процессов. С помощью модели определяются наиболее вероятные маршруты действий злоумышленника и рекомендации по закрытию уязвимых мест[3].

Введение:

Многочисленные исследования многих центров по безопасности информационных показывают, что 70-80% всех нарушений в информационных ресурсов (ИР) приходится на долю

внутренних нарушителей, а также владельца самой информации. Распределение долей основных источников приведено на рисунке 1.

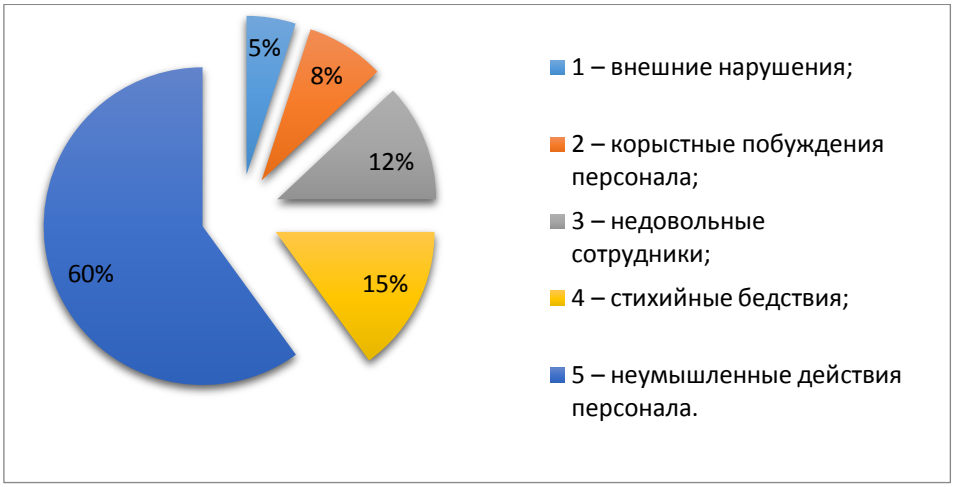


Рисунок 1. Распределение долей основных источников

Обеспечение безопасности ИР предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ИР, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов ИР – аппаратных средств, программного обеспечения, данных и персонала[2].

Злоумышленник обычно предваряет свои атаки предварительным зондированием всех компонентов ИР. На этом этапе он собирает информацию, которая является недоступной для него в рамках служебных полномочий. На практике злоумышленником определяются роли компьютеров в информационных сетях, выделяются файловые сервера и сервера баз данных, маршрутизаторы и интеллектуальные коммутаторы. На основе этой информации злоумышленником строится дерево уязвимостей ИР. И, что особенно важно, им выбирается инструментарий для проведения атак, например, подбираются эксплойты для осуществления непосредственно атак на узлы информационных ресурсов[1].

Основная модель.

Для построения математической модели злоумышленника ИР используются однородные марковские докритические ветвящиеся процессы.

Пусть случайные величины Z_0, Z_1, Z_2, … – число уязвимостей в нулевом, первом, втором, и.т.д. уровнях защиты информационных ресурсов, соответствуют числу вершин (состояний) корневого ориентированного дерева уязвимостей (дерева угроз). Дугам дерева уязвимостей приписаны вероятности перехода из состояния i-го уровня защиты в состояние (i+1)-го уровня. Длительность пребывания в каждом состоянии нулевого, первого, и.т.д. уровнях защиты равна соответственно T_0, T_1, T_2, … .

Если не оговаривается противное, то всегда полагается $Z_0=1$ с вероятностью 1 и математическое ожидание количества уязвимостей на первом уровне защиты $EZ_1<1$. Обозначим через P вероятностную меру процесса. Распределение вероятностей сл.в. Z_1 определяется числами $P\{Z_1=k\}=p_k$, $k=0, 1, 2, \ldots$; $\sum p_k=1$, где p_k интерпретируется как вероятность того, что уязвимость, существующая на первом уровне защиты, обеспечивает доступ к уязвимостям на втором уровне.

Условное распределение Z_{i+1} при условии $Z_i=k$, определяется из предположения, что разные уязвимости порождают другие уязвимости независимо. Отсюда вытекает, что Z_{i+1}распределена как сумма k независимых случайных величин, каждая из которых распределена так же, как Z_1. Если $Z_i=0$, то с вероятностью 1 $Z_{i+1}=0$.

Переходные вероятности рассматриваемого марковского процесса задаются в виде:

$$P_{ij}(\tau,t)=P\{Z_{n+1}(t)=j|Z_n(\tau)=i\},\ \text{i,j,n=0,1,2,}\ldots;\leq\tau\leq t. \qquad (1)$$

В процессе исследования модели (1) используются прямое и обратное уравнения Колмогорова (2), (3) и определяются распределение вероятностей и моменты случайной величины Z_t; вероятность того, что случайная последовательность Z_0, Z_1, Z_2, … сходится к нулю

(злоумышленник не может использовать уязвимости для проведения атак); поведение последовательности в случае, когда она не сходится к нулю, т.е. достигнет ли злоумышленник цели.

$$\begin{cases} \frac{\partial P_{ik}(\tau,t)}{\partial t} = -kb(t)P_{ik}(\tau,t) + b(t)\sum_{j=0}^{k+1} P_{ik}(\tau,t)jp_{k-j+1}(t) \\ P_{ik}(\tau,\tau+0) = \delta_{ik} \end{cases} \quad (2)$$

Здесь δ_{ik}=1 при k=i, а δ_{ik}=0 при $k \neq$i.

$$\begin{cases} \frac{\partial P_{ik}(\tau,t)}{\partial t} = -ib(t\tau)P_{ik}(\tau,t) - ib(\tau)\sum_{j=i-1}^{\infty} P_{ik}(\tau,t)p_{j-i+1}(\tau), i \\ \frac{\partial P_{0k}(\tau,t)}{\partial t} = 0, P_{ik}(\mathrm{t}-0,\mathrm{t}) = \delta_{ik} \end{cases} \quad (3)$$

где $b(t)\Delta + 0(\Delta)$–вероятность, что уязвимость, которая в момент времени t используется злоумышленником для своей атаки, к моменту времени (t+Δ) завершится успехом. Если уязвимость используется в момент τ, то с вероятностями $p_0(\tau)$, $p_2(\tau)$, $p_3(\tau)$, … злоумышленнику становятся доступны 0, 1, 2, 3, … новых уязвимостей. В соответствии с [2] определяются величины $b_i(t)$=i b(t) и $p_{ij}(t)=p_{j-i+1}(t)$. Часто вместо переходных вероятностей однородного ветвящегося процесса используются соответствующие производящие функции.

Производящая функция однородного ветвящегося процесса имеет вид:

$$f(t,z) \;\; = \sum_{k=0}^{\infty} P_k(t)z^k \; f_i(t,z) = \sum_{j=0}^{\infty} P_{ik}(t)z^j \quad (4)$$

где 1≤z и $p_k(t)=P(Z_t=k)$; с учетом (2) имеет место следующее равенство (5):

$$f_i(t,z)=[f(t,z)]^j \quad (5)$$

При решении таких задач, как определение моментов величин Z_t или вычисление вероятности того, что злоумышленник не сможет использовать уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей[3]. В исследованиях используются три основных типа: двоичное, троичное и m-арное деревья уязвимостей (могут быть использованы и их комбинации):

- если дерево уязвимостей ИР является двоичным, то злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью p_1=x, а правую — с p_2=y. Вероятности x и y выбираются из условий:

$$\begin{cases} 0 < x < 1, \\ \frac{x(1-x)}{2} < y \leq \mathrm{x}(1-\mathrm{x}) \end{cases}$$

- если дерево уязвимостей ИР является троичным деревом, злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью p_1=x, а правую с вероятность p_3=y. вероятности x и y выбираются из условий (1):

$$\begin{cases} 0 < x < 1, \\ 0 < y \leq \mathrm{x}(1-x)^2 \text{если } 0 < x \leq \frac{1}{2}; \\ y \leq \frac{\mathrm{x}(1-\mathrm{x})(3-2\mathrm{x})}{4}, \text{если} \frac{1}{2} < x < 1; \\ y > x(1-x)(2-x)/6\,, \text{если} 0 < x \leq 2/3; \\ \mathrm{y} > (12-12\mathrm{x}-\mathrm{x}2)/48, \text{если } 2/3 < \mathrm{x} < 6/7; \\ \mathrm{y} \geq \mathrm{x}(1-\mathrm{x})2, \text{если } 6/7 \leq \mathrm{x} < 1. \end{cases}$$

- если дерево уязвимостей ИР является m-арным деревом то злоумышленник выбирает для атаки уязвимости {1, 2, …, m; b_1,…,b_m}, где $p_1=b_1$, $p_2=b_2$, …, $p_m=b_m$, m≥3 с учётом выполнения следующей системы неравенств:

$$\begin{cases} 0 < b_1 < 1, \\ \dfrac{b_1(1-b_1)}{2} < b_2 \le b_1(1-b_1), \\ max\{0,(n+1)\beta_n - \alpha_n\} \le v_n \le \beta_n, n = 2, \dots, m-1, \end{cases}$$

где $\alpha_1=\beta_1(1-\lambda)$, $\beta_1=b_1(1-\sigma)$

$$\alpha_n = \alpha_2 - \sum_{k=0}^{n-1} k v_k \quad \beta_n = \beta_2 - \sum_{k=0}^{n-1} v_k$$

$$\sigma = \frac{b_1}{b_1^2 + 2b_2}, \lambda = b_1\ \sigma, \mathrm{n} = 3, \dots, \mathrm{m}.$$

Вероятности b_k, k=3, 4, …, m находятся из равенства:

$$v^k = (k-\lambda)b_k - (k+1)\sigma b_{k+1} - \frac{1}{b_1}\sum_{n=2}^{k-1}(k-n+1)v_n b_{k-n+1}$$

Результаты моделирования

Программа математической модели злоумышленника ИР реализована в среде Microsoft Visual Studio.NET 2005 на языке C#. Результаты моделирования действий злоумышленника в ИР приведены в экранной копии пользовательского интерфейса модели (см. рисунок.2)

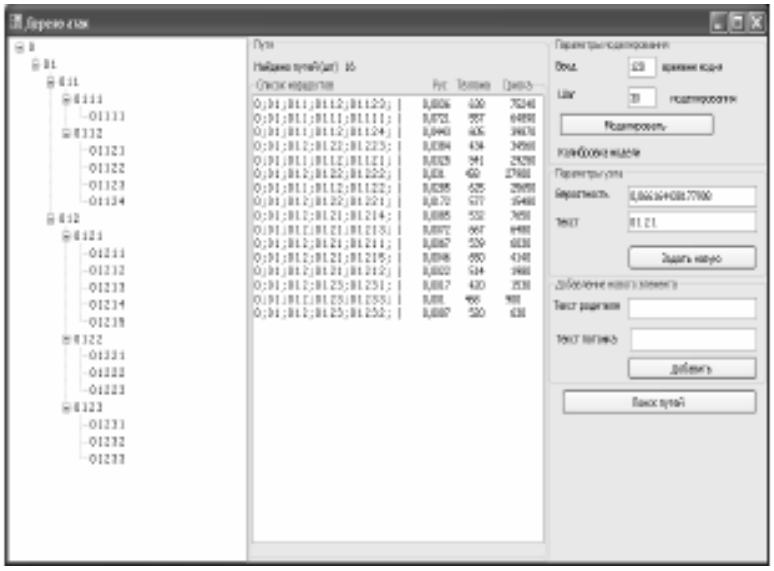


Рисунок 2. Пользовательский интерфейс модели (экранная копия)

Подсистема защиты ИР характеризуется пятью уровнями защиты, корневым деревом уязвимостей Z_0, Z_1, Z_2, Z_3, Z_4, длительности пребывания в каждом состоянии τ_0, τ_1, τ_2, τ_3, τ_4 (задается случайными числами, имеющими равномерное распределение на интервале 0-1000 сек.), располагаемое время для проведения атаки $T_{зад}$=800 сек. Стоимость защищаемой информации составляет 900 000. Основные результаты: максимальная вероятность достижения злоумышленником цели за $T_{зад}$,: $P_{ус}$=0,0836; время, затраченное злоумышленником на достижение цели, $T_{взлома}$=638 сек и степень риска составляет, $C_{риска}$=75 240. На основе этих результатов делаются рекомендации по модернизации средств защиты уязвимостей: 0; 01; 011; 0112; 01123.

Литература:

1. П.Б. Хорев. Методы и средства защиты информации в компьютерных системах. г. Москва 2005. с. 60-109.

2. Т. Харрис. Теория ветвившихся случайных процессов. Мир, 1996 с.-355

3. С.К. Ганиев, М.М. Каримов, К.А. Ташев. Информационная безопасность. г.Ташкент 2013 с.295-332

А.С. Виржанский

АНАЛИЗ И МЕТОДЫ ЗАЩИТЫ КАНАЛОВ СВЯЗИ

Ростовский государственный экономический университет (РИНХ),
г. Ростов-на-Дону, Россия

Ключевые слова: каналы связи, угрозы, утечка, анализ, прослушивание, система передачи.

Приведены основные виды каналов связи. Описаны методы поиска и устранения проблем в сфере защиты каналов связи. Рассмотрены основные виды угроз в сфере передачи по каналам связи. Приведены требования по подбору персонала для обслуживания систем передачи информации посредством каналов связи и методов мониторинга уязвимостей данной системы. Рассмотрен принцип работы программно-аппаратного комплекса Цикады М.

A.S. Virzhanskiy

ANALYSIS AND PROTECTION METHODS OF COMMUNICATION CHANNELS

Rostov State University of Economics (RINH), Rostov-on-Don, Russia

Keywords: communication channels, threats, leak, analysis, listening, transmission system.

The main types of communication channels. Views are described for troubleshooting in the field of protection of communication channels . The main types of threats in the field of communication channel . These are the requirements for the selection of personnel for service information transmission systems by means of communication channels and methods for monitoring the vulnerabilities of the system. View of operation Cicadas M.

Главной целью данной статьи является поиск уязвимых мест, устранение или предотвращение утечек информации, передающиеся через проводные или беспроводные каналы связи.

В данное время существует два вида каналов связи: проводные и беспроводные. Основными их характеристикой является надежность, так как передатчик и приёмник информации являются основной аппаратурой, связывающей источник информации с каналом связи, может подвергаться опасности со стороны злоумышленников.

Основными угрозами каналов связи являются:

- незаконное подключение специальной аппаратуры к устройствам системы или линиям связи.
- утечка информации во время приёма акустических сигналов, подслушивание разговоров с помощью технических средств радиоперехвата.
- IP-спуфинг[1].
- DDoS атаки[2],
- использование программных средств, для считывания информации и другие угрозы.

Чтобы проанализировать места утечки информации, потребуется классифицировать нарушителей [1]. Всех злоумышленников можно квалифицировать так (табл. 1):

[1] IP-спуфинг – Вид хакерской атаки, заключающийся в использовании чужого IP-адреса с целью обмана системы безопасности. [4].

[2] DDoS атака - хакерская атака на вычислительную систему с целью довести её до отказа.[5]

Таблица 1. Классификация злоумышленников сети

Номер группы	Уровень классификации	Описание
1	По уровню знаний информационной системы	Преступники должны иметь опыт в области работы технических средств и её обслуживания, знать механизмы действия средств защиты.
2	По уровню возможностей	Мошенники применяют пассивные средства перехвата, используют недостатки систем защиты.
3	По месту действия	Внутри помещения без доступа к техническим средствам или с доступом в зону данных.

При изучении типов злоумышленников, можно сказать, что уязвимость каналов связи – это места, которые могут использоваться угрозой для своей реализации. Уменьшение или ограничение этих мест может снизить или устранить риск от угроз информационной системы.

Как проводить анализ угроз и каналов утечки информации?

Анализировать опасность стоит на стадии проектирования локальной сети, так как она очень подвержена атакам [3]. В большинстве случаев проведения анализа возможных опасностей позволяет персоналу осознать проблему, которые могут появиться во время работы, что позволяет усилить программу управления рисками.

Кроме того (по-моему мнению) в рабочую группу, призванную проанализировать опасные ситуации, следует нанять следующие группы лиц:

- Аналитика по опасным ситуациям, ответственного за сбор данных, необходимых для выбора защитных мероприятий.
- Служащих, занимающихся эксплуатацией здания. Они должны будут предоставлять информацию руководству о проблемах, связанных с окружающей средой.
- Пользователей, ответственных за использование приложений и программ.
- Персонал сопровождения сети. Они будут обязаны информировать об аппаратном состоянии и программном обеспечении техники передачи информации.

Для конфиденциальности информации, передаваемой, через каналы связи используют средства криптографической защиты или средства физической защиты, такие как Цикада М и другие аппараты [2]. Цикада М предназначена для защиты помещение, где есть проводные линии связи, которые можно прослушать, с помощью средств добывания акустической информации.

Принцип работы программно-аппаратного комплекса Цикада М. В линию подаётся шумовая помеха. Из-за неё злоумышленник, с помощью средств считывания информации, слышит сильные посторонние шумы. И разговаривающие слышат незначительный шум, не мешающий разговору, благодаря фильтрации выходного сигнала.

На рис. 1 приведен алгоритм работы комплекса Цикада-М (метод маскирующей низкочастотной помехи).

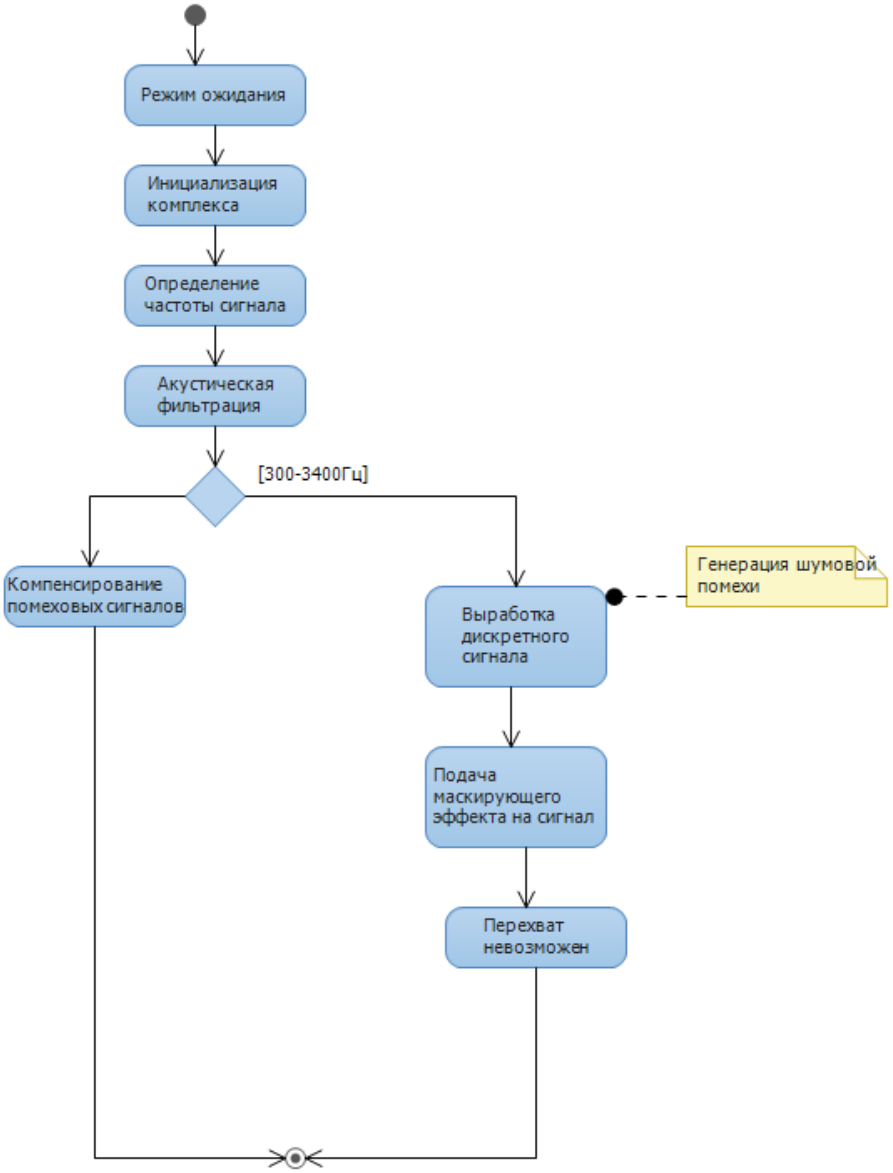


Рисунок 1. Алгоритм работы комплекса Цикада-М
(метод маскирующей низкочастотной помехи)

Вывод: Информация должна оставаться конфиденциальной не только в процессе перемещения, но и при отправке и приёме. Не следует забывать о возможности прослушивания по проводным каналам связи, и проникновения в беспроводную сеть.

Каналы связи являются техническими средствами распространения сигналов для передачи данных от источника к получателю.

Литература:

1. Биячуев Т.А. Безопасность корпоративных сетей /Под ред. Л.Г.Осовецкого. - СПб: СПб ГУ ИТМО, 2009. - 420 с. - ISBN: 5-279-02549-6

2. Гришина Н. В. Организация комплексной системы защиты информации. -- М.: Гелиос АРВ, 2007. - 256 с,

3. // Материалы сайта «Википедия - свободная энциклопедия». [Электронный ресурс]. - Режим доступа: http://ru.Wikipedia.org.

4. // Материалы сайта «Википедия - свободная энциклопедия». [Электронный ресурс]. - Режим доступа: http://ru.wikipedia.org/wiki/IP-спуфинг.

5. // Материалы сайта «Википедия - свободная энциклопедия». [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/DoS-%E0%F2%E0%EA%E0

Д.А. Воронин, М.Г. Гизатуллин

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ И СЕТЯХ МОБИЛЬНОЙ СВЯЗИ

Уральский юридический институт МВД России, г. Екатеринбург, Россия

Ключевые слова: информационная безопасность, мобильные системы и сети связи, радиоинтерфейс, базовая станция, мобильная станция.

Интегральный подход к обеспечению информационной безопасности в телекоммуникационных системах и сетях связи предполагает в первую очередь выявление возможных различного рода угроз и атак. Общей целью разработки типовых моделей угроз информационно-технической безопасности телекоммуникационных систем и сетей связи является определение совокупности основных значительных угроз, способов и средств их осуществления, уровня допустимых потерь, связанных с возможными проявлениями угроз в типовых условиях применения. В статье рассмотрена модель угроз информационно-технической безопасности систем и сетей мобильной связи.

D.A. Voronin, M.G. Gizatullin

THREATS OF INFORMATION SECURITY IN SYSTEMS AND NETWORKS OF MOBILE COMMUNICATION

Ural law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia

Keywords: information security, mobile systems and communication networks, radio interface, base station, mobile station.

Integrated approach to providing it is information safety in telecommunication systems and communication networks assumes first of all identification of possible different threats and attacks. An overall objective of development of standard models of threats of information and technical safety of telecommunication systems and communication networks is determination of set of the main considerable threats, ways and means of their implementation, level of the admissible losses connected with possible manifestations of threats in standard conditions of application. In article the model of threats of information and technical safety of systems and networks of mobile communication is considered.

Рассмотрим модель угроз информационно-технической безопасности систем и сетей мобильной связи. Общий комплекс угроз информационно-технической безопасности систем и сетей мобильной связи характеризуется следующими аспектами:

1. Угрозы информационному трафику систем и сетей мобильной связи – угрозы, направленные на индивидуальные сообщения пользователей сети. Объектом атаки может служить информационный обмен: между пользователями, между операторами связи, между пользователями и «сервис-провайдерами». Угрозы информационному трафику систем и сетей мобильной связи включают в себя:

1.1. Перехват информации. Объекты такой атаки: голосовые сообщения (конфиденциальная информация), системная информация управления (данные пользовательской авторизации, местоположения, уровня приоритетности, вида сервисов и т.д.), информация безопасности (ключи шифрования и аутентификации и др.). Результаты рассмотренной атаки могут использоваться для создания других видов угроз, в частности при осуществлении маскировки под другого пользователя или для несанкционированного управления данными. Несанкционированный перехват информации в радиоинтерфейсе между базовой станцией и мобильной станцией систем и сетей мобильной связи не может быть обнаружен или полностью предотвращен механизмами безопасности.

Данный вид угроз включает в себя:

– перехват в радиоинтерфейсе систем и сетей мобильной связи. Осуществляется с помощью сканеров, обладающих возможностью декодирования цифровых радиосигналов соответствующих протоколов, также абонент сети может

использовать свое терминальное оборудование для прослушивания информационных каналов. Сформулируем механизмы защиты от перехвата в радиоинтерфейсе: взаимная аутентификация через радиоинтерфейс между базовой станцией и мобильной станцией; шифрование радиоинтерфейса между базовой станцией и мобильной станцией; реализация «прозрачного» шифрования; применение механизма периодической смены ключей шифрования через радиоинтерфейс;

- перехват в проводном интерфейсе систем и сетей мобильной связи. В отличие от угрозы перехвата в радиоинтерфейсе для перехвата в проводном интерфейсе необходимо получение доступа к физическим объектам или проводным линиям. Атака осуществляется с использованием стандартизованного анализатора протокола и нуждается в физическом доступе к сетевому узлу, например, к базовой станции. Сформулируем механизмы защиты от перехвата в проводном интерфейсе: реализация «прозрачного» шифрования; обеспечение защиты информации на базовой станции;
- несанкционированное воспроизведение соответствующей информации. Данный вид атак является следствием осуществления перехвата и состоит в раскрытии конфиденциальной или служебной информации. Сформулируем механизмы защиты от несанкционированного воспроизведения информации: применение механизма периодической смены ключей шифрования через соответствующий радиоинтерфейс; введение в информационный поток избыточных (дополнительных) данных.

1.2. Маскировка, специальный вариант данной угрозы – маскировка под объект системы на интерфейсе, который не постоянно устанавливает соединение, например, межсистемный интерфейс между двумя системами и сетями мобильной связи различных стандартов. При осуществлении маскировки интерес для злоумышленников представляют данные системной безопасности. Данный тип угрозы включает в себя:

- маскировка под другой терминал (или пользователя). Этот тип атак может осуществляться как в проводном, так и в радиоинтерфейсе для получения информации, предназначенной этому пользователю. Данный вид атак может быть выявлен различными способами, например, с помощью переустановки данных;
- маскировка под базовую станцию систем и сетей мобильной связи для получения необходимых вызовов. Данный вид атак достаточно дорогой с точки зрения затрат и необходимого уровня компетентности, поэтому применяется, в основном, преступными группировками.

Сформулируем механизмы защиты от маскировки: взаимная аутентификация через радиоинтерфейс между базовой станцией и мобильной станцией; шифрование радиоинтерфейса между базовой станцией и мобильной станцией; применение механизма периодической смены ключей шифрования через соответствующий радиоинтерфейс.

1.3. Манипуляция информацией – такой вид угроз, заключающихся в возможности несанкционированного изменения информации в системе. Манипуляция информацией включает в себя:

- манипуляция информацией в радиоинтерфейсе систем и сетей мобильной связи. Характерные особенности данной атаки: у злоумышленников отсутствует возможность повторного запроса информационного трафика, соответственно удалить его можно лишь косвенным путем, например, переполнением декодера ошибочными символами; умышленные вставки новых данных и голосовых сигналов возможны только в паузах передачи, для этого применяется маскировка под пользователя или базовую станцию. Не обязательно расшифровывать сообщения, достаточно их модифицировать вставками. Данный тип угроз может распространяться и на механизмы аутентификации, когда путем переустановки некоторых аутентификационных данных (например, идентификаторов и паролей), происходит срыв опознавательных процедур; в случае голосового вызова, в случае, когда обе стороны связи знают друг друга, возможным нападением есть запись некоторых фрагментов. Если стороны сеанса связи не знакомы друг с другом или не гарантирована точная идентификация голоса, возможна вставка собственного голоса злоумышленника. Сформулируем механизмы защиты от манипуляции информацией

в радиоинтерфейсе: взаимная аутентификация через радиоинтерфейс между базовой станцией и мобильной станцией; шифрование радиоинтерфейса между базовой станцией и мобильной станцией; реализация «прозрачного» шифрования; применение механизма периодической смены ключей шифрования через соответствующий радиоинтерфейс;

– манипуляция информацией в кабельном интерфейсе систем и сетей мобильной связи. Данный тип угроз возможен при использовании оборудования, обеспечивающего доступ к управлению данными и голосовым трафиком. Данный тип атак требует хорошего знания внутренней работы системы, поэтому злоумышленником может быть и лицо из штата обслуживающего персонала. Возможны следующие атаки: простые изменения информации; удаления или вставки частей сообщения; запрос новой передачи сообщений. Сформулируем механизмы защиты от манипуляции информацией в кабельном интерфейсе: взаимная аутентификация через интерфейс между базовой станцией и центром коммутации и управления; реализация «прозрачного» шифрования.

1.4. Отказ от информации, данный вид угроз, при которых одна из сторон, вовлеченных в информационный обмен, отвергает (возможно, частично), свое участие в сеансе связи. Потенциальные злоумышленники являются обычными пользователями сети, отправителями и получателями трафика. Отказ от информации включает в себя:

– отказ от посылки информации – это тип угроз, при котором отправитель отрицает свое участие в сеансе связи. Сформулируем механизмы защиты от данного типа угроз: взаимная аутентификация через интерфейс между базовой станцией и Центром коммутации и управления; использование конкретных криптографических алгоритмов; разносторонняя регистрация трафика;

– отказ от получения информации – это тип угроз, при котором получатель отрицает свое участие в сеансе связи. Сформулируем механизмы защиты от данного типа угроз: взаимная аутентификация через интерфейс между базовой станцией и центром коммутации и управления; использование конкретных криптографических алгоритмов; разносторонняя регистрация трафика.

2. Угрозы служебному трафику систем и сетей мобильной связи – угрозы, направленные на изучение общего поведения пользователей с системами и сетями мобильной связи. Угрозы служебному трафику включают в себя:

2.1. Анализ трафика в системах и сетях мобильной связи. Для данного типа угроз первоочередной интерес представляет информация о характере передаваемой информации, а также об определенных информационных блоках, переданных в определенное время на определенных интерфейсах. Злоумышленники могут пользоваться теми же средствами, что и в случае перехвата. Объекты атаки при анализе трафика в системах и сетях мобильной связи: скорость передачи информации; длина информационных блоков; авторизация отправителя и получателя; другая информация. Сформулируем механизмы защиты от анализа трафика: взаимная аутентификация через радиоинтерфейс между базовой станцией и мобильной станцией; шифрование радиоинтерфейса между базовой станцией и мобильной станцией; реализация «прозрачного» шифрования (от терминала до терминала); применение механизма периодической смены ключей шифрования через соответствующий радиоинтерфейс; реализация и вставка фиктивных сообщений; введение информационной избыточности (дополнительных элементов).

2.2. Наблюдаемость в системах и сетях мобильной связи – означает, что поведение определенных (не обязательно известных) пользователей в сети может находиться под постоянным наблюдением. Объекты атаки наблюдаемости: типичное время осуществления вызовов; местоположение пользователя; принадлежность пользователя к абонентским группам; уровень приоритета; другое. Сформулируем механизмы защиты от наблюдаемости: применение временных идентификаций; реализация и использование механизмов периодической смены абонентской авторизации.

3. Угрозы системным связям систем и сетей мобильной связи – угрозы, направленные на системы и сети мобильной связи в целом. Атаки данного класса служат для того, чтобы повредить целостность системы, получить доступ к системным ресурсам или модифицировать ее функциональные возможности. Угрозы системным связям систем и сетей мобильной связи включают в себя:

3.1. Повреждение обслуживания в системах и сетях мобильной связи – угрозы преднамеренной блокировки обслуживания или вывода его из строя злоумышленниками. Другие виды угроз из данного класса – изменение конфигурации системы, преднамеренное создание заторов или злоупотребление дополнительным обслуживанием. Сформулируем механизмы защиты от анализа трафика: применение информационной избыточности (дополнительные элементы); обеспечение гибкости системы; разносторонняя ревизия функционирования сети.

3.2. Несанкционированное или запрещенное использование ресурсов систем и сетей мобильной связи. Ресурсы – весь комплекс технических средств систем и сетей мобильной связи, например, радиоканалы, оборудование, сервисы или системные базы данных. Сценарии реализации данных угроз: злоумышленник может производить маскировку под другого пользователя и реализовывать права доступа этого пользователя к запрещенным ресурсам; злоумышленник может использовать украденное или непрошедшее сертификацию оборудование; злоумышленник с достаточным знанием работы системы может приобретать дополнительные права доступа или обходить механизмы управления доступом. Сформулируем механизмы защиты от несанкционированного или запрещенного использования ресурсов: реализация и использование надежных механизмов пользовательской и операторской авторизации; администрирование соответствующих прав доступа.

3.3. Использование неуполномоченных ресурсов систем и сетей мобильной связи. Данный тип угроз возникает тогда, когда пользователь имеет право использования некоторых системных ресурсов, однако он начинает превышать предоставленные ему полномочия. Сценарии реализации данных угроз: злоумышленник может использовать по своему усмотрению некоторую системную информацию, например, оператор связи или «сервис-провайдер» может некорректно использовать персональные данные пользователей – абонентов; системное оборудование может быть использовано вне уполномоченных прав доступа и обслуживания; атаки могут быть направлены против организации доступа с целью перераспределения уровней приоритета, несанкционированно создавать льготные права доступа некоторым категориям пользователей и т.п. Сформулируем механизмы защиты от использования неуполномоченных ресурсов: взаимная аутентификация через радиоинтерфейс между базовой станцией и мобильной станцией; администрирование соответствующих функций и прав доступа; разносторонняя ревизия работы системы.

Литература:

1. Федеральный закон Российской Федерации от 07 июля 2003 г. №126-ФЗ. «О связи». – Режим доступа: http://garant.ru/

2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи. – М.: Горячая линия-Телеком, 2007, 360 с.

3. Официальный сайт Министерства связи и массовых коммуникаций Российской Федерации. – Режим доступа: http://minsvyaz.ru/

Р.Т. Гаипназаров, Н.С. Таджиев

АНАЛИЗ СЕТЕВЫХ УГРОЗ НА ВЕБ-САЙТЫ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: угрозы, сетевые атаки, информационная безопасность, информационно-коммуникационные системы, электронная почта.

Анализированы виды типовых угроз на веб-сайты, которые представляют собой возможные уязвимости программного обеспечения, а также ошибки в работе различных серверов.

R.T. Gaipnazarov, N.S. Tadjiev

ANALYSIS OF NETWORK THREATS ON THE WEBSITE

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: threats, network attacks, information security, information and communication systems, e-mail.

Analyze the types of threat to Web sites that are potential software vulnerabilities, as well as errors in the various servers.

В настоящее время неотъемлемой частью инфокоммуникационных технологий является глобальная сеть Internet. Конечно же, одной из главных задач является обеспечение безопасности обращения информации внутри сети. Одной из опасностей для безопасности являются сетевые атаки.

Сетевая атака - действие, целью которого является захват контроля над удалённой локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей пользующихся этой удалённой локальной вычислительной системой.

На данный момент выделяют следующие атаки:mail bombing, переполнение буфера, использование специализированных программ (вирусов, сиверов, троянских коней, почтовых червей, rootkit-во и т.д.), сетевая разведка,IP-спулинг, man-in-the-middle, инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), отказ в обслуживании (DoS- и DDoS- атаки), phishing-атаки. Рассмотрим каждую из них.

Mail bombing. Суть данной атаки заключается в том, что на почтовый ящик посылается огромное количество писем на почтовый ящик пользователя. Эта атака может вызвать отказ работы почтового ящика или даже целого почтового сервера. Данная атака может проводиться любым хотя бы немного подготовленным противником. Простым примером программы, с помощью которой можно осуществить подобную атаку- The Unabomber. Достаточно знать адрес сервера, позволяющего анонимно отправлять почтовые сообщения, и адрес пользователя, которому эти сообщения предназначены. Количество писем, которое можно отослать для этой программы равно 12 разрядному числу. Рассмотрим способы защиты от данной атаки.

1. Давать адрес электронной почты только проверенным источникам.
2. В качестве преграды для mail bombinga может выступать и Веб-сайт провайдера, иногда настраиваемый таким образом, чтобы он автоматически определял почтовые атаки. В большинстве случаев они распознаются сервером посредством сравнения исходных IP-адресов входящих сообщений. Если количество сообщений из одного источника превышает некие разумные пределы, то все они автоматически поступают в RecycleBin на сервере. Конечно же, ничто не мешает злоумышленнику фальсифицировать собственный IP-адрес [1].

Переполнение буфера(buffe rover flows). Атака на переполнение буфера основывается на поиске программных или системных уязвимостей, способных вызвать нарушение границ памяти и аварийное завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа работает под учетной записью администратора, то данная атака может позволить получить полный контроль над компьютером, на котором исполняется данная программа [2].

Реализации атаки требует решения двух подзадач:

1. Подготовка кода, который будет выполняться в контексте привилегированной программы.
2. Изменение последовательности выполнения программы с передачей управления подготовленному коду.

Классификация атак по переполнению буфера представлена в таблице.

Использование специализированных программ. Рабочие станции конечных пользователей очень уязвимы для вирусов и троянских коней. Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. В качестве примера можно привести вирус, который

прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com.

Таблица 1. Классификация атак по переполнению буфера

Подготовка кода Цель переполнения	Внедрение кода	Внедрение параметров	Не требуется
Искажение адреса возврата из функции	Атака “срыв стека”	Атака “срыв стека” с параметризацией	Атака “срыв стека” с передачей управления
Искажение указателей функций	Атака на указатели функций	Атака на указатели функций с параметризацией	Атака на указатели функций с передачей управления
Искажение таблиц переходов	Атака на таблицы переходов	Атака на таблицы переходов с параметризацией	Атака на таблицы переходов с передачей управления
Искажение указателей данных	Атака с искажением указателей данных	Атака с искажением указателей данных с параметризацией	Атака с искажением указателей данных с оригинальным кодом

«Троянский конь» - это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле выполняет вредную роль. Примером типичного «троянского коня» является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение [2].

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuousmode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам [1].

Root kit - программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. Большинство из реализаций современных rootkit могут прятать от пользователя файлы, папки и ключи реестра, скрывать запущенные программы, системные службы, драйверы и сетевые соединения. Т.е. злоумышленник имеет возможность создавать файлы и ключи реестра, запускать программы, работать с сетью и эта активность не будет обнаружена администратором. Кроме того, rootkits могут скрывать сетевую активность путем модификации стека протоколов TCP/IP. Так, например rootkit Hacker Defender перехватывает вызовы Winsock и может обрабатывать сетевой трафик до того как он будет передан приложению. Т.е. если в системе установлен веб сервер, и соответственно открыт 80й порт, rootkit может использовать его для взаимодействия с взломщиком, в то время как другие пользователи будут без проблем работать по протоколу HTTP [3].

Сетевая разведка. Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (pingsweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену

присвоены. Эхо-тестирование (pingsweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, злоумышленник анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома[3].

IP-спуфинг происходит, когда злоумышленник, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность злоумышленника.

Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик наложный IP-адрес, злоумышленник получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Для *атаки типа Man-in-the-Middle* злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии [3].

SQL-инъекция – это атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос приобретает совершенно иной смысл, и в случае недостаточной фильтрации входных данных способен не только произвести вывод конфиденциальной информации, но и изменить удалить данные [4].

PHP-инъекция - один из способов взлома веб-сайтов, работающих на PHP. Он заключается в том, чтобы внедрить специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд [4].

XPath-инъекция - вид уязвимостей, который заключается во внедрении XPath-выражений в оригинальный запрос к базе данных XML. XPath (XML PathLanguage) – это язык, который предназначен для произвольного обращения к частям XML документа. XML (eXtensibleMarkupLanguage) – это всем известный язык разметки, с помощью которого создаются XML документы, имеющие древовидную структуру.

Отказ в обслуживании (DoS- и DDoS- атаки). DoS, без всякого сомнения, является наиболее известной формой атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди злоумышленников атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

Phishing (фишинг) - процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют spam или компьютеры-боты. При этом размер компании-жертвы не имеет значения; качество личной информации полученной преступниками в результате нападения, имеет значение само по себе [4].

Анализ угроз сетевых атак даёт возможность выборов необходимых средств для защиты информации. Несмотря на возможное применение комплексных мер по защите компьютера, наиболее надежным способом защиты компьютера является использование проверенных электронных ресурсов, чтение писем из проверенных источников. Т.е. наибольшую защиту от атак может обеспечить сам пользователь, соблюдая меры предосторожности.

Литература:
А. В. Соколов, В. Ф. Шаньгин Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г. Internet URL h.com/hacker-dictionaryHacker Dictionaryttp://www.robergraham
В. Зима, А. Молдовян, Н. Молдовян Безопасность глобальных сетевых технологий, БХВ-Санкт-Петербург, 368 стр., 2002 г.
А.В. Лукацкий Обнаружение атак, БХВ-Санкт-Петербург, 596 стр., 2003 г.
И. Д. Медведковский, Б. В. Семьянов, Д. Г. Леонов, А. В. Лукацкий Атака из Internet, 368 стр., 2002 г.

М.Г. Гизатуллин, Д.С. Милютин

НЕКОТОРЫЕ АСПЕКТЫ, СВЯЗАННЫЕ С СОВЕРШЕНСТВОВАНИЕМ МЕХАНИЗМОВ БОРЬБЫ С «ВЫЗОВАМИ» ИНФОРМАЦИОННОГО МИРА

Уральский юридический институт МВД России, г. Екатеринбург, Россия

Ключевые слова: оператор связи, база данных информации, персональные данные, субъект персональных данных.

В статье рассматриваются общие вопросы возникновения «новых» угроз безопасности (вызовов) информации личности, общества, государства, которые в свою очередь усугубляются массовостью и трансграничностью потоков информации, передаваемых по различным каналам связи и т.д. Рассматриваемые в статье вопросы раскрываются с точки зрения действующих правовых норм российского законодательства в данной предметной области (области обеспечения защиты прав субъектов персональных данных), это, в свою очередь, дает нам предпосылки полагать, что при реализации норм права нельзя «замыкаться» в рамках одной страны, необходимо двигаться по пути международного взаимодействия.

M.G. Gizatullin, D.S. Milutin

SOME ASPECTS CONNECTED WITH IMPROVEMENT OF MECHANISMS OF FIGHT AGAINST «CALLS» OF THE INFORMATION WORLD

Ural law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia

Keywords: telecom operator, information database, personal information, subject of personal information.

In article the general questions of emergence of «new» threats to security (calls) of information of the personality, society, state which are in turn aggravated with mass character and a transgranichnost of the flows of information transferred on various communication channels, etc. are considered. The questions considered in article reveal from the point of view of the existing precepts of law of the Russian legislation in this subject domain (area of ensuring protection of the rights of subjects of personal information), it, in turn, gives us prerequisites to believe that at realization of rules of law it is impossible «to become isolated» within one country, it is necessary to move on the way of the international interaction.

Рассматривая современное общество, нельзя не отметить факт того, что существующие на сегодняшний день технологии, использующиеся повсеместно различными категориями пользователей во всех сферах деятельности с целью удовлетворения их информационных потребностей развиваются достаточно стремительно.

Более чем двадцать лет назад, различного типа устройства, например, сотовой (мобильной) связи были несомненной роскошью их обладателей, однако уже сегодня, в век информационных

технологий, использование подобного типа устройств и их аналогов, обладающих расширенным арсеналом возможностей, становится повсеместным и общепринятым явлением.

За удобством, простотой и легкостью использования современных информационных технологий порой «скрывается» регулярная и нередко бесконтрольная обработка персональных данных. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Изменения в данной области происходят все быстрее и требуют адекватного реагирования со стороны государства. Институт защиты прав субъектов персональных данных в Российской Федерации достаточно молод. Российская Федерация находится на пути совершенствования механизмов борьбы с различного рода появляющимися и возникающими вызовами. За 2014 г. в Российской Федерации произошел ряд существенных изменений в данной области, были предприняты «шаги» на пути защиты субъектов персональных данных и обеспечения безопасности (неприкосновенности) частной жизни. Принятый федеральный закон Российской Федерации от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» «отвечает» тем существующим вызовам информационного мира, которые являются актуальными на сегодняшний день. Согласно федеральному закону Российской Федерации от 21 июля 2014 г. № 242-ФЗ, базы данных информации, содержащие персональные данные граждан Российской Федерации должны находиться (размещаться) на федеральных серверах, находящихся на территории Российской Федерации. Мобилизация баз данных информации на территории Российской Федерации не является чем-то новым. Аналогичные требования по размещению баз данных информации (содержащих персональные данные граждан) размещающихся на серверах, находящихся на территории страны реализованы, например, в Китае, Индии, Сингапуре. Актуальность федерального закона Российской Федерации от 21 июля 2014 г. № 242-ФЗ обусловлена необходимостью исключить возможность «перевода» персональных данных граждан Российской Федерации на территории, не обеспечивающие «адекватной» защиты личной информации и не исполняющие требований российской юрисдикции. Данный федеральный закон Российской Федерации имел достаточно «громкий» общественный резонанс, однако, в целом, все обсуждения были связаны с опасениями операторов связи полного запрета на трансграничную передачу персональных данных клиентов, а также с некомпетентными предположениями, что данный федеральный закон Российской Федерации ввел ограничения прав граждан на свободное использование личной информации. Такого рода заявления не подкрепляются аргументированными доводами и не имеют отношение к реальной действительности. Российская Федерация при ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных взяла на себя ряд обязательств. Одним из обязательств является недопущение запрета трансграничных потоков персональных данных. Российская Федерация неукоснительно соблюдает требования Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и намерена соблюдать их впредь. Федеральный закон Российской Федерации от 21 июля 2014 г. № 242-ФЗ требует неукоснительного исполнения данных предпосылок не только со стороны государства, но и со стороны операторов связи (персональных данных).

Федеральный закон Российской Федерации от 21 июля 2014 г. № 242-ФЗ помимо того, что он обязал операторов связи (персональных данных) хранить персональные данные граждан Российской Федерации на территории Российской Федерации, ввел порядок ограничения доступа к сайтам в сети Интернет в случае злостных преднамеренных нарушений. В 2014 г. новые тренды в регулировании и защите персональных данных были реализованы и в Европе. В Российской Федерации еще в 2006 г. было предусмотрено право граждан требовать от оператора связи (персональных данных) прекратить обработку личной информации, в том числе в сети Интернет. Но предоставить населению какое-либо право недостаточно, нужно обеспечить его реализацию. Самозащита здесь не является исчерпывающим эффективным средством противодействия чрезмерному вмешательству в частную жизнь, а значит, не является полноценным ответом существующим угрозам информационного мира. Российская Федерация всегда стояла, и будет стоять на защите прав самой незащищенной стороны при правоотношениях, возникающих при обработке персональных данных (имеется в виду – гражданин). Имеется общемировая тенденция развития Института защиты прав субъектов персональных данных. Проблемы, связанные с

защитой персональных данных обсуждаются на международных площадках Совета Европы, Организации экономического сотрудничества и развития, Евразийского экономического союза, Азиатского тихоокеанского экономического союза и ряда других. На данных площадках участвуют и российские представители. Активное участие осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Литература:

1. Федеральный закон Российской Федерации от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». – Режим доступа: http://garant.ru/

2. Официальный сайт федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. – Режим доступа: http://rkn.gov.ru/

Д.Э. Гопанчук, В.В. Кормильченко, Н.О. Светличная

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Северо-Кавказский филиал Московского технического университета связи и информатики,
г. Ростов-на-Дону, Россия

Ключевые слова: Информация, информационная безопасность, информационные технологии, защищенность информации, конфиденциальность, целостность, доступность, электронные методы воздействия, естественные угрозы.

В настоящее время, в век информационных технологий, когда информация является одним из наиболее важных аспектов существования современного общества, встает вопрос о защите, безопасности информации. Существуют виды деятельности, которые могут нанести ущерб информационной безопасности, Соответственно есть виды защиты, такие как средства шифрования данных, межсетевые экраны.

D.E. Gopanchuk, V.V. Kormilchenko, N.O. Svetlichnaya

TO THE QUESTION OF MODERN METHODS OF INFORMATION PROTECTION

North-Caucasus branch of the Moscow technical university of communication and informatics,
Rostov-on-Don, Russia

Keywords: information, information technology, information security, confidentiality, integrity, availability, electronic methods of influence, natural threats.

At present, in the age of information technology where information is one of the most important aspects of modern society the problem of data protection, or information security is rather actual. There are activities that can cause damage to information security, ranging from improper storage and maintenance of equipment, and large-scale hacker attacks. In this paper we consider the different types of information protection, such as data encryption, firewalls.

Сегодня, в век информационных технологий, когда информация является одним из наиболее важных аспектов существования современного общества, встает вопрос о защите, безопасности информации. Под информационной безопасностью понимается защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

1. Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

2. Целостность – избежание несанкционированной модификации информации;
3. Доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

1. Действия, осуществляемые авторизованными пользователями

В эту категорию попадают:

- целенаправленная кража или уничтожение данных на рабочей станции или сервере;
- повреждение данных пользователем в результате неосторожных действий.

2. "Электронные" методы воздействия, осуществляемые хакерами.

Под хакерами понимаются люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках конкурентной борьбы), так и просто из любопытства. К таким методам относятся:

- несанкционированное проникновение в компьютерные сети;
- DOS-атаки.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т. п.

Атака типа DOS (сокр. от Denial of Service - "отказ в обслуживании") - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т. п.

3. Компьютерные вирусы

Отдельная категория электронных методов воздействия - компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

4. «Естественные» угрозы.

На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

- средства идентификации и аутентификации пользователей (так называемый комплекс 3А);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

Комплекс 3А" включает *аутентификацию* (или идентификацию), *авторизацию* и *администрирование*. Идентификация и авторизация - это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: "Кто вы" и "Где вы" - являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ.

Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты - обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования - высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Межсетевой экран представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

Основной принцип действия межсетевых экранов - проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов. Таким образом, межсетевые экраны значительно расширяют возможности сегментирования информационных сетей и контроля за циркулированием данных.

Для противодействия естественным угрозам информационной безопасности в компании должен быть разработан и реализован набор процедур по предотвращению чрезвычайных ситуаций (например, по обеспечению физической защиты данных от пожара) и минимизации ущерба в том случае, если такая ситуация всё-таки возникнет. Один из основных методов защиты от потери данных - **резервное копирование** с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т. д.).

Одна из крупнейших хакерских атак за последние 15 лет была совершена 25 января 2003 года.

25 января 2003 года в Республике Корея в результате действий хакеров произошел общенациональный сбой в интернете, в течение нескольких часов вся страна была лишена доступа в сеть. Впервые действия "кибертеррористов" отразились на деятельности компаний в общенациональном масштабе. Главным жертвами атаки стали компании, ведущие интернет-торговлю, ущерб понесли почти 17 млн пользователей. Помимо Южной Кореи пострадали практически все страны, включая Россию, по всему миру были поражены около 22 тыс. серверов.

Таким образом, вопрос информационной безопасности важен на всех уровнях, начиная от обычного пользователя , заканчивая государством.

Литература:

1. http://all-ib.ru/
2. www.lessons-tva.info
3. http://www.thg.ru/howto/fifteen_hacking_exploit/onepage.html

М.А. Горбачева, А.К. Сагдеев

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ ПРИ ВЕДЕНИИ ИНФОРМАЦИОННОЙ ВОЙНЫ

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия

Ключевые слова: инфотелекоммуникационная сеть военного назначения, информационная война, информационные самообучающиеся системы, информационное оружие.

В данной работе рассмотрено влияние операций, проводимых в ходе информационной войны, на показатели защищенности инфотелекоммуникационной сети военного назначения. Данная проблематика в настоящее время является актуальной в вопросах обеспечения обороноспособности страны. Разработка новых механизмов защиты от воздействия

информационного оружия позволит обеспечить устойчивое функционирование сетей военного назначения.

M.A. Gorbacheva, A.K. Sagdeev

THE PROBLEM OF ENSURING THE SECURITY OF INFOCOMMUNICATION NETWORK FOR MILITARY PURPOSES IN THE CONDUCT OF INFORMATION WARFARE

Saint-Petersburg state University of telecommunications
them. Professor M. A. Bonch-Bruevich, St. Petersburg, Russia

Keywords: infocommunication network for military purposes, information warfare, information self-learning systems, information weapons.

In this work the influence of the operations performed during the information war on the performance security infocommunication network for military purposes. This problem is currently relevant in ensuring the country's defence. Development of new mechanisms of protection from exposure to information weapons will ensure sustainable operation of networks for military purposes.

Любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Открыто говорить о приемах и методах информационной войны сегодня необходимо потому, что, во-первых, осмысление того или иного приема информационной войны позволяет перевести его из разряда скрытых угроз в явные, с которыми уже можно бороться, и, во-вторых, факт наличия теории информационной войны, представленной в данной работе, должен предостеречь потенциальную жертву от идеалистически наивного восприятия как внешнего, так и собственного внутреннего мира.

Информационная война (ИВ) − целенаправленные действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем [1, 5].

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия – алгоритмы генерации алгоритмов [1 -5].

Идя этим путем, всегда можно активизировать или сгенерировать для последующей активизации алгоритмы самоуничтожения.

Те системы, которые претерпевают изменения при информационном воздействии в дальнейшем будем называть информационными самообучающимися системами (ИСС). Человек, народ, государство являются классическими ИСС.

Любая система представляет собой совокупность объектов и связей между ними, т.е. определенную структуру. Новое знание приводит к изменению структуры за счет:

- изменения связей между элементами;
- изменения функциональных возможностей самих элементов;
- изменения количества элементов: элементы могут рождаться и умирать.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны.

Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

- включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);
- полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

- полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности (разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);
- разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;
- сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие "степень поражения информационным оружием", оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие дает максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Качество информации - показатель трудности ведения войны. Чем более качественной информацией владеет командир, тем большие него преимущества по сравнению с его врагом.

На концептуальном уровне можно сказать, что государства стремятся приобрести информацию, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию [2, 5].

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю или возможности вести борьбу. Таким образом, информационная война - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций [1, 4].

Это определение является основой для следующих утверждений.

Информационная война - это любая атака против информационной функции, независимо от применяемых средств. Бомбардировка АТС - операция информационной войны. То же самое можно сказать и про вывод из строя программного обеспечения компьютера АТС.

Информационная война - это любое действие по защите наших собственных информационных функций, независимо от применяемых средств. Укрепление и оборона здания АТС против бомбардировок - тоже часть информационной войны. То же самое можно сказать и про антивирусную программу, которая защищает программное обеспечение АТС.

Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия [3, 5].

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую врагом, косвенно путем восприятия, они атаковали информацию врага косвенно. То есть, для того чтобы хитрость была эффективной, враг должен был сделать три вещи:

- наблюдать обманные действия;
- посчитать обман правдой;
- действовать после обмана в соответствии с целями обманывающего.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии

позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации. Таким образом, краткий список характеристик современных информационных систем, приводящих к появлению подобной уязвимости, можно свести к следующим основным причинам: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Данное обстоятельство вызывает необходимость разработки адекватных механизмов защиты, но не надо забывать, что даже самые совершенные механизмы защиты не могут свести к нулю вероятность уязвимости, это позволяет говорить об актуальности создания нового методического аппарата по обеспечению пролонгированной защиты объектов инфотелекоммуникационной сети военного назначения.

Литература:

1. Байгузин Р. Информационная война. - М., 2000.
2. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектив//http://www.infwar.ru.
3. Костин Н.А. Общие основы теории информационной борьбы//Военная мысль. 2009. № 3.
4. Манойлов А.В., Фролов Д.Б. Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны//СПб.: Компьютерные системы, 2003, № 2.
5. Козырев В.М., Новак А.В. Информационная война в аспекте проблемы обеспечения защищенности ИТКС ВН//СПб.: сборник статей III Международной научно-технической конференции СПбГУТ, 2014.

Л.Л. Гусева, *Захарин Серафим

МОДЕЛИРОВАНИЕ ДИНАМИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ С ЭЛЕМЕНТАМИ СТОХАСТИЧНОСТИ

Северо-Кавказский федеральный университет, г. Ставрополь, Россия
*Малая академия наук, г. Ставрополя, Россия

Ключевые слова: компьютерный вирус, хищник-жертва, имитационное моделирование, динамика компьютерного вируса.

В работе описана имитационная модель динамики компьютерного вируса, реалистичность которой определяется бросанием фишек на игровое поле и случайным образом определяется жизненный этап вируса и жертвы. Эта модель позволяет оценить значения неизвестных, но значимых параметров таких как, например, откуда вирус стартовал, каково первоначальное количество зараженных машин, какие узлы надо отключить или «пропатчить» в первую очередь, чтобы погасить «эпидемию».

L.L. Guseva, *Zaharin Seraphim

MODELING THE DYNAMICS OF COMPUTER VIRUSES WITH ELEMENTS OF STOCHASTIC

North-Caucasian Federal University, Stavropol, Russia
*Small Academy of Sciences, Stavropol, Russia

Keywords: computer virus, predator-prey, simulation, dynamics computer virus.

The described simulation model of a computer virus, the realism of which is determined by throwing chips on the playing field, which is randomly determined life stage of the virus and the victim. This model allows to estimate the values of unknown, but significant parameters such as, for example, where the virus started, what the initial number of infected machines which nodes should be turned off or to "patch" in the first place, to pay off the "epidemic".

Использование математических моделей, основанных на дифференциальных уравнениях или их дискретных аналогах, далеко не единственный путь в компьютерном моделировании динамики популяций. Другую интересную группу составляют чисто стохастические модели или динамические модели с элементами стохастичности [4].

Для моделирования динамики компьютерных вирусов рассмотрим эволюционную игру хищник-жертва. В нашем случае хищник – это вирус, а жертва это «здоровый» компьютер. Незараженные вирусом компьютеры – «здоровые» машины X представляются X белыми фишками. Зараженные вирусом компьютеры Y представляются Y черными фишками.

Фишки бросают произвольно на доску, похожую на шахматную. Одна половина общей площади доски – белая, одна четвертая серая и одна четвертая черная. Кроме того, толстыми линиями доска поделена на 16 больших квадратов. Любой вирус, попадающий на черный квадрат считается убитым и снимается с доски. Любой незараженный компьютер – жертва, попадающий на белую клетку, считается воспроизведенным в виде нового компьютера и на доску рядом с первым ставиться белая фишка. Отождествляется как можно больше пар хищник – жертва, причем каждый большой квадрат рассматривается в порядке очереди. Затем незараженный компьютер в каждой паре заменяется зараженным. При этом в равных количествах уменьшается количество незараженных компьютеров и возрастает «популяция» зараженных вирусом компьютеров. В реальной жизни жертва выбирается случайно, поэтому зараженные машины «чихают» на здоровые и на самих себя. Чем больше будет зараженных машин, тем менее эффективно становиться случайное «чихание».

Это чисто имитационное моделирование, конечной целью которого является, установление судьбы популяций в зависимости от многих факторов, входящих в модель. Здесь нет дифференциальных уравнений, но зато в полной мере проявляется стохастика, моделирование случайных процессов. Реалистичность процессов реализуется случайным попаданием фишки на клетку в большом квадрате.

Интерес игрока связан с возможностью или невозможностью заражения вирусом всех машин в системе при исходных параметрах. Поскольку образование пар зависит от произведения «популяций» зараженных компьютеров и незараженных компьютеров, выше мы смоделировали взаимодействия хищника и жертвы. Так как фишки должны падать свободно на доску и их распределение должно быть равномерно, игровое поле необходимо доработать. Доску нужно установить на внутренней стороне крышки коробки так чтобы кромка мешала фишкам упасть с доски.

Результаты типичного броска фишки показывают сколько случайным образом появляются мертвых хищников (нет пищи) или в нашей модели – зараженные компьютеры без носителей не могут размножается (нет в окружении незараженных компьютеров или они отключены), сколько «рождается» неинфицированных компьютеров (кол-во компьютеров все время растёт), как размножается вирус при парном взаимодействии внутри больших квадратов, ограниченных толстыми линиями.

Новая реалистическая особенность, проявляющаяся в игре это возможность вымирания «вида» в нашем случае – полного заражения вирусом всех компьютеров. Эта возможность увеличивается, когда «популяция» небольшая, а случайная флуктуация неблагоприятна. На рисунке 1 показаны результаты нескольких игр.

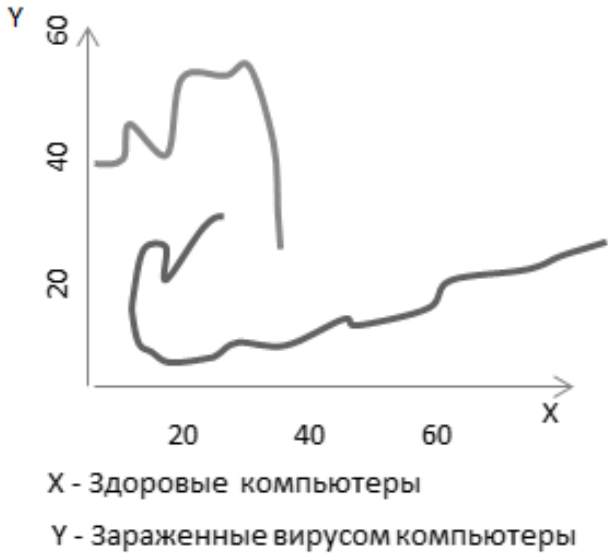


Рисунок 1. Некоторые из результатов игры, демонстрирующие возможность эпидемии или наоборот взрыв «популяции» здоровых компьютеров

Интерес представляет выбор начальной точки (количества зараженных и незараженных вирусом машин). От нее зависит возможность заражения всей популяции компьютеров вирусом или наоборот ростом незараженных компьютеров. Интересна начальная точка (10,20) (X=10 и Y=20) Здесь игра начинается медленно с небольших неустойчивых шагов до тех пор, пока большая флуктуация не образует более интенсивное фазовое движение. Количество незараженных машин уменьшается и возникает вопрос о выживании этой «популяции». Если все таки выживание произойдет, а «популяция» вирусов уменьшается, то может возникнуть типичных взрыв «популяции» здоровых машин.

Игру можно описать с помощью уравнений эквивалентным уравнениям Лотки - Вольтерры, описывающих динамику простой экологии типа хищник – жертва. Анализ правил и описание поля игры позволяет получить коэффициенты этих уравнений. Поскольку черное поле составляет четвертую часть площади всей доски, то Хри этом точно моделируется член -¼ Y, описывающий вымирание вирусов, но конечно с элементом случайности. Поскольку белый цвет занимает половину доски, то это правило моделирует член описывающий размножение незараженных компьютеров и равен + 1\2X.

Эксперимент показал, что при неоднократном бросании 20 фишек (вирусов) и 20 фишек (здоровых машин) в среднем получается 10 взаимодействий на бросок, значит ΔY=10 для X=20 и Y=20 и постоянная к произведению XY равна 1\40:

$$\Delta X = \frac{1}{2}X - \frac{1}{40}XY\,, \qquad \Delta Y = \frac{1}{40}XY - \frac{1}{4}Y. \tag{1}$$

Можно экспериментировать с правилами для усовершенствования игры и приближения к реалистичности. Можно ввести дополнительный элемент «эволюции» в виде незараженной машины с антивирусом. При взаимодействии с вирусом этот «супер компьютер» имеет 50 на 50 шансов уйти от хищника (быть незараженным) и это решается путем бросания монеты. Можно еще добавить размножение «суперкомпьютеров» когда белая фишка попадает на белый квадрат.

Для планирования и контроля необходимо знание динамики «популяций» в конкретный момент времени. Что в реальных условиях не возможно. Однако если в нашей игре предложить, что здоровым машинам могло помочь крупномасштабное уничтожение вирусов, и уменьшить популяцию вирусов до некоторого значения, то результатом может быть взрыв популяции здоровых машин, за которым последуют взрывы популяции вирусов с последующим почти несомненным заражением всех здоровых машин [5;6].

В реальных экспериментах учитываются гораздо больше факторов, влияющих на динамику «популяций». Это позволяет оценить значения неизвестных, но значимых параметров

таких как, например, откуда вирус стартовал, каково первоначальное количество зараженных машин, какие узлы надо отключить или «пропатчить» в первую очередь, чтобы погасить «эпидемию малой кровью» [1;2;3].

Литература:
1. The Workshop on Rapid Malcode (WORM), October 27, 2003, The Wyndham City Center Washington DC, USA. (http://pisa.ucsd.edu/worm03/)
2. Jasmin Leveille «Epidemic Spreading in Technological Networks» (http://www.hpl.hp.com/techreports/2002/HPL-2002-287.pdf)
3. Senthilkumar C.G. «Worms: How to stop them?» (http://wwwcsif.cs.ucdavis.edu/~cheetanc/worms/proposal.ps)
4. Эфрос А.Д. Физика и геометрия беспорядка.-М.:Наука,1982г.
5. Захаренко А. Черводинамика: причины и следствия. Интернет ресурс.http://az13.mail333.com/4/vh6.htm (дата посещения 02.04.2013)
6. Компьютерные вирусы — эволюция или революция? Ретроспектива глобальных эпидемий http://hackerzz.ucoz.ru/ (дата посещения 20.04.2014)

Л.У. Давронова, А.А. Абдумаликов, Б.Б. Бабатаев

АНАЛИЗ И КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: информационная система, информационная безопасность, угроза информационной безопасности, информационно-коммуникационные системы.

Анализированы угрозы информационной безопасности, изучены подходы при выборе классификационных признаков, определены положительные и отрицательные характеристики этих методов с точки зрения применимости для оценки информационных рисков.

L.U. Davronova, A.A. Abdumalikov, B.B. Babataev

ANALYSIS AND CLASSIFICATION OF INFORMATION SECURITY THREATS

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: information system, information security, information security threat, information and communication systems.

Analyze the threats to information security, studied approach to the choice of classification features are defined positive and negative characteristics of these methods in terms of the applicability of the information to assess the risks.

Под информационным процессом понимаются все действия, так или иначе связанные с преобразованием информации в жизнедеятельности активного субъекта при его работе с информационной системой (ИС), подключенной к внешней сети передачи данных. Так как в процессе участвуют персонал, технические средства обработки данных, информации и средства коммуникации, то, на каждом из этапов информационного процесса преобразование информации происходит в условиях действия различных факторов, стремящихся нарушить его естественное положение, то есть нарушить бесконфликтное течение заранее известных последовательных этапов информационного процесса. Факторы, нарушающие нормальное выполнение этапов информационного процесса (объективных и субъективных), принято называть угрозой информационной безопасности (УИБ). Известно большое количество определений УИБ [1], которые, несмотря на отличие в деталях, едины в своей сути: под угрозами понимается опасность (существующая реально или потенциально) совершения какого-либо деяния (действия),

направленного на нарушение основных свойств информации: конфиденциальности, целостности, доступности. Практически все исследователи, раскрывая виды возможных нарушений основных свойств информации, приводят один и тот же перечень: к угрозам нарушения конфиденциальности информации относят хищение (копирование) и утечку информации; к угрозам доступности - блокирование информации; к угрозам целостности - модификацию (искажение информации), отрицание подлинности информации или навязывание ложной информации. При подключении ИС к внешним коммуникационным сетям возникающие УИБ могут быть направлены на: информационные ресурсы, процессы, процедуры и программы обработки информации внутри ИС; информацию, передаваемую по сети передачи данных; коммуникационные узлы ИС; нарушение функционирования электронной почты [2].

Последствием воздействия угроз является нарушение безопасности системы. Рассмотрим также и последствия угроз, а также перечень и сущность различных видов угрожающих воздействий, которые являются причинами дискредитации системы защиты ИС.

В целом, последствия могут быть связаны с «несанкционированным вскрытием», «обманом», «разрушением» и «захватом» (Таблица.1).

Таблица. 1. Последствия реализации угроз

Последствия угроз информационный безопасности связаны с		**Причинами которых являются**		**Которые подразделяются на**	
	Несанкционированным вскрытием.		разоблачение		✓ Аппаратно-программные ошибки; ✓ Просмотр остатка данных ✓ Ошибки человека ✓ Аппаратно-программные ошибки
			перехват		✓ Кражу ✓ Прослушивание(пассивное) ✓ Анализ излучений
			умозаключение		✓ Анализ трафика ✓ Анализ сигналов
			вторжение		✓ Посягательство ✓ Проникновение ✓ Реконструкцию ✓ крипто анализ
	Обманом		маскарад		✓ мистификацию ✓ устройство для злонамеренных действий
			фальсификация		✓ подмену ✓ вставку
			отказ		✓ ложный отказ источника ✓ ложный отказ получателя
	Разрушением		вредительство		✓ устройства для злонамеренных действий ✓ физическое разрушение ✓ ошибки человека ✓ аппаратно-программные ошибки ✓ природные катаклизмы
			порча		✓ подделки ✓ устройства для злонамеренных действий ✓ ошибки человека ✓ аппаратно-программные ошибки ✓ природные катаклизмы
	Захватом		Незаконное присвоение		✓ кражу службы ✓ кражу функциональных возможностей ✓ кражу данных
			злоупотребление		✓ подделки ✓ устройство для злонамеренных действий ✓ нарушение дозволенности

Можно выделить следующие существующие подходы к классификации УИБ [2] и определим их основные принципы.

1. Подход «Оранжевой книги» и «Общих критериев». Подход заключается в сведении всех УИБ к трем основным классам - угрозам нарушения конфиденциальности, доступности и целостности. Данная классификация построена, в первую очередь, для оценки степени обеспечения ИБ в ИС. Соответственно, вопросы противодействия рассматриваются с точки зрения именно «оценки», а не «рекомендаций» для построения защищенных ИС.

2. Промышленный подход. Некоторыми коммерческими организациями в целях построения реальных промышленных коммерческих продуктов были разработаны несколько типов классификаций. Особенности этого подхода рассмотрим на примере классификации, разработанной специалистами компании DSECCT [3], которая является наиболее характерным для данного подхода к классификации. Изначально, для удобства создания конечного продукта, при разработке классификации специалистами этой компании во главу угла поставлен принцип попадания угроз только под один классификационный признак. Назовем его принципом «однозначности».

При этом появляется возможность формализации и программно-аппаратной реализации однозначного противодействия всем угрозам, попадающим под один классификационный признак. Так, в вышеуказанной классификации использованы пять уровней, различающие УИБ: по характеру, виду воздействия, источнику возникновения, объекту воздействия в целом и частному объекту воздействия. Следует отметить, что подобная классификация относится только к угрозам, имеющим технологический характер (1-й уровень классификации). Для угроз же организационного характера имеется 4 уровня. При этом 2-й уровень определяет объект, 3-й — вид и 4-й — цель воздействия угрозы. В этом подходе больше внимания уделено угрозам технологического характера. Кроме того, в данной классификации выпадают воздействия локального нарушителя, направленные на каналы связи, на протоколы, на оборудование и линии связи.

3. Антивирусный подход. Этот подход обусловлен тем, что на сегодняшний день наибольшая доля УИБ приходится на вирусные угрозы и является разновидностью промышленного подхода. Наиболее ярким примером такого подхода является классификация УИБ, разработанная создателем одной из самых популярных антивирусных программ Е. Касперским и опубликованная в журнале JetInfo [4]. При таком подходе классификация УИБ сводится к анализу и определению различных классов вирусов, глобальных сетевых атак и спама, т.е. рассматриваются основные разновидности угроз программного характера. Угрозы технического и организационного характера остаются вне поля зрения.

4. Подход Вихоревка. Основным принципом этого подхода является идентификация всех возможных источников УИБ, идентификация и сопоставление с источниками УИБ всех возможных факторов (уязвимостей), присущих объекту защиты, и сопоставление УИБ идентифицированным источникам и факторам [5]. Другими словами, классификация УИБ проводится на основе анализа взаимодействия логической цепочки: «источник угрозы — фактор (уязвимость) — угроза (действие) — последствия (атака)».

При этом под последствием понимается именно совершенная атака, направленная на нарушение ИБ, а не степень причиненного ущерба в результате ее совершения. С другой стороны, именно степень или величина причиняемого ущерба является наиболее существенной движущей силой, побуждающей принимать меры предосторожности для обеспечения гарантированного уровня ИБ информационных ресурсов не только при подключении ИС к внешним коммуникационным сетям, но и при построении замкнутых автономных компьютерных систем. Именно отсутствие классификации по величине и степени возможного причиняемого ущерба и является основным недостатком этого подхода. Резюмируя выше проведенный анализ можно сделать следующие выводы: существует большое количество способов классификации УИБ, которые сводятся к следующим основным разновидностям подходов:

- подход «Оранжевой книги» и «Общих критериев»;
- промышленный подход;
- антивирусный подход;
- подход Вихоревка.

Каждый из рассмотренных подходов, обладая несомненными положительными сторонами, тем не менее, имеют свои недостатки, которые не позволяют выбрать один из них в качестве универсального метода:

1. Основным недостатком подхода «Оранжевой книги» и «Общих критериев» является то, что одна и та же реальная угроза либо не подходит ни под один из классификационных признаков, либо, наоборот, удовлетворяет нескольким;
2. Промышленный подход используется для продвижения на рынке того или иного конкретного продукта и делает упор на его сильные стороны, приуменьшая значение факторов, по которым данный продукт является слабым. Например, классификация разработанная специалистами компании DSECCT, в которой основное внимания уделено угрозам технологического характера, но в ней недостаточно отражены угрозы на каналы связи, протоколы и коммуникационное оборудование;
3. При антивирусном подходе классификация УИБ сводится к анализу и определению различных классов вирусов, спама и глобальных сетевых атак, т.е. рассматриваются основные разновидности угроз программного характера. В то же время угрозы технического и организационного характера остаются вне поля зрения;
4. Отсутствие классификации по величине и степени возможного причиняемого ущерба является основным недостатком подхода Вихорева.

Таким образом, можно сформулировать основные требования к способу классификации угроз:

- реальная угроза по своим признакам должна подходить какому-либо одному квалификационному признаку и отнесена одному классу;
- свойства и признаки классификации по возможности должны отражать все виды угроз;
- классификация должна учитывать величину и степень возможного причиняемого ущерба.

Выполнение этих требований позволит получить такую классификацию угроз, которое позволит применить более простые методы оценки информационных рисков. Исходя из вышесказанного, можно сформулировать основные выводы по результатам проведенного анализа. Рассмотрев основные виды и признаки классификации угроз с точки зрения дальнейшего применения для оценки информационных рисков, было установлено, попытки использования данных классификаций для описания по возможности большего количества угроз показали, что во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким.

Литература:

1. Зегжда Д., Ивашко А. Основы безопасности информационных систем — М.: Горячая линия — Телеком, 2000. с. 18.

2. Домарев В. Безопасность информационных технологий. Методология создания систем защиты. Москва: DiaSoft — 2002 г.

3. «Классификация угроз Digital Security (Digital Security Classification of Threats)», http://www.dsec.ru/products/grif/fulldesc/classification.

4. Касперский Е. «Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения», JetInfo, 2003 г. №12, http://jetinfo.isib.ru/2003/12/2/article2.12.2003.html.

5. Вихорев С. «Классификация угроз информационной безопасности», http://c-news.ru/reviews/free/oldcom/security/elvis_class.shtml.

Д.Е. Демидов

СОВРЕМЕННЫЕ ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уральский технический институт связи и информатики, г. Екатеринбург, Россия

Ключевые слова: информационная безопасность, защита информации, идентификация, аутентификация, компьютерная система, программное обеспечение.

В данной статье рассматриваются современные программные средства защиты информации на примере конкретных программ, а также проанализированы их особенности. Представленные программы реализуют такие функции, как шифрование данных, аутентификация пользователей, теневой режим работы операционной системы, ограничение доступа к информации, межсетевое экранирование, защита от вредоносного программного обеспечения и резервное копирование данных. Также приведены общие теоретические сведения о программных средствах защиты информации, и указаны достоинства и недостатки их применения.

D.E. Demidov

MODERN DATA PROTECTION SOFTWARE

Ural institute of telecommunications and computer science, Yekaterinburg, Russia

Keywords: information security, data protection, identification, authentication, computer system, software.

This article reviews the current data protection software on the example of specific programs, and analyzed their features. Presents programs implement functions such as data encryption, user authentication, shadow mode operating system, limiting access to information, firewall, protection against malicious software, and data backup. Also provides general theoretical information about data protection software, and lists the advantages and disadvantages of their use.

Информация всегда играла чрезвычайно важную роль в жизни человека. Общеизвестно высказывание о том, что тот, кто владеет информацией, тот владеет миром. С течением времени роль информации в жизни человека становилась все существеннее. А с приходом научно-технического прогресса возросла компьютеризация информации, что и привело к необходимости обеспечения информационной безопасности компьютерных систем. Для этой цели широко используются программные средства защиты информации.

Цель работы – рассмотреть актуальное программное обеспечение, реализующее защиту информации в компьютерных системах.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения компьютерной системы (далее КС) для выполнения защитных функций.

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования данных;
- программы защиты информационных ресурсов (системных и прикладных программ, баз данных и т.д.) от несанкционированного доступа.

Под идентификацией понимается однозначное распознавание уникального имени субъекта КС.

Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности личности пользователя). [1, С.44]

Информационная безопасность – состояние защищенности информации от случайных или преднамеренных воздействий естественного или искусственного характера.

Защита информации представляет собой комплекс мер, направленных на обеспечение информационной безопасности.

В данной статье рассмотрены следующие программные средства защиты информации.

Folder Lock. Данное средство выполняет быстрое шифрование, защиту паролем файлов и папок. Кроме того, FolderLock имеет дополнительные особенности, такие как, блокировка, скрытый (невидимый) режим, предотвращение попыток взлома, мобильность, очистка историй браузеров, что позволяет сохранить конфиденциальность и безопасность личных данных. Программа позволяет осуществлять быстрое 256-битное AES шифрование файлов и папок любого типа; защищать папки паролем; блокировать файлы, папки и диски. Также она обладает поддержкой 64-разрядных операционных систем и включает быстрейшее программное обеспечение шифрования.

Rohos Logon Key. Эта программа предлагает удобный способ защитить доступ к компьютеру с использованием USB Ключа вместо обычного пароля. Это удобно – доступ выполняется быстро и автоматически – хотя Windows по-прежнему защищена сильным паролем.

Возможности программы:

- обычный вход по паролю может быть запрещен;
- замена слабой парольной авторизации на физический USB ключ;
- в качестве USB ключа можно использовать: любой USB-накопитель (флешка, съемный жесткий диск) , SD/MMC карты памяти, ключи AladdineToken, Yubikey, и т.д.;
- автоматический вход или разблокирование при обнаружении USB ключа;
- автоматическая блокировка Windows, когда пользователь извлекает USB ключ из компьютера;
- невозможно обойти защиту USB ключа, даже перезагрузив компьютер в Безопасном режиме;
- аварийный вход позволяет получить доступ к системе в случае утери USB ключа или, если забыт PIN код;
- гибкие варианты USB ключа: один ключ можно использовать, чтобы войти в несколько компьютеров, или компьютер может принимать только один ключ для входа, игнорируя чужой ключ;
- ограничивает доступ к компьютеру для некоторых пользователей на основе фактора времени. Когда время работы пользователя закончится, RohosLogon автоматически заблокирует рабочий стол;
- RohosLogon плавно интегрируется в любую конфигурацию Windows, автоматически выбирая режим авторизации;
- позволяет использовать USB ключ для доступа к удаленному рабочему столу.
- двухфакторная аутентификация: Физический USB ключ + PIN код [3].

Rohos Disk Encryption. Данная программа позволяет создать виртуальный зашифрованный диск. В действительности, он не является физическим диском, а всего лишь специальным большим файлом, где хранятся все данные. Но можно работать с ним точно также, как с любым логическим диском: копировать и стирать файлы, просматривать его содержимое через проводник Windows Explorer и т.д. Из преимуществ программы стоит отметить стойкие алгоритмы шифрования (AES256), скрытие данных, шифрование программ, автоматическую блокировку доступа, восстановление данных, встроенный файл-шредер (гарантирует физическое удаление файлов с винчестера), неограниченный размер диска и многое другое. [4]

Shadow Defender – программа для защиты конфиденциальности пользователя и операционной системы в целом. Shadow Defender позволяет отменить любые вредоносные, пользовательские или иные действия, произошедшие в операционной системе, простой перезагрузкой компьютера. Например, если произошло злонамеренное заражение операционной системы вирусами или по недосмотру пользователя были удалены какие-либо важные файлы (фотографии, документы и т.д.), но при этом система была защищена Shadow Defender, то после перезагрузки компьютера можно вернуть его первоначальное до заражения состояние. При этом все удалённые файлы будут восстановлены. Кроме того, использовать защиту ОС этой программой можно во время установки каких-либо приложений, игр и других экспериментов - после перезагрузки компьютера любые изменения будут отменены. Для удобства в настройках можно отметить, какие файлы и папки могут подвергаться изменениям, даже если операционная система в данный момент находится под защитой Shadow Defender. В этом случае после перезагрузки компьютера будут отменены все изменения кроме тех, что произошли в указанных папках и файлах[5].

Agnitum Outpost Firewall Pro – программа для защиты компьютера от хакерских атак из Интернета от российской компании Agnitum. Представляет собой программный межсетевой экран (файервол), который предотвращает несанкционированный доступ к информации через сеть Интернет со стороны хакеров и прочих нарушителей. Присутствует детальная настройка правил, по которым программы получают доступ к сети. Кроме этого, Outpost обеспечивает блокировку загрузки рекламы и активного содержимого веб-страниц, а тем самым — их более быструю загрузку [6].

Eset Smart Security – надежное средство защиты в цифровом мире. Данная программа включает в себя антивирус и файервол, а также сочетает в себе скорость, надежность и удобство. Ее можно использовать как для настольных ПК, так и для ноутбуков – при установке программа распознает аппаратную конфигурацию, и подстраивается под нужный режим. Работа программы включает в себя стандартный сигнатурный анализ, а также мониторинг сети и действий программ. Для разных приложений можно указать дополнительные правила безопасности. Кроме того, с помощью ESET Smart Security можно контролировать общее состояние системы с помощью встроенных инструментов. При подключении сменного носителя антивирус автоматически проверяет его на вирусы [7].

Exiland Backup – легкая и удобная программа, предназначенная для создания резервных копий рабочих файлов, документов, переписки, фотографий и т.д. Она сочетает в себе простоту интерфейса, гибкость настроек и скорость работы. Утилита может использоваться как дома, так и в организациях на рабочих КС и серверах. Создание резервных копий выполняется либо автоматически по расписанию, либо вручную. Присутствуют гибкая настройка расписания, возможность резервного копирования при включении/выключении компьютера, подключении флешки или жесткого диска в порт USB, а также запуск задания из командной строки. Поддерживается 4 типа резервного копирования: полное, добавочное, разностное и синхронизация папок [8].

Hide Folders – это удобная и простая в использовании программа для защиты конфиденциальной информации от посторонних. Программа позволяет скрывать и блокировать доступ к целым папкам и отдельным файлам, а так же защитить данные от модификации. Защита паролем гарантирует, что только владелец сможет получить доступ к защищенным данным. Имеется несколько различных способов защиты, поддержка доверенных процессов, огромное количество опций тонкой настройки и средства «заметания» следов дают возможность настроить уникальную политику файловой безопасности максимально гибко [9].

Encrypt Easy – очень эффективная утилита, позволяющая легко и просто предотвратить утечку важных файлов. Программа интегрируется в проводник Windows и в контекстном меню появляются два пункта: зашифровать и расшифровать. Для шифрования необходимо ввести пароль, выбрать один из 39 доступных методов шифрования, и один из 28 способов расчета хеша. Поддержка передачи параметров через командную строку позволяет автоматизировать процесс сокрытия данных с помощью скриптов. Одной из полезных функций является гарантированное удаление файлов или папок с помощью алгоритма DOD 5220.22-M с семью проходами. Кроме того, функция «Wipe Out» позволяет быстро очищать временные папки, историю и кэш браузеров, список последних открытых документов и cookies, что позволяет замести следы после работы на компьютере [10].

К преимуществам программных средств защиты информации относятся:

- простота тиражирования;
- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);
- простота применения — одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя ни каких новых (по сравнению с другими программами) навыков;
- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

С другой стороны, их недостатками являются:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты;
- более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты);
- пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС), что создает для нарушителя принципиальную возможность их обхода;
- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС. [1, С.44]

Перечисленные выше программы могут применяться как на предприятиях различных отраслей, так и в домашних условиях.

Для поддержания конфиденциальности информации на требуемом уровне не стоит ограничиваться каким-либо одним из рассмотренных видов программных средств защиты (например только шифрованием), а применять сразу несколько. Также не следует пренебрегать и аппаратными средствами защиты информации (специальными модулями, входящими в состав аппаратного обеспечения КС).

Литература:

1. Киреенко А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. – 2012. – №3. – с. 40-46
2. http://www.newsoftwares.net/folderlock/
3. http://www.rohos.ru/products/rohos-logon-key/
4. http://www.rohos.ru/products/rohos-disk/
5. http://www.wd-x.ru/shadow-defender/
6. http://www.agnitum.ru/outpost-firewall-pro.php
7. http://www.esetnod32.ru/home/products/smart-security/
8. http://www.exiland-backup.com/ru/
9. http://www.fspro.net/hide-folders/
10. http://www.encrypt-easy.com/

А.Э. Боярчук, *И.А. Енгибарян, *В.И. Юхнов

МЕРОПРИЯТИЯ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ

Донской государственный технический университет, г. Ростов-на-Дону, Россия
*Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: инженерно-техническая защита информации, система безопасности, коммерческая тайна, объект информатизации, выделенное помещение, контрольная точка.

Описана проблема автоматизации расчетных работ при выполнении комплекса мероприятий аттестационной проверки и включающая в себя контроль состояния акустической защищенности помещения аттестуемого объекта. Такой контроль помещения проводится в целях документального подтверждения соответствия показателей эффективности принятых мер технической защиты установленным требованиям или нормам эффективности защиты информации…..

A.E. Boyarchuk, *I.A. Yengibaryan, *V.I. Yukhnov

EVENTS OF DEDICATED SAFETY CONTROL PREMISES

Don state technical University, Rostov-on-don, Russia
*North-Caucasian branch of the Moscow technical University of communications and computer science, Rostov-on-don, Russia

Keywords: engineering and technical protection of information system security, trade secrets, object information allocated space, a checkpoint.

Described the problem of automation of computational operations during execution of complex activities proficiency tests and includes monitoring the status of the acoustic protection of the premises of the certified object. Such control of the premises is carried out in order documentary evidence of

conformity of the indicators of the effectiveness of technological protection measures established requirements or standards of the effectiveness of information security.....

На сегодняшний день инженерно-техническая защита информации имеет важное место в его системе безопасности любого предприятия. Проблема сохранения коммерческой тайны выходит на передний план. Многие организации заинтересованы в защите своей коммерческой информации, персональных данных сотрудников и клиентов и проводят мероприятия по предотвращению их утечки.

Одна из важнейших составляющих мероприятий по защите информации - проведение аттестации помещений для проведения совещаний и переговоров, помещений объектов информатизации. Аттестация таких объектов по требованиям безопасности информации представляет собой комплекс организационно-технических мероприятий, в результате которых подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утвержденные государственными органами обеспечения безопасности информации и контролируемые при аттестации. Этот комплекс мероприятий называется аттестационной проверкой и включает в себя контроль состояния акустической защищенности помещения аттестуемого объекта [1].

Такой контроль помещения проводится в целях документального подтверждения соответствия показателей эффективности принятых мер технической защиты установленным требованиям или нормам эффективности защиты информации. Он состоит из двух частей: организационной и инструментальной. Организационная часть включает в себя проверку исходных данных об объекте, инженерно-технической документации, а также актов о проведении специальной проверки выделенных помещений. Инструментальная часть основывается на контроле выполнения норм противодействия акустической речевой разведке и предполагает применение инструментально-расчетного метода определения отношений «речевой сигнал / акустический (вибрационный) шум» в контрольных точках в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц. Полученные отношения «сигнал/шум» сравниваются с нормированными. Методика ориентирована на использование контрольно-измерительной аппаратуры общего применения.

В каждой контрольной точки для октавных полос необходимо:

- рассчитать октавные уровни акустического (вибрационного) сигнала L_{c2} (V_{c2}) по формулам 1 и 2.

$$L_{c2_i} = \begin{cases} L_{(c+ш)_i}, при \;\; L_{(c+ш)_i} - L_{ш_i} \geq 10 \\ L_{(c+ш)_i} - \Delta, при \;\; L_{(c+ш)_i} - L_{ш_i} < 10 \end{cases}, \quad (1)$$

где Δ - поправка в дБ;

i – номер октавной полосы.

$$V_{c2_i} = \begin{cases} V_{(c+ш)_i}, при \;\; V_{(c+ш)_i} - V_{ш_i} \geq 10 \\ V_{(c+ш)_i} - \Delta, при \;\; V_{(c+ш)_i} - L_{ш_i} < 10 \end{cases}, \quad (2)$$

где Δ - поправка в дБ;

i – номер октавной полосы.

Значение поправки Δ берется согласно таблице 1.

Таблица 1 - Значение поправки для L_{c2} и V_{c2}.

$L_{(c+ш)_i} - L_{ш_i}$ $V_{(c+ш)_i} - V_{ш_i}$	>10	6..10	4..6	3	2	1	0,5
Δ, дБ	0	1	2	3	4	7	10

- рассчитать октавные уровни звукоизоляции (виброизоляции) Q_i (G_i) по формулам 3 и 4.

$$Q_i = L_{c1_i} - L_{c2_i}, \quad (3)$$

где i – номер октавной полосы.

$$G_i = V_{c1_i} - V_{c2_i}, \quad (4)$$

где i – номер октавной полосы.

После окончания расчетов сравниваются полученные результаты с установленными нормированными значениями.

Результаты проведенного контроля представляются в протоколе, а также формулируются рекомендации и предложения по обеспечению выполнения норм защищенности.

Акустический и вибрационный контроль ориентирован на использование контрольно-измерительной аппаратуры общего применения. Но даже специальные автоматизированные комплексы контроля выполнения норм противодействия акустической речевой разведке часто не имеют в своем составе расчетной программы. Учитывая то, что при проведении контроля приходится производить вычисления, в среднем, для 20-30 контрольных точек, данный процесс представляется весьма трудоемким, поэтому существует необходимость автоматизировать его составляющие.

Для этой цели был разработан программный продукт, основной задачей которого является расчет коэффициентов звуко- и виброизоляции, автоматизированный анализ результатов и формирование протокола инструментально - расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации. Внешний вид интерфейса главного окна программы показан на рисунке 1.

Программа позволяет осуществлять:

- ввод количества контрольных точек и ограждающих конструкций с указанием типов и их параметров;
- расчет уровня акустического (вибрационного) сигнала в каждой контрольной точке для октавных полос со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.;
- расчет коэффициентов звуко- и виброизоляции для каждой контрольной точки для октавных полос со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;
- анализ результатов расчетов и выявление контрольных точк, в которых не выполняются нормы защищенности;
- формирование состава и содержания протокола инструментально – расчетной оценки в формате MS Word;
- сохранение результатов измерений и расчетов в файлах.

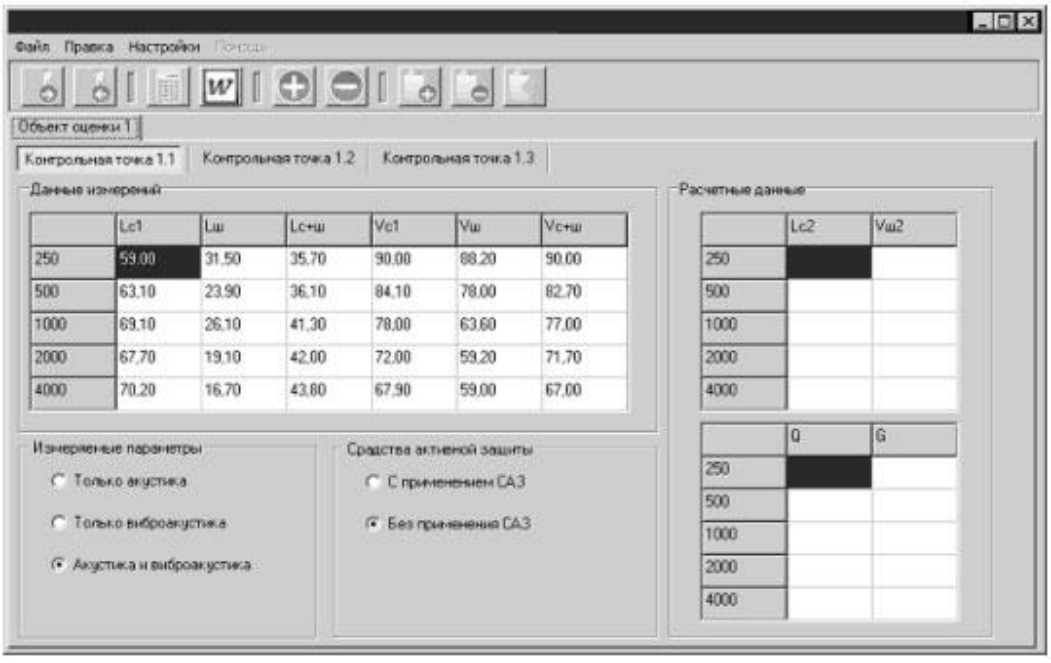


Рисунок 1. Интерфейс главного окна программы

Обладая удобным для оператора интерфейсом, автоматизируя этапы процесса расчета показателей защищенности и анализа результатов, а также составления протокола контроля объекта, программный продукт позволяет повысить эффективность аттестации помещений с использованием контрольно-измерительной аппаратуры общего применения.

Литература:
1. Зайцев А.П., Шелупанов А.А. Техническая защита информации. Учеб. пособие. - М.: Горячая линия-Телеком , 2007- 616 с.

А.Э. Боярчук, *И.А. Енгибарян, *В.И. Юхнов

ОСНОВНЫЕ УЯЗВИМОСТИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Донской государственный технический университет, г. Ростов-на-Дону, Россия
*Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: системы контроля и управления доступом, персональные данные, информационные системы персональных данных, каналы утечки информации, модель потенциального нарушителя.

Описана проблема широкого спектра угроз охраняемому объекту, его системе защиты и самой системе контроля и управления доступом как целостной системе защиты объекта. Обеспечение информационной безопасности систем контроля и управления доступом является одной из важнейших составных частей общей системы обеспечения безопасности объекта.….

A.E. Boyarchuk, *I.A. Yengibaryan, *V.I. Yukhnov

THE MAIN VULNERABILITY IN PROVIDING INFORMATION SYSTEM SECURITY MONITORING AND ACCESS CONTROL

Don state technical University, Rostov-on-don, Russia
*North-Caucasian branch of the Moscow technical University of communications and computer science, Rostov-on-don, Russia

Keywords: control systems and access control, personal data, the personal data information systems, channels of information leakage, the model potential offender.

Describes the wide range of threats to the protected object, the system for the panels and the control system and access control as an integral protection system object. Information security control systems and access control is one of the most important parts of the overall system security object.....

Практически повсеместно задача защиты информации представляется как предупреждение несанкционированного доступа и получения ее в системах обработки данных.

Сегодня системы контроля и управления доступом (СКУД) широко применяются как дополнение к существующим системам защиты и охраны и представляют собой самое интенсивно развивающееся направление в технике обеспечения безопасности. Следует отметить, что функциональность систем контроля и управления доступом увеличивается год от года и в настоящее время СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом.

Субъект доступа (сотрудник, посетитель) при доступе на объект (охраняемую территорию, помещение) для идентификации должен предъявить какой-либо идентификатор доступа. СКУД на основе установленных администратором политик безопасности и прав субъекта принимает решение о доступе субъекта на объект. При этом в качестве уникальных данных, присущих

субъекту доступа, СКУД оперирует сведениями о фамилии, имени, отчестве субъекта, его должности, служебном телефоне, адресе регистрации. В ряде случаев в СКУД фиксируются паспортные данные субъекта и иные сведения.

Системы контроля и управления доступом, не учитывающие (не обрабатывающие) персональные данные (ПДн), составляют малую часть множества различных СКУД и в настоящее время практически не применяются в организациях. Таким образом, сведения, обрабатываемые СКУД, в подавляющем большинстве случаев содержат персональные данные. Следовательно, СКУД являются информационными системами персональных данных (ИСПДн).

Выбор варианта структуры и аппаратно-программных средств СКУД неразрывно связан с требованиями системной концепции обеспечения безопасности объекта. Наиболее рациональной является реализация интегрированной СКУД, так как в ней решается большинство задач автоматического управления контроля доступом, перемещения персонала, анализа попыток несанкционированного проникновения, создания разного уровня вложенных баз данных, обслуживающих службу безопасности, и т. д.

Таким образом, легко видеть, что проблема обеспечения информационной безопасности системы контроля и управления доступом любого объекта является неотъемлемой частной проблемой общей задачи обеспечения защиты объектов.

Исследование уязвимостей в обеспечении информационной безопасности системы контроля и управления доступом позволяет определить основные каналы утечки информации в СКУД, виды угроз, а также сформировать основные модели потенциального нарушителя.

В общем виде все нарушения целостности информации могут происходить как преднамеренно, так и случайно. В качестве основных каналов утечки или нарушения целостности информации, нарушения работоспособности технических средств могут рассматриваться:

1. Случайное прослушивание конфиденциальных и телефонных разговоров без использования специальных технических средств при проведении профилактических работ;
2. Непреднамеренный просмотр информации с экранов дисплеев и других средств ее отображения;
3. Целенаправленный несанкционированный доступ к информации;
4. Побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;
5. Наводящий сигнал на провода и линии, выходящие за пределы защищенной зоны;
6. Акустическое излучение информативного речевого сигнала;
7. Прослушивание телефонных и радио переговоров;
8. Воздействие на технические и программные средства в целях нарушения целостности информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена;
9. Хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
10. Преднамеренный просмотр информации с экранов дисплеев и других средств отображения информации с помощью специальных оптических устройств;
11. Визуальное наблюдение за объектом в зоне прямой видимости, в том числе с помощью фотографических и оптических средств разведки [1].

Основными источникам угроз информационной безопасности в общем случае для всех объектов, и для объектов СКУД в том числе, являются: природные - стихийные бедствия и катастрофы, техногенные - отказы и неисправности технических средств и средств информатизации, человеческий фактор - деятельность человека.

Источники угроз информационной безопасности СКУД, как и для других объектов, могут быть внешними или внутренними.

Внешние угрозы исходят от природных явлений, катастроф, внешних нарушителей, лиц, входящих в состав пользователей и обслуживающего персонала СКУД.

Внутренние угрозы исходят от пользователей, обслуживающего персонала СКУД с различными правами доступа, а также от разработчиков системы.

Определим типы угроз, генерирующие отказы и неисправности технических средств и средств информатизации СКУД:

1. Отказы и неисправности технических средств идентификации личности, управления доступом, систем сбора и обработки информации от всех датчиков средств и систем информатизации, в том числе из-за нарушений в системе электропитания.
2. Отказы и неисправности средств защиты информации и технических средств контроля эффективности принятых мер по защите информации.
3. Сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности мер по защите информации.

Деятельность человека — основной источник угроз по отношению к информации и СКУД. Как правило, она классифицируется как непреднамеренная и преднамеренная.

Непреднамеренные действия человека:

- некомпетентные действия персонала, приводящие к ЧП и авариям;
- ошибки при проектировании СЮД и ее отдельных систем;
- ошибочные действия пользователей и обслуживающего персонала СКУД, в том числе администратора АС, приводящие к нарушению целостности и работоспособности СКУД, непреднамеренному заражению компьютеров;
- неосторожные действия персонала при техническом обслуживании или ремонте технических средств, приводящие к повреждению аппаратуры;
- неправильное обращение с магнитными носителями при использовании и хранении;
- халатность при исполнении служебных обязанностей.

Преднамеренная деятельность человека:

- деятельность спецслужб по добыванию информации, навязыванию ложной информации, нарушению работоспособности СКУД в целом и отдельных компонентов;
- противозаконная деятельность международных или отечественных формирований или лиц, направленная на проникновение на ядерно-опасные объекты для хищений, диверсий в отношении ядерных материалов;
- нарушение пользователями и обслуживающим персоналом СКУД установленных регламентов работы и требований информационной безопасности.

Преднамеренные действия вероятных нарушителей:

- хищение оборудования — частей системы;
- хищение магнитных носителей с целью копирования, подделки или уничтожения данных, получения доступа к данным и программам;
- разрушение оборудования, магнитных носителей или дистанционное стирание информации;
- считывание информации или копирование данных с носителей;
- внесение изменений в базу данных или файлы в пределах выделенных полномочий для подделки или уничтожения информации;
- считывание или уничтожение информации, ее изменение с присвоением полномочий подбором паролей при визуальном наблюдении;
- несанкционированное изменение собственных полномочий на доступ или полномочий других пользователей, минуя регламенты безопасности;
- сбор и анализ использованных распечаток, документации, других материалов и копирование ее;
- визуальный перехват информации с экранов дисплеев или клавиатуры;
- перехват электромагнитного излучения от технических средств СКУД для копирования информации и выявления процедур доступа;
- выявление паролей зарегистрированных пользователей при негласном активном подключении к кабелю локальной сети при имитации запроса сетевой операционной системы;
- установка скрытых передатчиков для вывода информации или паролей с целью копирования или доступа по легальным каналам связи с компьютерной системой в результате негласного посещения в нерабочее время или оставления их без присмотра в рабочее время;
- создание условий для разрушения информации, несанкционированного доступа к ней на разных этапах производства или доставки оборудования, разработки или

внедрения системы путем включения в аппаратуру и ПО программных закладок, программ-вирусов, ликвидаторов с дистанционным управлением и т. п.;

- проникновение в систему через телефонную сеть при перекоммутации канала на модем злоумышленника после авторизации легального пользователя в сети с целью присвоения его прав на доступ к данным;
- визуальное наблюдение за объектом в зоне прямой видимости с помощью технических средств разведки.

Наиболее вероятными способами нарушения информационной безопасности СКУД могут быть: информационные; программно - математические; физические; радиоэлектронные; организационно-правовые.

Информационные способы нарушения информационной безопасности: противозаконный сбор, распространение и использование информации; манипулирование ею (дезинформация, сокрытие, искажение); незаконное копирование, уничтожение, хищение информации; нарушение адресности и оперативности обмена, нарушение технологии обработки данных и обмена.

Программно-математические способы: внедрение программ-вирусов, «программных закладок» на стадиях проектирования и эксплуатации.

К физическим способам нарушения информационной безопасности относятся: уничтожение, хищение, разрушение средств обработки и защиты информации, средств связи, машинных и других оригиналов носителей информации; хищение ключей средств криптографической защиты; воздействие на обслуживающий персонал и пользователей системы для создания благоприятных условий для реализации угроз ИБ; диверсионные атаки на объекты информатизации.

Радиоэлектронные способы нарушения информационной безопасности включают: перехват информации в технических каналах и линиях связи, в сетях передачи данных; внедрение электронных устройств перехвата в технические средства и помещения; дезинформация по сетям передачи данных и линиям связи; подавление линий связи и систем управления.

Организационно-правовые способы нарушения ИБ — это невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных документов в области ИБ.

Наиболее опасными и реальными угрозами ИБ СКУД являются несанкционированный доступ и воздействие по отношению к информации, обрабатываемой средствами вычислительной техники и связи, а также средствам ее обработки, которые могут быть реализованы нарушителями, как персоналом СКУД, так и посторонними лицами.

Исходя из изложенного можно сделать вывод о широком спектре угроз охраняемому объекту, его системе защиты и самой системе контроля и управления доступом как целостной системе защиты объекта. Обеспечение информационной безопасности систем контроля и управления доступом является одной из важнейших составных частей общей системы обеспечения безопасности объекта.

Литература:

1. Ворона В. А.. Тихонов В. А. Системы контроля и управления доступом. М.: Горячая линия - Телеком, 2010. - 272 с.

А.Э. Боярчук, *И.А. Енгибарян, *В.И. Юхнов

ФОРМАЛИЗАЦИЯ МОДЕЛИ ЗНАНИЙ ОБУЧАЕМЫХ

Донской государственный технический университет, г. Ростов-на-Дону, Россия
*Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: предметная область, модель предметной области, семиотическая сеть, модель обучаемого.

Описана проблема формализации модели предметной области как для управления процессом обучения, так и для обоснованного решения вопроса о включении тех или иных фрагментов знаний в программу учебного курса. Она упрощает разработку и понимание учебных программ, особенно типовых и базовых, а также проведение экспертизы их качества….

A.E. Boyarchuk, *I.A. Yengibaryan, *V.I. Yukhnov

THE FORMALIZATION OF THE KNOWLEDGE OF THE TRAINEES

Don state technical University, Rostov-on-don, Russia
*North-Caucasian branch of the Moscow technical University of communications and computer science, Rostov-on-don, Russia

Keywords: domain, domain model, a semiotic network model of the learner.

Described the problem of formalization of the domain model for learning management and informed decision on the inclusion of certain fragments of knowledge in the curriculum. It simplifies the development and understanding of the curriculum, especially the standard and base, as well as examination of their quality....

В автоматизированном обучении модель предметной области (МПО) приобретает особую роль, т.к. качество обучения практически определяется алгоритмом управления процессом обучения, который базируется на этой модели. Предметная область (ПО) характеризуется сущностями и связями между ними. В качестве сущностей ПО в обучающих системах можно рассматривать понятия или темы, каждой из которых соответствует единица учебного материала, не требующая (с точки зрения преподавателя) деления на подтемы. Каждая тема описывается набором параметров (атрибутов), существенных для управления обучением.

Связь между темами i и j подразумевает зависимость между ними, которую можно интерпретировать так: для понимания темы j нужно знать тему i. Таким образом, связи могут определять последовательность изучения тем. Связи между темами могут быть факультативными и обязательными. В случае факультативной связи последовательность изучения тем носит рекомендательный характер. Связи могут иметь также различную семантику и взаимозависимости. В частности, структура ПО не может содержать циклов. В остальном никаких ограничений на структуру ПО не накладывается. Назовем курсом совокупность предметных знаний, внесенных в АОС на этапе заполнения и предназначенных для обучения по определенному предмету (специальности).

В большинстве существующих обучающих программ учебный материал имеет линейную структуру, соответствующую последовательности изложения материала. Такой подход не может считаться оптимальным, т.к. в общем случае учебный материал может не иметь заранее определенного наилучшего пути следования, поэтому, подчиняя процесс обучения некоторой однонаправленной форме, мы тем самым можем дать неверное представление об истинности тех или иных явлений или фактов.

Рассмотрим возможный вариант организации модели предметной области произвольной структуры. Для этого сначала определим требования, которым она должна удовлетворять.

На основании вышеизложенного понимания структуры предметной области ее модель должна удовлетворять следующим требованиям: возможность отражать различные типы связей между элементами; возможность получения целостного образа знаний; возможность объединения процедурных и декларативных знаний.

Этим требованиям удовлетворяют фреймовая и семантическая модели представления знаний. Семантические сети и фреймовые модели близки друг другу, но механизм вывода в семантических сетях более прозрачен.

Предлагается подход, при котором типы семантических связей не выделяются, а интерпретации связей выполняется процессами, относящимися к соответствующим вершинам. Кроме возможности не ограничивать пользователя определенными типами связей, такой метод позволяет ввести в модель предметной области прагматику, т.е. учет цели использования модели.

Семантическая модель базируется на семантической сети [1]. Это система знаний, имеющая определенный смысл в виде целостного образа сети. Механизм вывода заключается в распространении по сети возбуждения в зависимости от топологии сети и входных данных.

Определим семантическую сеть Ω как двойку вида

$$\Omega = \{V, D\}, \tag{1}$$

где $V = \{v_i\}$ – множество вершин (узлов сети), а $D = \{d_j\}$, – множество дуг.

Вершина v_i семантической сети может быть определена как

$$v_i = \{S, c\}, \tag{2}$$

где $S = \{s_k\}$ – множество точек входа в вершину, а с – функция, определяющая состояние вершины:

$$c = \vee f_n, \tag{3}$$

т.е. дизъюнкция состояний множества синапсов S, относящихся к вершине v_i.

Синапс s_k вершины v_i есть пара вида:

$$s_k = (p_k, f_k), \tag{4}$$

где p_k – процесс, связанный с данным синапсом, а функция f_k определяется как произвольная логическая функция от состояний вершин v_m, дуги от которых входят в синапс s_k, например, конъюнкция:

$$f_k = \vee v_m. \tag{5}$$

Узлами сети могут быть любые элементы процесса обучения: теоретический материал по определенной теме курса, лабораторные и контрольные работы, задания для самоконтроля и т.п. С программной точки зрения каждая вершина представляет собой некоторый процесс. Дуги между элементами определяют взаимосвязи между вершинами и задают последовательность изучения курса.

На основании такой структуры каждому обучаемому можно задавать свое подмножество изучаемых тем (выполняемых работ), которое будет определяться, например, списками начальных и конечных вершин сети. В качестве начальной вершины может выступать вершина, которая имеет хотя бы одну исходящую дугу, в качестве конечной – вершина, в которую можно попасть из заданных начальных вершин. Изучение курса заключается в прохождении по всем вершинам, входящим в маршруты от начальных до конечных вершин.

Организация МПО в виде семиотической сети, в основе которой лежит орграф, позволяет использовать для ее анализа аппарат теории графов.

Пусть *G* – орграф, описывающий МПО, $VG = \{v_i\}$ – множество вершин и $VE = \{e_i\}$ – множество дуг этого орграфа. Орграф *G* не должен содержать:

1. Петель, т.е. дуг (v_i, v_i).
2. Циклов, т.е. таких маршрутов $v_1, e_1, v_2, e_2, \ldots, e_k, v_{k+1}$, в которых $v_1 = v_{k+1}$. (где v_i, e_i – соответственно номера вершин и дуг, входящих в маршрут).
3. Несвязных вершин или подграфов. Для определения наличия несвязных вершин (подграфов) орграф рассматривается как неориентированный граф. Неориентированный граф является связным тогда и только тогда, когда для произвольной фиксированной вершины v существует маршрут $(v,\ldots,u)$, где u – любая другая вершина графа.

Последовательность освоения тем должна быть такова, чтобы к началу изучения темы *i* все предшествующие ей темы (понятия) были уже изучены. Эта задача сводится к задаче раскраски вершин графа. Напомним, что раскраской графа G называется произвольная функция вида

$$f: VG \to \{1,2,,k\}, \tag{6}$$

где k – количество различных красок. В данном случае решением задачи определения последовательности изучения тем является такая раскраска орграфа G, при которой для любого маршрута $v_1, e_1, v_2, e_2,\ldots, e_k, v_{k+1},$ вершины которого раскрашены цветами $l_1, l_2,\ldots, l_k,$ верно утверждение $l_i < l_j$, если $i < j.$

Модель предметной области предназначена для решения двух взаимосвязанных задач. Эта модель отражает связи между элементами учебного процесса и, следовательно, определяет последовательность изучения материала (административная задача), а также возможные причины ошибок обучаемого, возникших из-за незнания предшествующего материала (задача консультации и адаптивного управления).

Для организации управления процессом обучения недостаточно иметь модель предметной области. Система должна иметь информацию о том, в каком состоянии находится процесс обучения конкретного обучаемого. Для учета этих сведений вводится модель обучаемого (МО). Эту модель можно определить как совокупность набора характеристик обучаемого и методов (правил) обработки этого набора. Она должна включать в себя информацию: о цели обучения; о знаниях обучаемого в рамках изучаемого курса (текущее состояние процесса обучения); об особенностях подачи учебных материалов и выбора контрольных заданий и вопросов; о правилах изменения модели обучаемого по результатам работы с обучаемым.

Определим функции модели обучаемого: адаптация к обучаемому управляющих воздействий системы; определение уровня знаний студента по изучаемому курсу и степени достижения заданной цели обучения.

Модель обучаемого формируется (и изменяется) в процессе работы с ним.

Предоставляя преподавателю возможность определять для модели обучаемого произвольный набор параметров, логично определить целевую модель через эти же параметры (или их подмножество). Представим описательную часть МО как набор параметров $M\{p_1, p_2,\ldots, p_n\}.$ Каждый из этих параметров задается произвольным арифметическим или логическим выражением, которое может включать операции (арифметические или логические), константы и параметры, входящие в МО. Тогда для целевой модели обучаемого:

$$M^c\{p_1^c, p_2^c,\ldots, p_k^c\}, \tag{7}$$

где $k \le n.$

Представим декларативную часть модели обучаемого в виде комбинации параметров. Каждый из параметров является произвольной характеристикой обучаемого, отдельной темы или отдельного вопроса. Совокупность характеристик определяется преподавателем на этапе формирования описания модели обучаемого и предметной области. Для каждого параметра P_i устанавливаются возможные значения в виде диапазона или списка значений:

$$Pi = \begin{cases} < список\_значений > \\ \min\ :\ \max \\ NULL \end{cases}, \tag{8}$$

где <список значений> – перечисление возможных значений параметра; min, max – минимальное и максимальное значения параметра, а значение NULL в каждом конкретном случае означает, что для данного обучаемого (темы, вопроса) этот параметр не установлен.

Изначально об обучаемом ничего не известно, и значения всех параметров принимаются равными некоторым усредненным значениям, которые определяются преподавателем, а по умолчанию приравниваются нулю. При прохождении начального тестирования (и/или очередной темы) значения параметров модели, установленных для данной темы (не равных NULL), пересчитываются следующим образом. По результатам опроса обучаемого ему выставляется оценка $b: b \in [\min, \max].$ Эта оценка нормализуется:

$$b = 0.5\text{-}(\max - b)/(\max - \min). \tag{9}$$

Таким образом, оценка $b \in [-0.5,\ 0.5]$.

Новое среднее значение параметра P_i на текущий момент t дискретного локального времени рассчитывается исходя из предыдущего значения этого параметра

$$P_i(t=1) = P_i(t) + \frac{b * p_i}{(t+1)}, \tag{10}$$

где b – нормализованное значение последней оценки, полученной обучаемым, p_i – значение параметра P_i, установленное для данной темы, а $P_i(t)$ – среднее значение параметра P_i на предыдущий момент времени, которое рассчитывается как среднее арифметическое значение

$$P_i(t) = \frac{\sum_{i=1}^{t} p_i}{(t)}. \tag{11}$$

Под локальностью времени подразумевается, что для каждого параметра P_i ведется свой отсчет времени t, равный количеству тем (вопросов), для которых этот параметр установлен.

Значения параметров модели обучаемого используются в процессе работы с обучаемым для определения стратегии и тактики поведения системы. Управление моделью обучаемого также возлагается на базу знаний.

Литература:

1. Шихнабиева Т.Ш. Использование адаптивных семантических моделей для представления и контроля знаний в системах обучения информатике. // Мониторинг: Наука, Образование, Технологии. 2009. С. 66-72.

А.Э. Боярчук, *И.А. Енгибарян, *В.И. Юхнов

ФОРМАЛЬНОЕ ОПРЕДЕЛЕНИЕ ПОНЯТИЯ ЧАСТИЧНОЙ КОРРЕКТНОСТИ ПРОГРАММЫ

Донской государственный технический университет, г. Ростов-на-Дону, Россия
*Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: статический контроль программы, доказательство правильности, частичная корректность.

Описана проблема математически точного определения понятия частичной правильности программы. Определены основные разновидности контроля программного обеспечения - статический и динамический. Наибольшую сложность составляет верификация программы или формальное доказательство правильности на этапе статического контроля программы с помощью инструментальных средств. Определена корректность программы как ее свойство по отношению к целям, поставленным заказчиком перед ее разработкой …..

A.E. Boyarchuk, *I.A. Yengibaryan, *V.I. Yukhnov

FORMAL DENITION OF THE NOTION OF PARTIAL CORRECTNESS OF THE PROGRAM

Don state technical University, Rostov-on-don, Russia
*North-Caucasian branch of the Moscow technical University of communications and computer science, Rostov-on-don, Russia

Keywords: static control programs, proof of the correctness partial correctness.

The problem described mathematically precise definition of the notion of partial correctness of the program. Defined the basic types of control software - static and dynamic. The greatest difficulty is the verification program or a formal proof of the correctness of phase static control program using the workbench. Determined the correctness of the program as its property in relation to the objectives set by the customer before developing.....

После завершения проектирования программы и ее кодирования начинается этап ее контроля. Основными разновидностями контроля программного обеспечения являются визуальный, статический и динамический.

Третьей стадией статического контроля программы может являться ее верификация или формальное доказательство правильности (корректности).

Будем понимать под корректностью - свойство самой программы по отношению к целям, поставленным заказчиком перед ее разработкой.

Отличие понятий корректности и надежности заключается в следующем:

- надежность характеризует как программу, так и ее окружение (качество работы аппаратуры, квалификацию пользователей, параметры окружающей среды и т.п.);
- понятие надежной программы обычно допускает определенную, хотя и малую, долю ошибок в ней, а термин «надежность» как раз и оценивает вероятность их появления.

Очевидно, что не всякая синтаксически правильная программа является корректной в указанном ранее смысле, т.е. корректность характеризует семантические свойства программ.

С учетом специфики появления ошибок в программах можно выделить две стороны понятия корректности [1]:

- корректность как точное соответствие целям разработки программы, отраженным в ее спецификации, при условии завершения программы (частичная корректность);
- завершение программы, т.е. достижение ею в процессе выполнения своей конечной точки.

В зависимости от выполнения или невыполнения каждого из двух названных свойств корректности программы будем различать шесть задач анализа корректности: доказательство частичной корректности; доказательство частичной некорректности; доказательство завершения программы; доказательство незавершения программы; доказательство тотальной корректности; доказательство некорректности.

Определим математически точное определение понятия частичной корректности программы.

Пусть P есть некоторая программа, свойства которой во входной и выходной точках определяются некоторыми утверждениями на языке логики предикатов первого порядка (логическом языке спецификации).

Эти утверждения связывают входные и выходные переменные программы:

$$S\{P\}Q, \tag{1}$$

где $S(X)$ - входной предикат, определяющий множество допустимых значений входных переменных X; $Q(X,Y)$ - выходной предикат, формально определяющий цель программы, т.е. связывающий входные данные X с выходными данными Y.

Предикаты S и Q специфицируют программу P. Пусть предикат $term(P)$ есть предикат завершения программы P, т.е. $term(P) = true$, если P завершается, и $term(P) = false$, если P не завершается.

Тогда программа P будет называться частично корректной по отношению к S и Q, если

$$\forall A, S(A) \wedge term(P) \Rightarrow Q(A,B), \tag{2}$$

где A - множество значений входных данных P; B - множество значений выходных данных P.

Методы доказательства частичной корректности программ, как правило, опираются на аксиоматический подход к формализации семантики языков программирования.

Аксиоматическая семантика языка программирования представляет собой совокупность аксиом и правил вывода. С помощью аксиом задается семантика простых операторов языка (присваивания и вызова процедур ввода - вывода). Например, семантику оператора присваивания будем задавать следующей аксиомой:

$$P_e^x\{x := e\}P \tag{3}$$

(если формула P истинна для подстановки выражения e вместо всех свободных - не связанных кванторами - вхождений переменной x перед выполнением оператора присваивания $x := e$, то формула P должна быть истинна после выполнения присваивания).

Семантику составных операторов языка программирования (последовательности, выбора, цикла) зададим с помощью правил вывода, записываемых в виде

$$\frac{A,\ B}{C} \tag{4}$$

(из предпосылок A и B выводится результат C).

Например, семантика оператора условного выбора определим с помощью следующего правила вывода:

$$\frac{P)Q\{A\}R,\ P)(Q\{B\}R}{P\{if\ \ Q\ then\ \ A\ else\ \ B\}R}. \tag{5}$$

Особняком среди правил вывода для составных операторов языка программирования стоят правила вывода для операторов цикла, требующие знания так называемого инварианта цикла (формулы, истинность которой не изменяется при любом выполнении тела цикла).

Например, правило вывода для оператора цикла с предусловием определим следующим образом:

$$\frac{I)Q\{A\}I}{I\{while\ Q\ do\ A\}I)Q}, \tag{6}$$

где I - инвариант цикла.

Заметим, что инвариант цикла необязательно является единственным.

Построение инварианта для оператора цикла по его тексту является алгоритмически неразрешимой задачей, поэтому для описания семантики циклов требуется своего рода подсказка со стороны разработчика программы.

Аксиомы и правила вывода в совокупности могут образовывать формальную теорию семантики языка программирования, в которой можно проводить доказательство составленных на этом языке программ.

Рассмотрим метод доказательства частичной корректности программ.

Метод состоит из трех этапов.

1. Получение аннотированной программы. На этом этапе для синтаксически правильной программы должны быть заданы следующие утверждения на языке логики предикатов первого порядка: входной предикат; выходной предикат; по одному утверждению для каждого цикла (эти утверждения создаются для точки входа в цикл и характеризуют семантику вычислений в цикле).

Кроме перечисленных ранее обязательных могут быть заданы и другие утверждения (например, в точках вызова процедур). Эти утверждения (так называемые логические

спецификации) могут не совпадать с инвариантами соответствующих точек программы, но для корректной программы из истинности инвариантов должна следовать истинность логических спецификаций.

Первый этап метода индуктивных утверждений является неформальным и неавтоматизируемым. Могут быть лишь созданы инструментальные средства, которые укажут разработчику места в программе, в которых обязательно должны быть заданы логические спецификации, а также предложат «кандидатов» в инварианты цикла.

2. Генерация условий корректности. На этом этапе определяется множество формул на языке логики предикатов первого порядка, характеризующих свойство частичной корректности анализируемой программы. Генерация этих формул, называемых условиями корректности, происходит на основе полученного на первом этапе текста аннотированной программы и формальной аксиоматической семантики использованного языка программирования.

Этот этап может быть полностью автоматизирован.

3. Доказательство условий корректности, полученных на втором этапе. Истинность всех условий корректности будет означать выполнение свойства частичной корректности анализируемой программы.

Этот этап формализуем и автоматизируем лишь частично. При его проведении условия корректности рассматриваются как теоремы формальной теории для заданной предметной области.

Доказательство неистинности условий корректности свидетельствует о неправильности либо программы, либо ее спецификации, либо и программы и спецификации.

Динамический контроль программы - это проверка ее правильности при выполнении на компьютере (тестирование программы). Эффективность тестирования во многом определяется правильным определением его цели. Неверно определять тестирование как процесс выполнения программы с целью демонстрации отсутствия в ней ошибок.

Во-первых, эта цель недостижима, так как никакое самое тщательное тестирование не дает гарантии отсутствия ошибок в программе, во-вторых, подобная цель тестирования невольно ориентирует на щадящий режим испытаний программы.

Правильным является определение тестирования как процесса выполнения программы с целью обнаружения в ней ошибок. Такое определение стимулирует именно поиск ошибок в программе, и тест, не позволивший выявить ошибку в программе, будет считаться неудачным. Под тестом здесь и далее будем понимать набор значений входных данных, на котором проверяется правильность программы.

Можно предложить следующие принципы организации тестирования программного обеспечения:

- необходимой частью каждого теста должно являться описание ожидаемых результатов работы программы;
- следует по возможности избегать тестирования программы ее авторами;
- организация - разработчик программного обеспечения не должна единолично его тестировать, а должна привлекать для этого независимых экспертов;
- правилом должно являться доскональное изучение результатов каждого теста;
- необходим тщательный подбор тестов не только для правильных входных данных, но и для неправильных;
- анализ результатов каждого теста должен включать в себя проверку возможного выполнения программой не предусмотренных в спецификации действий;
- необходимо сохранение результатов каждого теста для повышения эффективности проверки программы после ее модификации или установки у пользователя;
- не следует планировать проведение тестирования исходя из предположения, что в программе не будут обнаружены ошибки;
- следует учитывать так называемый принцип скопления ошибок, согласно которому вероятность наличия необнаруженных ошибок в некоторой части программы прямо пропорциональна числу ошибок, уже обнаруженных в этой части;
- следует всегда помнить, что тестирование - творческий процесс, и не относиться к нему, как к рутинному занятию.

Несмотря на достаточную сложность процесса верификации и динамического контроля программы, а также на то, что даже успешно завершенная верификация и контроль не дают

гарантий качества программы (так как ошибка может содержаться и в спецификации, относительно которой доказана корректность программы), автоматизация методов аналитического доказательства правильности программы очень полезно для уточнения ее смысла, а знание этих методов благотворно сказывается на квалификации программиста.

Литература:

1. Соммервилл И. Инженерия программного обеспечения, 6-е издание.: Пер. с англ. – М.: Издат. Дом. «Вильямс», 2002. – 624 с.

А.В. Ерохин, А.А. Гусаров

ВИРУСЫ: НЕСАНКЦИОНИРОВАННАЯ УГРОЗА КОМПЬЮТЕРУ

Ростовский Государственный Экономический Университет (РИНХ),
г. Ростов-на-Дону, Россия

Ключевые слова: компьютерный вирус, классификация, информационная безопасность, файл, обнаружение, заражение.

Описана проблема возможного несанкционированного доступа к компьютеру и его содержимому, а также угроза заражения компьютерными вирусами различных информационных систем. Приведены классификации существующих компьютерных вирусов по различным критериям, их различные примеры, при помощи которых описываются алгоритмы работы компьютерных вирусов, принадлежащих к различным типам классификаций. Описаны некоторые алгоритмы и процессы, при помощи которых компьютерные вирусы препятствуют своему обнаружению различными антивирусными программами и детекторами.

A.V. Erokhin, A.A. Gusarov

VIRUSES: UNAUTHORIZED THREAT TO COMPUTER

Rostov State University of Economics (RINH), Rostov-on-Don, Russia

Keywords: virus, computer, classification, program code, file, detection, infection.

The problem of possible unauthorized access to computer and its contents is described and threat of infection different information systems with computer viruses. The classifications of existing computer viruses by different criterions are given. Different examples of computer viruses are given, with which help the algorithm of functioning of computer viruses which belongs to different types of classifications are described. Some algorithms and processes of computer viruses' resistance to detection by different antivirus programs and detectors are described.

Компьютерные вирусы прошли длительную эволюционную линию, приспосабливаясь к изменчивому миру операционных систем и защитных механизмов. По самым скромным подсчетам было написано более полумиллиона вирусов и разработана масса технологий противостояния различным защитным механизмам. Вирусы освоили практически все: начав с исполняемых объектов, пошло распространение вирусов и на файлы данных: начали с макросов в документах MSOffice, а затем все более смелые атаки на переполняющиеся буфера в jpg/gif/mp3/midi и прочих подобных форматах, считавшимися ранее принципиально недоступными для заражения. К концу прошлого века вирусы получили повсеместное распространение, освоив не только Windows, Linux/BSD, однако и мобильные платформы.

Компью́терный ви́рус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, загрузочные секторы, системные области памяти, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, приведения в негодность структур

размещения данных, удаления файлов, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Одним из первых вирусов по праву можно назвать Elk Cloner. Elk Cloner — один из прародителей компьютерных вирусов, появившийся «in-the-wild», то есть был обнаружен на компьютерах пользователей, находящейся не в системе, в которой он был разработан. Cloner был написан в 1981 году 15-летним школьником Ричардом Скрента для компьютеров Apple II.

Cloner распространялся, заражая операционную систему DOS для Apple II, записанную на гибких дисках. После загрузки компьютера с зараженной дискеты автоматически запускалась копия вируса. Вирус не оказывал влияния на работу компьютера, за исключением наблюдения за доступом к дискам. Когда происходил доступ к незараженной дискете, вирус копировал себя туда, заражая её, медленно распространяясь с диска на диск.

Elk Cloner не причинял вреда намеренно, хотя он мог повредить диски, содержащие нестандартный образ DOS, затирая резервные дорожки диска вне зависимости от их содержимого. После каждой 50-й загрузки выводился на экран стих.

Существует множество классификаций компьютерных вирусов, например, по их среде обитания и методам противостояния защитным механизмам.

По среде обитания вирусы делятся на 3 группы: файловые, загрузочные и макровирусы. Файловые вирусы внедряются чаще всего в исполняемые модули, то есть в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, в таком виде они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Макро-вирусы внедряются в форматы файлов, используемые наиболее популярными редакторами такими как Microsoft Word или Microsoft Excel. Эти вредоносные макросы, обладающие способностью создавать свои копии и совершать некоторые действия без ведома пользователя, например, изменять содержание документов, стирать файлы или директории. Это и есть макровирусы.

По методу противостояния защитным механизмам, вирусы получили названия стелс-вируса и полиморфного вируса. Сегодня, чаще всего эти методики применяются совместно.

Стелс-вирусы.

Стелс-вирус (англ. stealth virus — вирус-невидимка) — вирус, который полностью или частично скрывает свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (памяти, загрузочных секторах, элементах файловой системы и т. д.). Название данного типа вирусов происходит от названия малозаметных истребителей «Стелс». Оно подчеркивает, что такие вирусы могут оставаться незамеченными для антивирусных программ.

Для скрытия своего кода они используют в основном два способа. Суть первого заключается в том, что вирус автоматически перехватывает команды, которые направлены на чтение-запись зараженного сектора и моментально подставляет какой-либо незараженный файл. Благодаря таким действиям, вирус становится практически невидимым для антивирусных программ (которые не могут лечить оперативную память).

Второй способ разработан с целью борьбы с антивирусами, которые поддерживают специальные команды чтения секторов напрямую через отдельные порты контроллера жесткого диска. Во время запуска программы (антивируса, к примеру), такие вирусы восстанавливают ранее зараженные сектора жесткого диска, а после окончания ее работы опять восстанавливают зараженное состояние.

Антивирусы-полифаги эффективны в борьбе с уже известными стелс-вирусами, если они уже знакомы разработчикам и есть в базах, иначе, если вирус неизвестен, то он останется незамеченным. Главное в борьбе с таким типом вирусов — как можно чаще обновлять версии программы и вирусные базы.

Первым из стелс-вирусов является Brain. Эта программа должна была «наказать» местных «пиратов», ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру.

Вирус Brain инфицировал загрузочный сектор 5-дюймовых дискет объемом 360Kb. После заражения он постепенно заполнял все неиспользуемое пространство дискеты, замедляя работу флоппи-привода и со временем делая невозможным дальнейшее использование дискеты.

По сегодняшним меркам Brain — почти безобидный вирус, но тут надо делать скидку на время, ведь в те годы многие еще даже не пользовались жесткими дисками и запускали программы непосредственно с дискет. Так что ущерб Brain все-таки нанес. Подсчитано, что в США он заразил около 18 тысяч компьютеров.

У вируса Brain есть еще одна отличительная особенность — он был первым вирусом-невидимкой (stealth) и прятал себя от любой возможности обнаружения, маскируя инфицированное пространство на диске. При попытке чтения зараженного сектора, он «подставлял» и его незараженный оригинал.

Полиморфные вирусы.

К полиморфик–вирусам относятся те из них, детектирование которых невозможно осуществить при помощи так называемых вирусных масок – участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами – шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов – начиная от загрузочных и файловых DOS-вирусов до Windows-вирусов и даже макровирусов. Существуют также другие, достаточно экзотические примеры полиморфизма - DOS-вирус "Bomber", например, не зашифрован, однако последовательность команд, которая передает управление коду вируса, является полностью полиморфной. Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Ярким примером ранних полиморфных вирусов является вирус Tequila. Когда файл был заражен ею, она сразу начинала свое действие. Вирус заражал мастера записи загрузок. Также он уменьшал размер деления дисков на 6 секторов и помещал код в секторы, которые находятся вне деления. Когда загрузка с диска завершалась, вирус становился резидентом памяти. Затем начиналось исполнение .exe файлов, и вирус добавлял свои 2468 байт в них.

Вывод:

Каждый компьютер, подключенный к сети, не является больше вашим персональным компьютером. Проблема несанкционированного доступа к компьютерам и данным в них будет актуальна всегда для информационного общества, потому что здесь очень сильно завязаны различные сферы человеческой жизни, начиная от экономической (конфиденциальная экономическая информация), заканчивая социальной (личные данные), а это в свою очередь привлекает преступников всех мастей и видов. Разрабатываются множество методов защиты от вирусов, но редко какая-либо система может устоять против целенаправленной вирусной атаки, особенно проводимой изнутри самой системы. Как следствие всего вышесказанного, нужно проводить различные мероприятия и процедуры, для обеспечения полной безопасности и защиты от компьютерных вирусов.

Литература:

1. Соколов С.В., Бугаян И.Р., Тищенко Е.Н. Защита информационных процессов в компьютерных системах//Учебное пособие. Ростов н/Д. 2006. РГЭУ «РИНХ».

2. КОМПЬЮТЕРНЫЕ ВИРУСЫ: ПРОИСХОЖДЕНИЕ, РЕАЛЬНАЯ УГРОЗА И МЕТОДЫ ЗАЩИТЫ. - Электронный ресурс. URL: nkj.ru/archive/articles/7889/ (дата обращения 09.03.2015).

3. Вирусы: обнаружение, профилактика и защита. – Электронный ресурс. URL: http://otherreferats.allbest.ru/programming/00155514_0.html (дата обращения 09.03.2015).

Д.О. Ромашкин, А.А. Запорожцев

АНАЛИЗ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Ростовский Государственный Экономический Университет (РИНХ),
г. Ростов-на-Дону, Россия

Ключевые слова: информация, симметричный алгоритм, ключ, перестановка, текст, шифрование.

Описаны теоретические подходы к изучению алгоритмов шифрования. Приводится пример кода с использованием симметричного алгоритма шифрования методом перестановки «Магический квадрат Дюрера», реализованного на языке C++. Приведены достоинства и недостатки симметричных алгоритмов шифрования по сравнению с асимметричными.

D.O. Romashkin, A.A. Zaporozhtsev

CRYPTOSYSTEMS: SYMMETRIC CRYPTOGRAPHY ALGORITHMS

Rostov State University of Economics (RINH), Rostov-on-Don, Russia

Keywords: symmetric algorithms, key, permutation, text, cryptographic, encryption, information.

Theoretical approaches to the study of encryption algorithm are described. Example code with using of symmetrical encryption algorithm and permutation method "Dürer's magic square" is realized with C++ language are described. Advantages and disadvantages of symmetrical encryption algorithms compared with asymmetrical algorithms are described.

Симметричные алгоритмы шифрования (также несущие названия систем с единственным ключом (single-key), с общим секретом (shared-secret) или даже с закрытым ключом (private-key) [1]. Данный вид крипто-шифрования основывается в основном на том, что при шифровании и дешифровании используют одинаковый ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват. Наибольшей популярностью при таком типе шифрования пользуется стандарт DES (Data Encryption Standard) - комбинация нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований.

Далее будут рассмотрены наиболее распространенные методы симметричных алгоритмов шифрования:

Простая перестановка.

Для такого метода алгоритма симметричных криптографических систем ключом служит размер таблицы, в которую записывается шифруемая информация. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи текста, не несущего какой-то смысл.

Одиночная перестановка по ключу.

Этот метод шифрования отличается от метода простой перестановки тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Двойная перестановка.

Для дополнительной надежности шифруется сообщение, которое до этого уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были отличны от строк и столбцов начальной таблицы. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Также можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Перестановка «Магический квадрат Дюрера».

Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами от 1 до n, и удовлетворяют сразу нескольким условиям:

- если сложить все числа в каждой строке;

– если сложить все числа в каждом столбце;
– если сложить все числа в двух диагоналях

суммы равны 34-м. Ключом является расположение символов в таблице (рис. 1, а и б).

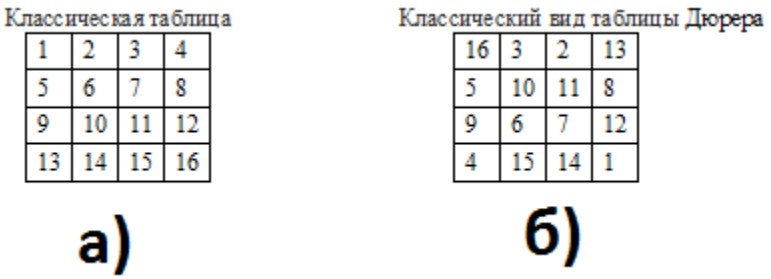


Рисунок 1. Таблица Дюрера

Зашифруем текст с помощью метода «Магического квадрата Дюрера» с целью оценки надежности симметричных криптографических алгоритмов, реализованного в Visual Studio 2013 на языке C++.

Листинг программы:

```
#include <iostream>
using namespace std;
void main()
{	setlocale(0, "");
	system("title Магический квадрат Дюрера");
	int i, j, n = 5, m = 5;
	char a[5][5],  b[5][5];
	cout << "Введите число: \n";
	for (i = 1; i < n; i++)
	{
		for (j = 1; j < m; j++) { cout << "a[" << i << "][" << j << "]= "; cin >> a[i][j]; }
	}
	cout << endl<<"Введенный массив:\n\n";
	for (i = 1; i < n; i++)
	{
		for (j = 1; j < m; j++) { cout << a[i][j]<<" "; }
		cout << "\n";
	}
	cout << "\n";
	b[1][1] = a[4][4];
	b[1][2] = a[1][3];
	b[1][3] = a[1][2];
	b[1][4] = a[4][1];

	b[2][1] = a[2][1];
	b[2][2] = a[3][2];
	b[2][3] = a[3][3];
	b[2][4] = a[2][4];

	b[3][1] = a[3][1];
	b[3][2] = a[2][2];
	b[3][3] = a[2][3];
	b[3][4] = a[3][4];

	b[4][1] = a[1][4];
	b[4][2] = a[4][3];
```

```
        b[4][3] = a[4][2];
        b[4][4] = a[1][1];

        cout << endl << "Зашифрованный массив:\n\n";
        for (i = 1; i < n; i++)
        {
                for (j = 1; j < m; j++) { cout << b[i][j] << " "; }
                cout << "\n";
        }
        cout << "\n";
        system("pause");
}
```

Результат работы программы приведен на рис. 2. Исходный текст: tablicadurera123. Полученный зашифрованный текст: 3baaireducarl21t.

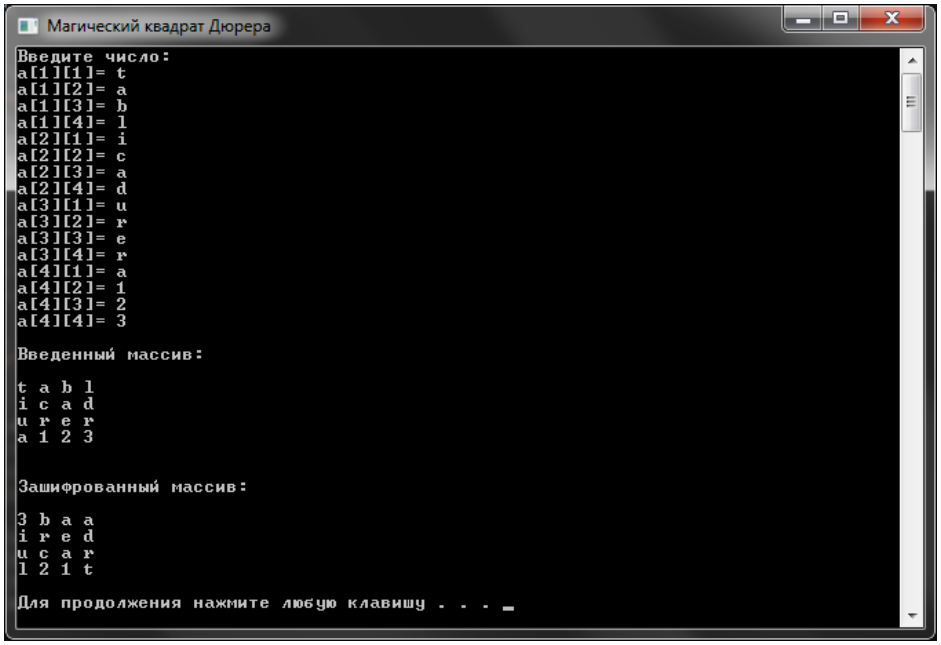


Рисунок 2. Результат работы шифрования

Достоинства симметричных алгоритмов шифрования по сравнению с асимметричными [2, 3]:

1. Скорость выполнения алгоритма.
2. Простота его реализации (благодаря достаточно простым математическим действиям).
3. Достаточно маленькая длина ключа для соответствующей стойкости алгоритма.
4. Изученность (т.к. данный вид алгоритмов возник очень давно).

Недостатки симметричных алгоритмов шифрования по сравнению с асимметричными:

1. Средняя устойчивость от дешифрования.
2. Сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен канал для передачи каждого ключа обеим сторонам секретным способом.

Вывод:

Симметричные системы шифрования могут использоваться для обмена информацией с маленьким сроком актуальности за счет простоты реализации алгоритма и высокой скорости его выполнения.

Литература:

1. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.

2. Кон П. Универсальная алгебра. - М.: Мир. - 1968.
3. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002.

Д.Я. Иргашева, Р.Т. Гаипназаров, Ж.Ф. Шомахамедов

ПОВЫШЕНИЯ НАДЕЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: система защиты информации, несанкционированный доступ, информационная безопасность, информационно-коммуникационные системы.

Данная статья посвящена, исследованию надежности системы защиты информации в обращении пользователя к информационным ресурсам, требующих выполнения защитных функций.

D.Y. Irgasheva, R.T. Gaipnazarov, J.F. Shomahamedov

IMPROVING THE RELIABILITY OF INFORMATION SECURITY SYSTEMS FROM UNAUTHORIZED ACCESS

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: information security system, unauthorized access, information security, information and communication systems.

This article is devoted, study reliability of information security in a user accesses information resources requiring protective functions.

Анализ принципов применения и особенностей работы системы защиты информации **(**СЗИ) от несанкционированного доступа (НСД) показал [1], что основная направленность данных систем - угрозы информационная безопасность искусственные по происхождению, преднамеренные по характеру возникновения, воздействующие с помощью программных средств, осуществляемые с подключением к линиям связи и на успешное осуществление которых повлиять невозможно. При обосновании требований к системе защиты информации существенной особенностью является их работа в составе общесистемного программного обеспечения информационно-коммуникационных систем (ИКС). Таким образом, требования к показателям надежности СЗИ должны обосновываться из имеющихся показателей надежности ИКС с последующей оптимизацией затрат на достижение требуемого уровня надежности. С точки зрения надежности характерной особенностью СЗИ являются следующие ее свойства:

- системы защиты информации выполнены в виде отдельных программно - технических продуктов;
- набор функциональных требований к СЗИ фиксирован руководящими документами;
- системы защиты информации работают непрерывно, в течение всего времени работы ИКС при обработке категорированной информации;
- запрещено обращение к информационным ресурсам ИКС в обход СЗИ.

Система защиты информации при применении оперативного контроля и восстановления работоспособности функционирует следующим образом. В начальный момент времени СЗИ работает в нормальном режиме некоторое случайное время. По окончанию этого времени СЗИ переходит в режим оперативного контроля и восстановления работоспособности. При отсутствии искажений вычислительного процесса и ошибок за предыдущий период времени СЗИ переходит опять в режим нормального функционирования. При наличии искажений вычислительного процесса и ошибок за предыдущий период времени СЗИ после проведения оперативного контроля

переходит в режим восстановления работоспособности. При нахождении СЗИ в этом состоянии возможно обращение пользователя к информационным ресурсам, требующим выполнения защитных функций. При этом нахождение СЗИ в режиме оперативного контроля и восстановления приводит к невозможности СЗИ выполнять защитные функции и классифицируется как отказ.

Процесс проведения оперативного контроля можно представить в виде ориентированного графа, изображенного на рисунке 1. На рисунке введены следующие обозначения начало: S_1 - начало i - го периода нормального функционирования и оперативного контроля СЗИ; S_1^1 - начало i - го периода оперативного контроля СЗИ; S_1^{11} - обращение пользователя к информационным ресурсам ИКС, требующим выполнение СЗИ защитных функций, приведшее к состоянию отказа; S_1^{10} - обращение пользователя к информационным ресурсам ИКС, требующим выполнение СЗИ защитных функций, не приведшее к состоянию отказа.

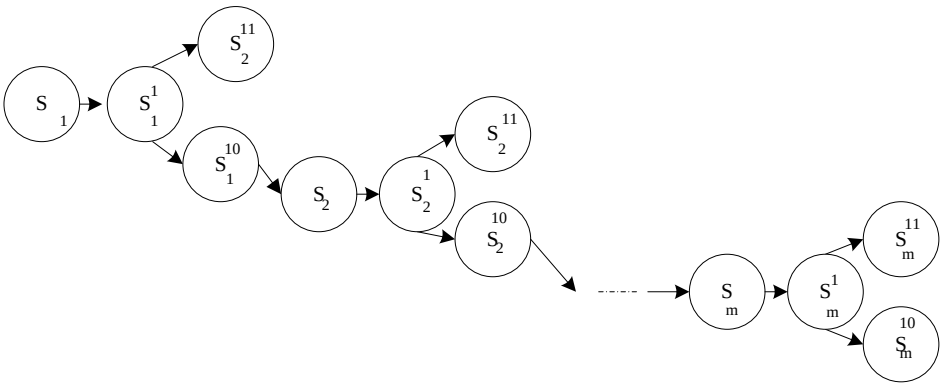


Рисунок 1. Процесс проведения оперативного контроля

Данный граф имеет вид дерева и отражает случайный характер процесса работы СЗИ. На графе отображены M последовательных периода полезной работы и оперативного контроля и восстановления СЗИ. Состояния S_1^{11} являются поглощающими (обращение пользователя к информационным ресурсам ИКС, требующим выполнение СЗИ защитных функций, приведшее к состоянию отказа). В качестве показателя эффективности оперативного контроля примем вероятность отказа СЗИ (вероятность обращения пользователя к информационным ресурсам ИКС, требующим выполнение СЗИ защитных функций, при нахождении ее в режиме оперативного контроля и восстановления работоспособно, приведшее к состоянию отказа) $P_{отк}(t)$.

Обозначим через $P_1^{11}(t)$ вероятность нахождения процесса функционирования СЗИ в состоянии S_1^{11} (СЗИ находится в состоянии отказа после i - го периода периодов полезной работы и оперативного контроля) к моменту времени t. Вероятность отказа СЗИ за все время эксплуатации (за M периодов полезной работы и оперативного контроля) можно определить как:

$$P_{отк}(t) = \sum_{S_1^{11}} P_1^{11}(t) \tag{1}$$

где, сумма берется по всему множеству состояний S_1^{11}.

Для получения показателя эффективности оперативного контроля будем характеризовать i - ый цикл работы СЗИ следующими величинами:

$\varphi_{pt}(t)$ - плотность распределения времени полезной работы СЗИ;

$\varphi_{okt}(t)$ - плотность распределения времени оперативного контроля;

P_{oi} - вероятность отказа СЗИ в i - ый период полезной работы и оперативного контроля.

В соответствии с существующей методикой анализа графов состояний сложных систем, определим передаточные функции переходов, соответствующих дугам графа, представляющих собой преобразование Лапласа от произведения переходных вероятностей на соответствующие плотности распределения времени переходов.

Введем следующие обозначения:

$$\varphi_{pt}(s) = L\{\varphi_{pt}(t)\}$$

$$\varphi_{okt}(s) = L\{P_{0i} * \varphi_{okt}(t)\}$$

$$\overline{\varphi_{okt}(s)} = L\{(1 - P_{0i}) * \varphi_{okt}(t)\}$$

где $L\{f(t)\} = \int_0^{\infty} f(t) * e^{-st} dt$ - оператор преобразования Лапласа;

S - переменная преобразования Лапласа.

Введем также обозначение $H_1^{11}(s)$ преобразование Лапласа от производсьвенной вероятностей переходов процесса в состояние S_1^{11} по времени.

$$H_1^{11}(S) = L\left\{\frac{dP_1^{11}(t)}{dt}\right\}$$

Если через $H_{отк}(S)$ обозначить преобразование Лапласа от производной вероятности отказа СЗИ, то с учетом математического выражения (1) можно записать:

$$H_{отк}(S) = \sum_{S_1^{11}} H_1^{11}(S) \tag{2}$$

Исходя из структуры графа состояний оперативного контроля, представленного на рисунке 1, можно определить плотность вероятности отказа СЗИ в i том цикле работы в области изображений как:

$$H_1^{11}(S) = \varphi_{pi}(S)\varphi_{okt}(S)\prod_{j=1}^{i-1}\varphi_{pj}(S)\overline{\varphi_{okj}(S)}$$

Подставив выражение для плотности вероятности отказа СЗИ в i - том цикле работы в области изображений в (2), получим:

$$H_{отк}(S) = \sum_{i=1}^{m}\varphi_{pi}(S)\varphi_{oktt}(S)\prod_{j=1}^{i-1}\varphi_{pj}(S)\overline{\varphi_{okj}(S)} \tag{3}$$

Типичной ситуацией для процессов оперативного контроля программных систем является ситуация когда время нормальной работы и время на проведение оперативного контроля составляют фиксированные промежутки времена T_p и T_{ok} соответственно [2]. В этом случае соответствующие времена переходов будут детерминированными, плотности распределения времени переходов будут представлять δ функции, а соответствующие переходам весовые функции будут иметь вид:

$$\varphi_{pt}(s) = \exp(-T_p * S)$$

$$\varphi_{okt}(s) = P_{0i} * \exp(-T_{ok} * S)$$

$$\overline{\varphi_{okt}(s)} = (1 - P_{0i}) * \exp(-T_{ok} * S)$$

Подставив данные выражения в (1), получим выражение для плотности вероятности отказа СЗИ в области изображений:

$$H_{отк}(S) = \sum_{i=1}^{m}\exp(-T_p * S) * P_{0i} * \exp(-T_{ok} * S) * \prod_{j=1}^{i-1}\exp(-T_p * S) * (1 - P_{0i}) * \exp(-T_{ok} * S)$$

Для получения искомого показателя - вероятности отказа СЗИ в результате невозможности выполнения защитных функций при оперативном контроле работоспособности, применим к

полученному математическому выражению обратное преобразование Лапласа с учетом того, что интегрирование ориги- эквивалентно делению изображения на S

$$P_{отк}(t) = L^{-1}\{H_{отк}(S)/S\} = \sum_{i=1}^{m} P_{oi} * h\left(t - i\left(T_p + T_{ok}\right)\right)\prod_{j=1}^{i-1}(1 - P_{0i}) * h(t - j(T_p + T_{ok}))$$

где $h(x) = \begin{cases} 1(x \geq 0) \\ 0(x \prec 0) \end{cases}$ единичная функция.

Исходя из особенностей функционирования СЗИ, как сложной программной системы [3], и неизменности характеристик пользователя в течение времени эксплуатации, можно сделать допущение о неизменности величины P_{oi} от времени $\left(P_{0i} = P_0^*\right)$. Найти финальную вероятность отказа СЗИ за M последовательные периоды полезной работы и оперативного контроля и восстановления СЗИ можно, используя математическое выражение, при $t \to \infty$. При этом $h(x \to 1)$ математическое выражение, приведенное выше, преобразуется к виду:

$$P_{отк}(t)_{t\to\infty} = P_0^* \sum_{i=1}^{m}\left(1 - P_0^*\right)^{i=1} \quad (4)$$

Используя выражение для суммы, убывающей геометрической прогрессии, преобразуем (4) и получим результирующее, выражение для вероятности отказа СЗИ:

$$P_{отк}(t)_{t\to\infty} = P_0^* \frac{1 - \left(1 - P_0^*\right)^m}{1 - \left(1 - P_0^*\right)}$$

Исследования надежности сложных систем показали, что функционирования СЗИ при выполнении защитных функций, позволяют оценивать характеристики их надежности, а также задавать требования к периодичности и глубине оперативного контроля.

Литература:

1. Домарев В.В. Безопасность информационных технологий. Методы создания систем защиты. Киев.2001 г.688 с.

2. Деч Г. Руководство к практическому применению преобразованию Лапласа. М.: Наука 1965 г. 215 с.

3. Липаев В.В. распределение ресурсов в вычислительных системах. М.:Статистика, 1979 г. 247 с.

Д.Я. Иргашева

ФУНКЦИОНАЛЬНО - РОЛЕВАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА С ЗОНАЛЬНОЙ ПОЛИТИКОЙ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: компьютерные сети, ролевая модель с зональным разграничением доступа, субъект, объект.

В работе предлагается функционально - ролевая модель разграничения доступа с зональной политикой, позволяющая установить отношения двухстороннего доверия. Предлагается механизм реализации разработанной ролевой модели с зональным разграничением доступа.

D.Y. Irgasheva

FUNCTIONAL - ROLE MODELS OF ACCESS CONTROL WITH ZONAL POLICY

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: computer networks, role model with zone access control, subject, object.

This paper proposes a functionally - role model of access control with zonal policy that allows to establish a relationship of bilateral trust. A mechanism implementation developed a role model with a zonal differentiation of access.

Большинство корпоративных компьютерных сетей (КС), предназначенные для управления крупными предприятиями, представляют собой многопользовательские программно-аппаратные системы, построенные на основе технологии «клиент-сервер».

В связи с особенностями функционально-ролевой модели, иерархическая ролевая модель используется в системе для управления пользователями, ролями и полномочиями ролей. Из вышеизложенного видно, что одним из недостатков ролевой модели является отсутствие ограниченной полноты функций пользователя. Поэтому существует необходимость ограничения области действия выданных пользователю полномочий и, как следствие, упрощения схемы доступа к объектам [1]. С этой целью в работе предлагается функционально - ролевая модель разграничения доступа с зональной политикой, позволяющая установить отношения двухстороннего доверия.

Ролевая модель с зональным разграничением доступа и механизм её реализации. В предлагаемой ролевой модели с зональным разграничением доступа введена роль «владелец» R_{own}, назначаемая пользователям в контексте тех объектов O_{ijk}, которыми они владеют [49]. Эта роль по своему поведению слегка отличается от обычных ролей. Во-первых, только один пользователь может играть роль «владелец» в контексте какого-то определенного объекта. Во-вторых, объект не должен наследовать роль «владелец» от родителя, если в его собственном контексте такая роль кому-либо назначена. Таким образом, данную роль по отношению к объекту O_{ijk} может выполнять только один пользователь $R_{own}(O_{ijk})$. Если, в контексте объекта роль «владелец» R_{own} не назначена, то владельцем считается родительский объект:

$O_{ijk} \in (O_{ijk}) else\ O_{ijk} \in R_{own}(O_{ij}) else\ O_{ijk} \in R_{own}(O_i) \ldots$

Для ограничения полноты функций пользователей предлагается ввести понятие «класс доступа» f_{OFR}. Класс доступа содержит набор правил, задающих права выполнения определенных операций для определенных ролей. Класс доступа – это отображение, связывающее права выполнения определенных функций с определенными ролями [49].

Выполнение функции пользователем разрешено, если данная функция определена и в роли пользователя f_{FR}, и в классе доступа объекта f_{OFR}, по отношению к которому функция f_{FR} выполняется условия:

$f_{FR}: F \times R;$

$F_{OFR}: F(O_i) \times R;$

$F_S \Leftrightarrow f_{FR} = f_{OFR}.$

Каждому объекту системы ставится в соответствие ровно один класс доступа, а любой класс доступа может быть назначен произвольному количеству объектов. Это позволяет иметь в системе несколько разных схем доступа к объектам, не заставляя нас связывать эти схемы с типами или какими-то другими признаками объектов. Причем назначения классов никак не связаны с иерархией объектов: дочерний объект может иметь любой класс доступа, независимо от того, какой класс назначен родительскому объекту [2].

Согласно единой иерархии объектов предлагается ввести наследование правил доступа от вышестоящих объектов. Подобный механизм часто встречается в файловых системах (дискреционная модель): файлы, лежащие в папке, могут не иметь своих собственных правил доступа, а наследовать эти правила у папки. При переносе этих файлов в другую папку, права пользователя на доступ к этим файлам могут поменяться.

При применении ролевой модели с зональным разграничением доступа необходимо ввести множества физических объектов системы $V(v_1, v_2, \ldots, v_l)$ - вычислительных установок (рабочие

станции, серверы), принтеров, коммуникационного оборудования и т.п. а также множество зон системы $Z(z_1, z_2, \dots, z_k)$.

При этом зоной в компьютерной сети называется совокупность подмножества пользователей, подмножества объектов доступа и подмножества физических объектов, обособленных в локальный сегмент с отдельной (внутризональной) политикой безопасности.

Внутризональная политика безопасности реализуется *внутризональным мониторингом безопасности,* который обеспечивает весь набор функций безопасности (аутентификация и порождение первичных субъектов доступа пользователей зоны, разграничение и управление доступом, аудит процессов) [2]. Внутризональным мониторингом безопасности (рисунок 1) является системный субъект, который реализует в отношении объектов зоны $z \in Z$ разрешенное множество доступов $P_L(z)$, которое в общем виде является объединением внутризональных доступов (отношение S_{zk} - субъект находящийся в k-той зоне, O_{zk} - объект находящийся в k-той зоне), регламентированных правилами (критериями) внутризональной политики пользователей зоны к объектам других зон, пользователям по правилам (критериям, процедурам) межзональной политики безопасности:

$$\mathrm{P_L(z)} = \mathrm{P_L^{in}(z)} \cup \mathrm{P_L^{out}(z)}, \quad (1)$$

где $\mathrm{P_L^{in}(z)}$ - множество безопасных внутризональных доступов;

$\mathrm{P_L^{out}(z)} = \mathrm{P_L^{out}(z\rightarrow)} \cup \mathrm{P_L^{out}(z\leftarrow)}$ - множество безопасных удаленных доступов для зоны $z \in Z$, являющееся объединением множества удаленных доступов пользователей зоны z с объектами зоны z $\mathrm{P_L^{out}(z\leftarrow)}$.

Зональная структура системы определяется отображениями множеств сущностей, выражаемыми следующими функциями:

$f_{phys}: V \rightarrow Z$ – значением функции $z = f_{phys}(v)$ является зона $z \in Z$, в которой находится физический объект $v \in V$;

$f_{user}: U \rightarrow Z$ – значением функции $z = f_{user}(u)$ является зона $z \in Z$, в которой уполномочен для работы пользователей $u \in U$;

$f_{fobject}: O \rightarrow V$ – значением функции $v = f_{fobject}(o)$ является физический объект $v \in V$, в котором находится объект $o \in O$.

Следует отметить, что совокупность функций $v_{fobject}(o)$ и $z = f_{phys}(v)$ реализует функцию $z = f_{iobject}(o)$, определяющую принадлежность объекта доступа $o \in O$ к определенной зоне $z \in Z$, что можно трактовать как «зональную окрашенность» всех объектов доступа зонально - распределенной системы [2].

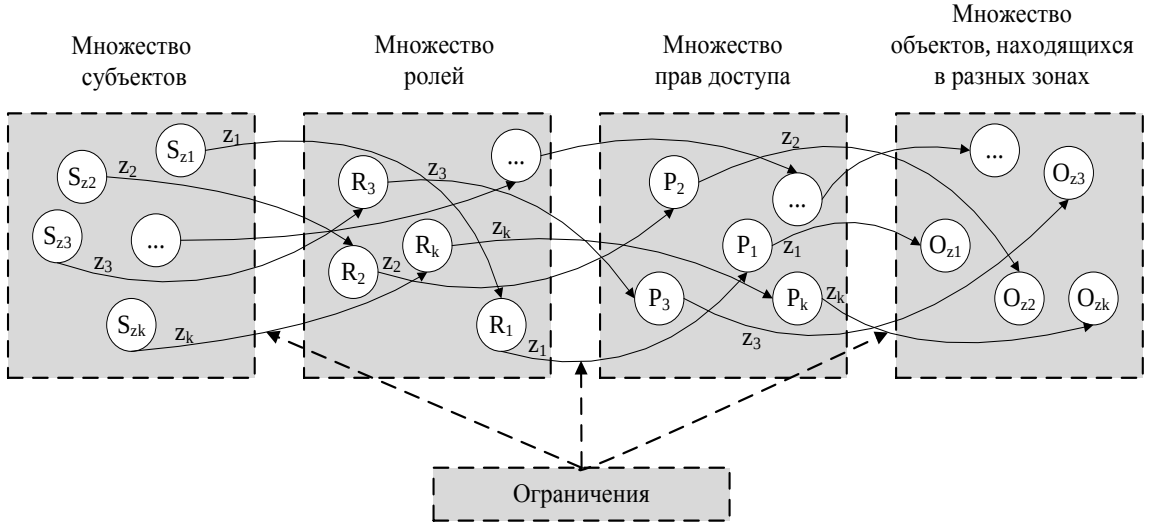


Рисунок 1. Модель внутризонального мониторинга безопасности

На множестве зон системы Z определяется частичный нестрогий порядок, устанавливающий систему межзональных доверительных отношений: $f_{zz}: Z \times Z$ - отношение, определяющее приоритет доверия одних зон безопасности по отношению к другим и задающее оператор доминирования " $\leq$ ", такое что:

1. Если для $S_{zk}, O_{zk}, \in Z$ и $S_{zk}" = "O_{zk}$, то между зоной S_{zk} и зоной O_{zk} установлены отношения двустороннего доверия, т.е. зоны S_{zk}, O_{Zk} доверяют друг другу, иначе говоря, принципиально возможны удаленные доступы пользователей зоны S_{zk} к объектам зоны O_{zk}, и наоборот, пользователей зоны O_{zk} к объектам зоны S_{zk}-
$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) \neq \emptyset \quad (2)$$
2. Если для $S_{zk}, O_{zk}, \in Z$ и $S_{zk} > O_{zk}$, то между зоной S_{zk} и зоной O_{zk} установлены отношения одностороннего доверия, зона O_{zk} доверяет зоне S_{zk}, но зона S_{zk} не доверяет зоне O_{zk}, иначе говоря, принципиально возможны удаленные доступы пользователей зоны S_{zk} к объектам зоны O_{zk}, но удаленные доступы пользователей зоны O_{zk} к объектам зоны S_{zk} принципиально невозможны –
$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) = \emptyset \quad (3)$$
3. Если для $S_{zk}, O_{zk}, \in Z$ и $S_{zk}" \neq " O_{zk}$, то отношения доверия между зонами S_{zk}, O_{zk} не установлены, т.е. зоны S_{zk}, O_{zk} не доверяют друг другу, иначе говоря, принципиально невозможны удаленные доступы пользователей зоны S_{zk} к объектам зоны O_{zk} и удаленные доступы пользователей зоны O_{zk} к объектам зоны S_{zk} -
$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) = \emptyset \quad (4)$$

Отметим, что отношение частичного нестрогого порядка на множестве Z адекватно воспроизводит доверительные отношения, так как обладает свойствами рефлективности, антисимметричности и транзитивности:

$\forall z \in Z : z \leq z;$

$\forall z_1, z_2 \in Z: (z_1 \leq z_2 \wedge z_2 \leq z_1) \Longrightarrow z_1 " = " z_2;$

$\forall z_1, z_2, z_3 \in Z: (z_1 \leq z_2 \wedge z_2 \leq z_3) \Longrightarrow z_1 \leq z_3;$

В предложенной ролевой модели с зональным разграничением доступа любая зона доверяет самой себе, т.е. внутризональные доступы не запрещены (рефлективность). Если одна зона доверяет другой (возможны удаленные доступы пользователей первой зоны к объектам во второй зоне) и, одновременно, другая зона доверяет первой (возможны удаленные доступы пользователей второй зоны к объектам первой зоны), это означает наличие отношений двустороннего доверия (антисимметричность). И, наконец, если одна зона доверяет другой, а другая доверяет третьей, запрещать удаленные доступы пользователей первой зоны к объектам третьей зоны не имеет смысла, так как по цепочке удаленных доступов информация может быть перенесена из третьей зоны в первую (транзитивность).

Литература:

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для ВУЗов.- М.: Издательский центр: Академия, 2005. - с. 144.

2. Ганиев С.К., Каримов М.М., Иргашева Д.Я. О способе разграничения доступа к информационным ресурсам в телекоммуникационных системах // Международная научно – практическая Конференция / Инновация – 2009: Сборник научных статей. - Ташкент, 2009.- с. 287-289.

В.И. Петренко, А.С. Кадурина

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ МЕДИЦИНСКОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ ДЛЯ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ РАЙОННОГО МАСШТАБА

Северо-кавказский федеральный университет, г.Ставрополь, Россия

Ключевые слова: информационная безопасность, персональные данные, учреждения здравоохранения, защищённость медицинской информации, угрозы безопасности, информационные системы персональных данных, риски, оценка рисков, конфиденциальность.

Описана проблема обеспечения защищённости медицинской информации, персональных данных для учреждений здравоохранения районного масштаба, рассмотрены этапы, необходимые

для реализации обеспечения полной защиты медицинской информации и персональных данных пациентов, описаны этапы разработки рекомендаций по защите персональных данных пациентов учреждений здравоохранения и анализ актуальных угроз для информационных систем персональных данных, рассмотрены этапы оценки рисков.

V.I. Petrenko, A.S. Kadurina

DEVELOPMENT OF RECOMMENDATIONS ON THE PROTECTION OF MEDICAL INFORMATION AND PERSONAL DATA OF PATIENTS FOR HEALTH CARE INSTITUTIONS OF REGIONAL SCALE

North-Caucasian Federal University, Stavropol, Russia

Keywords: information security, personal data, health care, protected health information, security threats, personal data information systems, risk, risk assessment, privacy.

The problem is the ensuring security of medical information, personal data for the facilities at the district scale, consider the steps necessary to implement to ensure the full protection of health information and personal data of patients described the stages of developing recommendations for the protection of personal data of patients of health care institutions and the analysis of actual threats to the information systems of personal data, the stages of risk assessment.

Наиболее остро вопросы управления информационной безопасностью возникают, в частности, в медицине, потому что данные о состоянии здоровья пациентов относятся к самой высокой категории персональных данных.

Основной целью деятельности учреждений здравоохранения является оказание медицинской помощи всего населения района. Поэтому данная деятельность учреждения напрямую связана с персональными данными

Защищенность медицинской информации наряду с правом на высококачественную медицинскую помощь издавна считается основным пожеланием всех пациентов медицинских учреждений. Пациенты готовы раскрывать самые интимные подробности о себе и своем здоровье врачам только будучи уверенными, что информация об их проблемах со здоровьем останется конфиденциальной и защищенной, не зависимо от того где и в какой форме она хранится.

В большинстве лечебно-профилактических учреждений информационные системы создавались без учета требований по защите персональных данных и врачебной тайны. Персональные данные могут быть похищены злоумышленниками, в том числе и из числа сотрудников медицинской организации. Разглашение персональных данных, как пациентов, так и сотрудников учреждения здравоохранения может привести к значительным негативным последствиям для субъектов персональных данных, нанести непоправимый урон, моральный или материальный вред. Поэтому защита персональных данных является актуальной темой в области здравоохранения нашей страны.

В настоящее время индустрия здравоохранения постепенно переходит на использование электронной медицинской документации. Создаются базы данных, содержащие данные о миллионах жителей и состоянии их здоровья. И соответственно увеличивается число людей, имеющих доступ к защищаемой медицинской информации (ЗМИ), что приводит к возникновению новых несанкционированных возможностей для доступа к такой информации. В результате чего ЗМИ может быть случайно или преднамеренно раскрыта, потеряна или украдена. Но, несмотря на то, что с внедрением современных технологий возникают и новые несанкционированные возможности получения ЗМИ, новые технологии никак не изменяют профессиональную этику, а даже наоборот поощряют решение защитить частную жизнь и обезопасить медицинскую информацию, сохранив доступ к качественному медицинскому обслуживанию[1].

Сейчас довольно часто появляется информация, что не все организации, которым поручено обеспечивать безопасность ЗМИ, в полной мере выполняют свои обязанности. Число нарушений безопасности ЗМИ в нашей стране постоянно увеличивается. Одной из причин нарушения безопасности ЗМИ являются недостаточно обученные сотрудники, которые в основном и становятся главными виновными. Наряду с этим необходимо осознавать, что и уровень злоумышленников с каждым годом растет. Такие нарушения могут нанести существенный ущерб,

как людям, конфиденциальность информации которых была нарушена, так и организациям, ответственным за ее защиту.

На деле, конфиденциальность и реализация программ обеспечения безопасности ЗМИ, скорее всего, стали бы более приоритетными, если бы в медицинских учреждениях чаще обращали внимание на увеличивающиеся затраты от не выполнения требований по безопасности ЗМИ и вытекающих из этого штрафов и исков.

В настоящее время угрозы безопасности ЗМИ являются реальными и повсеместными, финансовые, репутационные и юридические последствия для людей от реализации этих угроз высоки, и организации при этом несут серьезные потери.

Опираясь на зарубежный опыт, для медицинских учреждений нашей страны можно выделить следующие основные этапы, которые необходимо реализовать для обеспечения адекватной и полной защиты ЗМИ пациентов [2]:

- определить подход организации к оценке рисков ЗМИ;
- идентифицировать риски ЗМИ;
- проанализировать и оценить риски ЗМИ;
- идентифицировать и оценить возможности по обработке рисков ЗМИ;
- разработать, опубликовать, утвердить и довести до сотрудников политику информационной безопасности, которая включает описание ежегодного процесса идентификации угроз и уязвимостей ЗМИ, завершающегося формализованной оценкой рисков ЗМИ;
- выработать подход и периодически корректировать методику оценки рисков нарушения безопасности ЗМИ;
- определить критерии принятия рисков нарушения безопасности ЗМИ и уровень допустимого риска нарушения безопасности ЗМИ.

Для разработки рекомендаций по защите персональных данных для учреждений здравоохранения районного масштаба в первую очередь нужно провести анализ общей информационной структуры учреждения. Анализируется локальная сеть медицинского учреждения, её топология, расположение компьютеров, сервера, т.к. с помощью компьютеров, объединённых в локальную сеть, ведутся административные процедуры, электронные карты пациентов, истории болезней, направления для обследования и т.д. Также анализируется система видеонаблюдения (расположение камер).

Следующим этапом для разработки рекомендаций по защите персональных данных является анализ информационных систем, т.к. каждое из подразделений учреждения здравоохранения формирует свою базу данных с персональными данными, отвечающую специфике своей деятельности.

Учреждение должно создать, внедрить, эксплуатировать, осуществлять мониторинг, анализировать, сопровождать и совершенствовать документированную систему управления информационной безопасностью в контексте общих бизнес активностей и рисков организации.

Запись данных пациентов ведётся с помощью информационной систем учёта оказанных медицинских услуг, установленных на компьютерах медицинских учреждений в кабинете врачей. Вносятся такие данные, как: ФИО, пол, адрес, дата рождения, возраст, номер карты и полис пациента, также ФИО, специальность лечащего врача, диагноз, исход лечения, начало и окончание полиса, начало и окончание больничного листа, сведения о хронических и ранее выявленных заболеваниях, номер направления и дата направления пациента. Также регистрируются истории болезней пациентов хирургического отделения, гинекологического, инфекционного, детского, терапевтического и акушерского в информационных системах учреждений здравоохранения районного масштаба. Учётом всех лекарственных средств в больницах занимается провизор. Заказ медикаментов осуществляется через информационную систему, связанную с мониторингом лекарственных средств. Использование наркотических средств и психотропных веществ за каждый год фиксируется в отчёте. Все административные операции, финансовое обеспечение медицинских учреждений также регулируется с помощью информационных систем, содержащих персональные данные.

Следующей неотъемлемой частью для разработки рекомендация является исследование уязвимостей персональных данных учреждения и анализ актуальных угроз для информационных систем персональных данных. Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-

аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным [3].

Данная процедура исследования информационных систем персональных данных с определением актуальных угроз является подготовительным этапом для разработки рекомендаций по защите персональных данных для медицинских учреждений районного масштаба.

В соответствии с Приказом ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». [4], определяются рекомендации для исследуемых информационных систем персональных данных учреждения.

Практически каждый специалист по информационной безопасности проводит оценку рисков. Пусть даже весь этот процесс происходит в его голове и не формализуется на бумагу, но он точно происходит, причем именно по той схеме, как это описывается в стандартах (ISO 27001, PCI DSS, СТО БР ИББС-1.0 и др.).

И в основном весь этот процесс происходит следующим образом:

1. Выявляются основные активы, которые представляют ценность для учреждения и разглашение, уничтожение, модификация или хищение которых может нанести ущерб.
2. Выявляются проблемы и уязвимости.
3. Устанавливаются возможные последствия от не устранения этих проблем (определяются угрозы).
4. Разрабатывается проект плана мероприятий (действий) по устранению выявленных нарушений, эффективность и необходимость которого обосновывается руководству учреждения, после чего расставляются приоритеты по проведению мероприятий по ИБ (это и есть оценка и ранжирование рисков ИБ и закрытие их на приоритетной основе) [1].

Риск – это вероятная частота и вероятная величина будущих потерь [5]. Так же наряду с этим определением существует множество других. Риском также считают вероятность причинения ущерба вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости [6].

Основная тенденция к проведению оценки рисков прослеживается в новый редакции Федерального закона «О персональных данных» [7], который в качестве мер направленных на обеспечение выполнения оператором обязанностей по защите персональных данных предписывает выполнять оценку вреда, который может быть причинен субъектам персональных данных, а также соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом по защите персональных данных.

Литература:

1. Петренко В.И., Копытов В.В., Суховей Д.Н. Методика расчета затрат от нарушений защищаемой медицинской информации Материалы XII Международной научно-практической конференции «ИБ-2012», Часть II Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 81-87.

2. BSISO/IEC 27001:2005 (BS7799-2:2005) Informationsecuritymanagement. Specification with guidance for use.

3. ФСТЭК: Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).

4. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Factor Analysis of Information Risk (FAIR).Industry standard.

6. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

7. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ (ред. от 25.07.2011) «О персональных данных».

Я.О. Калмыкова, С.В. Мухачев

ОГРАНИЧЕНИЕ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Уральский юридический институт МВД России, г. Екатеринбург, Россия

Ключевые слова: информация, распространение информации, запрещенная информация, единый реестр, оператор реестра, правовое регулирование, сеть Интернет.

В статье раскрываются вопросы, связанные с запретом на распространение некоторых видов информации в глобальной сети Интернет. Приводится краткая история вопроса. Рассматривается нормативно-правовая база, регулирующая правоотношения, связанные с таким ограничением, а также перечисляются виды информации, запрещенной для распространения. Обсуждаются вопросы правовой и организационной реализации такого ограничения, ведения реестра запрещенной информации. Приведены статистические данные о динамике количества обращений, количества записей в реестре запрещенной информации, структуре реестра по видам запрещенной информации в период 2013-2014 год.

Y.O. Kalmykova, S.V. Mukhachev

LIMITING THE DISSEMINATION OF INFORMATION ON THE INTERNET

Urals law Institute of MIA of Russia, Yekaterinburg, Russia

Keywords: information, dissemination of information, prohibited information, a single registry, the registry operator, the legal regulation of the Internet.

The article describes issues related to the prohibition on the dissemination of certain types of information in the global network Internet. A brief history of the issue. Considered normative-legal base, regulating the relations connected with this limit, and also lists the types of information prohibited for distribution. Discusses the legal and institutional implementation of such restrictions, the maintenance of the register of prohibited information. Provides statistical data on the dynamics of the number of calls, number of entries in the register of prohibited information, the registry structure by types of Smoking information during the 2013-2014 year.

Сегодня невозможно представить мир без получения и распространения информации с использованием сети Интернет. В России активное использование глобальной сети началось всего около 15 лет назад. Однако, за столь короткое по историческим меркам время, Интернет охватил все сферы информационной жизнедеятельности общества. Социальные сети, обмен всевозможными произведениями (книги, музыка, кино), интернет-торговля, развлечения, форумы, сетевые сообщества, государственные услуги, дистанционное обучение - вот лишь часть возможностей, которые предоставляет сегодня глобальная сеть любому пользователю. Еще совсем недавно в сети Интернет можно было найти любую информацию, начиная с рецептов приготовления каких-либо блюд и заканчивая литературой экстремистского характера. Совершенно ясно, что долго так продолжаться не могло: государство, общество, личность необходимо оградить от некоторых видов информации. Этот тезис нашел свое отражение в понятии «информационная безопасность», которое активно развивается и обсуждается [1].

Общество и государство пришли к пониманию необходимости ограничительных мер в сфере распространения информации с использованием сети Интернет. Некоторое время это понимание выражалось в форме частных высказываний, обсуждений в прессе и в научных работах [2]. В Государственной Думе не раз обсуждались вопросы регулирования правоотношений, возникающих при использовании сети Интернет. Можно вспомнить, например, что еще 18 мая 2000 г. состоялись масштабные парламентские слушания «О правовом регулировании использования сети Интернет в Российской Федерации». Однако стремительное развитие информационного обмена посредством сети Интернет подтолкнуло законодателя к разработке и принятию законодательства, регулирующего отношения, связанные с таким распространением информации.

Распространение информации в сети Интернет имеет ограничения, сформулированные законодателем в системообразующем Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Запрет на распространение некоторых видов информации появился относительно недавно (начиная с 2012 г.) и введен в действие рядом Федеральных законов [3-7].

Виды информации, ограниченной для распространения, перечислены в статье 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации»: материалы с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера; информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений; информация о способах совершения самоубийства, а также призывов к совершению самоубийства; информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами; информация, нарушающая требования Федерального закона от 29 декабря 2006 года № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи; информация, признанная вступившим в законную силу решением суда запрещенной для распространения.

Технически распространение информации в сети Интернет реализуется на основе сайтов, имеющих специальные IP-адреса и связанные с ними доменные имена. В целях ограничения доступа к сайтам, содержащим запрещенную для распространения информацию, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». В реестр включаются доменные имена и (или) указатели страниц сайтов, содержащих информацию, распространение которой в Российской Федерации запрещено; сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

Создание, формирование и ведение реестра согласно Постановлению Правительства Российской Федерации [8] осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомназор) и оператором реестра - организацией, зарегистрированной на территории Российской Федерации, которая может привлекаться к формированию и ведению единого реестра. Ведение единого реестра осуществляется в электронной форме в ежедневном круглосуточном режиме. На официальном сайте Роскомнадзора в электронном виде размещена форма для приема обращений органов государственной власти и органов местного самоуправления, а также юридических лиц, индивидуальных предпринимателей, общественных объединений и иных некоммерческих организаций, а также граждан о наличии на страницах сайтов в сети Интернет запрещенной информации и для взаимодействия с указанными органами власти, физическими и юридическими лицами в рамках деятельности по формированию и ведению единого реестра. Федеральный закон «Об информации, информационных технологиях и о защите информации»» и Постановление Правительства подробно определяют процедуру взаимодействия Роскомнадзора с провайдером хостинга, владельцем сайта и оператором реестра по поводу блокирования и разблокирования сайта, а также содержание реестровых записей и порядок доступа к ним.

Обратимся к статистике количества заявок на включение интернет-сайтов в Единый реестр и заблокированных сайтов. На 1 ноября 2013 года в Роскомнадзор из различных источников (в том числе от интернет-пользователей) поступило более 70 тыс. заявок на включение интернет-сайтов в Единый реестр [9]. Структура обращений выглядела следующим образом: в 55% обращений указывались сайты, пропагандирующие наркоманию, в 15% – суицид, 30% заявляли на ресурсы с детской порнографией. Из всех обращений четверть тех, что прошли первичный контроль, были направлены в уполномоченные органы на дальнейшую экспертизу. За прошедший год в Единый реестр вносилось более 14,5 тыс сайтов. Значительная часть из реестра была исключена после

удаления противоправной информации администраторами. Как показала практика, не удаляют запрещенную информацию не более 4% владельцев ресурсов, включенных в реестр. В их числе большую часть составляли сайты-наркоторговцы, интернет-магазины и форумам, на которых торгуются так называемые спайсы и курительные смеси.

На 1 ноября 2013 года в Едином реестре содержалось 3,4 тыс интернет-ресурсов, в числе которых примерно в 600 случаях был внесен IP-адрес. В работе с информацией из реестра принимают участие около 4 тыс операторов связи, которые предоставляют доступ к сети Интернет.

За первые 6 месяцев 2014 года в уполномоченные государственные органы поступило 28,5 тысяч обращений граждан, содержание которых было связано с исполнением федерального закона «Об информации, информационных технологиях и о защите информации» в Интернете [10]: к категории «распространение информации о наркотиках» относилось более 14,5 тысяч, к категории «детская порнография» - более 7 тысяч, к категории «информация о способах самоубийства» - более 6,5 тысяч обращений. Свыше 18 тысяч сообщений были отклонены при первичном рассмотрении обращений. За полгода в Единый реестр запрещенной информации было внесено 10235 записей (в том числе связанны с наркотиками - 6771 запись, из категории «детская порнография» - 1523 записи, связанные с суицидом - 1079 записей). Владельцам сайтов и хостинг-провайдерам направлены соответствующие уведомления. В установленные законом сроки запрещенная информация была удалена с 9194 ссылок. Можно видеть, что коэффициент эффективности уведомительной работы Роскомнадзора в рамках ведения Единого реестра в первом полугодии 2014 года составил 0,9. По состоянию на 3 июля 2014 года операторами связи был ограничен доступ к 2469 ресурсам в сети Интернет (в это число включены записи, которые были внесены в реестр в более ранние периоды).

И, наконец, в декабре 2014 года, при подведении итогов работы Роскомнадзора за год, были приведены следующие данные: в Единый реестр запрещенной информации на 22 декабря 2014 года внесено более 45700 ссылок, 64% ресурсов уличены в пропаганде и распространении наркотических средств, 15% - детской порнографии, 12% - суицида. В реестр блогеров внесено 317 человек, ожидают внесения 187 [11].

Подводя итоги, можно констатировать, что в России создана правовая база для регулирования правоотношений, связанных с распространением информации в сети Интернет. Разработан и отлажен механизм работы с обращениями о распространении запрещенной информации. Создан и успешно функционирует реестр запрещенной информации.

Литература:

1. Костюченко К.Л. Новые акценты в обеспечении информационной безопасности органов внутренних дел// Вестник Уральского юридического института МВД России, 2014, № 4, с. 30-32.

2. Наумов В.Б. Право и Интернет: очерки теории и практики. - М.: Книжный дом «Университет», 2002. - 432 с.

3. Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» /URL:http://www.garant.ru (дата обращения: 04.03.2015).

4. Федеральный закон от 28 декабря 2013 г. № 398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» /URL:http://www.garant.ru (дата обращения: 04.03.2015).

5. Федеральный закон от 5 апреля 2013 г. № 50-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части ограничения распространения информации о несовершеннолетних, пострадавших в результате противоправных действий (бездействия)» /URL:http://www.garant.ru (дата обращения: 04.03.2015).

6. Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» /URL:http://www.garant.ru (дата обращения: 04.03.2015).

7. Федеральный закон от 21 июля 2014 г. № 222-ФЗ «О внесении изменений в Федеральный закон «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской

Федерации» и отдельные законодательные акты Российской Федерации» /URL:http://www.garant.ru (дата обращения: 04.03.2015).
8. Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»» /URL:http://www.garant.ru (дата обращения: 04.03.2015).
9. http://rkn.gov.ru/news/rsoc/news22524.htm (дата обращения: 04.03.2015).
10. http://rkn.gov.ru/news/rsoc/news26141.htm (дата обращения: 04.03.2015).
11. http://rkn.gov.ru/news/rsoc/news29403.htm (дата обращения: 04.03.2015).

А.В. Котов

АНАЛИЗ РАЗВИТИЯ БЕСПРОВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ КОДОВОГО РАЗДЕЛЕНИЯ КАНАЛОВ И ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ

Северо-Кавказкий федеральный университет, г.Ставрополь, Россия

Ключевые слова: беспроводные телекоммуникационные системы, технология 3G, стандарт CDMA, угрозы информационной безопасности.

В статье проведен анализ тенденций развития современных беспроводных телекоммуникационных систем широкополосного доступа. Исследованы и проведена классификация угроз сетей 3-го поколения на основе технологии CDMA. Обоснована актуальность повышения эффективности системы защиты информации беспроводных сетей на основе технологии 3G с учетом специфики их угроз.

A.V. Kotov

THE ANALYSIS OF DEVELOPMENT WIRELESS TELECOMMUNICATION SYSTEMS ON THE BASIS OF CODE CHANNEL SEPARATION AND REASONS FOR NEED OF ENHANCEMENT OF METHODS OF INFORMATION SECURITY

Severo-Kavkazky federal university, Stavropol, Russia

Keywords: wireless telecommunications system, the technology 3G, standard CDMA, information security threats.

In article the analysis of tendencies of development of the modern wireless telecommunication systems of broadband access is carried out. Are probed and is carried out classification of threats of networks of the 3rd generation on the basis of the CDMA technology. Relevance of increase of system effectiveness of information security of wireless networks on the basis of technology 3G taking into account specifics of their threats is justified.

В настоящее время среди современных беспроводных телекоммуникационных систем идет стремительное развитие технологии 4G/LTE, но несмотря на это, сети 3-го поколения на основе семейства стандартов CDMA еще как минимум несколько лет будет оставаться основным источником доходов операторов мобильной связи. Главными факторами, поддерживающими интерес к системам третьего поколения, являются постоянное расширение зоны покрытия, рост скоростей передачи данных в этих сетях и увеличение проникновения смартфонов и других устройств с поддержкой этой технологии.

По данным J'son & Partners Consulting на 2014 год доля населения, проживающего на территории, охваченной сетями 3G превысила 75%, в то время как в 2012 г. этот показатель составлял около 65% [1].

На рисунке 1 представлен прогноз J'son & Partners Consulting до 2018 г. Технологии третьего поколения будут доминировать в России с долей около 78% по количеству абонентов. На долю доходов от мобильной передачи данных в сетях 2G/3G придется до 80% всех поступлений от мобильного интернет-доступа в России к концу прогнозного периода.

Главным фактором актуальности 3G-технологий является развитие мобильного интернет-доступа: пользователи нуждаются в постоянном увеличении скорости передачи данных из-за стремительного роста трафика. В ближайшие годы будет происходить модернизация 3G систем, направленная на усовершенствовании и увеличении скорости передачи данных.

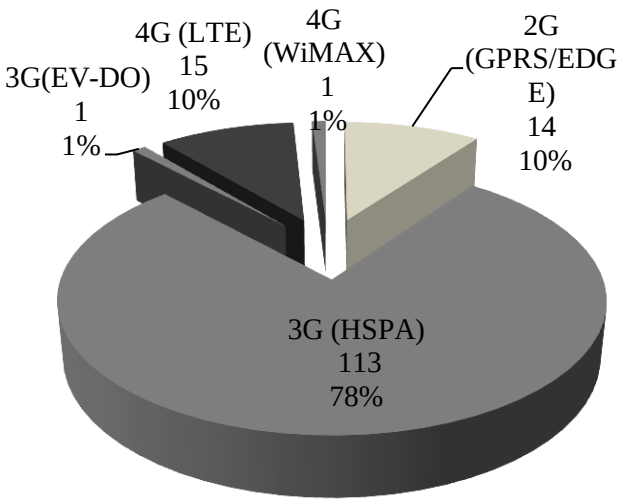


Рисунок 1. Прогноз количества абонентов (млн) и долей (%) различных технологий мобильного ШПД в России на 2018 г.

По прогнозу Ericsson, в 2018 г. в мире технология 3 поколения WCDMA/HSPA будет доминировать на мировом рынке (рисунок 2). В 2015 г. ожидается появление технологий HSPA+Advanced и WCDMA+. Согласно прогнозу Informa Telecoms & Media, количество подключений к HSPA в мире к концу 2017 года вырастет до 4,2 млрд., в то время как число 4G/LTE-подключений составит 940 млн.

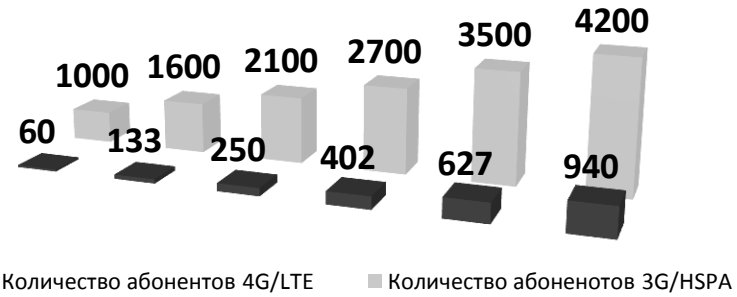


Рисунок 2. Прогноз динамики абонентской базы 3G/HSPA и 4G/LTE (млн пользователей) 2012-2017гг.

Сети связи 3G являются публичными высокотехнологичными информационными системами, использующими самые современные решения в области мобильной связи, построении сетей связи, автоматизированной обработки информации и предоставления широкого спектра услуг пользователям. Как и любая информационная система такого типа и класса, сеть связи 3G подвержена атакам нарушителей информационной безопасности, реализующим угрозы и уязвимости, присущие информационной сфере сети, причем функциональные преимущества сетей

связи третьего поколения по сравнению с сетями предыдущих поколений порождают новые угрозы и уязвимости.

В сетях связи 3G на основе технологии CDMA предусмотрен широкий перечень механизмов защиты информации, однако он охватывает не весь спектр вопросов, связанных с безопасным использованием информационных ресурсов сети. В связи с этим возникает необходимость в разработке дополнительных механизмов и мер обеспечения информационной безопасности. Для этого необходимо начиная с этапа проектирования и развертывания сетей связи 3G создавать систему защиты информации, применение которой позволит учитывать интересы в обеспечении информационной безопасности различных групп пользователей услугами сетей связи 3G, операторов и государства.

Одной из основных целей обеспечения информационной безопасности сетей 3G является необходимость предотвращения или снижение уровня ущерба субъектам, интересы которых затрагиваются при проведении атак на объекты защиты, материального, морального и иного случайного или преднамеренного ущерба из-за нарушения конфиденциальности, целостности, достоверности, подконтрольности и доступности защищаемой информации.

К объектам защиты относятся информационные ресурсы, обрабатываемые в рамках инфраструктуры сети, а также информационные ресурсы самой инфраструктуры сети, влияющие на эффективность обеспечения информационной безопасности [2]. Основными направлениями обеспечения информационной безопасности в сетях связи 3G являются [3]:

- исключение или существенное затруднение несанкционированного доступа к объектам сети, к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение перехвата информации, передаваемой по каналам связи с помощью технических средств;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств, ее обработки, хранении и передачи;
- предотвращение бесконтрольного развития эпидемий самораспространяющегося вредоносного кода (мобильных или компьютерных червей);
- ограничение и контроль выхода конфиденциальной информации за пределы сети;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств сети связи 3G;
- предотвращение мошенничества в информационной сфере сетей связи 3G.

Система защиты информации в сетях связи 3G должна строиться в соответствии с результатами анализа угроз, обусловленных наличием потенциального нарушителя, и уязвимостей объектов защиты, на которые эти угрозы распространяются [4].

Сеть связи 3G как объект информационной защиты имеет следующие основные особенности:

- пространственная распределенность сети и ее неоднородность, наличие удаленных, управляемых дистанционно, объектов;
- большое количество типовых объектов (базовые станции, контроллеры базовых станций, коммутаторы, мобильные терминалы), функционирующих в одинаковых условиях;
- большое количество субъектов с различными полномочиями по доступу к информации и услугам сети;
- наличие большого количества основных услуг и дополнительных видов обслуживания;
- использование цифрового коммутационного оборудования, характеризуемого наличием систем управления;
- использование аппаратуры, оборудования и программного обеспечения различных производителей, преимущественно импортного производства;
- взаимосвязь сети связи 3G с другими сетями связи и информационными системами;
- обязательное выполнение требований руководящих документов по защите информации и др.

Реализация угроз конфиденциальности ресурсов может привести к разглашению циркулирующих в системе сведений, не предназначенных для использования лицами без

соответствующих полномочий. Наиболее критичным является нарушение конфиденциальности информации в корпоративной сети компании-оператора, а так же компрометация аутентификационных центров и реестров. Так же существенным нарушением информационной безопастности является нарушение конфиденциальности переговоров (сеансов передачи данных).

Реализация угроз доступности ресурсов сети связи может привести к перегрузкам каналов связи и телекоммуникационных систем, появлению сбоев и отказов оборудования и программного обеспечения, и возникновению проблем с предоставлением услуг. Максимальный вред может быть нанесен отдельным подсистемам сети, обеспечивающим перенос и коммутацию трафика, а также стыковку с другими сетями. Вместе с тем, ряд подсистем являются умеренно чувствительными к реализации угроз доступности информационных ресурсов.

Реализация угроз целостности и достоверности ресурсов сети связи может привести к искажению информации во всех подсистемах сети, что может вызвать серьезные ошибки в обслуживании клиентов и предоставлении им информации, управлении техническими средствами, выполнении биллинговых операций. Кроме того, реализация данного класса угроз способна нарушить функционирование прикладного программного обеспечения и предоставить потенциальному злоумышленнику плацдарм для развития атаки на систему. В связи с этим для повышения эффективности системы безопасности беспроводных телекоммуникационных систем на основе технологии CDMA необходим совершенствование способов повышения защищенности системы, в частности на основе использования новых видов ортогональных последовательностей [5].

Выводы:

При использовании технологии CDMA может быть достигнута повышенная конфиденциальность передачи информации. Перехват данных в каналах связи таких систем связи существенно затруднен, поскольку в них имеется больше препятствий на пути злоумышленников по сравнению с другими системами связи.

Значительное расширение перечня предоставляемых сетями связи 3G услуг приводит к попыткам реализации новых незаконных способов получения конфиденциальной информации и новых видов угроз. Наиболее значимыми угрозами являются как широко известные угрозы для любых информационных систем, так и специфические угрозы, характерные для сетей мобильной связи.

При проектировании эффективной системы безопасности беспроводных телекоммуникационных систем на основе CDMA необходим поиск новых способов повышения защищенности системы.

Литература:

1. Состояние, перспективы развития и рыночный потенциал 3G (HSPA и HSPA+) в России и в мире [Электронный ресурс]. URL: http://www.json.ru.

2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие - М.: РИОР ИНФРА-М, 2013. – 392 с.

3. Формализация описания угрозы безопасности информации в информационно телекоммуникационных системах / Батищев Р.В., Язов Ю.К., Остапенко Г.А., Ференец С.С // Информация и безопасность. Вып. 3. - Воронеж: ВГТУ, 2003. С. 110-112.

4. Бельфер Р.А. Информационная безопасность цифровых систем связи // Безопасность информационных технологий. М — 2000. № 1.

5. Пашинцев В.П., Малофей О.П., Жук А.П., Самус М.В., Гайчук Д.В., Сазонов В.В. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн: Монография. - М.: Физматлит, 2010. – 196 с.

В.С. Долбня, Д.П. Кузнецова, М.С. Лугарь

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Белгородский государственный национальный исследовательский университет, г. Белгород, Россия

Ключевые слова: информационная безопасность государства, угроза безопасности информации, информационный терроризм, антитеррористическая информационная безопасность.

В современном мире, говоря об информационной безопасности, подразумевают компьютерную безопасность. Всё большую роль в жизни общества играет информация, находящаяся на электронных носителях. Такая информация очень уязвима в отличие, например, от информации на бумажном носителе, безопасность которой достигается физической защитой. Компьютеры и интернет дают возможность доступа к огромному количеству информации. Ведь вследствие стремительного процесса информатизации населения в автоматизированных системах накапливается большие объемы данных. В связи с этим растет количество компьютерных преступлений. Поэтому вопрос защиты информации в наше время носит очень веский характер.

V.S. Dolbnya, D.P. Kuznetsova, M.S. Lugar

THE PROBLEMS OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION

Belgorod National Research University, Belgorod, Russia

Key words: information security of the state, the threat of information security, information terrorism, anti-terrorism information security.

In today's world, speaking about information security, computer security meant. Increasingly important role in society is information stored on electronic media. Such information is very sensitive, in contrast, for example, the information on paper, security is achieved physical protection. Indeed, due to the rapid process of informatization of the population in automated systems accumulated large amounts of data. In this connection increasing number of computer crimes. Therefore, the issue of information security in our time is a very strong character.

Ещё недавно проблеме обеспечения информационной безопасности в России не уделяли должного внимания, практически игнорировали. Информацию защищали путём тотальной секретности и ограничением передачи. А тем временем вероятность перемещения значительных объёмов информации через границы государств стала действительно реальной. Вместе с огромной пользой и преимуществами, которые пришли с развитием информационных технологий, в нашей жизни появились и новые проблемы и угрозы, борьба с которыми непрерывна и должна постоянно совершенствоваться.

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на неё. [5]

Проблема информационной безопасности – возможность взлома системы. И эта возможность представляет собой постоянную угрозу безопасности международного масштаба.

Государственная политика РФ в области информационной безопасности придерживается следующих принципов:

- федеральная программа ИБ;
- нормативно-правовая база;
- регламентация доступа к информации;
- юридическая ответственность за сохранность информации;
- контроль над разработкой и использованием средств защиты информации;
- предоставление гражданам доступа к мировым информационным системам.

Также для обеспечения информационной безопасности Российской Федерации стало приоритетным направлением совершенствование правовых механизмов регулирования общественных отношений, задействованных в информационной сфере.

Обширное распространение информационных технологий в жизни общества привело к необходимости гарантировать непрерывность и точность функционирования информационных систем, связанных с безопасностью жизни общества, а также обеспечить защиту гражданских прав и свобод и имущественных прав в соответствии с законодательством и конституцией Российской Федерации.

Информацию можно использовать как оружие, и это её применение стремительно развивается. Выявление источника атаки информационным оружием бывает невозможным. Что делает его еще более опасным и заманчивым для информационных террористов.

Информационный терроризм проявляется в запугивании населения и органов власти, с целью достижения преступных намерений. Терроризм проявляется в угрозе насилия, поддержания людей в постоянном страхе ради достижения своих целей. Информационный терроризм может повлечь за собой не только материальный и моральный ущерб, но и человеческие жертвы, а также вызвать последствия национального характера.

В связи с появлением информационного терроризма появилось такое понятие как антитеррористическая информационная безопасность.

Антитеррористическая информационная безопасность – совокупность механизмов, инструментальных средств, методов, мер и мероприятий, позволяющих предотвратить, обнаружить, а в случае обнаружения, - оперативно реагировать на действия, способные привести:

- к разрушению инфраструктуры сети посредством вывода из строя системы управления ею или отдельных её элементов;
- к несанкционированному доступу к информации, охраняемой законом и носящей высокий уровень секретности, нарушению её целостности, конструктивной управляемости и защищенности. [5]

Информационное оружие может нанести удар по национальной безопасности Российской Федерации. Причина этого – стремление ряда стран к лидерству в мировом информационном пространстве, а угроза – вытеснение России с информационного рынка.

Чтобы минимизировать риск вытеснения с внешнего и внутреннего информационного рынка, принимаются следующие меры:

- постановка и проведение научных исследований, направленных на получение методик исследования программного обеспечения и выявления закладных устройств;
- развитие отечественной индустрии в области создания и производства оборудования элементов телекоммуникационных систем;
- минимизация числа иностранных фирм - поставщиков;
- координация действий по проверке надёжности указанных фирм;
- уменьшение номенклатуры поставляемого оборудования;
- переход от поставок оборудования к поставкам комплектующих на элементарном уровне;
- установление приоритета в использовании отечественных средств защиты этих систем.

Информационная политика государства сейчас выдвинута на передний план, так как эффективность работы различных государственных, а также общественных структур во многом зависит от правильно выбранной концепции и успешной реализации информационной политики.

Способы обеспечение информационной безопасности должны непрерывно обновляться и совершенствоваться, необходим постоянный контроль, выявление слабых мест и потенциальных каналов утечки информации. Информационная безопасность является одним из главных аспектов государственной безопасности на всех её уровнях.

Литература:

1. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002, с.208.

2. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006, с.264.

3. Галицкий А. В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004, с.616.

4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000, с.428.

5. Пилипенко В. Ф. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.

А.В. Леонов

КОНФИДЕНЦИАЛЬНОСТЬ В ИНТЕРНЕТЕ ВЕЩЕЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Омский государственный технический университет, г. Омск, Россия

Ключевые слова: Интернет вещей, конфиденциальность, радиочастотная идентификация (RFID).

Интернет вещей характеризуется неоднородностью технологий, позволяющих предоставить инновационные услуги в различных сферах деятельности. Таким образом, удовлетворение требованиям безопасности и конфиденциальности играет фундаментальную роль. В данном исследовании проанализированы основные научные проблемы и существующие решения в области конфиденциальности IoT, представлены направления работы для перспективных исследований.

A.V. Leonov

PRIVACY IN THE INTERNET OF THINGS: PRESENT STATE AND FUTURE PROSPECTS

Omsk State Technical University, Omsk, Russia

Keywords: Internet of Things (IoT), privacy, radio-frequency identification (RFID).

Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this scenario, the satisfaction of security and privacy requirements plays a fundamental role. In this survey we present the main research challenges and the existing solutions in the field of IoT privacy and suggesting some hints for future research.

Безопасность является важнейшим компонентом для обеспечения широкого внедрения технологий и приложений Интернета вещей (англ. Internet of Things, IoT). При этом конфиденциальность является фундаментальным требованием и определяет правила, по которым можно получить доступ к данным, принадлежащим разным пользователям (людям и устройствам).

Интернет вещей – это новая парадигма, которая быстро набирает силу в контексте развития современных телекоммуникаций. Основной идеей этой концепции является повсеместное присутствие вокруг нас множества вещей и объектов. К ним, например, могут быть отнесены: радиочастотная идентификация меток (англ. Radio Frequency Identification, RFID), сенсоры, датчики, мобильные телефоны и т.д., которые посредством уникальных схем адресации могут взаимодействовать друг с другом и окружающими их предметами для достижения общих целей [1].

IoT находит применение во множестве различных областей. Это, например, удаленный мониторинг за состоянием пациентов, контроль за потреблением энергии, регулирование движения, производственная цепочка, гражданская оборона. Пользователи требуют обеспечения защиты конфиденциальной информации. Понятие частной жизни глубоко укоренилось в реалиях современного мира и признается законодательствами всех цивилизованных стран. Опасения по

обеспечению конфиденциальности данных оказались серьезным препятствием на пути к распространению технологий, задействованных в IoT Для решения этой проблемы было предпринято несколько попыток, которые проанализированы в ходе подготовки данной статьи.

Статья [2] фокусирует внимание на идее маркировки данных для управления конфиденциальностью. На основе методов управления информационными потоками данные, представляющие конфиденциальную информацию, могут быть помечены. Это позволяет системе обеспечить сохранность персональных данных. Очевидно, что использование меток в условиях ограниченных ресурсов узлов/датчиков не может являться эффективным решением, поскольку метки могут быть слишком большими по отношению к размеру передаваемых данных, они генерируют избыточный трафик, а в случае с IoT это нежелательно.

В работе [3] предложен протокол управления доступом, контролируемый пользователем на основе контекстно-зависимых политик конфиденциальности. Пользователи имеют возможность контролировать, какие из их персональных данных собираются и доступны, кто и когда имеет доступ к этой информации.

Публикация [4] содержит описание процесса непрерывной анонимизации потоковых данных через адаптивную кластеризацию (англ. Continuously Anonymizing STreaming data via adaptive cLustEring, CASTLE). Предложена схема на основе кластера, которая анонимизирует потоки данных «на лету» и в то же время обеспечивает актуальность анонимизированных данных путем удовлетворения требований по задержке.

В материалах статьи [5] традиционные механизмы конфиденциальности разделяются на две категории: контролируемый и ограниченный доступ. Первая служит для предотвращения получения и клонирования конфиденциальных данных; вторая направлена на ограничение доступа и предотвращения атак.

В [6] анализируется угроза обеспечения конфиденциальности, возникающая, когда статическое доменное имя присваивается определенному IoT узлу. В данной работе авторами предложено усовершенствование для увеличения защищенности персонального DNS (англ. Domain Name System) для смарт(интеллектуальных)-устройств, которые могут проверить подлинность личность пользователя и отклонить несанкционированный доступ к устройству. Схема совместима с широко используемыми DNS и DNSSEC (англ. Domain Name System Security Extensions) протоколами.

В статье [7] представлен полностью децентрализованный анонимный протокол аутентификации для обеспечения конфиденциальности IoT приложений. Система определяет две возможных роли для узлов участников: пользователи представляют собой узлы, формирующие данные, сборщики, в свою очередь, отвечают за сбор данных от авторизованных пользователей/узлов. Пользователи могут анонимно подтвердить свою подлинность перед сборщиками, которые обладают действительными учетными данными анонимного доступа (англ. Anonymous Access Credential, AAC), кодирующих определенный набор атрибутов, установленных самой системой. Протокол состоит из трех этапов: 1) создание; 2) регистрация пользователей (пользователи получают учетные данные анонимного доступа); 3) пользователь должен подтвердить свою легитимность перед сборщиком данных. Такой протокол гарантирует анонимность пользователя, устойчивость к различным типам атак. Кроме того, такая система использует полностью распределенный подход, исключает проблему единой точки отказа.

В [8] выполнен сравнительный анализ двух основных типов атрибутов для шифрования ABE (Attribute-Based Encryption,): KP-ABE (Key-Policy Attribute-Based Encryption) и CP-ABE (Ciphertext-Policy Attribute-Based Encryption). Моделирование проводилось с учетом классификации типов мобильных устройств (ноутбук и смартфон) с целью выявления оптимальных показателей ABE для IoT.

Альтернативный подход, использующий схему подписи основанную на атрибутах (англ. Attribute-Based Signature, ABS), представлен в [9]. В новой схеме, названной ePASS, пользователи не могут подделать подписи с атрибутами, которыми они не владеют, при этом подпись обеспечивает уверенность, что только пользователь с соответствующими атрибутами, удовлетворяющими политике, может одобрить сообщение.

Особое внимание защите конфиденциальности IoT уделяется в [10]. Предложен протокол взаимной аутентификации для систем WSN (англ. Wireless Sensor Network) и RFID. Он объединяет в метке генератор случайных чисел и считыватель, принимает одностороннюю хэш функцию, обновление ключа в режиме реального времени и резервный ключ в качестве механизма для

уменьшения рисков, связанных с воспроизведением (англ. Replay), копированием (англ. Replication), отказом в обслуживании (англ. DoS), подменой (англ. Spoofing) и т.д.

Оценка требований к конфиденциальности данных, предоставляемых различными источниками, рассматривается в [11]. В статье определяется многоуровневая архитектура IoT для того, чтобы оценить качество данных, безопасность и уровень конфиденциальности.

Подводя итог, отметим следующее: требование конфиденциальности в IoT в настоящее время раскрыто частично, поэтому есть широкий простор для проведения дальнейших исследований. Формулирование требования о конфиденциальности на ранних стадиях развития имеет очень важное значение для обеспечения доверия со стороны пользователей и содействия по повсеместному принятию новых систем IoT.

Литература:

1. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010.

2. D. Evans, D. Eyers, Efficient data tagging for managing privacy in the internet of things, in: Proceedings – 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012, Besancon, France, 2012, pp. 244–248.

3. X. Huang, R. Fu, B. Chen, T. Zhang, A. Roscoe, User interactive internet of things privacy reserved access control, in: 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, 2012, pp. 597–602.

4. J. Cao, B. Carminati, E. Ferrari, K.L. Tan, CASTLE: continuously anonymizing data streams, IEEE Trans. Dependable Secure Comput. 8 (3) (2011) 337–352.

5. J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Universities Posts Telecommun. 8 (2) (2011) 109–112.

6. Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.

7. A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy preserving iot targetdriven applications, Comput. Secur. 37 (2013) 111–123.

8. X. Wang, J. Zhang, E. Schooler, M. Ion, Performance evaluation of attribute-based encryption: Toward data privacy in the IoT, in: 2014 IEEE International Conference on Communications, ICC 2014, Sydney, NSW, 2014, pp. 725–730.

9. J. Su, D. Cao, B. Zhao, X. Wang, I. You, ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things, Future Gener. Comput. Syst. 33 (0) (2014) 11–18.

10. L.b. Peng, W.b. Ru-chuan, S. Xiao-yu, C. Long, Privacy protection based on key-changed mutual authentication protocol in internet of things, Commun. Comput. Inf. Sci. 418 CCIS (2014) 345–355.

11. S. Sicari, C. Cappiello, F.D. Pellegrini, D. Miorandi, A. Coen-Porisini, A security-and quality-aware system architecture for internet of things, Inf. Syst. Frontiers (2014) 1–13.

12. S. Sicari, A. Rizzardi, C. Cappiello, A. Coen Porisini, A NFP model for internet of things applications, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 164–171.

А.С. Любухин

РАЗРАБОТКА МЕТОДИКИ УСОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия.

Ключевые слова: несанкционированный доступ, криптография, аутентификация, идентификация, биометрия, пароль, шифрование, симметричные алгоритмы, ассиметричные алгоритмы.

Описана проблема деструктивного воздействия на информационные системы и необходимость совершенствования системы защиты от несанкционированного доступа к информации. Описаны основные преимущества и недостатки каждого из методов защиты, а также предложены меры по улучшению системы защиты информации от незаконного доступа к ней.

A.S. Lyubuhin

DEVELOPMENT OF A TECHNIQUE TO IMPROVE PROTECTION AGAINST UNAUTHORIZED ACCESS TO INFORMATION

Rostov State University of Economics (RINH)
Rostov-on-Don, Russia.

Keywords: unauthorized access, cryptography, authentication, identification, biometrics, password, encryption, symmetric algorithms, asymmetric algorithms.

Described the problem of destructive impact on information systems and the need to improve the system of protection against unauthorized access to information. The basic advantages and disadvantages of each method of protection, as well as proposed measures to improve the protection of information from unauthorized access to it.

Компьютеры обеспечивают хранение и обработку информации. В современном мире компьютерные сети не только помогают общаться, учиться и всесторонне развиваться человеческой личности, но и обеспечивают защиту систем обороны и безопасности страны.

Именно этим, прежде всего, и обусловлена высокая степень актуализации проблемы защиты от несанкционированного доступа к информации, поскольку высокий уровень автоматизации всех сфер в обществе, на мой взгляд, порождает риск снижения безопасности (как личной в частности, так и государственной в целом).

Для разработки способов решения проблемы несанкционированного доступа к информации (в дальнейшем НСД) нужно подробно детализировать методы и конфигурацию незаконного проникновения к данным.

Прежде всего, нужно оценить, насколько степень компьютерной грамотности в нашей стране изменилась по сравнению с периодом начала 90-х годов 20 века. Проведя аналитические действия, можно сказать, что между этими двумя периодами имеется колоссальный разрыв. Компьютеры в то время были, пожалуй, только в научно-исследовательских институтах, которые представляли особую важность для страны. В ВУЗах в то время студентам были доступны "большие" ЭВМ и мини-ЭВМ , которые по своим возможностям соответствовали тем зарубежным моделям, которые уже тогда вышли из производства.

И вот в одночасье все вдруг изменилось. Словно гром среди ясного неба, компьютеры ворвались в нашу жизнь. Вычислительные машины сейчас повсюду: в офисах не только крупных компаний, но и мелких организаций, даже на складах и в крохотных магазинах, ну и, конечно же, практически в каждом доме, и зачастую не в единственном экземпляре. А уровень компьютерной грамотности сотрудников не всегда соответствует норме, и именно поэтому зачастую НСД становится возможным из-за некомпетентных и ошибочных действий пользователей вычислительных машин.

Таким образом, посредством анализа уровня подготовки пользователей злоумышленники используют различные методы, в зависимости от конкретной ситуации. Среди них следующие методы: «Работа между строк», «Отказы в обслуживании», «Анализ трафика» и некоторые другие.

Основным и самым распространенным барьером, защищающим от НСД, по-прежнему остается идентификация и аутентификация: парольная и биометрическая. Однако преступнику не стоит особых усилий преодолеть эту преграду. Любой пароль должен соответствовать двум обязательным критериям: быть не слишком сложным и запоминаемым для аутентифицируемого объекта и в то же время сложным для подбора и генерации ключа для взломщика. Длинные и сложные пароли, как известно, персонал организации зачастую сохраняет на своих персональных компьютерах, а с внедрением в повседневную жизнь Интернета понятие «персональный компьютер» перестает иметь смысл, поскольку, пока пользователь находится в сети, его данные, хранящиеся на ПК подвержены несанкционированному доступу других пользователей сети, имеющих необходимый уровень мастерства. А короткие и простые легко взломать.

Поэтому в противовес парольной аутентификации одной из приоритетных разработок в сфере информационной безопасности является активно внедряемая аутентификация по биометрическим характеристикам человека, которые являются уникальными и исключают возможность их фальсификации. Этот метод осуществляется посредством идентификации по физиологическим и поведенческим характеристикам: по отпечаткам пальцев, особенностям сетчатки глаз, геометрии руки, лица, по динамике рукописной подписи, по особенностям голоса, по способу работы на клавиатуре и некоторым другим характеристикам, присущим лишь данному объекту.

Биометрические данные идентифицируемого объекта обрабатываются компьютерной системой, и биометрический шаблон помещается в базу данных. В дальнейшем этот шаблон является критерием подлинности, и в соответствии с результатом проверки определяется уровень доступа для этого объекта. Очень часто биометрическая аутентификация – это только первый рубеж защиты и часто служит для активизации других защитных барьеров. Одним из таковых являются интеллектуальные карты, хранящие криптографические алгоритмы. Наряду с огромным количеством достоинств у биометрии есть масса недостатков. Первый недостаток заключается в том, что биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с характеристиками человека на данный момент времени. А, как известно, за время пути может произойти масса событий, влияющих на процесс идентификации. Даже банальная семейная ссора сотрудника может повлечь за собой волнение и напряженность, вследствие чего изменяются биометрические параметры. Например, голос колеблется и не соответствует шаблонному тембру на 100%. Помимо этого эта система похожа на простую базу данных, где данные можно сфальсифицировать, украсть, исказить. Ну и самым основным недостатком является то обстоятельство, что биометрические данные человека в процессе его жизнедеятельности изменяются, поэтому база шаблонов нуждается в сопровождении и постоянном редактировании, что создает определенные проблемы и для пользователей, и для администраторов, прежде всего требуя сильных затрат со стороны руководства.

К тому же биометрический идентификатор (глаз, голос и др.) сменить нельзя. Если биометрические данные будут скомпрометированы, придется существенн модернизировать всю систему защиты, что является крайне сложным, долговременным и также весьма затратным процессом.

Следующей ступенью при защите информации от НСД являются криптографические методы. Различают два класса криптографии: симметричная и ассиметричная.

Самым распространенным алгоритмом шифрования является DES (Data Encryption Standard). Шифруется блок размером в 64 бита с использованием 64-битного ключа. При этом осуществляется 16 проходов. Алгоритм DES может быть использован в различных методах шифрования.

Вот основные методы, использующие алгоритм DES.

Метод CBC (Cipher Block Changing - Сцепление зашифрованных блоков). Здесь k-ый блок шифруемого текста образуется в результате выполнения команды XOR над (k-1)-м блоком зашифрованного текста и k-ым блоком открытого текста. Метод CFB (Cipher FeedBack – Обратная связь по шифру). В нем предыдущая часть зашифрованного текста интегрируется со следующей частью незашифрованного (открытого) текста. Метод OFB (Output FeedBack – Обратная связь по выходу) заключается в том, что алгоритм DES используется для создания псевдослучайного

потока битов, который объединяется с открытым текстом, и в результате этого создается поток зашифрованного текста.

Метод PCBC (Propagating Cipher Block Changing - Сцепление зашифрованных блоков с множественной связью). Данный алгоритм отличается от метода CBC тем, что с k-ым блоком зашифрованного текста объединяется и (k – 1)-й блок зашифрованного текста и (k – 1)-й блок открытого текста.

Методы шифрования и дополнения блоков, используемые с алгоритмом DES, по своей природе, универсальны и могут быть использованы с другими шифрами, например, с DESede (3-DES) [1, С 90-91.]

В связи с популярностью алгоритма DES и по мере выявления его недостатков, во второй половине 90-х годов специалисты криптографии искали способы повышения его стойкости, при одновременном сохранении его в качестве базового алгоритма шифрования. В алгоритмах 3-DES выполняется троекратное шифрование по алгоритму DES, что приводит к эффективной длине ключа в 168 разрядов. В одном из вариантов 3-DES третий ключ равен первому, эффективная длина ключа в таком случае составляет 112 разрядов. Также весьма распространен «Каскадный 3-DES» - это стандартный тройной DES, к которому добавлен механизм обратной связи (такой как CBC, OFB или CFB). Он очень стоек к атакам с целью вскрытия.

Также имеет место быть шифрование с открытым ключом. В алгоритмах с открытым ключом необходимо, чтобы закрытый ключ было невозможно вычислить по открытому ключу.

Первый алгоритм - это алгоритм Ривеста-Шамира-Эдлемана носящий инициалы его изобретателей. Стойкость этого алгоритма определяется сложностью разложения больших чисел на множители. Основным недостатком шифра RSA и других алгоритмов с открытым ключом, является их низкая производительность, по сравнению с алгоритмами с секретным ключом. К тому же алгоритм RSA уступает по скорости сопоставимым реализациям алгоритма DES в 100, а то и в 1000 раз. При появлении эффективного способа разложения больших чисел на множители шифр RSA можно легко раскрыть. К тому же алгоритм RSA и другие алгоритмы с открытым ключом не защищены от множества атак, которые определяются способами использования этих алгоритмов.

Следующим популярным алгоритмом является AlGamal, который был разработан в 1984 г. Тэгером Эль-Гамалом. Алгоритм до сих пор не запатентован и может использоваться всеми свободно и без ограничений. Защищенность алгоритма AlGamal основывается на сложности вычисления дискретного логарифма в конечном поле.

Проведя детальный анализ методов несанкционированного доступа и способов его предотвращения, можно придти к выводу, что наибольшего положительного результата по решению этой проблемы можно добиться путем использования комплексного подхода. Это подразумевает, что он должен включать в себя комплекс мер по совершенствованию парольной идентификации, биометрического способа защиты, криптографических защитных алгоритмов, ну и, конечно, механизм переподготовки кадров, занятых в работе компьютерными системами.

Основами повышения эффективности парольной аутентификации являются следующие меры: наложение технических ограничений; управление сроком действия паролей; ограничение доступа к файлу паролей; ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы"); использование программных генераторов паролей.

Для улучшения парольной аутентификации можно предложить систему S/KEY, которая имеет статус Internet-стандарта (RFC 1938). Кроме системы аутентификации S/KEY весьма эффективной является генерация нового пароля через небольшой промежуток времени (например, каждые 60 секунд). Для этого могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; помимо этого, часы клиента и сервера должны быть синхронизированы. Можно использовать сервер аутентификации Kerberos. Это программный продукт, разработанный в середине 1980-х годов и претерпевший с тех пор ряд принципиальных измененийСистема представляет собой доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов. Эта система помогает им в обоюдной проверке подлинности. [3, С 5-6]

Уместным будет порекомендовать средство защиты информации от несанкционированного доступа Secret Net 6.0. Программный продукт компании «Код

Безопасности» Secret Net 6.0 является сертифицированным средством защиты информации от несанкционированного доступа.

Ключевые возможности СЗИ от НСД Secret Net: аутентификация пользователей; разграничение доступа пользователей к информации и ресурсам автоматизированной системы; контроль утечек и каналов распространения конфиденциальной информации; контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации; оперативный мониторинг, аудит безопасности.

СЗИ от НСД Secret Net на сегодняшний день – один из самых надежных и широко используемых программных продуктов в области защиты информации. Он активно используется как в государственных структурах, таких как Управление Федерального Казначейства, так и в частных организациях, работа которых связанна с обработкой конфиденциальной информации. [2, С 30-33]

Литература:

1. Фомичев В.М. Дискретная математика и криптология. Курс лекций — М.: Диалог-мифи, 2003. — 400 с.

2. Гатчин Ю.А., Коробейников А.Г., Краснов А.Г. Управление доступом к информационным ресурсам: Учебно методическое пособие. 2010г.

3. RFC4120 — The Kerberos Network Authentication Service (V5).

А.В. Макарова

УСОВЕРШЕНСТВОВАНИЕ АЛГОРИТМА ВЫЧИСЛЕНИЯ ИНТЕРВАЛЬНОГО НОМЕРА В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

Северо-Кавказский федеральный университет, г. Ставрополь, Россия

Ключевые слова: полиномиальная система классов вычетов, ошибка, корректирующие коды, позиционные характеристики, интервальный номер.

Актуальность статьи связана с тем, что одним из наиболее перстпективных направлений обеспечения отказоустойчивости специализированных вычислительных устройств цифровой обработки сигналов является широкое применение кодов, способность обнаруживать и корректировать возникающие ошибки

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет обнаруживать и корректировать ошибки в процессе функционирования непозиционного спецпроцессора.

A.V. Makarova

IMPROVEMENT OF THE ALGORITHM FOR COMPUTING THE INTERVAL NUMBER IN POLYNOMIAL SYSTEM OF RESIDUE CLASSES

North-Caucasus Federal University, Stavropol, Russia

Keywords: polynomial system of residue classes, error correcting codes, positional characteristics, interval number.

The relevance of the article is the fact that one of the most perstpektivnyh directions resiliency specialized computing devices of digital signal processing is widely used codes, the ability to detect and correct errors that occur

The use of a polynomial system of residue classes (PSKV) to detect and correct errors in the operation nonpositional special processor.

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет обнаруживать и корректировать ошибки в процессе функционирования непозиционного спецпроцессора. Применение ПСКВ позволяет свести операции умножения, сложения и вычитания к соответствующим операциям над остатками.

В полиномиальной системе классов вычетов в качестве оснований системы используются неприводимые полиномы $p_i(x)$, где $i = 1,2,...,n$, любой полином $A(x)$, удовлетворяющий условию $\deg A(x) < \deg P(x),$ где $P_{\text{раб}}(\text{x}) = \prod_{i=1}^{n} p_i(x)$ – рабочий диапазон системы, $P_{\text{пол}}(x) = P_1(x) \cdot P_2(x) \cdot P_3(x) \cdot P_4(x) \cdot P_5(x)$, $P(x)$ – степень полинома, можно однозначно представить в виде набора остатков $A(x) = (\alpha_1(x), \alpha_2(x),..., \alpha_n(x)),$ где $\alpha_i(x) \equiv \text{A(x) mod } \text{p}_\text{i}(x); i = 1, 2,..., n.$ Для обнаружения и исправления ошибок в модулярном коде полинома $A(x) = (\alpha_1(x), \alpha_2(x),..., \alpha_n(x))$ вводим избыточность, добавляем контрольные основания $p_{n+1}(x)$ и $p_{n+2}(x)$, удовлетворяющие условию

$$\deg p_{n+1}(x) + \deg p_{n+2}(x) \geq \deg p_n(x) - \deg p_{n-1}(x).$$

Проведенные исследования показали, что решающее значение на построение процедур контроля и коррекции ошибок в непозиционных кодах оказывает алгоритм вычисления позиционной характеристики. Выявление зависимости между местоположением ошибочных полиномов $A^*(x)$ относительно нулевого интервала $P_{полн}(x)$ и оставшимися работоспособными вычислительными модулями $p_j(x)$ ПСКВ, позволит строить более эффективные чем традиционные процедуры контроля и коррекции ошибок.

Говоря о непозиционных кодах с изменяемой структурой, базисом, положенным в основу определения позиционной характеристики – интервальный полином $l_{инт}(x)$ модулярной кодовой конструкции, является размещение элемента $A(x)$ относительно множества $M(x)$ [1, 2, 3].

Возникновение ошибки в непозиционной кодовой конструкции $A(x)$ переводит последнюю из подмножества разрешенных комбинаций в подмножество запрещенных. Согласно КТО значение ошибочного полинома $A^*(x)$ определяется выражением

$$A^*(x) = \sum_{i=1}^{k+r} \alpha_i(x) B_i(x) \bmod P_{пол}(x) = A(x) + \left|\Delta\alpha_j(x) B_j(x)\right|^+_{P_{пол}(x)}. \quad (1)$$

Анализ выражения (1) показывает, что местоположение ошибочного полинома $A^*(x)$ относительно рабочего диапазона $P_{раб}(x)$ определяется величиной второго слагаемого.

Предположим, что в полиноме $A(x)$, представленном в непозиционном коде ПСКВ $(\alpha_1(x), \alpha_2(x),..., \alpha_{k+r}(x))$ произошла ошибка по j-ому основанию. Тогда интервал, в который попал полином определяется равенством $l^j_{инт}(x) = \left[\frac{A^*(x)}{P_{раб}(x)}\right]$.

Воспользуемся китайской теоремой об остатках

$$l^j_{инт}(z) = \left[\frac{A^*(x)}{P_{раб}(x)}\right] = \left[\frac{A(x) + \Delta A_j(x)}{P_{раб}(x)}\right] = \left[\frac{A(x)}{P_{раб}(x)} + \frac{\Delta A_j(x)}{P_{раб}(x)}\right], \quad (2)$$

где $\Delta A_j(x) = \Delta\alpha_j(x) B_j(x) \bmod P_{полн}(x)$ – величина ошибки.

Исходя из условия $A(x)$ принадлежит рабочему диапазону, имеем $l_{инт}(x) = \left[\frac{A(x)}{P_{раб}(x)}\right] = 0$. Тогда выражение (3) примет вид

$$l^j_{инт}(x) = \left[\frac{\Delta\alpha_j(x) B_j(x) \bmod P_{полн}(x)}{P_{раб}(x)}\right] = \left[\frac{\left|\Delta\alpha_j(x) m_j(x)\right|^+_{P_j(z)} \frac{P_{полн}(x)}{p_j(x)}}{\prod_{i=1}^{k} p_i(x)}\right] =$$

$$= \left| \frac{\left| \Delta\alpha_j(x) m_j(x) \right|_{P_j(x)}^{+} \prod_{i=k+1}^{k+r} p_i(x)}{p_j(x)} \right|_{P_{конт}(x)}^{+} \quad (3)$$

Вес ортогонального базиса равен

$$m_j(x) = \left(\prod_{\substack{i=1 \\ i \neq j}}^{k+r} m_j^i(x) \right) \bmod p_j(x) \quad (4)$$

Подставив (4) в (3), и упростив выражение, имеем

$$l_{инт}^j(x) = \left| (\Delta\alpha_j(x) \prod_{\substack{i=1 \\ i \neq j}}^{k+r} m_j^i(x)) \bmod p_j(x) \frac{1}{p_j(x)} \right|_{P_{конт}(x)}^{+}$$

Рассмотрим пример классического расчета интервального номера.

Пусть задано расширенное поле $GF(2^5)$, в котором определены минимальные многочлены: $p_1(x)=x^5+x^3+1$; $p_2(x)=x^5+x^2+1$; $p_3(x)=x^5+x^4+x^3+x^2+1$; $p_4(x)=x^5+x^4+x^3+1$; $p_5(x)=x^5+x^4+x^2+1$.

В качестве контрольного основания используются $p_4(x)=x^5+x^4+x^3+1$ и $p_5(x)=x^5+x^4+x^2+1$.

При этом рабочий диапазон – $P_{раб}(x) = \prod_{i=1}^{3} p_i(x) = x^{15} + x^{14} + x^{12} + x^8 + 1$. При этом полный диапазон составляет $P_{полн}(z)=z^{31}+1$.

Вычислим:

$B_1 = m_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$,

Для основания $p_1(x)=x^5+x^3+1$ заданы следующие элементы

$\beta^0 = x^4 + x^3 + x^2 + x$

$\beta^1 = x^4 + x^2 + 1$

$\beta^2 = x^2 + 1$

$\beta^3 = x^3 + x$

$\beta^4 = x^4 + x^2$

$B_2 = m_2 \cdot p_1 \cdot p_3 \cdot p_4 \cdot p_5$,

для основания $p_2(x)=x^5+x^2+1$:

$\beta^0 = x^4 + x^3 + x^2 + x$

$\beta^1 = x^4 + x^2 + 1$

$\beta^2 = x^3 + x^2 + x + 1$

$\beta^3 = x^4 + x^3 + x^2 + x$

$\beta^4 = x^4 + x^3 + 1$

$B_3 = m_3 \cdot p_1 \cdot p_2 \cdot p_4 \cdot p_5$,

для основания $p_3(x)=x^5+x^4+x^3+x^2+1$:

$\beta^0 = x^2 + x$

$\beta^1 = x^3 + x^2$

$\beta^2 = x^4 + x^3$

$\beta^3 = x^3 + x^2 + 1$

$\beta^4 = x^4 + x^3 + x$

Подбираем значение m_{i1}, $m_1 = x^3 + 1$, $m_2 = x^3 + x + 1$, $m_3 = x^3 + x$

$P_1 = p_2 \cdot p_3 \cdot p_4 \cdot p_5 = (x^{20} + x^{19} + x^{18} + x^{15} + x^{13} + x^{12} + x^9 + x^7 + x^6 + x^5 + x^2 + 1)$

$P_2 = p_1 \cdot p_3 \cdot p_4 \cdot p_5 = (x^{20} + x^{19} + x^{15} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + 1)$

$P_3 = p_1 \cdot p_3 \cdot p_4 \cdot p_5 = (x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^7 + x^4 + x^2 + 1)$

$$B_1 = (x^3+1)\cdot(x^{20}+x^{19}+x^{18}+x^{15}+x^{13}+x^{12}+x^9+x^7+x^6+x^5+x^2+1) = x^{23}+x^{22}+x^{21}$$
$$+x^{20}+x^{19}+x^{16}+x^{13}+x^{10}+x^8+x^7+x^6+x^2+1$$
$$B_2 = (x^3+x+1)\cdot(x^{20}+x^{19}+x^{15}+x^{13}+x^{11}+x^9+x^8+x^7+x^6+x^5+x^3+1) =$$
$$= (x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{15}+x^{13}+x^9+x^8+x^6+x^5+x^4+x+1)$$
$$B_3 = (x^3+x)\cdot(x^{20}+x^{18}+x^{17}+x^{16}+x^{15}+x^{13}+x^{11}+x^{10}+x^7+x^4+x^2+1) = x^{23}+x^{20}+$$
$$+x^{17}+x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x$$

Исходя из условия появления однократной ошибки в остатке числа *A(z)*, получаем номера диапазонов.

Допустим, что ошибка произошла в 0-м разряде 1-го основания $p_1(x)= x^5+x^3+1$ и ее глубина $\Delta\alpha_j(x)=1$. Тогда имеем

$$l_1^1(x) = \left[\frac{B_1(x)}{P_{раб}(x)}\right] = \left[\frac{x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{16}+x^{13}+x^{10}+x^8+x^7+x^6+x^2+1}{x^{15}+x^{14}+x^{12}+x^8+1}\right] =$$
$$= x^8+x^6+x^5+x^3+1$$

Если ошибка произошла в 0-м разряде 2-го основания $p_1(x)= x^5+x^2+1$ и ее глубина $\Delta\alpha_j(x)=1$. Тогда имеем

$$l_2^1(x) = \left[\frac{x^0 B_2(x)}{P_{раб}(x)}\right] = \left[\frac{x^0(x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{15}+x^{13}+x^9+x^8+x^6+x^5+x^4+x+1)}{x^{15}+x^{14}+x^{12}+x^8+1}\right] =$$
$$= x^8+x^6+x^4+x^3+x^2+x+1$$

Если ошибка произошла в 1-м разряде 3-го основания $p_3(x)=x^5+x^4+x^3+x^2+1$и ее глубина $\Delta\alpha_j(x)=1$. Тогда имеем

$$l_3^1(x) = \left[\frac{x^1 B_3(x)}{P_{раб}(x)}\right] = \left[\frac{x^{24}+x^{21}+x^{18}+x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^8+x^2)}{x^{15}+x^{14}+x^{12}+x^8+1}\right] =$$
$$= x^9+x^8+x^7+x^6+x^4+x^3$$

Применение алгоритма вычисления позиционной характеристики – интервального номера в ПСКВ позволяет обнаруживать и локализовывать однократные ошибки и определять их интервалы при меньших схемных и временных затрат по сравлению с другими алгоритмами.

Литература:

1. Акушский И.Я., Пак И.Т. Вопросы помехоустойчивого кодирования в непозиционном коде//Вопросы кибернетики. 1977, Т.28. С.36-56.

2. Калмыков И.А., Гахов Р.П. Математическая модель пересчета коэффициентов обобщенной полиадической системы для спецпроцессора с деградируемой структурой/ Материалы IV Международная научно-техническая конференция «Проблемы информатики и моделирования», Харьков, 2004, С 68.

3. Калмыков И.А., Шилов А.А., Чипига А.А. Разработка метода пересчета ортогональных базисов в полиномиальной системе класса вычетов и его нейросетевая реализация/Материалы VI Международной научно-практической конференции «Информационная безопасность». - Таганрог, 2004. – с.152-154.

Х.А. Мирзахмедов

ТОЛЕРАНТНОГО СОЗНАНИЯ В ГЛОБАЛИЗИРОВАННОМ ОБЩЕСТВЕ

Наманганский государственный университет, г.Наманган, Узбекистан

Ключевые слова: глобализация, общества, образования, толерантность, толерантное сознание, воспитания, махалла, семья.

Влияние глобализации на различные страны разнообразно. Это связанно с экономическим, политическим, духовным положения стран мира. Для того, чтобы предотвратить отрицательное влияние интенсивных процессов, происходящих в мире, на каждую из стран; и для умножения положительных влияний необходимо глубоко вникнуть в суть самого явления. Подобная ситуация стимулирует общество на поиск новых отношений, окрашенных в цвета сотрудничества и диалога, акцентирует внимание на ценностях, формирующих толерантное сознание членов общества.

H.A. Mirzahmedov

TOLERANT CONSCIOUSNESS IN THE GLOBALIZED SOCIETY

Namangan State University, Namangan, Uzbekistan

Keywords: globalization, society, education, tolerance, tolerance, education, mahalla, family.

Impact of globalization on different countries varied. This is due to economic, political and spiritual situation of the countries of the world. In order to prevent the negative impact of intensive processes taking place in the world for each of the countries; and to multiply the positive effects need to deeply understand the essence of the phenomenon. This situation encourages society to find new relationships, painted in the colors of cooperation and dialogue, focuses on the values that form of tolerance in society.

На современном периоде развития любое государство претерпевает крупномасштабные изменения, как в области политики, экономики, права, так и в сфере духовной жизни общества, и в сфере образования. Можно с полной уверенностью сказать, что к XXI века не осталось ни одной страны, которая не была бы подвергнута влиянию со стороны других стран. Даже страны, всячески стремящиеся ограничить себя от международных организаций, не могут полностью избежать этого процесса [1, Б.64].

Глобализация – это процесс под влияние, которого попадает та страна, которая старается всячески избежать его. А такое непроизвольное влияние в большинстве случаев бывает отрицательным. Влияние глобализации на различные страны разнообразно. Это связанно с экономическим, политическим, духовным положения стран мира. Для того, чтобы предотвратить отрицательное влияние интенсивных процессов, происходящих в мире, на каждую из стран; и для умножения положительных влияний необходимо глубоко вникнуть в суть самого явления[4, С.54].

Глобализация – это ещё такой процесс, в котором нельзя участвовать, будучи незнакомым, с его стратегией и не выработав свою тактику и технику. Подобная ситуация стимулирует общество на поиск новых отношений, окрашенных в цвета сотрудничества и диалога, акцентирует внимание на ценностях, формирующих толерантное сознание членов общества, взаимопонимание, личная ответственность, свобода, абсолютная ценность жизни. Всё это свидетельствует о том, что общество осознаёт необходимость обеспечения толерантного мироустройства. Именно толерантность должна стать сегодня тем сильнейшим регулятором жизни людей, который направляет государственное устройство, социальные культуры и индивидуальные стратегии поведения и существования по пути гуманизации и социально-культурного равновесия.

Толерантность–это ценность и социальная норма гражданского общества, проявляющаяся в праве всех граждан быть различными; обеспечении устойчивой гармонии между различными конфессиями, политическими, этническими и другими социальными группами; уважении к разнообразию различных мировых культур, цивилизаций и народов; готовности к пониманию и сотрудничеству с людьми, различающимися по внешности, языку, убеждениям, обычаям и верованиям. Толерантный путь – это путь человека, хорошо знающего себя, комфортно

чувствующего себя в окружающей среде, понимающего других людей и готового всегда прийти на помощь, человека с доброжелательным отношением к иным культурам, взглядам, традициям. Толерантный человек видит мир во всём его многообразии [1, С.64].

Особую значимость формирование толерантности приобретает сегодня в Республика Узбекистана. Процесс формирования толерантности происходил полномасштабно и наиболее эффективно, правительство приняло формирование установок толерантного сознания и профилактика экстремизма и терроризма в гражданском обществе (1991 – 2014 гг.). Данный процесс даёт «зелёный свет» современному национальному образованию на целенаправленную разработку средств и обеспечение условий формирования толерантности у граждан своего государства.

Международный день толерантности ежегодно отмечается 16 ноября. Этот Международный день был торжественно провозглашён в «Декларации принципов терпимости» ЮНЕСКО. Декларация была утверждена в 1995 году на 28-ой Генеральной конференции ЮНЕСКО.

Цель воспитания толерантности – воспитание в подрастающем поколении потребности и готовности к конструктивному взаимодействию с людьми и группами людей независимо от их национальной, социальной, религиозной принадлежности, взглядов, мировоззрения, стилей мышления и поведения. Достижение данной цели возможно при решении конкретных задач, которые объединены в два взаимосвязанных блока:

1. Воспитание у молодого поколения миролюбия, принятия и понимания других людей, умения позитивно с ними взаимодействовать:
   - формирование уважения и признания к себе и к людям, к их культуре;
   - развитие способности к межнациональному и межрелигиозному взаимодействию;
   - формирование умения определять границы толерантности.
2. Создание толерантной среды в гражданском обществе и в сфере образования:
   - гуманизация и демократизация существующих взаимоотношений семья и махаллей*, системы обучения и воспитания;
   - включение в реформирование образования ведущих идей педагогики толерантности;
   - реформирование системы подготовки будущих педагогов к воспитанию толерантности у детей и подростков.

Проявлять толерантность – это значит признавать то, что люди различаются по внешнему виду, положениям, интересам, поведению и ценностям и обладают правом жить в мире, сохраняя при этом свою индивидуальность. Открытым остаётся вопрос о формировании толерантного сознания. Воспитание толерантности на основе предписаний не учитывает непредвиденных ситуаций, при которых человек испытывает рассеянность. «Желаемая толерантность теряется в решающие моменты». Сложность толерантности «не в переоценке человеческого познания, а в недооценке человеческих ощущений». Проблема толерантности берёт начало в коммуникационном дефиците и может быть решена с помощью межкультурных коммуникаций [3, С.152].

Формирование коммуникативной толерантности подразумевает групповую работу, поскольку невозможно овладеть толерантностью для себя. Она является качеством, которое проявляется в процессе общения. И.В.Гёте считал толерантность переходным состоянием на пути к признательным отношениям. С каждым годом на обучение приходит всё большее количество молодежи разных национальностей. Педагогу важно донести до учащихся мысль, что разные индивидуальные качества людей (цвет кожи, вероисповедание, национальность) лишь дополняют друг друга, составляя многообразный мир.

Определённое отношение к людям разных национальных культур у молодежи, растущих на территории со смешанным составом жителей, возникает не только в результате того, что они живут в одном махалле, на одной улице, вместе участвуют в подготовке и проведении общих для

* **Махалла** (узб.) - В исламском мире часть города размером с квартал, жители которого осуществляют местное самоуправление. Как правило, центром такого квартала — *махалла* — является мечеть, служащая своего рода культурным центром, в котором проходят пятничные собрания населения махалли и совершается торжественная пятничная молитва (намаз).

них праздников. В процессе обучения происходит активное общение между обучающимися. С первого дня они сообща выполняют разные виды деятельности, а в процессе выполнения совместной творческой деятельности возникают общие интересы, склонности, потребности, адекватное отношение к тем или иным явлениям, фактам, процессам, событиям. Очень важно отметить, что всё это развивает взаимопонимание, необходимость совместных усилий, взаимодействие и взаимовыручку.

Дружеские и товарищеские отношения молодёжи разных национальностей в процессе обучения в одной группе оказывают благотворное влияние на процесс формирования их личности. Довольно часто можно встретиться с фактом, когда на основе дружбы, возникшей между молодежь, развиваются добрые отношения между их семьями, а затем между махаллями. А такие отношения часто способствуют тому, что друзья перенимают друг у друга вкусы, интересы, увлечения. Стало быть, такая дружба имеет благотворные социальные последствия, она способствует развитию толерантных отношений между народами, проживающими на данной территории [2, С.33].

Работу по формированию толерантного сознания, выработке умений и навыков доброжелательного поведения в группе со смешанным национальным составом учащихся целесообразно начинать с первых дней поступления молодёжи в ВУЗу. В обычных условиях, когда молодёжь растут и развиваются в однородной этнической среде, на их эстетическое развитие огромное влияние оказывают различные формы их национальной культуры. Определённую роль играет бытовая культура, сказки данного народа, его песни и сказания, национальная музыка и танцы, различные виды декоративно-прикладного искусства. Национальный колорит сохраняется и в организации художественной самодеятельности, различных кружков. Однако, определённая часть молодёжи, проживающих в махаллах со смешанным национальным составом жителей, подвергается систематическому воздействию своей национальной художественной культуры, получая первоначальные сведения о ней в семье. Особенно сложным в этом отношении является положение молодёжи тех культур, которые в данном группе представлены единицами. Так как они лишены возможности приобщиться к национальной культуре народа, к которому принадлежат, то происходит процесс обогащения сведениями из культуры других народов, что в определённой степени компенсирует культурный дефицит, однако происходит ассимиляция культур. Таким образом, в условиях, когда совместно обучаются представители разных этнических, расовых и религиозных групп, образование должно быть построено с учётом этнического состава учащихся. Этническое содержание необходимо интегрировать во все преподаваемые предметы на протяжении всех лет обучения.

Определённая роль в системе формирования толерантного сознания принадлежит вне аудиторной работе. Она позволяет связать гражданское просвещение с художественным творчеством учащихся. При этом обучающиеся получают возможность проявлять свою индивидуальность. вне аудиторной время и коллективные творческие дела, направленные на воспитание терпимости по отношению к людям, позволят успешно адаптироваться не только в ВУЗе, но и за её пределами.

Литература:

1.Каримов И.А. Ўзбекистон: миллий истиқлол, иқтисод, сиёсат, мафкура. - 1-жилд. Т.: Ўзбекистон, 1996, б.64

2.Муртазаева Р.Ҳ. Ўзбекистонда миллатлараро муносабатлар ва бағрикенглик. – Т.: Университет, 2007, б.33

3.Мчедлов М.П. Толерантность.- М.: Республика, 2004, с.152.

4.Ярочкин В.И. Информационная безопасность. - М.: 2008, с.54.

О.А. Новикова, В.В. Кормильченко

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ

Северо-Кавказский филиал Московского технического университета связи и информатики,
г. Ростов-на-Дону, Россия

Ключевые слова: Информация, информационная безопасность, информационные системы, нормативно-правовые основы информационной безопасности, защита информации.

Современные условия развития России требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, соотнесения его со своей системой законов и правовых актов РФ.

O.A. Novikova, V.V. Kormilchenko

INFORMATION SECURITY OF RUSSIA

North-Caucasus branch of the Moscow technical university of communication and informatics,
Rostov-on-Don, Russia

Keywords: information, informational security, information systems, statutes and regulations fundamentals for information security, data security.

The current conditions of Russia’s development require and determine a need for a complex approach to form laws on data protection, as well as their correlation with the entire laws system and regulatory acts.

Современные условия развития России требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, соотнесения его со своей системой законов и правовых актов РФ.

Информационную систему, вычислительную систему и компьютерную систему с позиций защиты информации мы будем рассматривать как синонимы (предполагаем, что ИС является автоматизированной).

ИС иногда разделяют на две основные группы:

a) Системы информационного обеспечения (входят в состав других автоматизированных систем);
b) Системы, имеющие самостоятельное целевое назначение и область применения, например, информационно-поисковые системы.

В соответствии с Концепцией национальной безопасности РФ под информационной безопасностью понимается состояние защищенности национальных интересов страны (личности, общества и государства) в информационной сфере от внутренних и внешних угроз.

Рассматривая безопасность информации с позиции ее защиты, необходимо ответить на три вопроса: что защищать, от чего защищать и как защищать, Ответим на эти вопросы применительно к автоматизированным информационным системам.

С вопросом «Что защищать?» связано понятие объекта защиты. Под объектом защиты будем понимать комплекс физических, аппаратных, программных и документальных средств, предназначенных для сбора, передачи, обработки и хранения информации.

Выделяют принципы обеспечения безопасности информационных систем и сетей:

a) Информированность;
b) Ответственность;
c) Реагирование;
d) Этика;
e) Оценка риска;
f) Управление безопасностью.

Говоря о прикладном аспекте защиты объекта, выделяют такие направления:

1) Безопасность операционных систем, процессов, процедур и программ обработки информации;

2) Безопасность вычислительных сетей и каналов связи;
3) Безопасность баз данных и других объектов И С;
4) Безопасность инфраструктуры и т. д.

Необходимость защиты информационных систем обосновывается несколькими основными причинами.

1) Современные компьютеры за последние годы приобрели гигантскую вычислительную мощь, но, одновременно с этим, стали гораздо проще в эксплуатации. Это означает; что пользоваться ими стало намного легче, поэтому всё большее количество новых пользователей получают доступ к компьютерам. Это приводит к снижению средней квалификации пользователей. Эта тенденция существенно облегчает задачу нарушителям.
2) Повсеместное распространение сетевых технологий объединило отдельные машины в локальные сети. Безопасность сети определяется защищенностью всех входящих в нее компьютеров и сетевого оборудования. Злоумышленнику достаточно нарушить работу только одного компонента, чтобы скомпрометировать всю сеть.
3) Развитие Интернета вызвано всплеск интереса к проблеме информационной безопасности и поставило вопрос об обязательном наличии средств защиты у сетей и систем, подключенных к Интернету, независимо от характера обрабатываемой в них информации.
4) Прогресс в области аппаратных средств сочетается с еще более бурным развитием программного обеспечения. Как показывает практика, большинство распространённых современных програмных средств, защита которых не отвечает даже минимальным требованиям безопасности.

Система информационной безопасности представляет совокупность законодательных актов и нормативно-правовых документов (правовое обеспечение), органов государственной власти и управления, структур по безопасности в организациях и организационных мероприятий в области защиты информации (организационное обеспечение), научных разработок, математических методов и программно-технических средств (научно!- техническое обеспечение).

Следует отметить, объектом информационной безопасности может быть предприятие (организация), сведения о его состоянии, структуре, результатах деятельности, включая персонал, технологии, материальные, финансовые и информационные ресурсы.

Развитие гибких и мобильных технологий обработки информации привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов.

Необходимость создания глобального информационного пространства и обеспечение безопасности протекающих в нем процессов потребовала разработки международных стандартов.

Вследствие совокупного действия всех перечисленных факторов перед разработчиками современных информационных систем, стоят следующие задачи, требующие немедленного и эффективного решения:

1) Обеспечение безопасности новых типов информационных ресурсов.
   Системы защиты должны обеспечивать безопасность на уровне информационных ресурсов, а не отдельных документов, файлов или сообщений.
2) Развитие локальных сетей и Интернета диктует необходимость осуществления эффективной защиты при удаленном доступе к информации, а также взаимодействии пользователей через общедоступные сети.
3) Защита от средств нападения. Опыт эксплуатации существующих систем показал, что сегодня требуется защита от компьютерных вирусов, автоматизированных средств взлома, агрессивных агентов.

Современная государственная политика РФ в области защиты информации сформировалась в начале 90-х годов и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

При анализе состояния нормативно-методической базы управления информационной безопасностью необходимо выделить такие направления: модели безопасности, общие принципы управления информационной безопасностью, методы и механизмы безопасности информационных технологий, а также методы оценки безопасности.

Защита информации регулируется законами «Об информации, информатизации и защите информации», «О государственной тайне», «О коммерческой тайне», «О персональных данных».

Учитывает вопросы информационной безопасности Уголовный кодекс РФ (редакция 2002 г). В главе 28 «Преступления в сфере компьютерной информации», имеется три статьи:

1) статья 272 «Неправомерный доступ к компьютерной информации»,

2) статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ»,

3) статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Функции службы информационной безопасности многообразны и связаны с контролем и перекрытием каналов утечки закрытой информации, уменьшением материального и финансового ущерба организации.

Г.Н. Палютина

ДВУХЭТАПНАЯ АУТЕНТИФИКАЦИЯ КАК МЕРА ЗАЩИТЫ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Ростовский Государственный экономический университет РГЭУ (РИНХ), г. Ростов-на-Дону, Россия

Ключевые слова: меры защиты информации, информационная система, класс защищенности информационной системы, степень возможного ущерба, идентификация и аутентификация, двухэтапная аутентификация.

Рассмотрены меры защиты информации в информационных системах, методика определения классов защищенности информационных систем, основывающаяся на определении масштаба информационной системы и степени ущерба от нарушения конфиденциальности, целостности и доступности информации. Осуществлена попытка определения класса защищенности социальной сети для рассмотрения базового набора мер защиты информации. А также отражен опыт применения двухэтапной аутентификации Google с использованием приложения Google Authenticator как меры для повышения защиты аккаунта в социальной сети.

G.N. Palyutina

TWO STEP AUTHENTICATION AS A MEASURE OF INFORMATION PROTECTION OF INFORMATION SYSTEM'S USER

Rostov State University of Economics, RSUE, Rostov-on-Don, Russia

Keywords: measures of information protection, information system, class of information system's protection, degree of possible damage, identification and authentication, two step authentication.

The measures of information protection in information systems, the methods of determining the class of information system's protection, based on determining the scale of information system and the degree of possible damage caused by branches of information's confidentiality, integrity and availability are reviewed. The attempt of determining the class of information system's protection of the social network for studying the basic set of measures of information protection is put into practice. The experience of using the two step authentication Google with using the application Google Authenticator as measure of improving the security of your account of the social networks is described.

Согласно методическому документу ФСТЭК от 11 февраля 2014 г., защита информации в информационных системах направлена на обеспечение следующих составляющих: конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации); целостность (исключение неправомерного уничтожения или

модифицирования информации); доступность информации (исключение неправомерного блокирования информации) [1].

Нарушение вышеперечисленных составляющих может привести к материальному, моральному ущербу пользователя, а также подрыву его репутации.

В связи с этим, актуальным является обеспечение безопасности пользователя по всем трем составляющим.

Выбор мер защиты информации в информационной системе осуществляется исходя из класса защищенности информационной системы (базовый набор мер ЗИ), структурно-функциональных характеристик информационной системы (адаптированный базовый набор мер ЗИ), угроз безопасности информации (уточненный адаптированный базовый набор мер ЗИ), а также с учетом требований нормативно-правовых актов (дополненный уточненный адаптированный базовый набор мер ЗИ).

К основным мерам, реализуемым в информационных системах, относят следующие: идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации; регистрация событий безопасности; антивирусная защита; обнаружение (предотвращение) вторжений; контроль (анализ) защищенности информации; обеспечение целостности информационной системы и информации; обеспечение доступности информации; защита среды виртуализации; защита технических средств; защита информационной системы, ее средств и систем связи и передачи данных [1].

В настоящее время практически все пользователи сети Интернет обладают собственными учетными записями электронной почты, страницами в социальных сетях, личными кабинетами в Интернет-порталах и т.д. Необходимо обеспечивать должный уровень безопасности пользователя.

Рассмотрим такую информационную систему как социальная сеть Вконтакте. Попытаемся определить для нее класс защищенности информации, позволяющий определить базовый набор мер защиты информации.

Класс защищенности (К) = [уровень значимости информации (УЗ); масштаб системы].

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)]

В таблице 1 представлены описания трех существующих степеней возможного ущерба [1].

Таблица 1. Степени возможного ущерба от нарушения конфиденциальности, целостности или доступности информации

Высокая	Средняя	Низкая
Существенные негативные последствия в социальной, политической, международной, экономической, финансовой; ИС, обладатель информации не могут выполнять возложенные на них функции	Умеренные негативные последствия; ИС, обладатель информации не могут выполнять хотя бы одну из возложенных на них функций	Незначительные негативные последствия; ИС, обладатель информации могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России.

Масштаб информационной системы определяется назначением и распределенностью сегментов информационной системы. Существует три вида масштабов информационных систем [1]. Их описание представлено в таблице 2.

Таблица 2. Масштаб информационной системы

Федеральный	Региональный	Объектовый
На территории РФ и имеет сегменты в субъектах РФ, муниципальных образованиях и (или) организациях	На территории субъекта РФ и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях	На объектах одного федерального органа государственной власти, органа государственной власти субъекта РФ, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Для определения класса защищенности будем руководствоваться Приказом ФСТЭК от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [2].

Предположим, что масштаб выбранной информационной системы является федеральным, так как ее сегменты распространяются по всей территории РФ. А степень возможного ущерба от нарушения конфиденциальности, доступности и целостности определим следующим образом:

УЗ = [низкая, низкая, низкая] => уровень значимости информации – УЗ 3

К = [УЗ 3, федеральный]

Таким образом, из четырех установленных классов защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4), при условии, что самый низкий класс – четвертый, а самый высокий – первый) выбранную нами информационную систему можно отнести ко второму классу (К2).

Определение угроз безопасности необходимо для определения уточненного адаптированного базового набора мер защиты информации. Для определения угроз безопасности (УБИ) используется следующая запись [1]:

УБИ = [возможности нарушителя; уязвимости информационной системы; способ реализации угрозы; последствия от реализации угрозы].

Модель угроз безопасности информации представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разрабатываемые и утверждаемые ФСТЭК России.

Таким образом, определение класса защищенности информационной системы, угроз безопасности информации, а также структурно-функциональных характеристик конкретной информационной системы позволяет осуществить выбор мер защиты информации.

Обязательной мерой защиты информации для класса защищенности 2 является идентификация и аутентификация субъектов и объектов доступа. В качестве метода реализации идентификации и аутентификации в социальной сети Вконтакте используется парольная идентификация/аутентификация. К ее преимуществам относятся простота и привычность использования. А к недостаткам следующее: использование слабых и редкая смена паролей пользователями; злоумышленник может получить БД паролей, хранящихся в зашифрованном виде, и воспользоваться ею; пароли можно подсмотреть (с помощью оптических приборов), сообщить другу/подруге, записать на бумаге и т.п.

Таким образом, требуется обеспечение дополнительной защиты при идентификации и аутентификации пользователя.

ФСТЭК рекомендует пользователям использовать вместо аутентификации на основе статических паролей многофакторную аутентификацию.

Одним из возможных решений данной проблемы является использование двухэтапной аутентификации Google [3].

Подключив двухэтапную аутентификацию, пользователь при входе под своим аккаунтом помимо собственного пароля должен ввести дополнительный одноразовый код. Данный код является уникальным, его можно получить по SMS, с помощью голосового вызова или приложения, установленного на телефоне.

Таким приложением является приложение Google Authenticator, которое можно использовать на устройствах под операционными системами Android, iOS, Blackberry. К данному приложению можно «подвязать» несколько аккаунтов. Оно будет генерировать одноразовые коды для каждого из них, и каждые тридцать секунд коды будут обновляться.

Настройка двухэтапной аутентификации осуществляется в настройках аккаунта, здесь пользователь может выбрать, как получать одноразовый код. Настройка осуществляется в несколько шагов. Интерфейс приложения легок для восприятия пользователем. Так, достаточно простым способом можно повысить уровень безопасности пользователя данной социальной сети.

Таким образом, была изучена методика выбора мер защиты информации, осуществлена попытка ее реализации на примере социальной сети Вконтакте, а также повышение защиты собственного аккаунта с помощью двухэтапной аутентификации Google с использованием приложения Google Authenticator.

Литература:

1. Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г. [Эл. ресурс]. URL: http://fstec.ru/component/attachments/download/675

2. Приказ № 17 ФСТЭК от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Эл. ресурс]. URL: http://fstec.ru/component/attachments/download/566

3. Двухэтапная аутентификация Google. [Эл. ресурс]. URL: http://www.google.ru/intl/ru/landing/2step/#tab=why-you-need-it

В.В. Парышев

МЕТОДЫ РАЗРАБОТКИ ЗАЩИЩЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Ростовский государственный экономический университет, г. Ростов-на-Дону, Россия

Ключевые слова: защищенное программное обеспечение, методы разработки программного обеспечения.

При разработке любого приложения встает вопрос о его защищенности, а когда разрабатывается защищенное приложение этот вопрос является основополагающим. Приводится анализ существующих методов разработки защищенного программного обеспечения и их сравнение.

V.V. Paryshev

METHODS OF DEVELOPING PROTECTED SOFTWARE

Rostov State University of Economics, Rostov-on-Don, Russia

Keywords: secure software, software design methods.

In developing any application raises the question of its security, if developing protected application this question is fundamental. The analysis of existing methods of development protected software and compare them .

Процесс разработки программного обеспечения определяется структурой, согласно которой построена разработка программного обеспечения. Эта структура включает в себя несколько шагов, которые при разных трактовках могут называться по разному, но при этом присутствуют в той или иной форме в любой методологии: сбор и анализ требований, проектирование, разработка, отладка, документирование и внедрение. В случаях, когда

подразумевается разработка защищенного программного обеспечения, структура сохраняется, но на каждом шаге предпринимаются дополнительные меры безопасности. Процесс разработки такого программного обеспечения также называется защищенным процессом разработки приложения. Защищенная разработка - это набор мер, которые направлены на обеспечение нужного уровня безопасности информации, разрабатываемого программного продукта.

Существует множество методик разработки защищенного программного обеспечения, большая часть из них введена крупнейшими разработчиками программного обеспечения и различными государственными организациями.

Microsoft Security Development Lifecycle - структурированное описание процесса разработки защищенных программных продуктов, разработанное компанией microsoft. На этапе сбора требований, обязательным условием является дополнительное обучение основам информационной безопасности и создание контролируемых условий качества и конфиденциальности, а также оценку рисков безопасности. На этапе разработки используются только проверенные средства создание программного обеспечения и отказ от использования небезопасных функций рабочего окружения и постоянный статический анализ программного кода. На этапе отладки вводится необходимость в нечетком тестировании (фаззинге) и проверка возможных направлений для атак злоумышленников. На этапе внедрения проводится окончательная проверка безопасности и сертификация выпуска. [1]

Представляется, что данная методика является наиболее доступной и четко сформулированной для разработки крупного проекта защищенного программного обеспечения, но при этом, данная методика избыточна, если предъявляются только общие требования к защищенности продукта.

Build Security In - несистематизированный набор процессов и общих рекомендаций по разработке безопасного программного обеспечения. Представлен департаментом национальной безопасности США. На этапе проектирование вводится необходимость сбора общих рекомендаций по основам безопасности. При разработке рекомендуется использовать общие практики по безопасной разработки. При отладке производится тестирование по основным шаблонам атак и рекомендуется делать основной упор на тестирование по принципу "белого ящика". [2]

Методика Build Security In идеальна, в случае частичного совмещения на некоторых этапах с методикой Security Development Lifecycle. Она не имеет избыточности и проста для быстрого ввода в уже существующий процесс разработки программного обеспечения. Недостатком данной методики, является ее неполнота и нечеткая трактовка конечных материалов.

Cisco Security Development Lifecycle - формализованное описание процесса защищенной разработки программного обеспечения с упором на безопасность. Методика вводит особые требования на этапе сбора требования к проектированию моделей риска, которые в последствии используются на этапе разработке в качестве основы для проектирования будущего приложения. Также на этапе разработке при выборе готовых решений приоритет отдается в первую очередь самым защищенным решениям. На этапе отладки рекомендуется нечеткое тестирование (фаззинг) и проверка выполнений требований по безопасности. [3]

Данная методика подходит в основном компаниям, которые часто используют сторонние решения. Поэтому важно уделить внимание безопасности именно внедренным сторонним решениям, именно на это делается основной упор данной методики. Методика сложна для внедрения, с учетом большого количества требований и большим количеством мелких деталей.

В заключение, хочется отметить, что выбор методики зависит сугубо от желаемого результата. Методика Microsoft Security Development Lifecycle избыточна, но являясь классической в чистом виде и не рекомендуется к использованию. При совмещении Build Security In с другими методиками, является идеальным компромиссным решением, между затратами на внедрение и уровнем безопасности. Методика Cisco Security Development Lifecycle подходит компаниям, которые часто внедряют готовые решения.

Литература:

1. Michael Howard and Steve Lipner, The Security Development Lifecycle, 2006
2. Gary McGraw, Software Security: Building Security In, 2006
3. Catherine Paquet, Network Security Concepts and Policies, 2013

А.П. Плёнкин, К.Е. Румянцев

ОДНОФОТОННЫЙ РЕЖИМ СИНХРОНИЗАЦИИ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ[1]

Южный федеральный университет
Институт компьютерных технологий и информационной безопасности
Кафедра информационной безопасности телекоммуникационных систем

Ключевые слова: распределение ключей, синхронизация, квантовая криптография.

Приведена структура системы квантового распределения ключей (СКРК) с фазовым кодированием состояний фотонов. Описан процесс вхождения в синхронизм СКРК. Представлена энергетическая модель этапов определения длины волоконно-оптической линии связи (ВОЛС) в процессе обеспечения синхронизации на базе коммерческой СКРК id3100 Clavis2 фирмы Quantique (Швейцария). Даны рекомендации по повышению защищенности подсистемы синхронизации СКРК путем применения однофотонного режима регистрации.

A.P. Pljonkin, K.E. Rumyantsev

SINGLE-PHOTON SYNCHRONIZATION MODE OF QUANTUM KEYS DISTRIBUTION SYSTEM

Southern Federal University
Institute of Computer technologies and information safety

Keywords: keys distribution, synchronization, quantum cryptography.

The structure of quantum key distribution systems (QKDS) phase-encoded states of photons. The process of synchronization QKDS are describes. The energy model of the steps of determining the length of the fiber-optic communication line in the process of synchronization based on commercial QKDS id3100 Clavis2 idQuantique (Switzerland) are shows. Recommendations to improve the security synchronization subsystem of QKDS by applying the single-photon mode recording.

Защищенность существующих систем криптографии в телекоммуникационных сетях ограничивается вычислительными возможностями злоумышленника.

В отличие от подавляющего большинства классических криптосистем, защищённость которых основывается на математических положениях и алгоритмах, защищённость квантовых криптографических систем базируется на фундаментальных законах квантовой механики. Надлежащая реализации таких систем делает принципиально невозможным перехват передаваемых данных [1]. Квантовая криптография реализуется в системах квантового распределения ключей. На сегодняшний день успешно реализованы и применяются несколько коммерческих квантовых криптографических систем [2, 3].

Типовая структура СКРК с фазовым кодированием состояний фотонов включает в себя основные компоненты: источник излучения, оптический интерферометр «Маха-Цендера», фазовые модуляторы, ВОЛС, линию задержки оптического излучения, поляризационное зеркало, детекторы фотоэлектронов (оптические лавинные фотодетекторы - ОЛФД), синхронизирующие генераторы.

Эффективная работа СКРК возможна только при условии обеспечения синхронизации. Под синхронизацией в СКРК понимается определяемый с высокой точностью момент регистрации фотодетекторами фотонного импульса. Для обеспечения момента регистрации, определяется общая длина оптического пути распространения фотонного импульса от источника излучения до поляризационного зеркала и в обратном направлении до ОЛФД. Отметим, что определяемая длина оптического пути распространения включает волоконно-оптическую линию связи и длины всех оптических компонентов внутри СКРК.

[1] Работа выполнена в рамках государственного задания Министерства образования и науки РФ высшим учебным заведениям в части проведения научно-исследовательских работ. Тема № 213.01-11/2014-9.

Процессы генерации и распределения квантовых ключей в таких системах проходят в однофотонном режиме, причем средним числом фотоэлектронов на импульс считается величина (n_w), равная порядка 0,1-0,3. Однако процесс синхронизации реализуется в многофотонном режиме, что потенциально позволяет злоумышленнику использовать часть энергии оптического излучения для синхронизации своей аппаратуры.

В общем виде процесс синхронизации двухпроходных автокомпенсационных СКРК с фазовым кодированием заключается в следующем: оптический импульс, сгенерированный модулем отправителя, разделяется оптическим делителем на два импульса (смотри рисунок 1) которые проходят по разным оптоволоконным «плечам» интерферометра «Маха-Цендера» и следуют на модуль получателя, где отражаются при помощи поляризационного зеркала, ортогонально изменяя свою поляризацию. При обратном прохождении оптического пути фазовая задержка сохраняется, импульсы интерферируют в блоке отправителя и регистрируются ОЛФД детекторами. Процесс синхронизации в СКРК состоит и нескольких последовательных этапов, различающихся параметрами оптических импульсов и аппаратуры детектирования [4].

Рисунок 1 демонстрирует осциллограмму импульсов после разделения оптическим делителем в блоке отправителя, «жестко» связанных между собой фазовой задержкой.

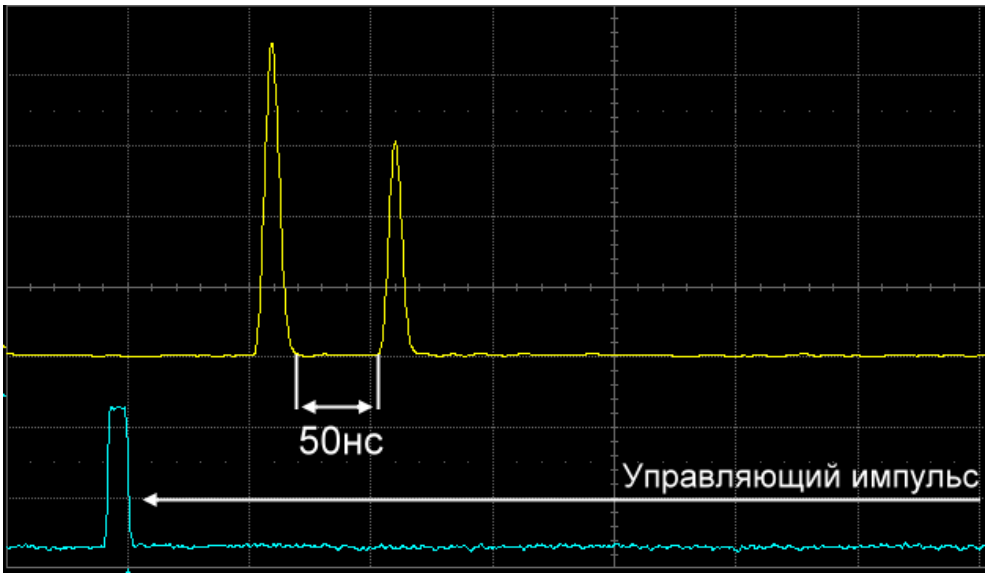


Рисунок 1. Осциллограмма импульсов в режиме синхронизации СКРК.

Результатом процесса вхождения в синхронизм является высокоточное определение временного интервала (временного окна). Длительность определяемого временного интервала для каждого этапа синхронизации имеет свое значение, так, например, при первом этапе длительность временного окна соответствует 1 нс.

В таблице 1 представлены энергетические характеристики этапов вхождения в синхронизм СКРК id3100 Clavis2 фирмы Quantique (Швейцария). Эксперимент проводился путем подключения в различные точки оптического пути прохождения импульса измерительного оборудования в процессе синхронизации.

Таблица 1. Энергетические характеристики оптического импульса последовательных этапов синхронизации СКРК.

Параметр	*Этап синхронизации*		
	Первый	*Второй*	*Третий*
Точка подключения: на выходе источника излучения			
Уровень по мощности	-46 дБм	-53 дБм	-18 дБм
Точка подключения: в разрыве ВОЛС			
Уровень по мощности	-49 дБм	-57 дБм	-22 дБм
Точка подключения: перед аттенюатором (модуль получателя)			
Уровень по мощности	-62 дБм	-69 дБм	-35 дБм
Точка подключения: после длинной линии задержки (модуль получателя)			
Уровень по мощности	-73 дБм	-81 дБм	-46 дБм
Точка подключения: на входе ОЛФД (модуль отправителя)			
Уровень по мощности	-82 дБм	-91 дБм	-54 дБм

Опираясь на экспериментальные данные из таблицы 1, параметры оптических импульсов, учитывая скорость распространения фотонного импульса в волокне и коэффициент преломления, получим усредненное количество фотоэлектронов в оптическом импульсе в режиме синхронизации СКРК

$$n_w = 10^3.$$

На основе полученных данных можно заключить, что при синхронизации в СКРК используется многофотонный режим, что потенциально может служить возможностью для злоумышленника использовать часть отведенной оптической мощности для синхронизации своей аппаратуры.

В [5] приведены аналитические выражения для расчёта вероятностных характеристик СКРК в режиме вхождения в синхронизм при использовании фотонных импульсов ($n_w = 0{,}1 - 0{,}3$), которые в совокупности с экспериментальными данными позволяют апробировать использование однофотонного режима при синхронизации в системах квантового распределения ключей для повышения защищённости от несанкционированного синхронизма и дальнейшего съема информации.

Литература:

1. Bennet C.H. Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. – Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, P. 175–179.

2. Румянцев К.Е. Системы квантового распределения ключа: Монография. − Таганрог: Издательство ТТИ ЮФУ, 2011. − 264 с.

3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, № 1. – P. 145−195.

4. Румянцев К.Е., Плёнкин А.П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. – 2014. – № 10. – С. 11–16.

5. Румянцев К.Е., Плёнкин А.П. Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81–96.

Н.А. Полванова, А.К. Сагдеев

КОНЦЕПЦИИ ДИНАМИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ВЕДЕНИЯ ТЕХНОСФЕРНОЙ ВОЙНЫ

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия

Ключевые слова: информационно-телекоммуникационная сеть военного назначения, техносферная война, динамическая защита, техническая компьютерная разведка.

Необходимость развития основных взглядов на обеспечение динамической защиты ИТКС ВН обусловлена концептуальными изменениями, происходящими в рамках иерархии оперативного искусства и тактики. Поэтому, в предлагаемой статье, для разработки Концепции динамической защиты, предложены принципы, которым должна удовлетворять Концепция… Целью реализации данных принципов является обеспечение устойчивого функционирования ИТКС ВН в условиях ведения технической компьютерной разведки.

N.A. Polvanova, A.K. Sagdeev

THE CONCEPT OF DYNAMIC SECURITY OF INFORMATION AND TELECOMMUNICATION NETWORK FOR MILITARY PURPOSES IN TERMS OF DOING TECHNOSPHERE WAR

Saint-Petersburg state University of telecommunications
them. Professor M. A. Bonch-Bruevich, St. Petersburg, Russia

Keywords: information and telecommunications network for military purposes, technosphere war, dynamic protection, technical computer intelligence.

The need for the development of basic views regarding the dynamic protection of information-telecommunication network for military purposes due to conceptual changes within the hierarchy of operational art and tactics. Therefore, in the proposed article, to develop the Concept of dynamic protection, the proposed principles, which must satisfy the Concept... the Purpose of the implementation of these principles is to ensure sustainable functioning of information-telecommunication network for military purposes in the terms of reference technical computer intelligence.

Необходимость развития основных взглядов на обеспечение динамической защиты ИТКС ВН, в первую очередь, обусловлена концептуальными изменениями, происходящими в рамках системы, находящейся на более высоком уровне иерархии оперативного искусства и тактики. Некоторые из этих изменений отражают и действующие руководящие документы по организации защиты ИТКС ВН. В то же время этот процесс далеко не закончен и находится в стадии своего интенсивного развития, и об этом свидетельствует как временный характер руководящих документов, так и непрекращающиеся исследования, проводимые в интересах войск связи ВС РФ [1-3].

Правовой базой для разработки настоящей концепции служат требования действующих в России законодательных и нормативных документов.

Для разработки Концепции динамической защиты ИТКС ВН в условиях ведения техносферной войны положены следующие принципы:

- адаптивное резервирование устройств управления сетевых элементов ИТКС ВН под сложившиеся условия обстановки;
- динамическое изменение параметров устройств управления сетевых элементов ИТКС ВН учитывающее вредоносное воздействие;
- непересекаемость множеств основных и резервных устройств управления сетевых элементов ИТКС ВН;
- универсальность используемой платформы управления сетевых элементов ИТКС ВН (специального программного обеспечения).

Современные и перспективные элементы, составляющие ИТКС ВН, являются комплексами аппаратно-программных средств связи (КАПСС) (цифровые телекоммуникационные платформы, маршрутизаторы, мультиплексоры, конверторы протоколов, многофункциональные цифровые оконечные устройства). Вследствие этого реализация основных функций будет определяться специальным программным обеспечением (СПО), которое является совокупность программ, необходимых для функционирования технического комплекса по реализации задач связи и управления. Ориентация разработчика на возможность двойного применения (коммерческих предложений) следствием является недостаточный уровень защищенности из-за стремления максимально уменьшить стоимость разработки и повысить универсальность создаваемого программного продукта [5].

Прогнозируемость воздействий и формирование возможных стратегий управления для своевременного восстановления ИТКС;

Соответствие проводимых мероприятий динамической защиты ИТКС ВН условиям организации управления войсками;

Конечности и стационарности ресурса защиты (создается и используется постоянно при этом он сосредоточен на сетевых элементах и возможно избыточен);

Ограниченности ресурса разведки и воздействий противника (ресурс не превышает возможности ИТКС ВН, а по отношении к ЕСЭ РФ многократно меньше);

Своевременность проведение мероприятий проводимых защитных действий по отношению к интервалу времени между вскрытием сетевого элемента ИТКС ВН и реализацией определенного воздействия (при этом разрабатываемые механизмы динамической защиты должна быть реализованы как система реального времени).

Таким образом, реализация приведенных принципов создания и функционирования динамической защиты ИТКС ВН позволит обеспечить требуемый уровень защиты ИТКС ВН при выявленных закономерностях изменения квазистационарного состояния с учетом заданного количества и качества услуг и сервисов информационного обслуживания (обмена) органов военного и государственного управления [3-5].

В настоящее время для обеспечения защиты информационно-телекоммуникационных сетей связи военного назначения определяют несколько возможных состояний узла связи, которые соответствовали определенной угрозе и переход в определенное состояние (одно в интервале времени) осуществлялся по управляющим воздействиям системы управления с центрального узла. При этом установившиеся состояние «защищенности» ИТКС ВН в большинстве случаев не соответствовало уже изменившимся воздействиями атакующей системы (режимов разведки). Кроме того при формировании управляющего воздействия не учитывается изменившиеся условия обстановки в реальном времени и сформирован только один вариант, что не обеспечивает достижения оперативности защиты ИТКС ВН.

Кроме того, особенностями современных ИТКС ВН в настоящее время влияющие на состояние защиты от программных воздействий является то, что транспортной основой преимущественно являются арендованные пропускные возможности (передаваемый трафик) в ЕСЭ РФ в условиях ведения технической компьютерной разведки (ТКР) (учитывается особенности управления разворачиваемых сетей NGN связанные с использованием Web-технологии т.е. на основе стека протоколов TCP/IP) и современной тенденции образования Общемирового единого телекоммуникационного пространства (ОМЕТП). В настоящее время основным способом ведения программного подавления является компьютерная атака, под которой понимают целенаправленное воздействие на компьютерные системы и сети с целью организации доступа к информационным ресурсам или их блокирования для легальных пользователей, модификации, уничтожения. Организация программного подавления осуществляется на основе данных добытых ТКР.

При этом сетевая атака является заранее спланированным целенаправленным воздействием на компьютерные или информационно-телекоммуникационные системы и сети программно-аппаратными средствами через установление соединения на сетевом уровне или попытки установления соединения на канальном или сетевом уровнях Эталонной модели взаимодействия открытых систем или пятиуровневой модели Интернет с объектом данного воздействия, осуществляемые, в том числе с целью создания условий для организации доступа, перехвата, сбора и анализа данных [1, 2, 5].

Сложившаяся ситуация позволяет рассматривать возможность ведения техносферной войны [4, 5] определяемой как систему согласованных по цели, месту и времени информационных действий, направленных на захват управления (частичный, полный) выбранных систем автоматизированного (автоматического) управления, либо перевод их в деструктивный режим функционирования.

Принцип воздействия будет заключаться в поиске доступа к управляемым параметрам и их изменение, которое может привести к критической ситуации (подавление (блокирование) информационного обмена в ИТКС ВН) (рис. 1). Результат такой ситуации будет характеризоваться временем неработоспособностью сети $T_{\text{блок}}$, которое зависит от времени восстановлении системы связи $T_{\text{восс}}$ (если это возможно) и соответственно будет приводить к потерям вызовов (понижение качества обслуживания *QoS* пользователей).

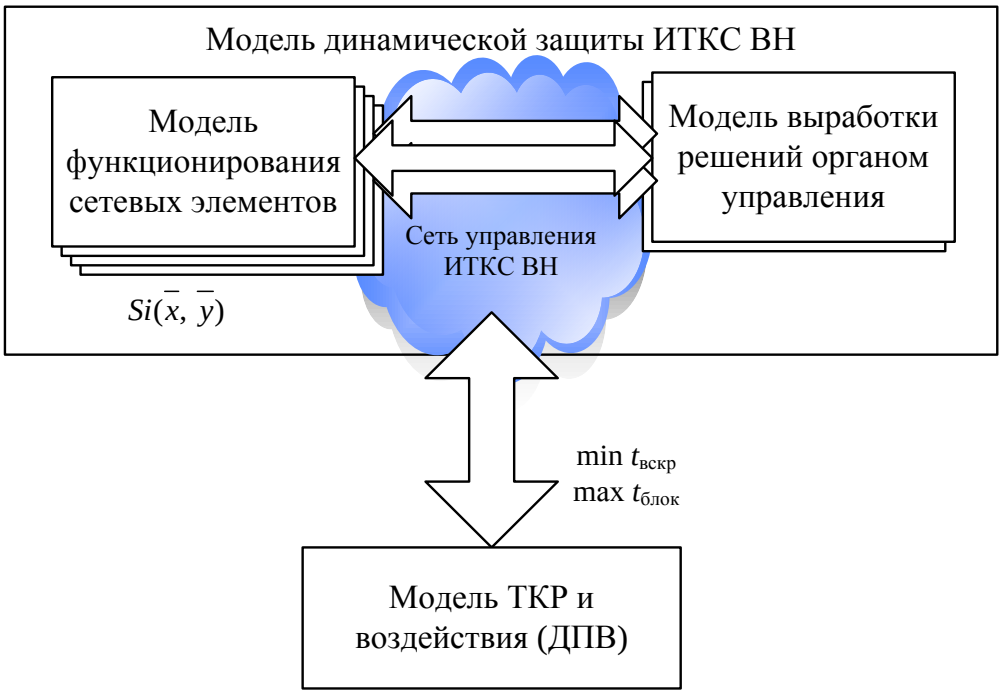


Рисунок 1. Обобщенное графическое представление конфликтной ситуации противоборствующих сторон

Соответственно, получить защищенную ИТКС ВН в стационарных (относительно времени) условиях не возможно т.к. в быстро меняющихся условиях (используемые технологии построения ИТКС ВН, возможности средств разведки) достигнутый уровень (состояние) защиты не будет соответствовать требуемому, и защита будет постоянно отставать (состояние системы защиты не соответствует изменившимся условиям). Учитывая выше сказанное целесообразнее построение динамической защиты ИТКС ВН, основным принципом которой является изменения состояния (параметров) узлов ИТКС ВН с учетом воздействий (проведения разведки) по динамически изменяемой стратегии управления в минимальном временном интервале.

Таким образом, основными принципами динамической защиты ИТКС ВН будет являться: адаптивное резервирование устройств управления под сложившиеся условия обстановки; динамическое изменение параметров устройств управления учитывающее вредоносное воздействие; непересекаемость множеств основных и резервных устройств управления; универсальность используемой платформы управления (специального программного обеспечения); прогнозируемость воздействий и формирование возможных стратегий управления для своевременного восстановления ИТКС ВН.

Литература:
1. Киреев В.С., Савицкий О.К., Стародубцев Ю.И., Тараскин М.М. Контроль безопасности связи и информации. – СПб.: ВУС, 2005. – 292 с.
2. Киреев В.С. и др. «Возможности АК США по ведению информационных операций». Учеб. пособие. СПб.: ВУС, 2000. 93 с.
3. Киреев В.С., Погорелов А.А. Информационное противоборство в войнах и вооруженных конфликтах. – СПб.: ВАС, 2005. – 120 с.
4. Основы оперативного искусства. Под ред. Мотылева. СПб.: ВУС, 1999. 438с.
5. Стародубцев Ю.И., Коцыняк М.А., Фролов В.Ю. и др. Основы защиты систем связи и автоматизации от технических средств разведки. Учебное пособие. – СПб.: ВАС, 2010. – 416 с.

А.С. Саламан, В.Н. Репинский

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА СООБЩЕНИЯ ГАММА-ПОСЛЕДОВАТЕЛЬНОСТЬЮ, СИНТЕЗИРУЕМОЙ СЛУЧАЙНЫМ ОБРАЗОМ ПО ПРИНЦИПУ «МАГИЧЕСКОГО КВАДРАТА» ЧЕТВЕРТОГО ПОРЯДКА

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: гамма-последовательность, магический квадрат, словарь, шифр, синтез,.

При криптографической защите сообщения всегда стоит проблема охраны ключа к шифру. Очень важно, чтобы ни на стороне передачи, ни на стороне приема операторы не знали ключа и не были потенциальными источниками утечки информации. В настоящей работе эта проблема решается использованием различных шифрующих гамма-последовательностей, синтезируемых случайным образом из расстановок магического квадрата четвертого порядка.

A.S. Salaman, V.N. Repinsky

CRYPTOGRAPHY POSTS GAMMA SEQUENCE SYNTHESIZED RANDOMLY ON A "MAGIC SQUARE" OF THE FOURTH ORDER

Moscow Technical University of Communications and Informatics, Moscow, Russia

Key words: gamma-sequence, magic square, Dictionary, code, synthesis.

When cryptographic protection message is always the problem of protecting the key to the cipher. It is important that neither the transmission side nor the reception side does not know the key operators were not potential leak sources. In this paper, this problem is solved using different ciphering gamma sequences synthesized at random from the constellations of the magic square of fourth order.

При криптографической защите сообщения всегда стоит проблема охраны ключа к шифру. Очень важно, чтобы ни на стороне передачи, ни на стороне приема операторы не знали ключа и не были потенциальными источниками утечки информации. В настоящей работе эта проблема решается использованием различных шифрующих гамма-последовательностей, синтезируемых случайным образом из расстановок магического квадрата четвертого порядка.

Известно, что числовой квадрат, размером 4x4 может быть превращен в магический 880 различными способами. Для шифровки сообщения используется гамма–последовательность из 16 чисел, выписанных по строчкам из магического квадрата (порядок выписывания чисел в принципе может быть любым, в том числе и «по ломаной»). Шифрование при передаче осуществляется путем случайного выбора одного из вариантов построения магического квадрата, который синтезируется с помощью Функции ENCRIPT. Шифрование осуществляется с применением международного телеграфного кода, использующего пятиразрядные последовательности символов. Зашифрованное сообщение поступает в канал связи, где, в случае использования радиосвязи, подвергается помехоустойчивому кодированию.

При приеме сигнала происходит декодирование, а затем сообщение дешифруется. Процедура дешифрования такова:

1. Поскольку гамма-последовательность в пункте приема сообщения неизвестна, происходит синтез магических квадратов последовательно одного за другим (в наименее благоприятном случае 880 раз).
2. Затем каждая полученная из магического квадрата гамма-последовательность накладывается на сообщение, порождая некоторый расшифрованный текст.
3. Для проверки правильности выбранного варианта магического квадрата часть дешифрованного сообщения проверяется на корректность путем сравнения его слов с данными словаря. Если фиксируется совпадение, то вариант считается правильным и происходит дешифровка сообщения до конца.

В качестве пояснения к работе программы приведем пример синтеза магического квадрата 3 порядка. Известно, что решение задачи синтеза магического квадрата 3x3 имеет единственное решение, однако принцип построения алгоритма синтеза будет тем же и для квадратов более высоких порядков.

```
Public Class MagicanSquare
   Public Massive(3,3) As Integer
    Shared Sub Syntesize (ByVal Mass(,) As Integer)
         Randomize()
         Dim a As Integer = CInt(Math.Floor((10-1+1) * Rnd()))+1
         Dim b As Integer = CInt(Math.Floor((10-1+1) * Rnd()))+1
         Dim c As Integer = CInt(Math.Floor((10-1+1) * Rnd()))+1
Mass(0,0) = a : Mass(0,1) = a + 3*b +c :Mass(0,2) = a +3*c : Mass(0,3)
= a + 3*b + 2*c
Mass(1,0) = a + b +3*c : Mass(1,1) = a + 2*b + 2*c : Mass (1,2) = a + b
: Mass(1,3) = a + 2*b + c
Mass(2,0) = a + 3*b : Mass(2,1) = a + c : Mass (2,2) = a + 3*b +3*c :
Mass(2,3) = a + 2*c
Mass(3,0) = a + 2*b +3*c : Mass(3,1) = a + b + 2*c : Mass (3,2) = a + 2*b
: Mass(3,3) = a + b + c
End Sub
Sub MassiveToString(ByRef str As String)
    Str = “”
    For I = 1 To 3
        For j = 0 To 3
            str = str + Massive(I,j).ToString
    Next
    Processing.ConvertToFiveChars(str)
    End Sub
End Class
```

Программа криптографической защиты сообщения, описанная в данной работе при использовании стандартного словаря (который, в принципе, может быть любым, но достаточно обширным) имеет время дешифрования несколько секунд, независимо от длины сообщения, поскольку основные затраты времени приходятся на перебор 880 гамм (в среднем около 400) и на сверку со словарем. Нетрудно усовершенствовать алгоритм, используя на каждые 16 знаков сообщения новую гамма-последовательность из 880 возможных. При этом защищенность существенно возрастает, однако и увеличивается время работы системы – в пределе до 30 минут. Максимальная длина практически нерасщифруемого сообщения в этом случае составит 14 000 знаков.

Изготовив специализированный чип обработки, можно получить систему криптографической защиты полностью отделенную от операторов и максимально снизить влияние «человеческого фактора» технического персонала на сохранение конфиденциальности.

Литература:

1. Ю. В. Чебраков Магические квадраты. Теория чисел, алгебра, комбинаторный анализ. — СПб.: СПб гос. техн. ун-т, 1995.
2. Ю. В. Чебраков Теория магических матриц. — СПб., 2008.

В.Н. Смоляков, В.В. Булатов

РАЗРАБОТКА СИСТЕМЫ КРИПТОЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОАО «НОВОШАХТИНСКИЙ ЗАВОД НЕФТЕПРОДУКТОВ

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: автоматизированное рабочее место, асинхронные поточные шифры, генератор псевдослучайных чисел, система криптографической защиты информации, синхронные поточные шифры, электронная цифровая подпись, несанкционированный доступ, локальная вычислительная сеть.

Обеспечение информационной безопасности особенно важно для успешной работы систем телекоммуникации, банков, систем управления воздушным и наземным транспортом, предприятий газоснабжения и нефтепереработки, а также систем обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих объектов необходимо обеспечить безопасность и целостность их информационных систем. Криптографическая защита информации является надежным и недорогим средством. Любой объем информации от нескольких байт до гигабайт, будучи зашифрованным с помощью более или менее стойкой криптосистемы, недоступен для прочтения без знания ключа. Против самых новейших технологий и миллионных расходов здесь стоит математика и этот барьер до сих пор невозможно преодолеть.

V.N. Smolaykov, V.V. Bulatov

DEVELOPMENT OF INFORMATION SYSTEM ENCRYPTION OF «NOVOSHAHTINSK PLANT OIL»

Moscow State Technical University, North Caucasian Branch, Rostov-on-Don, Russia

Keywords: workstation, asynchronous stream ciphers, random number generator, the system of cryptographic protection of information, synchronous stream ciphers, digital signature, unauthorized access, local area network.

Providing information security is particularly important for the successful operation of telecommunication systems, banks, control systems for air and ground transportation, gas and oil companies, as well as data processing and storage of sensitive and confidential information. For the normal and safe operation of these facilities is necessary to ensure the security and integrity of their information systems. Cryptographic protection of information is reliable and affordable media-stvom. Any amount of information from a few bytes to gigabytes, being encrypted nym using more or less resistant cryptosystem is not available to be read without knowing the key. Against the very latest technologies and the vast expenditure is worth mathematics and the barrier is still impossible to overcome.

Вопросы защиты информации (ЗИ) актуальны с тех пор, как только люди научились писать и даже раньше. Всегда существовала информация, которую должны знать не все. Люди, обладающие такой информацией, прибегали к разным способам ее защиты. Из известных примеров это такие способы как тайнопись (письмо симпатическими чернилами), шифрование

(«тарабарская грамота», шифр Цезаря, более совершенные шифры замены, подстановки). В настоящее время с увеличением количества обрабатываемой информации увеличился риск ее хищения, кражи и уничтожения.

Обеспечение информационной безопасности (ИБ) особенно важно для успешной работы систем телекоммуникации, банков, систем управления воздушным и наземным транспортом, предприятий газоснабжения и нефтепереработки, а также систем обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих объектов необходимо обеспечить безопасность и целостность их информационных систем (ИС).

Компьютер уже давно стал неотъемлемой частью жизни людей. Практически в любой сфере деятельности человека используются персональные компьютеры (ПК): образовательные программы, медицинское обслуживание, промышленные процессы. На сегодня компьютеризация достигла такого уровня, что без нее не обойтись. Отдельная эра в истории развития ПК началась с появлением локальных вычислительных сетей (ЛВС), которые позволяют объединять ПК между собой. Именно ЛВС подняла функциональность ПК на невиданную до сих пор высоту. Даже один ПК способен выполнять огромное количество операций и выдавать требуемый результат, не говоря уже о том, что можно сделать с помощью многих ПК, объединенных в сеть. Преимущества использования ЛВС очевидны: общее использование ресурсов, баз данных (БД), общение, интернет и многое другое.

Сегодня, в условиях рыночной экономики, информация и информационное обеспечение предприятия является стратегически важным ресурсом. Успех деятельности любой коммерческой организации напрямую зависит от своевременного обмена важной информацией между ее подразделениями. В свою очередь накладные расходы на передачу информации должны быть минимальными.

Атака на информацию – это умышленное нарушение правил работы с информацией. Такие атаки могут принести предприятию огромные убытки. В последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах заполнили средства массовой информации. При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец накладывает набор правил по работе с ним. Умышленное их нарушение классифицируется как атака на информацию. С массовым внедрением ПК объем информации, хранимой в электронном виде, вырос в тысячи раз. И теперь скопировать и унести флэшку с файлом, содержащим, например, план закупки оборудования или чертежи перспективных разработок продукции предприятия, намного проще, чем копировать или переписывать кипу бумаг. А с появлением ЛВС даже отсутствие физического доступа к ПК перестало быть гарантией сохранности информации.

Проблемы ЗИ в ИС постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. ИС могут быть любой архитектуры и любого функционального назначения, включая системы управления производством. Главная отличительная особенность современных ИС - для обработки информации в них используются средства вычислительной техники, а под ЗИ понимается использование специальных методов, мероприятий и программных средств для предотвращения утери и хищения информации, находящейся в ИС.

Проблема ЗИ путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человечество с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более или менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Постоянно расширяется использование ЛВС и сети Интернет для передачи больших объемов информации государственного, военного, коммерческого и частного характера, не допускающего доступа к ней посторонних лиц.

Одновременно появляются все более мощные ПК, технологии сетевых и нейрон-ных вычислений, что делает возможным дискредитацию криптографических систем, еще недавно считавшихся практически не раскрываемыми.

Целью данного исследования является защита ИС ОАО «Новошахтинский завод нефтепродуктов» с помощью криптографических методов. Информационную систему НЗНП будем рассматривать на примере одной из важнейших частей ИС – бухгалтерской подсистемы. Особое внимание обратим на ту часть этой подсистемы, которая обеспечивает финансовую деятельность автотранспортного цеха завода. Действительно, затраты на транспортировку производимых нефтепродуктов автотранспортом составляет значительную часть себестоимости. Поэтому грамотно организованная бухгалтерская поддержка и логистика деятельности автотранспортного цеха и входящей в него службы эксплуатации автотранспорта позволит существенно снизить себестоимость, а значит и повысить чистую прибыль предприятия. Разумеется, эта часть ИС ОАО НЗНП требует особой защиты.

Для достижения цели защиты ИС необходимо решить следующие задачи:

- провести анализ деятельности предприятия;
- разработать криптографическую программу;
- рассчитать экономическую эффективность проекта.

В проекте исследуется организационная структура предприятия и его документооборот, рассматриваются технико-экономические показатели, разрабатывается функциональная модель, описываются используемые на предприятии информационные технологии и обосновывается необходимость защиты информации.

Была обоснована актуальность и рассчитана экономическая эффективность внедрения криптографической защиты информации, заключающаяся в предотвращении возможных убытков от хищения или подмены информации в ОАО «Новошахтинский завод нефтепродуктов».

Криптографическая защита информации является надежным и недорогим средством. Любой объем информации от нескольких байт до гигабайт, будучи зашифрованным с помощью более или менее стойкой криптосистемы, недоступен для прочтения без знания ключа. И уже совершенно не важно, хранится он на жестком диске, на дискете или компакт-диске и неважно, под управлением какой ОС. Против самых новейших технологий и миллионных расходов здесь стоит математика и этот барьер до сих пор невозможно преодолеть.

В проекте была использована криптографическая программа R Crypto. В качестве основного средства для разработки программы криптозащиты использовалась среда визуального программирования C++ BUILDER 6. Программа R Crypto позволяет шифровать все типы файлов. «Сердцем» криптографической программы является криптоалгоритм.

Разработанная криптографическая программа является завершенной комплексной моделью, способной производить двусторонние криптопреобразования над данными произвольного объема. Шифрование файлов осуществляется по оригинальному алгоритму с использованием симметричного ключа, который формируется на основании пароля, введенного пользователем. В результате хеширования пароля ключ достигает необходимой длины. Алгоритм шифрования является блочным шифром, то есть информация шифруется блоками определенной длины. Шифрование каждого последующего блока данных зависит от всех предыдущих.

В процессе шифрования происходит также сжатие данных, что обеспечивает еще большую надежность шифрования, так как между зашифрованными блоками данных отсутствует корреляционная зависимость. Временная задержка в проверке пароля не позволяет злоумышленникам узнавать пароль методом полного перебора. Кроме того, к зашифрованному файлу добавляется электронная цифровая подпись, которая позволяет проверять целостность информации. Расшифровка зашифрованного файла возможна только при правильно введенном пароле, который использовался при шифровании этого файла.

Была рассчитана экономическая эффективность от внедрения криптографической защиты информации. Она заключается в предотвращении возможных убытков от хищения или подмены информации. Затраты на создание программного продукта составляют 447440 рублей. Эти затраты являются незначительными и составляют 0,0365 % годовой себестоимости автотранспортных услуг, или 0,22 % прибыли автотранспортного цеха. В то же время, хищение или подмена информации может привести к существенным негативным, а в ряде случаев и к катастрофическим последствиям, которые разработанная система криптозашиты надежно предотвратит:

1. Экономические потери, т.к. раскрытие коммерческой информации может привести к серьезным прямым убыткам завода на рынке.
2. Кражу информации, которой могут воспользоваться фирмы-конкуренты, если кража осталась незамеченной. В этом случае конкуренты могут полностью разорить предприятие, навязывая ему фиктивные либо заведомо убыточные сделки.
3. Подмену информации как на этапе передачи, так и на этапе хранения в информационной системе НЗНП – такая подмена также может привести к огромным убыткам завода.

Таким образом, можно сделать вывод об экономической целесообразности создания подсистемы криптографической защиты информации на предприятии ОАО «Новошахтинский завод нефтепродуктов».

Литература:

1. Автоматизированные информационные технологии в экономике. Учебник. Под. ред. проф. Г.А. Титоренко. – М.: Юнити, 2010. 216 с.

2. Алферов А.: Основы криптографии. Учебное пособие. – СПб.: БХВ – Петербург, 2012.382 с.

3. Байбурин В.Б.: Введение в защиту информации. – СПб.: БХВ – Петербург, 2009. 242 с.

4. Введение в защиту информации в автоматизированных системах. Учебное пособие для вузов. Малюк А.А., Пазизин С.В., Погожин Н.С. 2-е изд. – СПб.: БХВ – Петербург, 2010. 410 с.

В.Н. Смоляков, С.В. Гусишная

МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНОЙ ЛВС СЕТИ СУПЕРМАРКЕТОВ «ПЕРЕКРЕСТОК» Г. РОСТОВА-НА-ДОНУ

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: система защиты информации, программное обеспечение, локаль-ная вычислительная сеть, автоматизированное рабочее место, информационная безопасность, несанкционированный доступ, персональный компьютер, межсетевой экран.

Злоумышленник, находясь в любой точке планеты, может получить несанкционированный доступ (НСД) к любым конфиденциальным данным, хранящимся в ЛВС организации. В настоящее время над проблемой защищенности передаваемой по сетям информации работает большое количество специалистов во всех экономически развитых странах мира. Информационная безопасность (ИБ) сформировалась в отдельную быстро развивающуюся науку. Несмотря на усилия многочисленных организаций, занимающихся защитой информации (ЗИ), обеспечение ИБ остается чрезвычайно острой проблемой.

Обеспечение ЗИ требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер. Комплексный характер и защиты проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для них информацию.

V.N. Smolaykov, S.V. Gusishnaya

MODERNIZATION OF INFORMATION SECURITY CORPORATE LAN NETWORK OF SUPERMARKETS «CROSSROADS» IN ROSTOV-ON-DON

Moscow State Technical University, North Caucasian Branch, Rostov-on-Don, Russia

Keywords: information security system, software, local area network, workstation, information security, unauthorized access, personal computer, firewall.

The attacker, from anywhere in the world can gain unauthorized access (unauthorized access) to all confidential data stored in the Organization's LAN. At present, on the issue of security of information transmitted over networks running a large number of specialists in all economically developed countries. Information Security (IS) was formed as a separate rapidly developing science. Despite the efforts of many organizations, occupying the protection of information (RFI) to ensure information security is an extremely serious problem. Providing GI requires not only the development of mechanisms for the protection of private and re-implementation of the system approach, which includes a set of interrelated actions. Comprehensive and integrated protection stems from the actions of intruders seeking any means to get important information for them.

Применение вычислительных средств в системе управления государственных и коммерческих структур требует наличия мощных систем обработки и передачи данных. Эта задача решается путем создания единой инфраструктуры, включающей локальную вычислительную сеть (ЛВС) организации, имеющую высокоскоростной доступ к глобальной сети Интернет. Тогда сотрудник, имеющий персональный компьютер (ПК) в составе ЛВС, получает доступ к информации крупнейших библиотек и баз данных мира, может быстро обмениваться информацией с другими респондентами независимо от расстояния и страны проживания, осуществлять платежи и покупки, используя пластиковые карты, осуществлять крупные транши «электронных» денег и т.д.

Но такие информационные системы (ИС) повлекли ряд проблем, одна из которых - безопасность обработки и передачи данных. Особенно «беззащитными» оказались данные, передаваемые внутри ЛВС и между ЛВС через глобальную сеть.

Злоумышленник, находясь в любой точке планеты, может получить несанкционированный доступ (НСД) к любым конфиденциальным данным, хранящимся в ЛВС организации. В настоящее время над проблемой защищенности передаваемой по сетям информации работает большое количество специалистов во всех экономически развитых странах мира. Можно сказать, что информационная безопасность (ИБ) сформировалась в отдельную быстро развивающуюся науку. Однако, несмотря на усилия многочисленных организаций, занимающихся защитой информации (ЗИ), обеспечение ИБ остается чрезвычайно острой проблемой.

Под ИБ понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений (владельцам и пользователям информации).

ЗИ в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются:

- массовое распространение средств вычислительной техники (ВТ);
- усложнение шифровальных технологий;
- расширяющиеся возможности НСД к информации и действий над ней;
- необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн.

Кроме того, в настоящее время получили широкое распространение средства и методы НСД и негласного добывания информации. Они находят все большее применение не только в деятельности государственных правоохранительных органов, но и в деятельности разного рода преступных группировок.

Определенные трудности связаны с изменениями в технологиях обработки и передачи информации. С одной стороны, использование современных информационных технологий (ИТ) дает ряд очевидных преимуществ: повышение эффективности процессов управления, обработки и передачи данных и т.п. В наше время уже невозможно представить крупную организацию без применения новейших ИТ, начиная от создания автоматизированных рабочих мест (АРМ) и заканчивая построением корпоративных распределенных ИС.

С другой стороны, развитие ЛВС, их усложнение, взаимная интеграция, открытость приводят к появлению качественно новых угроз, увеличению числа злоумышленников, имеющих потенциальную возможность воздействовать на ИС с целью кражи, подмены или уничтожения хранящейся в ней информации.

Для обеспечения ЗИ требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер. Комплексный

характер и защиты проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для них информацию.

Сегодня можно утверждать, что рождается новая современная технология - технология ЗИ в телекоммуникационных сетях. Сказанное выше обусловило выбор темы предлагаемого проекта.

Объектом исследования является информация, передаваемая по внутренним и внешним телекоммуникационным каналам корпоративной ЛВС сети супермаркетов «Перекресток» г. Ростова-на-Дону. Предметом исследования является обеспечение ИБ данной ЛВС. Основной целью является модернизации существующей системы ЗИ (СЗИ) в ЛВС сети супермаркетов «Перекресток».

Поставленная цель достигается путем решения следующих задач:

1. Определение сути проблемы и рассмотрение задачи ЗИ в ИС.
2. Выявление угроз информации и способов воздействия на объекты ЗИ.
3. Анализ методов и средств ЗИ и концепции ИБ предприятия.
4. Разработка программно-аппаратного комплекса, обеспечивающего заданный уровень ИБ рассматриваемой ЛВС.

На сегодняшний день сформулировано три базовых принципа ИБ, задачей которой является обеспечение:

- целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожению;
- конфиденциальности информации;
- доступности информации для авторизованных пользователей.

Рассматривая проблемы, связанные с защитой данных в ИС, возникает вопрос о классификации сбоев и НСД, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций (РС) и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов ЗИ. Условно их можно разделить на три класса:

- аппаратные средства защиты;
- программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

Наиболее эффективными с точки зрения защиты информации в ЛВС являются первые два класса, которые и рассмотрены в данном проекте для модернизации СЗИ корпоративной ЛВС сети супермаркетов «Перекресток» г. Ростова-на-Дону.

Проведен обзор технологий построения и функционирования ЛВС сети супермаркетов «Перекресток», включающий анализ организационной структуры сети «Перекресток», топологий построения ЛВС, сетевой технологии Fast Ethernet, топологии построения ЛВС сети магазинов.

Проанализирована система безопасности ЛВС сети супермаркетов. Дана характеристика аппаратным компонентам ЛВС сети магазинов.

Проведен анализ существующей системы безопасности ЛВС. Рассмотрены особенности обеспечения безопасности посредством ОС Windows. Выбраны способы модернизации системы защиты ИС.

Проведены анализ атак на информационную систему и анализ компьютерных атак на ЛВС сети магазинов «Перекресток».

Выполнен анализ информационной безопасности сети супермаркетов. Рас-смотрены модели ИБ, требования к системе ИБ, защита терминалов ИС и методы обеспечения безотказности работы ИС.

Проведена модернизация СЗИ корпоративной ЛВС сети магазинов «Перекресток» аппаратно-программными средствами, в качестве которых предложены электронный замок «Соболь», программный комплекс криптографической защиты File-PRO, антивирус-ная программа ESET NOD32 Antivirus, файрвол Symantec Enterprise Firewall v8.0 и прог-раммно-аппаратный комплекс Symantec Network Security 7100. Разработаны структурные схемы ЛВС магазина и корпоративной ЛВС главного офиса сети супермаркетов.

С учетом выбранных программно-аппаратных средств защиты, структурные схемы модернизированных систем защиты информации корпоративной ЛВС сети супермаркетов «Перекресток» г. Ростова-на-Дону примут следующий вид:

1. В главном офисе:
   1.1. На все АРМ устанавливаются Антивирус ESET NOD32;
   1.2. На все АРМ устанавливаются Электронный замок «Соболь»;
   1.3. На все АРМ устанавливаются Комплекс криптозащиты File-PRO.
   1.4. Канал связи ЛВС главного офиса с Интернет дополнительно защищается межсетевым экраном Symantec Enterprise Firewall и программно-аппаратным комплексом Symantec Network Security 7100.
2. В магазинах в состав ЛВС входят от 16 до 20 АРМ. В каждом магазине:
   2.1. На все АРМ устанавливаются антивирус ESET NOD32.
   2.2. На восемь АРМ (директора магазина, зам. директора – ОКЗИЦ, старшего кассира, старшего кладовщика и трех менеджеров) устанавливаются ЭЗ «Соболь» и комплекс криптозащиты File-PRO.
   2.3. Канал связи ЛВС магазина с Интернет дополнительно защищается межсетевым экраном Symantec Enterprise Firewall.

Было выполнено технико-экономическое обоснование эффективности решений проекта. Вычислены полные затраты на разработку и внедрение проекта модернизации СЗИ ЛВС главного офиса и магазинов сети «Перекресток». Разработка сохранит эффективность не менее пяти лет. За это время она принесет чистый дисконтированный доход в размере 1457495 руб. Расчеты показали выгодность разработки.

Литература:

1. Байбурин В.Б., Бровкова М.Б., Пластун И.Л., Мантуров А.О., Данилова Т.В., Макарцова Е.А. Введение в защиту информации. Учебное пособие (Серия «Профессиональное образование»). - М.: «Инфра-М», 2009. - 128 с.

2. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2011, с 64.

3. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. М.: Мир, 2009.

4. Боккер П. Цифровая сеть с интеграцией служб. Понятия, методы, системы: Пер. с нем. М.: Радио и связь, 2008. – 212 с.

5. Булгак В.Б., Варакин Л.Е., Ивашкевич Ю.К. и др. Концепция развития связи Российской Федерации. М.: Радио и связь, 2010. – 289 с.

В.Н. Смоляков, М.С. Шипицина

ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ЗАПАДНО-КУБАНСКОГО ПОЧТАМТА УФПС КРАСНОДАРСКОГО КРАЯ – ФИЛИАЛА ФГУП «ПОЧТА РОССИИ»

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: система защиты информации, информационная безопасность, межсетевые экраны, локальная вычислительная сеть, несанкционированный доступ, методы и средства защиты информации, базы данных.

Проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут значительные финансовые убытки. С широким распространением ЛВС появляются новые проблемы, которые требуют новых решений. Точно так же, как не стоит на месте научно-технический прогресс, не стоят на месте и те, кто пытается получить несанкционированный доступ (НСД) к информации, постоянно совершенствуя способы и методы

НСД, используя любые каналы утечки. Поэтому администратор сети должен смотреть на шаг вперед, предпринимая превентивные меры для защиты информации.

V.N. Smolaykov, M.S. Shipicina

PROTECTION OF INFORMATION IN A LOCAL AREA NETWORK WEST KUBAN KRASNODAR REGION AFPS POST OFFICE - FSUE «RUSSIAN POST»

Moscow State Technical University, North Caucasian Branch, Rostov-on-Don, Russia

Keywords: system of information protection, information security, firewalls, local area network, unauthorized access, methods and means of protecting information, database

The problem of network security remains unresolved and today, as the vast majority of companies have not addressed the issues of security, causing them to suffer significant financial losses. With the wide spread LAN there are new problems that require new solutions. Similarly, it does not stand still scientific and technological progress, not standing still, and those who try to gain unauthorized access to information, constantly improving techniques and methods of unauthorized access using any leakage channels. Therefore, the network administrator needs to look a step further by taking preventive measures to protect the information.

Вопрос обеспечения сохранности информации от несанкционированного доступа (НСД) или преднамеренного искажения достаточно остро стоит уже не одну тысячу лет. На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на каменных табличках, позже записывались на бумагу. Для их защиты также использовались материальные объекты: стены, рвы. Информация часто передавалась с посыльным и в сопровождении охраны. К сожалению, физическая защита имела крупный недостаток: при захвате сообщения враги узнавали все, что было написано в нем. Еще Юлий Цезарь принял решение защищать ценные сведения в процессе передачи. Он изобрел шифр Цезаря. Данная концепция получила свое развитие во время Второй мировой войны - Германия использовала машину Enigma для шифрования воинских сообщений.

Конечно, способы защиты информации (ЗИ) постоянно меняются, как меняется наше общество и технологии. Появление и широкое распространение компьютеров привело к тому, что большинство людей и организаций стали хранить информацию в электронном виде. Возникла потребность в защите такой информации.

В настоящее время огромное количество сетей объединено посредством Интернет. Поэтому очевидно, что для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации, причем опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа.

Учитывая эти факты, можно с уверенностью сказать, что проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут значительные финансовые убытки.

В наши дни эти проблемы стали еще серьезнее. Со стремительным распространением ЛВС появляются новые проблемы, которые требуют новых решений. Точно так же, как не стоит на месте научно-технический прогресс, не стоят на месте и те, кто пытается получить НСД к информации, постоянно совершенствуя способы и методы НСД, используя любые каналы утечки. Поэтому администратор сети ЭВМ должен смотреть на шаг вперед, предпринимая превентивные меры для ЗИ. В соответствии с этим, весьма актуальной и практически значимой является задача разработки комплекса мероприятий для обеспечения всесторонней системы защиты права доступа к элементам локальной вычислительной сети (ЛВС) и тем самым ЗИ в ней. Решению этой задачи и посвящен данный проект.

Обеспечение необходимого уровня ЗИ требует не просто осуществления некоторой совокупности научно-технических и организационных мероприятий, а создания целостной системы организационных мероприятий и применения специальных средств и методов ЗИ.

Рассматривая проблемы, связанные с защитой данных в информационной сети, возникает вопрос о классификации сбоев и НСД, которые ведут к потере или нежелательному изменению данных. Это могут быть сбои оборудования, потери информации (из-за инфицирования вирусами, неправильного хранения архивных данных, НСД), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в ЛВС вызвали необходимость создания различных видов ЗИ. Условно их можно разделить на три класса:

- аппаратные средства защиты;
- программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

Наиболее эффективными с точки зрения ЗИ являются первые два класса, которые и будут рассмотрены для организации ЗИ.

В общем случае программными средствами защиты называются специальные программы, которые включаются в состав программного обеспечения (ПО) компьютерных сетей специально для осуществления функций защиты. К недостаткам программных средств относится необходимость расходования ресурсов процессора на их функционирование и возможность их несанкционированного изменения.

Ряд проблем в решении задачи защиты права доступа к ресурсам сети целесообразнее решать аппаратными способами.

Одним из решений проблем безопасности подключения к сети Интернет является применение межсетевых экранов (МЭ). МЭ - это программно-аппаратная система, находя-щаяся в точке соединения внутренней сети организации и Интернет и осуществляющая контроль передачи данных между сетями.

Таким образом, основной целью проекта является изучение и анализ методов и средств ЗИ в сетях и на этой основе - разработка системы ЗИ (СЗИ) в ЛВС Западно-Кубанского почтамта УФПС Краснодарского края - филиала ФГУП «Почта России».

Для достижения указанной цели необходимо было решить ряд задач:

- проанализировать проблемы информационной безопасности в ЛВС Западно-Кубанского почтамта:
- провести анализ путей построения межсетевых экранов;
- разработать предложения по защите информации МЭ в ЛВС почтамта;
- составить рекомендации по применению устройств, методов и мероприятий по ЗИ в ЛВС почтамта.

Теоретическая значимость проекта состоит в анализе существующих технологий построения СЗИ и обоснованном выборе одной из них.

Практическая значимость состоит в реализации на практике проекта ЗИ в ЛВС почтамта.

Экономическая эффективность обуславливается решением проблемы защиты информации, хранящейся на сервере БД от НСД к ней.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий (ИТ).

Актуальность и важность проблемы обеспечения информационной безопасности (ИБ) обусловлены следующими факторами:

1. Современные уровни и темпы развития средств ИБ значительно отстают от уровней и темпов развития ИТ.
2. Высокие темпы роста парка ПК, применяемых в разнообразных сферах человеческой деятельности. Согласно данным исследований компании Gartner Dataquest в настоящее время в мире более двух миллиардов ПК.
3. Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных. Доступность средств вычислительной техники, и, прежде всего, ПК, привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих систем, как со злым умыслом, так и из чисто «спортивного интереса».

4. Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации. По оценкам специалистов в настоящее время около 70-90% интеллектуального капитала компании хранится в цифровом виде – текстовых файлах, таблицах, БД.
5. Многочисленные уязвимости в программных и сетевых платформах. Стремительное развитие ИТ открыло новые возможности для бизнеса, однако привело и к появлению новых угроз. Современные программные продукты из-за конкуренции попадают в продажу с ошибками и недоработками. Разработчики, включая в свои изделия всевозможные функции, не успевают выполнить качественную отладку создаваемых программных систем. Ошибки и недоработки, оставшиеся в этих системах, приводят к случайным и преднамеренным нарушениям ИБ.
6. Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире. Подобная глобализация позволяет злоумышленникам практически из любой точки земного шара, где есть Интернет, за тысячи километров, осуществлять нападение на корпоративную сеть.
7. Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Например, в настоящее время свыше 90% всех преступлений связано с использованием автоматизированных систем обработки информации.

Под угрозой безопасности понимается возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации. Поэтому обеспечение ИБ компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

Из всего выше перечисленного можно сделать вывод о целесообразности и необходимости разработки проекта СЗИ в ЛВС Западно-Кубанского почтамта.

В ходе обследования Западно-Кубанского почтамта была дана общая характеристика локальным вычислительным сетям, изучены организационно-штатная структура почтамта, технические и программные средства его ЛВС.

Был проведен анализ информационной безопасности ЛВС почтамта и методов защиты ЛВС от НСД из сети Интернет, рассмотрены пути решения проблем обеспечения ИБ и основные подходы к защите ЛВС почтамта от НСД из сети Интернет.

Рассмотрены назначение, возможности и пути построения межсетевых экранов, их архитектура и классификация.

Проведен анализ различных типов окружений и показателей уровней защищенности межсетевых экранов, а также выполнен анализ защищенных виртуальных частных сетей VPN.

На основании вышеизложенного, предлагаются следующие меры для защиты информации в ЛВС Западно-Кубанского почтамта:

1. Необходимо ввести в состав ЛВС аппаратный МЭ SonicWall TZ 170, обеспечивающий надежную защиту при работе с Интернет на скорости до 100 Мбит/с. По критерию «Цена – качество» - это оптимальная платформа безопасности для малых офисов и филиалов, количество устройств в ЛВС которых колеблется от нескольких единиц до ста.
2. Предлагается дополнительно к сетевой ОС установить на сервер операционную систему SonicWALL с дополнительными возможностями - SonicOS Enhan-ced. SonicOS Enhanced - это мощная ОС нового поколения, предлагающая более широкий по сравнению с SonicOS Standard выбор функций, реализуемых устройствами Sonic WALL, для обеспечения непрерывности бизнес приложений, отвечающая современным и прогнозируемым в будущем требованиям к сетям любой сло-жности и масштаба.
3. Необходимо в полной мере реализовать предложенные рекомендации по применению устройств, методов и мероприятий по защите ЛВС Западно-Кубанского

почтамта, рекомендации по категорированию пользователей и нформации в ИС почтамта, а также рекомендации по защите используемой в ЛВС информации.

Литература:

Байбурин В.Б., Бровкова М.Б., Пластун И.Л., Мантуров А.О., Данилова Т.В., Макарцова Е.А. Введение в защиту информации. Учебное пособие (Серия «Профессиональное образование»), (ГРИФ). - М.: «Инфра-М», 2009. - 128 с.

Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2011, с 64.

Галатенко В.А. Стандарты информационной безопасности. - М.: Изд-во «Интернет-университет информационных технологий - ИНТУИТ.ру», 2010. - 328 с.

В.Н. Смоляков, Н.Н. Юрчевская

РАЗРАБОТКА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ООО «РКЦ АНАПА»

Северо-Кавказский филиал Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия

Ключевые слова: локальная вычислительная сеть, персональный компьютер, комплексная система защиты информации, несанкционированный доступ, информационная безопасность, информационная система, программно-аппаратные средства защиты информации.

Проблемы защиты информации (ЗИ) в локальных вычислительных сетях (ЛВС) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под ЗИ понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в ЛВС. Широкое распространение и повсеместное применение вычислительной техники (ВТ) очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации. ЗИ в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств ВТ; усложнение шифровальных технологий; необходимость промышленной, коммерческой и финансовой тайн.

V.N. Smolaykov, N.N. Yurchevskaya

DEVELOPMENT COMPLEX INFORMATION SECURITY SYSTEMS IN THE LOCAL AREA NETWORK OF «"RCC ANAPA»

Moscow State Technical University, North Caucasian Branch, Rostov-on-Don, Russia

Keywords: local area network, a personal computer, a complex system of information security, unauthorized access, information security, information systems, software and hardware protection of information.

Problems of protection of information (PI) in local area networks (LANs) are always the center of attention not only specialists in the development and use of these systems, but also a wide range of users. Under the GI refers to the use of special tools, methods and activities in order to prevent the loss of information in the LAN. Widespread and widespread use of computer technology (CT) is very sharply increased the vulnerability of the collected, stored and processed on the LAN information. PI in modern conditions is becoming more difficult problem, which is caused by several factors, the main ones are: mass distribution of funds CT; complexity of encryption technology; the need for industrial, commercial and financial secrets.

Вопрос защиты информации поднимается с тех пор, как только люди научились писать. Всегда существовала информация, которую должны были знать не все. Люди, обладающие такой информацией, прибегали к разным способам ее защиты: тайнопись, шифрование (шифр Цезаря). В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности (ИБ) компьютерных систем, а также контроля и управления различными объектами. К таким объектам можно отнести системы телекоммуникаций, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, системы обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих систем необходимо поддерживать их безопасность и целостность.

Проблемы защиты информации (ЗИ) в локальных вычислительных сетях (ЛВС) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под ЗИ понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в ЛВС. Широкое распространение и повсеместное применение вычислительной техники (ВТ) очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации.

ИБ – сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ). Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. Состояние защищенности в информационной сфере определяется совокупностью сбалансированных интересов личности, общества и государства.

Под ИБ понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений (владельцам и пользователям информации).

ЗИ в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств ВТ; усложнение шифровальных технологий; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированного доступа (НСД) к информации и действий над ней.

Кроме того, в настоящее время получили широкое распространение средства и методы НСД и негласного добывания информации. Они находят все большее применение не только в деятельности государственных правоохранительных органов, но и в деятельности разного рода преступных группировок.

Необходимо помнить, что естественные каналы утечки образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте ЗИ. Что касается искусственных каналов утечки информации, то они создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического канала утечки с использованием специальных технических средств. К ним можно отнести незаконное подключение к каналам, проводам и линиям связи, высокочастотное навязывание и облучение, установка в технических средствах и помещениях микрофонов и телефонных закладных устройств, НСД к информации, обрабатываемой в информационных системах и т.д. Поэтому особую роль и место в деятельности по ЗИ занимают мероприятия по созданию комплексной системы ЗИ (КСЗИ), так как ЗИ – это комплекс мероприятий направленных на обеспечение ИБ.

С методологической точки зрения правильный подход к проблемам ИБ начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Угрозы ИБ – это оборотная сторона использования ИТ.

Говоря о системах безопасности, нужно отметить, что они должны не только и не столько ограничивать допуск пользователей к информационным ресурсам, сколько определять и делегировать их полномочия в совместном решении задач, выявлять аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их последствия, гибко адаптируя структуру в условиях отказов, частичной потери или длительного блокирования ресурсов.

Не стоит забывать и об экономической целесообразности применения мер обеспечения ИБ, которые всегда должны быть адекватны существующим угрозам.

Параллельно с развитием средств ВТ и появлением все новых способов нарушения ИБ, развивались и совершенствовались средства ЗИ. Необходимо отметить, что более старые виды

атак никуда не исчезают, а новые только ухудшают ситуацию. Существующие сегодня подходы к обеспечению ЗИ несколько отличаются от существовавших на начальном этапе. Главное отличие современных концепций в том, что сегодня не говорят о каком-то одном универсальном средстве защиты, а речь идет о КСЗИ, включающей в себя:

- нормативно-правовой базис ЗИ;
- средства, способы и методы защиты;
- органы и исполнителей.

Другими словами, на практике ЗИ представляет собой комплекс регулярно используемых средств и методов, принимаемых мер и осуществляемых мероприятий с целью систематического обеспечения требуемой надежности информации, генерируемой, хранящейся и обрабатываемой на объекте, а также передаваемой по каналам. Защита должна носить системный характер, то есть для получения наилучших результатов все разрозненные виды ЗИ должны быть объединены в одно целое и функционировать в составе единого программно-аппаратного комплекса для обеспечения ИБ, представляющего собой слаженный механизм взаимодействующих элементов, предназначенных для выполнения задач по обеспечению ИБ.

Более того, КСЗИ предназначена обеспечивать, с одной стороны, функционирование надежных механизмов защиты, а с другой - управление механизмами ЗИ. В связи с этим должна предусматриваться организация четкой и отлаженной системы управления ЗИ. Сказанное выше подтверждает актуальность разработки эффективной КСЗИ для обеспечения ИБ в ЛВС. Решению этой проблемы и посвящен данный проект. В качестве объекта для обеспечения ИБ выбрана ЛВС ООО «РКЦ - Анапа», осуществляющее абонентское и расчётно-кассовое обслуживание ресурсосодержащих и управляющих компаний, принимающее коммунальные платежи и предоставляющее прочие персональные услуги населению города Анапа, а также станиц, сел и поселков Анапского района Краснодарского края.

В настоящее время информационная безопасность – одна из актуальных проблем, стоящих не только перед коммерческими предприятиями, но и перед каждым современным человеком. В наше время повсеместной информатизации, доступ злоумышленников к некоторым ЛВС может привести к поистине катастрофическим последствиям. Поэтому защите информации в ЛВС должно уделяться постоянное внимание. К сожалению, абсолютной защиты не существует. Обход тех или иных средств защиты только вопрос времени, денег и желания. Поэтому при разработке системы защиты необходимо учитывать ценность защищаемого объекта и не останавливаться на достигнутом уровне безопасности. Практически совершенная сегодня защита, завтра может превратиться лишь в небольшую помеху на пути злоумышленников. Поэтому был разработан программно-аппаратный комплекс для обеспечения информационной и физической безопасности ЛВС «РКЦ Анапа» с возможностью достаточно простой дальнейшей модернизации с учетом вновь возникающих угроз.

В проекте было проведено обоснование необходимости защиты информации, рассмотрены структура и основные виды деятельности ООО «РКЦ Анапа», характеристика его информационной системы, модель нарушителя и концепция безопасности, защищенный электронный документооборот на базе ViPNet.

Выполнен обзор устройств и средств защиты информации (программно-аппаратные средства защиты информации от НСД, программные средства защиты информации, межсетевые экраны и частные виртуальные сети).

На этой основе разработана система защиты информации в ЛВС ООО «РКЦ Анапа» - выполнен обзор технических средств и систем безопасности, рассмотрены организация защиты информации от НСД, особенности использования межсетевого экрана и антивирусной защиты, защищенного электронного документооборота и системы безопасности объектов «РКЦ Анапа».

В результате на основе проведенных аналитических исследований были предложены конструкторские решения по оснащению объекта информационной защиты охранно-пожарной сигнализацией и программно-аппаратными средствами защиты информации для компонентов вычислительной сети организации.

Проведено технико-экономическое обоснование эффективности решений проекта (выполнены оценка эффекта от внедрения КСЗИ в ЛВС и расчет стоимости разработки и установки КСЗИ в ЛВС ООО «РКЦ Анапа»). Расчет показал, что затраты на разработку и внедрение всего программно-аппаратного комплекса для обеспечения информационной безопасности ЛВС являются незначительными, составляют всего 1,5 % от прибыли предприятия и

являются экономически оправданными. Действительно, внедрение данной КСЗИ позволяет достаточно надежно защитить информационную систему ЛВС офиса фирмы и удаленных отделений кассового обслуживания от вирусов, хакерских атак, кражи или подмены конфиденциальной и коммерческой информации и т.д. Разработанная система безопасности надежно защитит главный офис от физического проникновения злоумышленников, а также своевременно передаст сигнал тревоги при возникновении пожара.

Таким образом, в проекте изложен комплекс мер, охватывающий физическую охрану объекта, техническое и программно-аппаратное обеспечение информационной безопасности. На основании вышесказанного можно сделать вывод, что цели, поставленные в проекте, были достигнуты, а задачи - выполнены.

Литература:

1. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам: учебник для вузов - М.: Гротеск, 2009. - 248 с.

2. Андрианов В.И. Шпионские штучки и устройства для защиты объектов и информации: учебник для вузов / В.И. Андрианов, В.А. Бородин, А.В. Соколов. - СПб.: Лань, 2004. - 272 с.

3. Анин Б.Ю. Защита компьютерной информации. - СПб.: BHV-Санкт-Петербург» - 2008. - 384 с.

4. Баранов В.М. Защита информации в системах и средствах связи: учебное пособие для вузов / В.М. Баранов, Г.В. Вальков, М.А. Еремеев - Санкт- Петербург: ВИККА имени А.Ф. Можайского, 2007. – 113 с.

5. Бармен С.К. Разработка правил информационной безопасности - М.: Издательский дом «Вильямс», 2007. - 208 с.

К.А. Ташев, У.Ю. Рахмонов

МЕТОДЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Ташкентский университет информационных технологий, г. Ташкент, Узбекистан

Ключевые слова: инфокоммуникационных сети, информационная безопасность, угроза информационной безопасности, сигнатурный подход.

Анализирована существующие методы мониторинга информационной безопасности, определена необходимость использования комплексных методов контроля состояния для достижения высокой эффективности надежности защиты инфокоммуникационной сети.

K.A. Tashev, U.Y. Rakhmonov

METHODS OF MONITORING INFORMATION SECURITY IN INFOCOMMUNICATION NETWORKS

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: info-communication networks, information security, information security threat, signature approach.

Analyze existing methods of monitoring information security, identified the need to use complex methods of condition monitoring to achieve high efficiency infocomm security protection network.

Одной из задач при систем поддержки принятия решений организации защиты является мониторинг параметров функционирования объекта защиты, на основании анализа данных которого решается вопрос о необходимости проектирования системы безопасности обследуемого объекта[1]. Назначение систем мониторинга — обнаруживать аномалии в работе

инфокоммуникационных сетях (ИКС) и оперативно на них реагировать. Обнаружению подлежит подозрительная активность компонентов системы - от пользователей (внутренних и внешних) до программных и аппаратных средств. Существующие системы мониторинга, используют для обнаружения атак и подозрительной активности в ИКС либо сетевой, либо системный подход.

При проведении мониторинга на сетевом уровне используют в качестве источника данных для анализа необработанные сетевые пакеты. Как правило, при проведении мониторинга сетевого уровня используют сетевой адаптер, функционирующий в режиме «прослушивания», и анализируют трафик в реальном масштабе времени по мере его прохождения через сегмент сети. Модуль распознавания атак использует один из методов обнаружения атак и как только атака обнаружена, модуль реагирования уведомляет об атаке или выдает сигнал тревоги.

Мониторинг системного уровня контролирует систему, события и журналы регистрации событий безопасности. Когда какой-либо из этих файлов изменяется, то происходит сравнение новых записей с сигнатурами атак, чтобы проверить, есть ли соответствие. Если такое соответствие найдено, то система посылает администратору сигнал тревоги или приводит в действие другие заданные механизмы реагирования.

Традиционно в системах обнаружения вторжений используется сигнатурный подход [2], основная идея которого заключается в сравнении записей о событиях в системе с определенными шаблонами – правилами, описывающими атаки. Так как набор правил фиксирован, такие системы зависят от эксперта и невосприимчивы к новым типам вторжений, пока эксперт не опишет новые правила. В подобных системах обычно используется техника периодического просмотра собранных системой журналов (лог-файлов) аудита и приложений, однако набор журналов, используемых такими системами, зачастую достаточно ограничен, отчасти из-за необходимости для каждого вида журналов разрабатывать свои правила. Сигнатурный подход имеет ряд серьезных недостатков.

Системы, построенные на основе сигнатурных методов, не обнаруживают новые типы вторжений, поскольку базы знаний для подобных систем формируются экспертом и обновляются вручную или через третьи организации, предоставляющие системы защиты. Особенностью систем обнаружения внутренних вторжений, построенных на основе сигнатурных методов, является необходимость «ручной» настройки системы обнаружения администратором или экспертом под конкретную конфигурацию защищаемой компьютерной системы. Такая настройка требует как серьезных временных затрат, так и высокой квалификации администратора.

Существуют методы, позволяющие «замаскировать» вторжение так, что с помощью набора правил его невозможно будет определить как несанкционированное действие. Профессиональный злоумышленник, имея доступ к базе знаний системы защиты (он может всегда ее получить, в частности, приобретя ее, как легальный пользователь), почти всегда может «обмануть» традиционную систему обнаружения вторжений, основанную на сигнатурных методах.

Существует класс потенциальных потребителей систем обнаружения вторжений, для которых использование внешних баз знаний недопустимо по соображениям безопасности. Кроме того, качество функционирования систем, построенных на основе внешних баз знаний, существенно зависит от качества и оперативности работы компаний, поддерживающих наполнение этих баз. Таким образом, деятельность этих компаний становится уязвимым звеном в системе обеспечения компьютерной безопасности.

Большинство сигнатурных систем работают в рамках одного источника информации об активности пользователя (например, осуществляют мониторинг работы с файловой системой или «просматривают» сетевой трафик и т.д.), используя при этом специфические для этого источника правила и политику безопасности. Но как показывают исследования, для внутренних вторжений одного источника информации, как правило, недостаточно, поэтому необходимо осуществлять мониторинг многих разнородных показателей одновременно, консолидировать полученную информацию в единый поток событий и отслеживать зависимости и корреляции для разнотипных событий безопасности.

На сегодняшний день актуально создание программных технологий построения эффективных систем защиты от внутренних вторжений, основанных на не сигнатурных методах и обладающих свойствами автономности, адаптируемости и само обучаемости [3].

Подобного рода системы защиты должны решать следующие задачи:

– сбор и анализ статистики работы пользователей и приложений;
– построение и визуализация моделей поведения пользователей;
– выявление аномалий в работе пользователей и программного обеспечения (ПО);
– выявление внутренних угроз.

Каждый уровень проведения мониторинга в ИКС имеет свои особенности и охватывает определенную область действия, результаты сравнение возможностей проведения мониторинга на разных уровнях представлено в таблице 1. Анализ показывает, что при проведении мониторинга и сетевого, и системного уровней есть свои недостатки, достоинства и преимущества, которые эффективно дополняют друг друга.

Методы мониторинга состояния сети. Выбор способов и объектов мониторинга сети зависит от множества факторов – конфигурации сети, действующих в ней сервисов и служб, конфигурации серверов и установленного на них ПО, возможностей ПО, используемого для мониторинга и т.п.

На самом общем уровне можно говорить о таких элементах как:

1. Проверка физической доступности оборудования;
2. Проверка состояния (работоспособности) служб и сервисов, запущенных в сети;
3. Детальная проверка не критичных, но важных параметров функционирования сети: производительности, загрузки и т.п.;

Проверка параметров, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах БД, содержимое лог-файлов).

Таблица 1. Сравнительный анализ систем мониторинга безопасности.

№	Уровень мониторинга	Вид	Достоинства	Недостатки
1	Системный уровень	1. Система 2. События 3. Журнал безопасности	1. Подтверждает успех или отказ атаки; 2. Контролирует деятельность конкретного узла; 3. Обнаруживает атаки, которые упускают системы сетевого уровня; 4. Хорошо подходит для сетей с шифрованием и коммутацией; 5. Не требуют дополнительных аппаратных средств; 6. Низкая стоимость эксплуатации.	Зависит от ОС и не обнаруживает аномалии возникающие на сетевом уровне
2	Сетевой уровень	1. Анализ сетевых пакетов 2. Анализ трафика	Низкая стоимость эксплуатации; Обнаруживает атаки или аномалии в поведении, которые возникают на сетевом уровне; Обнаруживает и реагирует в реальном масштабе времени; Обнаруживает неудавшиеся атаки или подозрительные намерения; Не зависит от ОС.	Не может обнаруживать атаки системного уровня

Начальный уровень любой проверки – тестирование физической доступности оборудования (которая может быть нарушена в результате отключения самого оборудования либо отказе каналов связи). Как минимум, это означает проверку доступности по ICMP-протоколу (ping), причем желательно проверять не только факт наличия ответа, но и время прохождения сигнала, и количество потерянных запросов: аномальные значения этих величин, как правило, сигнализируют о серьезных проблемах в конфигурации сети. Некоторые из этих проблем легко отследить при помощи трассировки маршрута (traceroute) – ее также можно автоматизировать при наличии «эталонных маршрутов».

Следующий этап – проверка принципиальной работоспособности критичных служб. Как правило, это означает TCP-подключение к соответствующему порту сервера, на котором должна быть запущена служба, и, возможно, выполнение тестового запроса (например, аутентификации на почтовом сервере по протоколу SMTP или POP или запрос тестовой страницы от веб-сервера).

Способы проверки этих величин варьируются, но один из основных, доступных почти всегда – проверка по SNMP-протоколу. Помимо этого, можно использовать специфические средства, предоставляемые ОС проверяемого оборудования: к примеру, современные серверные версии ОС Windows на системном уровне предоставляют так называемые счетчики производительности (performancecounters), из которых можно «считать» довольно подробную информацию о состоянии компьютера [3].

Наконец, многие окружения требуют специфических проверок – запросов к БД, контролирующих работу некоего приложения; проверка файлов отчетов или значений настроек; отслеживание наличия некоторого файла (например, создаваемого при «падении» системы).

Контроль безопасности сети. Безопасность компьютерной сети (в смысле защищенности ее от вредоносных действий) обеспечивается двумя методами: аудитом и контролем. Аудит безопасности – проверка настройки сети (открытых портов, доступности «внутренних» приложений извне, надежности аутентификации пользователей).

Сущность контроля безопасности состоит в выявлении аномальных событий в функционировании сети. Предполагается, что базовые методы обеспечения и контроля безопасности встроена во все серверное ПО [3]. Однако, во-первых, не всегда можно доверять этому предположению; во-вторых, не всегда такой защиты достаточно. Для полноценной уверенности в безопасности сети в большинстве случаев необходимо использовать дополнительные, внешние средства. При этом проверяют, как правило, следующие параметры:

- нагрузку на серверное ПО и «железо»: аномально высокие уровни загрузки процессора, внезапное сокращение свободного места на дисках, резкое увеличение сетевого трафика зачастую являются признаками сетевой атаки;
- журналы и отчеты на наличие ошибок: отдельные сообщения об ошибках в лог-файлах программ-серверов или журнале событий серверной ОС допустимы, но накопление и анализ таких сообщений помогает выявить неожиданно частые или систематические отказы;
- состояние потенциально уязвимых объектов – например, тех, «защищенность» которых тяжело проконтролировать напрямую (ненадежное стороннее ПО, изменившаяся/непроверенная конфигурация сети): нежелательные изменения прав доступа к некоторому ресурсу или содержимого файла может свидетельствовать о проникновении «врага».

Во многих случаях аномалии, замеченные при мониторинге и контроле, требуют немедленной реакции технических специалистов, соответственно, средство мониторинга сети должно иметь широкие возможности для пересылки оповещений. Изменения других контролируемых параметров реакции не требуют, но должны быть учтены для последующего анализа. Зачастую же необходимо и то, и другое – непрерывный сбор статистики плюс немедленная реакции на «выбросы»: например, отмечать и накапливать все случаи загрузки процессора более 80%, а при загрузке более 95% – немедленно информировать специалистов. Полноценный мониторинговый софт должен позволять организовывать все эти (и более сложные) сценарии.

Литература:

1. Лукацкий, А. Обнаружение атак / А. Лукацкий. – СПб. : БХВ–Петербург, 2001.– 624с.

2. Лукинова О.В. Формализация задачи планирования защиты распределенной компьютерной сети на основе бизнес-процессного подхода // Надежность. – 2009. – №1. – С. 72-80.

3. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

В.Н. Трипута, Е.В. Жилина

ПРОТОКОЛ РАЗРЕШЕНИЯ АДРЕСОВ ARP: ОТ ТЕОРИИ К ПРАКТИКЕ

Ростовский государственный экономический университет (РИНХ)

Ключевые слова: ARP-протокол, IP-адрес, MAC-адрес, ARP-таблица, Packet Tracer, язык программирования C++.

В статье рассмотрено понятие протокола разрешения адресов ARP, описаны принципы работы узлов по построению ARP-таблиц, проведена симуляция работы ПК в программном средстве Cisco Packet Tracer 6, реализована программа на языке программирования C++ по получению MAC-адресов хостов сети.

V.N. Triputa, E.V. Zhilina

ADDRESS RESOLUTION PROTOCOL ARP: FROM THEORY TO PRACTICE

Rostov State University of Economics (RINH)

Keywords: ARP-protocol, IP-address, MAC-address, ARP-table, Packet Tracer, the programming language C ++.

The article deals the notion of Address Resolution Protocol ARP, describes the principles of operation of units for the construction of ARP-tables, carried out a simulation of PC in software Cisco Packet Tracer 6, program was implemented in the programming language C ++ to obtain MAC-addresses of network hosts.

В локальной сети Ethernet сетевая интерфейсная плата принимает кадр только в том случае, если он отправлен на MAC-адрес широковещательной рассылки или MAC-адрес сетевого адаптера.

С помощью IP-протокола, который называется протоколом разрешения адресов (ARP), можно определить MAC-адрес любого узла из той же локальной сети

Протокол Address Resolution Protocol (ARP) используется для простой задачи – выяснить по известному адресу сетевого уровня (IP) неизвестный адрес канального уровня (например, MAC). Данные ARP вкладываются в протокол канального уровня и являются, по уровню вложения, протоколом 3-го уровня, а вот по функционалу остаются протоколом 2-го уровня. Для идентификации ARP внутри кадра Ethernet используется код протокола 0x0806 [1].

В состав ARP-пакета входят следующие поля:

- Тип оборудования длиной поля в 2 байта. Обозначает тип рабочей среды. Для Ethernet равняется единице.
- Тип протокола сетевого уровня, который задействован в ARP-пакете, равняется двум байтам. Стандартный код протокола, для IPv4 – это 0x0800.
- Длина адреса канального уровня, равняется 1 байту.
- Длина адреса сетевого уровня, равняется 1 байту.
- Код операции ARP, равняется 2 байтам. У операции ARP Request это единица, у ARP Response – двойка.
- Адрес канального уровня отправителя – уникастовый MAC-адрес интерфейса, с которого отправляется запрос.
- Адрес сетевого уровня отправителя – уникастовый IP-адрес интерфейса, с которого отправляется запрос.
- Искомый адрес канального уровня. В случае ARP – широковещательный адрес вида FF-FF-FF-FF-FF-FF.
- Искомый адрес сетевого уровня.

Принцип работы:

1. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
2. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным.
3. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Преобразование адресов выполняется путем поиска в таблице. Эта таблица, называемая ARP-таблицей, хранится в памяти и содержит строки для каждого узла сети. В двух столбцах содержатся IP- и Ethernet-адреса. Если требуется преобразовать IP-адрес в Ethernet-адрес, то ищется запись с соответствующим IP-адресом [2].

Маршрутизаторы перемещают данные между локальной и удаленной сетью [4]. Пример таблицы маршрутизации (содержит наименование сетей) и ARP-таблицы маршрутизатора (содержит IP и MAC-адреса), объединяющего две сети приведен на рис. 1.

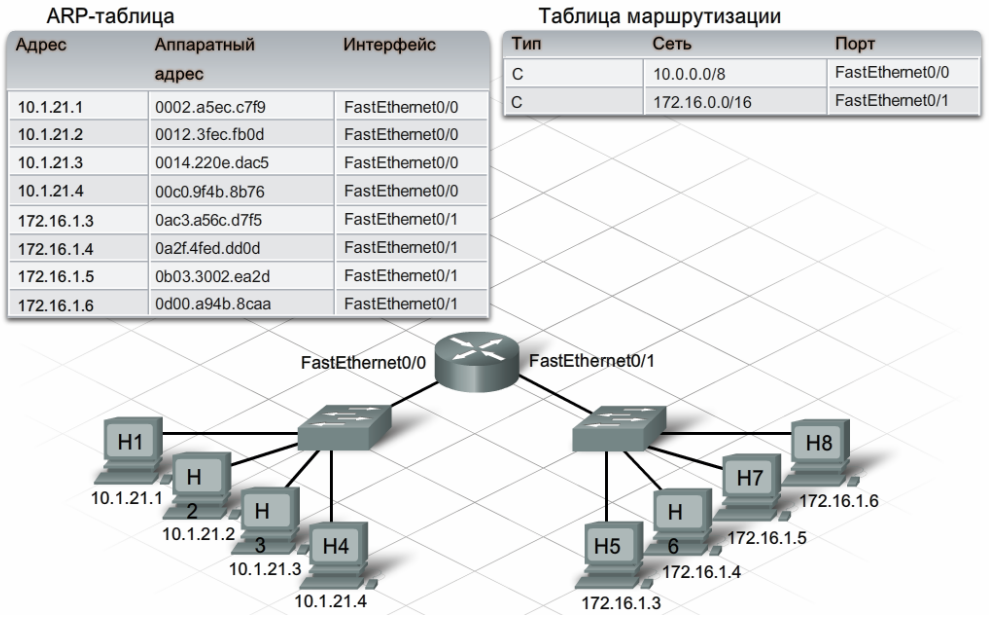


Рисунок 1. Таблицы маршрутизатора, объединяющего две сети

Ниже приведен пример упрощенной ARP-таблицы, полученной в консоли ОС Windows, используя стандартную команду **arp -a** (рис. 2).

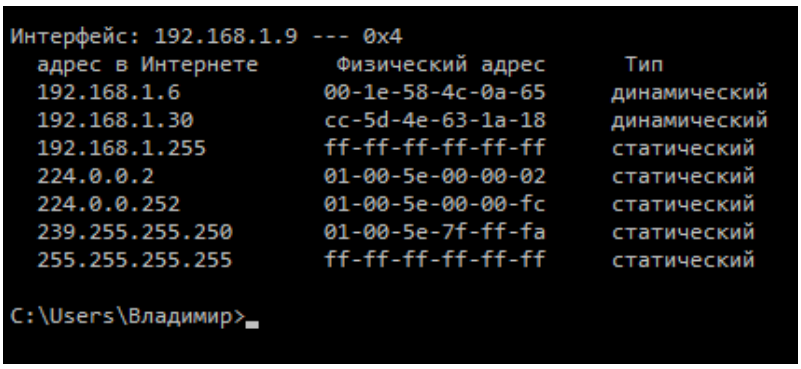


Рисунок 2. Пример ARP-таблицы в консоли ОС Windows

Далее проведем наблюдение за потоком данных от PC-A к PC-B при создании сетевого трафика. Симуляция проведена в программном средстве Cisco Packet Tracer 6, применялась IPv4-адресация, фильтр ARP и ICMP-протоколы. Два компьютера соединены концентратором (рис. 3).

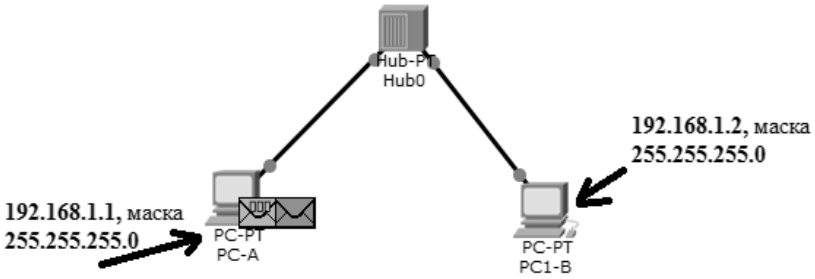


Рисунок 3. Постановка симуляции в Cisco Packet Tracer 6

Один конверт PC-A – это сообщение, передаваемое по протоколу ICMP, другой - сообщение, передаваемое по протоколу ARP. Результаты успешного моделирования приведены на рис. 4, команда **arp –a** была введена соответственно на PC-A и PC-B.

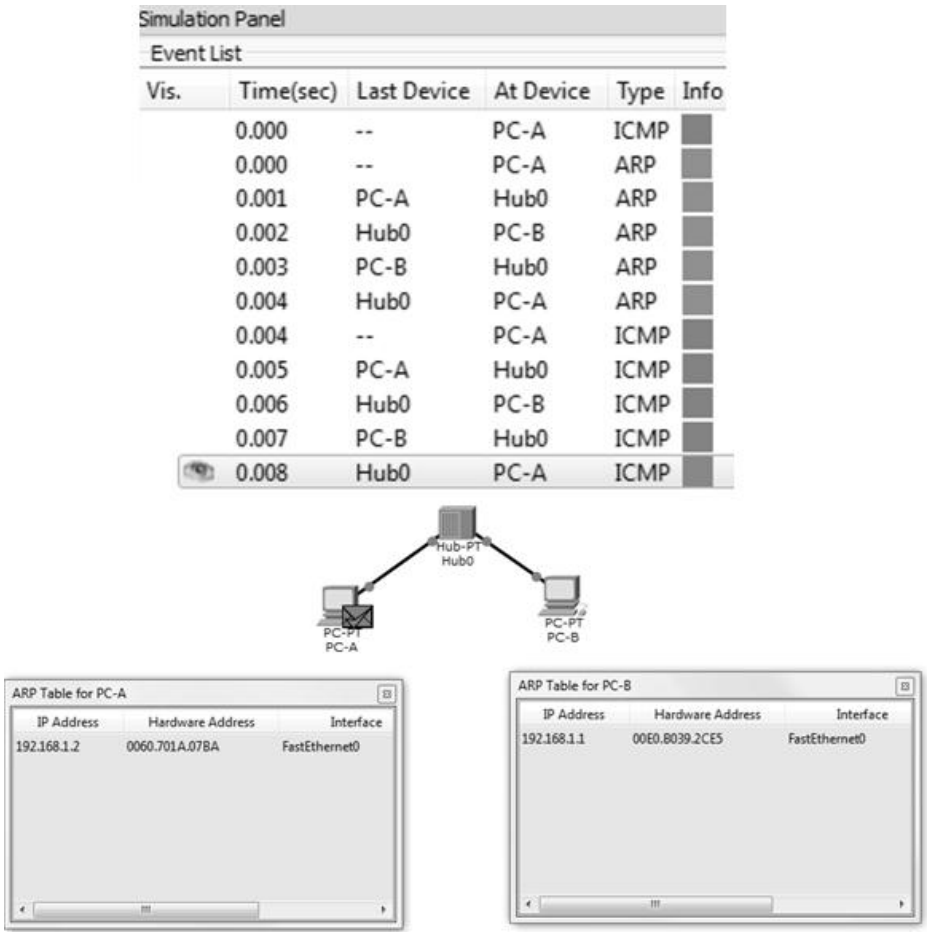


Рисунок 4. Результаты моделирования: отображение ARP-таблиц

Далее приведем пример реализации приложения по использованию протокола ARP.

Программ реализована на языке C++ с использованием стандартных библиотек. Программ запускается из командной строки. Нужно прописать название программы (в нашем случае ARP.exe), и интересующий IP-адрес.

```
#ifndef WIN32_LEAN_AND_MEAN
#define WIN32_LEAN_AND_MEAN
#endif
#include "stdafx.h"
#include <winsock2.h>
#include <iphlpapi.h>
#include <stdio.h>
```

```
#include <stdlib.h>
#include <clocale>
#pragma comment(lib, "iphlpapi.lib")
#pragma comment(lib, "ws2_32.lib")

void usage(char *pname)
{
	printf("Использование: %s [параметр] ip-адрес\n", pname);
	printf("\t -h \t\tпомощь\n");
	printf("\t -l length \tMAC длина адреса для установки\n");
	printf("\t -s src-ip \tискомый IP адрес\n");
	exit(1);
}

int __cdecl main(int argc, char **argv)
{
	setlocale(LC_ALL, "RUS");
	DWORD dwRetVal;
	IPAddr DestIp = 0;
	IPAddr SrcIp = 0;
	ULONG MacAddr[2];
	ULONG PhysAddrLen = 6;

	char *DestIpString = NULL;
	char *SrcIpString = NULL;

	BYTE *bPhysAddr;
	unsigned int i;

	if (argc > 1) {
		for (i = 1; i < (unsigned int)argc; i++) {
			if ((argv[i][0] == '-') || (argv[i][0] == '/')) {
				switch (tolower(argv[i][1])) {
				case 'l':
					PhysAddrLen = (ULONG)atol(argv[++i]);
					break;
				case 's':
					SrcIpString = argv[++i];
					SrcIp = inet_addr(SrcIpString);
					break;
				case 'h':
				default:
					usage(argv[0]);
					break;
				}
			}
			else
				DestIpString = argv[i];
		}
	}
	else
		usage(argv[0]);

	if (DestIpString == NULL || DestIpString[0] == '\0')
		usage(argv[0]);

	DestIp = inet_addr(DestIpString);

	memset(&MacAddr, 0xff, sizeof (MacAddr));

	printf("ARP запрос для IP-адреса: %s\n", DestIpString);
```

```
	dwRetVal = SendARP(DestIp, SrcIp, &MacAddr, &PhysAddrLen);

	if (dwRetVal == NO_ERROR) {
		bPhysAddr = (BYTE *)& MacAddr;
		if (PhysAddrLen) {
			for (i = 0; i < (int)PhysAddrLen; i++) {
				if (i == (PhysAddrLen - 1))
					printf("%.2X\n", (int)bPhysAddr[i]);
				else
					printf("%.2X-", (int)bPhysAddr[i]);
			}
		}
		else
			printf
			("Предупреждение: ARP запрос выполнен ошибка, но ответ равен 0\n");
	}
	else {
		printf("Ошибка: Ошибка ARP запроса: %d", dwRetVal);
		switch (dwRetVal) {
		case ERROR_GEN_FAILURE:
			printf(" (ERROR_GEN_FAILURE)\n");
			break;
		case ERROR_INVALID_PARAMETER:
			printf(" (ERROR_INVALID_PARAMETER)\n");
			break;
		case ERROR_INVALID_USER_BUFFER:
			printf(" (ERROR_INVALID_USER_BUFFER)\n");
			break;
		case ERROR_BAD_NET_NAME:
			printf(" (ERROR_GEN_FAILURE)\n");
			break;
		case ERROR_BUFFER_OVERFLOW:
			printf(" (ERROR_BUFFER_OVERFLOW)\n");
			break;
		case ERROR_NOT_FOUND:
			printf(" (ERROR_NOT_FOUND)\n");
			break;
		default:
			printf("\n");
			break;
		}
	}
	return 0;
}[3]
```

Результат работы программы приведен на рис. 5.

```
C:\Users\Владимир\Documents\Visual Studio 2013\Projects\ARP\Debug>ARP.exe 192.168.1.30
ARP запрос для IP-адреса: 192.168.1.30
CC-5D-4E-63-1A-18
```

Рисунок 5. Пример работы программы

Как видно из результата, программ корректно выдает MAC-адрес на интересующий пользователя IP-адрес.

Вывод:

1. ARP-протокол, протокол разрешения адресов, является обязательным стандартом TCP/IP, описанным в документе RFC 826 «Address Resolution Protocol (ARP)». ARP разрешает IP-адреса, используемые программным обеспечением TCP/IP, в аппаратные адреса сетевых адаптеров локальной сети.

2. Несмотря на свою простоту, протокол ARP требует детального изучения его теоретических основ.
3. Программный продукт Cisco Packet Tracer 6 позволяет проводить детальное моделирование сети, в частности при проведении широковещательных рассылок по протоколу ARP.
4. Язык программирования C++ позволяет изучать компоненты сетевых хостов, используя стандартные библиотеки, по нахождению MAC-адресов через ARP-протокол.

Литература:

1. Семейка протокола ARP. – Электронный ресурс. URI: http://www.atraining.ru/arp-inarp-rarp-proxy-gratuitous-dai-sticky-and-more/ (дата обращения 08.03.2015).

2. Протокол определения адреса. - Электронный ресурс. URI: https://ru.wikipedia.org/wiki/ARP (дата обращения 08.03.2015).

3. SendARP function. - Электронный ресурс. URI: https://msdn.microsoft.com/en-us/library/windows/desktop/aa366358(v=vs.85).aspx (дата обращения 08.03.2015).

4. Сетевые технологии для дома и малого бизнеса // Курс CCNA Discovery. – Сетевая академия CISCO.

Ю.А. Фролова, А.К. Сагдеев

ТРЕБОВАНИЯ К СТРУКТУРЕ ВООРУЖЕННЫХ СИЛ В УСЛОВИЯХ ВЕДЕНИЯ СЕТЕЦЕНТРИЧЕСКИХ ВОЙН

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия

Ключевые слова: структура Вооруженных Сил, сетецентрическая война, информационная война.

В данной работе рассмотрены особенности и ограничения, которые объективно накладываются на структурную составляющую Вооруженных Сил при сетецентрическом воздействии. Описаны требования, реализация которых позволит обеспечить структурно-функциональную адаптацию войск к новым требованиям ведения войн и вооруженных конфликтов, что обеспечит достойную конкурентоспособность Вооруженных Сил Российской Федерации по сравнению с армиями других стран. Данная проблематика особенно актуальна в сложившихся геополитических условиях.

J.A. Frolova, A.K. Sagdeev

REQUIREMENTS TO THE STRUCTURE OF THE ARMED FORCES IN THE CONDUCT OF NETWORK-CENTRIC WARS

Saint-Petersburg state University of telecommunications
them. Professor M. A. Bonch-Bruevich, St. Petersburg, Russia

Key words: structure of the Armed Forces, network-centric warfare, information warfare.

In this paper the peculiarities and limitations, which, objectively, are superimposed on the structural component of the Armed Forces with net-centric effects. Describes the requirements, the implementation of which will allow structural and functional adaptation of troops to the new requirements of conducting wars and armed conflicts that will provide decent competitiveness of the Armed Forces of the Russian Federation in comparison with the armies of other countries. This issue is particularly relevant in the current geopolitical conditions.

Опыт войн XXI века свидетельствует, что вторжения строятся в два этапа. На первом этапе будут наноситься высокоточные воздушно-космические удары на всю глубину территории. В качестве целей для поражения будут выбраны жизненно важные объекты «жертвы». В западных источниках указывается, что списки первоочередных объектов поражения составляются в соответствии с концепцией «пяти колец полковника Уордена» (рис.1), которая рассматривает противника в качестве системы, состоящей из пяти радиальных колец.

В центре – политическое руководство, затем следуют система жизнеобеспечения; инфраструктура; население и, лишь в последнюю очередь вооруженные силы.

Однако известны [1-4] варианты реализации бесконтактных операций которые описываются гораздо проще. Удары наносятся по жизненно важным объектам технологического уровня (промышленность, энергетика, связь). К тому же промышленно-энергетическая система (кольцо №2) – это составляющая часть инфраструктуры (кольцо №3) любого государства и разделять их, не корректно. Чаще всего косвенно, а реже прицельно объектами воздействия являются гражданские и военные структуры (лица). Таким образом, основным объектом воздействий будет инфраструктура (кольцо №2+№3), а не политическое руководство (кольцо №1), как указывает в понятиях СВ. После некоторого порога воздействий, результатом является недовольство населения и ВС приводящее к смене политического руководства.

Рисунок 1. Схема объектов поражения по концепции «5 колец Уордена»

Вторым этапом является – наземное вторжение, которое начнется только в том случае, если оно будет признано целесообразным. Главная особенность этого этапа состоит в том, что вести классические боевые действия проводиться не будут, а будут происходить «точечные» операции. Напротив, они будут избегать вступления в прямое столкновение. Бесконтактные войны стали реальностью, имеется ряд работ отечественных ученых, посвященных данным войнам [4].

Предполагается, что концепция сетецентричности якобы обеспечит превосходство в скорости и внезапности действий. Все процессы управления и сами боевые действия должны стать более динамичными, активными и результативными. Вместо привычной формы последовательных боев и операций, военные действия приобретут форму точечных, практически мгновенных акций и ударов[2, 4]. Однако в явно выраженном виде недостаточно материала, который можно классифицировать как концепцию. В настоящее время опубликовано много спорных, разнородных и противоречивых утверждений и предположений. Существуют упоминания, что якобы разработана теория и соответствующие ей принципы сетецентрической войны, однако в доступных источниках сведения о ней в явном виде отсутствуют.

Имеющиеся взгляды на сетецентрические и информационные войны опираются на «информационное превосходство». Одним из основных способов его достижения является внесение большой доли автоматизации в процесс управления. По данным различных источников уровень автоматизации систем управления в вооруженных силах РФ состовляет порядка 20%, в вооруженных силах США порядка 80% [1-4]. Но при этом вопрос ведения противоборства именно на инфокоммунакационном пространстве рассматривается вскользь. В настоящее время, в связи с

развитием ИТКС появились новые возможности по ведению технической разведывательной деятельности и дистанционных деструктивных воздействий.

При формировании структуры Вооруженных Сил, соответствующей условиям ведения сетецентрических войн, к ней предъявляется ряд требований, реализация которых должна обеспечить достижение так называемой структурно-функциональной адаптации войск. К числу этих требований относятся следующие [1, 3-4]:

- устойчивость – способность войск эффективно выполнять все возложенные на них задачи;
- восстанавливаемость – способность войск к функционированию или восстановлению боеспособности после нанесения им поражения противником;
- оперативность – способность своевременного реагирования на изменение оперативной обстановки;
- гибкость – способность к генерированию (формированию) и реализации различных вариантов достижения цели;
- инновационность – способность к применению новых технических средств и новых способов решения задач;
- адаптивность – способность (некритичность) к изменению процессов выполнения задач и организационной структуры в соответствии с изменением концепций боевого применения войск;
- самосинхронизация.

Первые четыре требования не содержат никаких новшеств и в том или ином виде всегда предъявлялись любой военной организации или воинскому формированию. Что же касается пятого и шестого требований, то на них следует остановиться.

Инновационность в последние годы стала важнейшим принципом развития вооруженных сил передовых зарубежных стран. Особенно это характерно для армии США, которая по количеству инноваций превзошла армии всех стран мира. И это достигается не только вложением средств в создание новых типов вооружений, но и формированием условий, когда созданные новые образцы быстро включаются в состав подразделений частей и соединений армии США [2]. А это непростая задача, решение которой предполагает не только тривиальное издание приказа о принятии на вооружение нового образца, а включение его в штат того или иного воинского формирования, переработку боевых уставов и наставлений по боевому применению и техническому обеспечению войск, определению заказчика этого образца, порядка его заказа, поставки в войска, эксплуатации (включая нормы расходов всех видов ресурсов), ремонта, утилизации. Но, как полагают зарубежные специалисты, без реализации принципа инновационности надеяться на создание вооруженных сил, соответствующих требованиям новой информационной эпохи, бессмысленно.

Следующее требование «адаптивность» предполагает такое построение воинских формирований, при котором введение в их состав (исключение из состава) дополнительных подразделений или частей, изменение условий их боевого применения (например, при переброске на другой ТВД) не нарушало бы процесса прохождения информации, алгоритмы подготовки и принятия решений, управления структурными подразделениями. Это требование весьма важно с точки зрения реализации сетецентрической схемы управления войсками: любой элемент боевого построения должен иметь возможность быстро включиться в сеть или отключиться в процессе ее функционирования без отрицательных последствий для работоспособности и своей, и сети [2-4]. Говоря языком программистов, сеть должна быть способна «опознать» новое структурное подразделение и обеспечить его эффективное функционирование в составе сети. Так же точно при смене ТВД сеть должна быть способна «считывать» новые данные и адаптировать алгоритмы взаимодействия элементов сети исходя из новых условий.

Самосинхронизация – это способность частей и подразделений планировать и выполнять свои задачи там, тогда и так, где, когда и как они обеспечат наибольшую эффективность не только своих действий, но и действий обеспечиваемых ими (взаимодействующих с ними) других частей и подразделений. Следовательно, самосинхронизация – это достижение высочайшей степени взаимного согласования действий, которое можно назвать самооптимизацией. [2-3].

Для обеспечения самосинхронизации действий войск, по мнению зарубежных специалистов, необходимо[1, 4]:

- ясное и логичное формулирование замысла командования, обеспечивающее его адекватное и единое (одинаковое) восприятие войсками;
- компетентность во всех звеньях управления войсками;
- полнота доводимой до войск информации (в объеме, необходимом и достаточном для принятия ими своих решений);
- гарантированное отсутствие искажений информации в процессе ее передачи;
- наличие системы правил согласования действий частей и подразделений при подготовке и в ходе ведения боя (операции). Причем эти правила должны ориентироваться не на традиционный иерархический принцип управления, а на результат согласования задач управления взаимодействующими воинскими формированиями с учетом реально складывающейся обстановки.

Первое и второе условия самосинхронизации могут быть в значительной степени реализованы благодаря формализации (стандартизации и унификации) процессов разработки и доведения до подчиненных замысла командования. Но тем не менее за рубежом придается особое внимание повышению интеллектуальных способностей субъектов вооруженной борьбы. То есть роль человеческого фактора нисколько не уменьшается, она по-прежнему высока. Причем для этого военное руководство зарубежных стран создает систему обеспечения непрерывного профессионального роста военнослужащих, одновременно изыскивая способы повышения степени автоматизации процессов подготовки и принятия решений. То есть сетецентрическая война – это не война роботов (возможно, пока), а война интеллекта, во-первых, человеческого и, во-вторых, – тоже человеческого, но материализованного в машинных кодах.

Третье и четвертое условия самосинхронизации никакой новизны не содержат, но обращает на себя внимание, как «трепетно» идеологи сетецентрических войн относятся к качеству доводимой до войск информации. Вмешательство в этот процесс, разрушение информационных потоков – это разрушение идеи таких войн, перевод ее в состояние, поддающееся описанию уравнениями Ланчестера (упрощенно говоря – «перемалывание» силы силой). В этом слабое место идеи сетецентрических войн [1, 4]. Разрушение информационных потоков может «уравнять шансы» противоборствующих сторон. Как это сделать: уничтожить технические средства передачи данных, внести искажения в информационные тракты, поставить помехи, препятствующие приему информации.

Поэтому можно уверенно говорить, что последнее, пятое условие корректно и адекватно реализуется только при выполнении третьего и четвертого. А вот это последнее и составляет суть самосинхронизации. Оно предполагает наличие систем поддержки принятия решений, ориентированных на непрерывный мониторинг обстановки. Насколько далеко шагнули в зарубежных армиях в реализации этого условия – сказать трудно [1, 4]. В специализированной литературе, касающейся теории сетецентрических войн, практически невозможно найти описание алгоритмов автоматизированной выработки решений органами управления различного уровня (за исключением, может быть, простейших). Возможно, пока их попросту нет, поскольку крайне сложно в полном объеме формализовать мыслительный процесс командиров, когда они на основе анализа больших массивов неформализованной и слабоструктурированной информации принимают зачастую интуитивное решение.

Литература:

1. Попов И. М. Сетецентрическая война Пентагона // НВО № 9 (369), 2012.

2. Горбачев Ю.Е. Сетецентрическая война: миф или реальность? // Военная мысль. 2010.№1.

3. Раскин А. В., Пеляк В.С. К вопросу о сетевой войне // Военная мысль. 2007. № 3.

4. Демидюк А.В., Хамзатов М.М. Молниеносная война нового поколения: возможный сценарий // Военная мысль. 2014. № 10.

И.А. Шалабаева

МЕТОДИКА ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Западно-Казахстанский инженерно-гуманитарный университет, г.Уральск, Казахстан

Ключевые слова: криптография, аутентификация, цифровая подпись.

В этой статье рассмотрены инструменты защиты информации, виды обеспечения защиты информации, защита информации с помощью шифрования, в особенности расширенно рассматривалась наука криптографии, методы шифрования информации. На сегодняшний день не все знают о видах угроз в компьютерных сетях, о методах защиты от них, об обеспечении защиты информации.

I.A. Shalabaeva

THE METHODS OF PROTECTING THE INFORMATION ON THE WIRELESS NETS

West-Kazakhstan engineering-humanitarian University, Uralsk

Key words: cryptography, authorization, digital signature

In this report it is discussed the instruments of protecting the information, the types of providing the protection of the information, protecting the using the crypto operation, particularly it is considered the science of cryptography, and methods of crypto operating of information. Today not everyone knows the types of danger in nets of computers, about the methods of protection, how to provide the protection of the information.

Вопрос защиты информации поднимается уже с тех пор, как только люди научились письменной грамоте. Всегда существовала информацию, которую должны знать не все. Люди, обладающие такой информацией, прибегали к разным способам ее защиты. Из известных примеров это такие способы как тайнопись (письмо симпатическими чернилами), шифрование («тарабарская грамота», шифр Цезаря, более совершенные шифры замены, подстановки). В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, а также контроля и управления различными объектами. К таким объектам (их называют критическими) можно отнести системы телекоммуникаций, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, а также системы обработки и хранения секретной и конфиденциальной информации [1].

В последнее время вырос интерес к вопросам защиты информации. Это связывают с тем, что стали более широко использоваться вычислительные сети, что приводит к тому, что появляются большие возможности для несанкционированного доступа к передаваемой информации.

В литературе выделяют различные способы защиты информации среди них выделим:

- физические (препятствие);
- законодательные;
- управление доступом;
- криптографическое закрытие.

Как будет показано ниже, наиболее эффективными являются криптографические способы защиты информации.

Криптография в переводе с древнегреческого означает "тайнопись". Суть ее заключается в том, что последовательность символов (открытый текст) подвергается некоторому преобразованию (в котором используется ключ) и в результате получается закрытый текст, непонятный тому, кто не знает алгоритма шифрования и, конечно, ключа [3].

Для преобразования (шифрования) обычно используется некоторый алгоритм или устройство, реализующее заданный алгоритм, которые могут быть известны

широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет просто и надёжно расшифровать текст. Однако без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования. Даже простое преобразование информации является весьма эффективным средством, дающим возможность скрыть её смысл от большинства неквалифицированных нарушителей.

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения ПЭВМ резко повышают уязвимость информации. Основными факторами, способствующими повышению этой уязвимости, являются :

- резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;
- усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение мультипрограммного режима, а также режима разделения времени;
- автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

Защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются технические, организационные и правовые.

Обеспечение безопасности информации — дорогое дело, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Развитие информационных технологий ставит актуальные задачи повышения надежности функционирования компьютерных сетей. Для решения таких задач необходимы исследования существующих сетевых протоколов, сетевых архитектур, разработка способов повышения безопасности при передаче информационных ресурсов по сети.

Выбор в пользу беспроводных технологий позволяет получить преимущества в скорости, мобильности. Появление нового класса широкополосных беспроводных сетей с ячеистой структурой (меш-сети) позволило достичь значительного увеличения зоны информационного покрытия. Основным достоинством данного класса сетей является наличие особых устройств — меш-порталов, позволяющих интегрировать в меш-сеть другие беспроводные сети (WiMAX, Wi-Fi, GSM) и Интернет, а значит, и предоставить пользователю всевозможные сервисы этих сетей [2].

К недостаткам меш-технологии можно отнести тот факт, что протоколы маршрутизации меш-сети весьма специфичны, а их разработка — сложная задача с множеством критериев и параметров. При этом существующие протоколы требуют значительных доработок в вопросах повышения безопасности и надежности передачи информации.

Сетевые атаки, сбои и отказы сетевого оборудования — основные факторы, влияющие на безопасность передачи информации в распределенных беспроводных сетях. Проблемой обеспечения безопасности передачи информации в распределенных беспроводных сетях занимались I. Akyildiz, W.Wang, X.Wang, T. Dorges, N. Ben Salem. Под обеспечением безопасности передачи информации в компьютерной сети понимается защита ее конфиденциальности, целостности и доступности.

Среди методов обеспечения доступности информации в беспроводных сетях исследователями выделяется комбинирование различных методов контроля, дублирования, резервирования. Целостность и конфиденциальность информации в беспроводных сетях обеспечивается методами построения виртуальных каналов, основанных на применении криптографических инструментов [4].

Общий недостаток данных методов - снижение производительности сети, связанное с требованиями к дополнительной обработке передаваемой информации. Указанный недостаток особенно критичен для передачи цифровой видеоинформации. Кроме того, совершенствование методов криптоанализа все более снижает надежность существующих криптоалгоритмов.

Из вышесказанного следует вывод о необходимости разработки новых способов защиты информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак.

Литература:

1. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. — СПб.: БХВ— Петербург, 2000. 384 с.

2. Барнс К. Защита от хакеров беспроводных сетей / К. Барнс, Т. Боутс, Д. Лойд М.: ДМК-Пресс, 2005. - 480с.

3. Белоусов С.А. Троянские кони: принципы работы и методы защиты / С.А. Белоусов, А.К. Гуц, М.С. Планков — Омск, 2003. 83 с.

4. Взлом беспроводных сетей: электронный журнал Hack Zone Электронный ресурс. — Режим доступа: http://www.fssr.ru/hz.php?name=News&file=article&sid=7273, свободный.

КРАТКИЕ СВЕДЕНИЯ ОБ АВТОРАХ

1. **Абдумаликов Акмал Абдухоликович**, магистрант кафедры «Информационная безопасность», Ташкентский университет информационных технологий;
2. **Абрамов Анатолий Константинович**, к.т.н., доцент, Академия Федеральной службы охраны Российской Федерации;
3. **Абрамов Денис Владимирович**, ЗАО «Русская Телефонная Компания»;
4. **Абрамов Ярослав Борисович**, ассистент, СКФ МТУСИ;
5. **Агафонов Александр Анатольевич**, магистр, Северо-Кавказский федеральный университет;
6. **Агафонова Александра Сергеевна**, курсант, Уральский юридический институт МВД России;
7. **Агеев Виталий Валериевич**, студент, СКФ МТУСИ;
8. **Аджемов Артем Сергеевич**, д.т.н., профессор, ректор МТУСИ;
9. **Александров Павел Александрович**, студент, Академия Федеральной службы охраны Российской Федерации;
10. **Алимова Фотима Муратовна**, студент, Ташкентский университет информационных технологии;
11. **Аль-Аззави Эсса Мохаммед**, аспирант, Одесская национальная академия связи им. А.С. Попова;
12. **Амирсаидов Улугбек Бобурович**, к.т.н., Ташкентский университет информационных технологий;
13. **Анисимов Дмитрий Анатольевич**, студент, СКФ МТУСИ;
14. **Антонов Данил Евгеньевич**, студент, ЮФУ;
15. **Арипов Хайрулла Кабилович**, профессор, ф-м.д.н., Ташкентский университет информационных технологий;
16. **Арипова Умида Хайруллаевна**, старший преподаватель, Ташкентский университет информационных технологий;
17. **Арус Кинан**, аспирант, Харьковский национальный университет радиоэлектроники;
18. **Ашихина Анастасия Валерьевна**, студентка, Северо-Кавказский федеральный университет;
19. **Бабатаев Бекзод Бахтиёрович**, магистрант кафедры «Информационная безопасность», Ташкентский университет информационных технологий;
20. **Баранова Наталья Николаевна**, аспирантка, Ульяновский государственный технический университет;
21. **Басов Олег Олегович**, докторант, к.т.н., Академия Федеральной службы охраны Российской Федерации;
22. **Баталов Алексей Эдуардович**, аспирант, МТУСИ;
23. **Батенков Кирилл Александрович**, сотрудник, Академия Федеральной службы охраны Российской Федерации;
24. **Белан Надежда Викторовна**, студент, Северо-Кавказский федеральный университет;
25. **Беленький Павел Павлович**, к.п.н., доцент, директор СКФ МТУСИ;
26. **Белянко Михаил Алексеевич**, студент, МТУСИ;
27. **Белянский Владимир Борисович**, к. ф-м. н., МТУСИ;
28. **Бережной Сергей Александрович**, студент, ДГТУ;
29. **Бесчетная Снежана Владимировна**, к.э.н., ст. преподаватель, СКФ МТУСИ;
30. **Бинеев Энвер Абдулхакович**, профессор, к.х.н., СКФ МТУСИ;

31. **Болдырихин Николай Вячеславович**, доцент каф. СССК, СКФ МТУСИ;
32. **Борисов Борис Петрович**, к.т.н., доцент, СКФ МТУСИ;
33. **Боровков Никита Вячеславович**, курсант, Уральский юридический институт МВД России;
34. **Бородин Алексей Викторович**, к.ф.-м.н., доцент, СКФ МТУСИ;
35. **Боярчук Андрей Эдуардович**, к.т.н., профессор, профессор кафедры «Кибербезопасность информационных систем», ДГТУ;
36. **Буйдинов Евгений Владимирович**, заместитель Генерального директора ГПКС по инновационному развитию;
37. **Булатов Виктор Владимирович**, студент, СКФ МТУСИ;
38. **Бумагина Юлиана Андреевна**, студент, СКФ МТУСИ;
39. **Бурдюг Владислав Владимирович**, курсант, ВУНЦ ВВС «ВВА»;
40. **Буренин Андрей Николаевич**, главный специалист, кандидат технических наук, доцент, ОАО НИИ «Рубин»;
41. **Бурмистров Владимир Александрович**, аспирант, Северо-Кавказский федеральный университет;
42. **Быкадоров Родион Витальевич**, студент, ЮФУ;
43. **Быстров Сергей Александрович**, аспирант, магистр в области телекоммуникации и технологии, УрТИСИ;
44. **Вайтеховская Алена Владимировна**, студент, СКФ МТУСИ;
45. **Вакказова Алсу Наильевна**, соискатель кафедры МСИБ, ПГУТИ;
46. **Варисов Акмал Аббасович**, докторант, ассистент, Ташкентский университет информационных технологий;
47. **Вартанян Артур Суренович**, соискатель, ВУНЦ ВВС «ВВА»;
48. **Васечкин Евгений Александрович**, адъюнкт, Академия Федеральной службы охраны Российской Федерации;
49. **Васильев Виктор Афанасьевич**, главный специалист, к.т.н., доцент, ОАО НИИ «Рубин»;
50. **Васильева Зинаида Анатольевна**, студент, СКФ МТУСИ;
51. **Верховцев Александр Юрьевич**, студент, УрТИСИ ФГОБУ ВПО «СибГУТИ»;
52. **Виржанский Александр Сергеевич**, студент, Ростовский Государственный Экономический Университет (РИНХ)
53. **Власенко Елена Сергеевна**, аспирантка кафедры инфокоммуникационных систем, СПбГУТ им. проф. Бонч-Бруевича;
54. **Власюк Игорь Викторович**, к.т.н., МТУСИ;
55. **Волгарев Евгений Алексеевич**, аспирант, Уральский технический институт связи и информатики;
56. **Волобуева Александра Андреевна**, магистрант, Северо-Кавказский федеральный университет;
57. **Воронин Дмитрий Александрович**, курсант, Уральский юридический институт МВД России;
58. **Гаврилкина Марианна Геннадьевна**, ассистент кафедры экономики связи, МТУСИ;
59. **Гавришев Алексей Андреевич**, аспирант, Северо-Кавказский федеральный университет;
60. **Гаипназаров Рустам Тахритдинович**, ассистент кафедры «Информационные технологии», Ташкентский университет информационных технологий;

61. **Гаркуша Елена Владимировна**, старший преподаватель каф. документоведения и информационной деятельности в экономических системах, к.т.н. Полтавский университет экономики и торговли;
62. **Гаркуша Сергей Владимирович**, доцент каф. документоведения и информационной деятельности в экономических системах, д.т.н., доцент, Полтавский университет экономики и торговли;
63. **Гафуржанова Нодыра Фозыловна**, магистрант, Ташкентский университет информационных технологий;
64. **Гахов Кирилл Юрьевич**, аспирант кафедры экономики связи, МТУСИ;
65. **Герасименко Виктор Евгеньевич**, студент, СКФ МТУСИ;
66. **Гизатуллин Марат Галимянович**, доцент кафедры информационного обеспечения органов внутренних дел, к.т.н., доцент, Уральский юридический институт МВД России;
67. **Гладков Денис Эдуардович**, студент, Академия Федеральной службы охраны Российской Федерации;
68. **Глух Елена Григорьевна**, ст. преподаватель каф. ЭиУ, СКФ МТУСИ;
69. **Глушак Елена Владимировна**, к.т.н., инженер кафедры автоматической электросвязи, ПГУТИ;
70. **Головина Ирина Витальевна**, к.э.н., доцент кафедры ЭиУ, СКФ МТУСИ;
71. **Головской Василий Андреевич**, старший научный сотрудник научно-технического отдела, к.т.н., Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации;
72. **Голубев Альберт Константинович**, профессор, к.т.н., профессор кафедры экономики предприятия и корпоративного управления, Одесская национальная академия связи им. А.С. Попова;
73. **Гончарова Оксана Владимировна**, к.э.н., СКФ МТУСИ;
74. **Гопанчук Дмитрий Эдуардович**, студент, СКФ МТУСИ;
75. **Горбачева Мария Анатольевна**, студент, СПбГУТ им. проф. Бонч-Бруевича;
76. **Григорьев Вадим Алексеевич**, студент, РГЭУ;
77. **Григорьев Илья Дмитриевич**, студент, МТУСИ;
78. **Гуриков Сергей Ростиславович**, к.п.н., доцент кафедры Информатика, МТУСИ;
79. **Гуров Владимир Владимирович**, студент, МТУСИ;
80. **Гусаров Артем Андреевич**, студент, Ростовский Государственный Экономический Университет (РИНХ);
81. **Гусева Елена Сергеевна**, студент, СКФ МТУСИ;
82. **Гусева Людмила Леонидовна**, доцент, к.т.н., доцент, Институт информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет;
83. **Гусишная Светлана Вячеславовна**, студент, СКФ МТУСИ;
84. **Давронова Лола Уктамовна**, ассистент кафедры «Информационная безопасность», Ташкентский университет информационных технологий;
85. **Данилов Виктор Александрович**, профессор кафедры СПОИ, д.т.н., СКФ МТУСИ;
86. **Данилова Анастасия Михайловна**, бакалавр, Ташкентский университет информационных технологий;
87. **Данилова Екатерина Михайловна**, магистр, Ташкентский университет информационных технологий;
88. **Данилова Людмила Викторовна**, доцент, к.ф-м.н., доцент кафедры высшей математики, ФГБОУ ВПО РГУПС;

89. **Данилова Наталья Викторовна**, к.ф-м.н., доцент кафедры высшей математики и исследования операций института математики, механики и компьютерных наук, ЮФУ;
90. **Дели Марина Степановна**, студентка, Одесская национальная академия связи им. А.С. Попова;
91. **Демидов Дмитрий Евгеньевич**, студент, Сибирский государственный университет телекоммуникаций и информатики;
92. **Дерещук Дмитрий Олегович**, студент, СКФ МТУСИ;
93. **Джамбеков Азамат Матифулаевич**, ФГБОУ ВПО Астраханский государственный технический университет;
94. **Дмитриев Владимир Александрович**, студент, СКФ МТУСИ;
95. **Дмитриев Максим Игоревич**, студент, ДГТУ;
96. **Долбня Владимир Сергеевич**, магистрант, Белгородский государственный национальный исследовательский университет;
97. **Долгополова Ольга Владимировна**, студент, СКФ МТУСИ;
98. **Дорошкевич Виктор Александрович**, студент, ЮФУ;
99. **Дунаев Валерий Александрович**, преподаватель, Академия Федеральной службы охраны Российской Федерации;
100. **Дымченко Антон Алексеевич**, студент, ДГТУ;
101. **Евдакова Лилия Николаевна**, к.э.н., доцент, зав. кафедрой Экономики связи, Сибирский государственный университет телекоммуникаций и информатики;
102. **Евсеева Оксана Юрьевна**, д.т.н., доц., проф. кафедры телекоммуникационных систем, Харьковский национальный университет радиоэлектроники;
103. **Евсеева Оксана Юрьевна**, д.т.н., доц., проф. кафедры ТКС, Харьковский национальный университет радиоэлектроники;
104. **Егоров Дмитрий Аркадьевич**, студент, МТУСИ;
105. **Егорова Ольга**, студент, СКФ МТУСИ;
106. **Екатериновский Владислав Сергеевич**, студент, СКФ МТУСИ;
107. **Елфимов Михаил Андреевич**, студент, ДГТУ;
108. **Енгибарян Ирина Алешаевна**, к.т.н., доцент каф «МТС», СКФ МТУСИ;
109. **Еремеев Артем Вадимович**, студент, ЮФУ;
110. **Еремеева Евгения Вячеславовна**, студент, магистр, Донецкий национальный технический университет;
111. **Еременко Александра Сергеевна**, к.т.н., снс., доц. каф. ТКС, Харьковский национальный университет радиоэлектроники;
112. **Ерохин Антон Викторович**, студент, Ростовский Государственный Экономический Университет (РИНХ);
113. **Жабинский Юрий Владиславович**, к.т.н., доцент, СКФ МТУСИ;
114. **Жилина Елена Викторовна**, к.э.н., доцент каф. Информационных технологий и защиты информации, Ростовский государственный экономический университет (РИНХ);
115. **Жильцов Дмитрий Викторович**, студент, СКФ МТУСИ;
116. **Жук Александр Павлович**, профессор, к.т.н., профессор кафедры Организации и технологии защиты информации, Северо-Кавказский федеральный университет;
117. **Заварыкина Юлия Валерьевна**, преподаватель кафедры информационного обеспечения органов внутренних дел, Уральский юридический институт МВД России;
118. **Зайнидинов Хакимджан Насритдинович**, д.т.н., профессор, Ташкентский университет информационных технологии;

119. **Запорожцев Артем Александрович**, студент, Ростовский Государственный Экономический Университет (РИНХ);
120. **Зарецкая Мария Сергеевна**, студент, ПГУТИ;
121. **Захарин Серафим**, слушатель Малой академии наук города Ставрополя;
122. **Звездина Марина Юрьевна**, д.ф.-м.н., доцент, зав. кафедрой «Радиоэлектроника», ДГТУ;
123. **Зверев Алексей Петрович**, доцент, Академии ГЗ МЧС;
124. **Земляков Вячеслав Викторович**, к.ф.-м..н., доцент, доцент кафедры, ЮФУ;
125. **Знаменский Дмитрий Андреевич**, студент, ЮФУ;
126. **Зуев Алексей Валерьевич**, аспирант 1-го года обучения, ПГУТИ;
127. **Зызыкалов Сергей Александрович**, студент, СКФ МТУСИ;
128. **Иванов Иван Николаевич**, аспирант кафедры экономики связи, МТУСИ;
129. **Иванов Станислав Валерьевич**, к.т.н., доцент кафедры «Автоматизация производственных процессов», ДГТУ;
130. **Иващук Ольга Александровна**, д.т.н., профессор кафедры информационных систем управления, Белгородский государственный национальный исследовательский университет;
131. **Иевлева Анастасия Александровна**, студент, СКФ МТУСИ;
132. **Ильиных Нина Иосифовна**, к.ф.-м.н., доцент кафедры ВМиФ, Уральский технический институт связи и информатики;
133. **Ильяшенко Евгений Николаевич**, соискатель, Харьковский национальный университет радиоэлектроники;
134. **Иргашева Дурдона Якубджановна**, к.т.н., заведующая кафедрой «Информационная безопасность», Ташкентский университет информационных технологий;
135. **Кадурина Анастасия Сергеевна**, магистрант, Северо-Кавказский федеральный университет;
136. **Казаков Константин Петрович**, студент, ПГУТИ;
137. **Каковкин Александр Сергеевич**, аспирант, Сибирский государственный университет телекоммуникаций и информатики;
138. **Калинин Роман Николаевич**, аспирант, Академия Федеральной службы охраны Российской Федерации;
139. **Калмыков Игорь Анатольевич**, профессор, д.т.н., Северо-Кавказский федеральный университет;
140. **Калмыкова Яна Олеговна**, курсант, Уральский юридический институт МВД России;
141. **Каримова Венера Аркиновна**, к.т.н, заведующая кафедрой «Информационные технологии», Ташкентский университет информационных технологий;
142. **Карпенко Юрий Александрович**, студент, ДГТУ;
143. **Касьяненко Наталья Георгиевна**, к.т.н., доцент, доцент кафедры прикладной информатики и дизайна, Северо-Кавказский гуманитарно-технический институт;
144. **Ковалев Евгений Иванович**, доцент, к.т.н., доцент УрФУ;
145. **Ковбель Александр Александрович**, аспирант, Сибирский государственный университет телекоммуникаций и информатики;
146. **Козачок Александр Иванович**, доцент, к.п.н., Академия Федеральной службы охраны Российской Федерации;
147. **Колдынская Лариса Михайловна**, ст. преп., СКФ МТУСИ;
148. **Конкин Борис Борисович**, к.ф.-м.н., доцент, заведующий кафедрой ОНП, СКФ МТУСИ;

149. **Коновальчук Евгений Викторович**, к.т.н., доцент, полковник, начальник факультета, ВУНЦ ВВС «ВВА»;
150. **Константинова Яна Борисовна**, к.ф.-м.н., доцент, СКФ МТУСИ;
151. **Кормильченко Валентина Васильевна**, КЭИУ, к.с.н., доцент, СКФ МТУСИ;
152. **Корниенко Роман Сергеевич**, студент, Институт информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет;
153. **Корниенко Сергей Александрович**, к.т.н., доцент кафедры информационная безопасность автоматизированных систем, Институт информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет;
154. **Корчагин Мстислав Сергеевич**, студент 2-го курса, СПбГУТ им. проф. М.А. Бонч-Бруевича, Институт военного образования, учебный военный центр;
155. **Косачева Светлана Витальевна**, ст. преподаватель, СКФ МТУСИ;
156. **Косиченко Виталий Олегович**, студент, СКФ МТУСИ;
157. **Костюченко Константин Леонидович**, к.т.н., доцент, доцент кафедры информационного обеспечения органов внутренних дел, Уральский юридический институт МВД России;
158. **Котельницкая Любовь Ивановна**, к.т.н., РЭУ им. Плеханова;
159. **Котов Андрей Валерьевич**, студент, Северо-Кавказский федеральный университет;
160. **Кочетков Вячеслав Анатольевич**, к.т.н., доцент, Академия Федеральной службы охраны Российской Федерации;
161. **Крамар Екатерина Владимировна**, бухгалтер, Новошахтинский почтамт УФПС Ростовской области;
162. **Крымов Сергей Михайлович**, д.э.н., профессор, профессор каф. Экономики и управления, СКФ МТУСИ;
163. **Крюкова Анастасия Александровна**, к.э.н., доцент кафедры Электронной коммерции, ПГУТИ;
164. **Кубегенов Ерлан Сагингалиевич**, студент, Западно-Казахстанский инженерно-гуманитарный университет;
165. **Кузнецова Дарья Павловна**, магистрант, Белгородский государственный национальный исследовательский университет;
166. **Кузовков Александр Дмитриевич**, аспирант кафедры экономики связи, МТУСИ;
167. **Кузовкова Татьяна Алексеевна**, д.э.н., профессор, декан ФЭУ, МТУСИ;
168. **Кутукова Валерия Дмитриевна**, студент, ДГТУ;
169. **Кучук Герман Германович**, Академия Федеральной службы охраны Российской Федерации;
170. **Лабунько Олег Степанович**, к.ф.-м.н., доцент МТУСИ, директор филиала федерального государственного унитарного предприятия «Радиочастотный центр Центрального федерального округа» в Южном и Северо-Кавказском федеральных округах;
171. **Лагунков Олег Александрович**, аспирант, Ульяновский Государственный Технический Университет;
172. **Лазарева Оксана Владимировна**, к.филос.н., Центр развития детских и молодежных социальных инициатив, методист, МБОУ ДОД Дворец творчества детей и молодежи;
173. **Лебеденко Дмитрий Михайлович**, аспирант, Донецкий национальный технический университет;

174. **Лебеденко Евгений Викторович**, к.т.н., профессор кафедры, Академия Федеральной службы охраны Российской Федерации;
175. **Легков Константин Евгеньевич**, заместитель начальника, к.т.н., ОАО НИИ «Рубин»;
176. **Ледянкин Иван Александрович**, старший преподаватель, к.т.н., ОАО НИИ «Рубин»;
177. **Лемешко Александр Витальевич**, д.т.н., профессор, профессор кафедры ТКС, Харьковский национальный университет радиоэлектроники;
178. **Леонов Алексей Викторович**, соискатель, Омский государственный технический университет;
179. **Лесничий Андрей Владимирович**, соискатель, Академия Федеральной службы охраны Российской Федерации;
180. **Литвинов Сергей Михайлович**, студент, СКФ МТУСИ;
181. **Литвинова Ирина Николаевна**, доцент каф. ЭиУ, СКФ МТУСИ;
182. **Луганская Людмила Алексеевна**, аспирант, Северо-Кавказский федеральный университет;
183. **Лугарь Марина Сергеевна**, магистрант, Белгородский государственный национальный исследовательский университет;
184. **Лутцев Антон Владимирович**, инженер, СКФ МТУСИ;
185. **Лысак Антон Александрович**, студент, ДГТУ;
186. **Лысенко Алексей Алексеевич**, бакалавр, Северо-Кавказский федеральный университет;
187. **Львов Владимир Леонтьевич**, ассистент, СКФ МТУСИ;
188. **Любухин Алексей Сергеевич**, студент, Ростовский государственный экономический университет (РИНХ);
189. **Лялина Марина Павловна**, аспирантка, МТУСИ;
190. **Ляхов Алексей Владимирович**, ассистент кафедры информационной безопасности автоматизированных систем, Северо-Кавказский федеральный университет;
191. **Макарова Алена Васильевна**, аспирант, Северо-Кавказский федеральный университет;
192. **Максименкова Анжела Руслановна**, студент, ЮФУ;
193. **Малкова Ирина Андреевна**, Уральский технический институт связи и информатики;
194. **Мамараджабов Мирсалим Элмирзаевич**, к.п.н., доцент, зав.каф. «Информатики и методики ее преподавания», Ташкентский государственный педагогический университет;
195. **Мамлин Сергей Александрович**, аспирант, МТУСИ;
196. **Манин Александр Анатолиевич**, к.т.н., зав. кафедрой СССР, СКФ МТУСИ;
197. **Маргарита Георгиевна Битадзе**, студентка, Ростовский государственный экономический университет (РИНХ);
198. **Мариносян Эмиль Хачатурович**, аспирант, МТУСИ;
199. **Махаматова Зулфия Комилжоновна**, научный исследователь, Ташкентский государственный педагогический университет;
200. **Меерович Владимир Давидович**, аспирант, СКФ МТУСИ;
201. **Межуев Александр Михайлович**, к.т.н., доцент, полковник, начальник кафедры, ВУНЦ ВВС «ВВА»;
202. **Мизонова Надежда Владимировна** ,студент, СКФ МТУСИ;
203. **Милютин Дмитрий Сергеевич**, курсант, Уральский юридический институт МВД России;

204. **Мирзахмедов Хуршид Абдирашидович**, преподаватель, Наманганский Государственный университет;
205. **Миронов Олег Юрьевич**, Академия Федеральной службы охраны Российской Федерации;
206. **Мозоль Александр Анатольевич**, младший научный сотрудник научно-технического отдела, к.т.н., Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации;
207. **Молоковский Игорь Алексеевич**, к.т.н., доцент, преподаватель, Донецкий национальный технический университет;
208. **Молчанова Яна Владимировна**, студент, Институт высоких технологий и пьезотехники, ЮФУ;
209. **Момот Александр Иванович**, д.э.н., профессор, профессор кафедры, ЭиУ СКФ МТУСИ;
210. **Момот Роман Александрович**, студент, Ростовский государственный экономический университет (РИНХ);
211. **Мухаммадиева Феруза Ишназаровна**, соискатель, Ташкентский государственный педагогический университет;
212. **Мухачев Сергей Валентинович**, к.ф-м.н., доцент, начальник кафедры информационного обеспечения органов внутренних дел, Уральский юридический институт МВД России;
213. **Назирова Элмира Шодмановна**, к.т.н., Ташкентский университет информационных технологии;
214. **Науменко Даниил Олегович**, аспирант 2 года обучения, Северо-Кавказский федеральный университет;
215. **Нашвандова Гулрухсор Муродовна**, студент, Ташкентский Государственный технический университет;
216. **Невзорова Елена Сергеевна**, инженер-исследователь, Харьковский национальный университет радиоэлектроники;
217. **Негодин Дмитрий Валерьевич**, преподаватель, ОАО НИИ «Рубин»;
218. **Немчицкий Эдуард Александрович**, студент, СКФ МТУСИ;
219. **Нестеренко Олег Евгеньевич**, адъюнкт, ОАО НИИ «Рубин»;
220. **Новикова Ольга Александровна**, студентка, ст. лаборант, СКФ МТУСИ;
221. **Новичков Серафим Алексеевич**, студент-магистратуры, бакалавр, МТУСИ;
222. **Оганесян Наталья Сергевна**, студентка, Одесская национальная академия связи им. А.С. Попова;
223. **Орлов Владимир Георгиевич**, к.т.н., МТУСИ;
224. **Орлова Анна Юрьевна**, к.э.н., доцент кафедры прикладной информатики, Северо-Кавказский федеральный университет;
225. **Орлова Анна Юрьевна**, к.э.н., доцент кафедры прикладной информатики, Московский государственный университет приборостроения и информатики, Ставропольский филиал;
226. **Осия Дмитрий Леонидович**, аспирант, МТУСИ;
227. **Павлов Андрей Николаевич**, д.ф-м.н., профессор, Зав. кафедрой ЭБЖиЭ, МТУСИ;
228. **Палютина Галия Наилевна**, студентка, Ростовский Государственный Экономический Университет РГЭУ (РИНХ);
229. **Папасов Глеб Константинович**, студент, СКФ МТУСИ;

230. **Паринова Ирина Романовна**, студент, СКФ МТУСИ;
231. **Пархоменко Павел Алексеевич**, студент, ДГТУ;
232. **Парышев Василий Витальевич**, студент, Ростовский государственный экономический университет (РИНХ);
233. **Пашинцев Владимир Петрович**, д.т.н., профессор, профессор кафедры информационной безопасности автоматизированных систем, Северо-Кавказский федеральный университет;
234. **Петренко Вячеслав Иванович**, к.т.н., доцент, заведующий кафедрой организации и технологии защиты информации, Северо-Кавказский федеральный университет;
235. **Плёнкин Антон Павлович**, аспирант, Институт компьютерных технологий и информационной безопасности (ИКТИБ) Южного федерального университета (ЮФУ);
236. **Пляскин Кирилл Валерьевич** .студент, ДГТУ;
237. **Подболотова Алена Геннадиевна**, студент, СКФ МТУСИ;
238. **Поддубная Наталья Александровна**, к.ф-м.н., доцент, доцент кафедры Информатика, Северо-Кавказский федеральный университет;
239. **Позднякова Александра Владимировна**, студент, ДГТУ;
240. **Полванова Наталья Александровна**, студент, СПбГУТ им. проф. Бонч-Бруевича;
241. **Половинчук Николай Яковлевич**,, к.т.н., профессор, профессор кафедры «Авиационные электросистемы и пилотажно-навигационные комплексы» Ростовский филиал МГТУ ГА;
242. **Полоскин Александр Владимирович**, сотрудник, Академия Федеральной службы охраны Российской Федерации;
243. **Пономарева Татьяна Владимировна**, студент, СКФ МТУСИ;
244. **Попандопуло Дмитрий Валерьевич**, к.ю.н., Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова;
245. **Попандопуло Иван Дмитриевич**, аспирант, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова;
246. **Портнов Эдуард Львович**, д.т.н., профессор, заведующий кафедрой НТС, МТУСИ;
247. **Пронина Евгения Дмитриевна**, аспирантка, МТУСИ;
248. **Прысь Виктория Александровна**, студент, магистр, Донецкий национальный технический университет;
249. **Пшеничников Анатолий Павлович**, к.т.н., профессор, зав. кафедрой ССиСК, МТУСИ;
250. **Рахманов Умид Юнусович**, магистрант кафедры «Информационная безопасность», Ташкентский университет информационных технологий;
251. **Резников Николай Сергеевич**, студент, СКФ МТУСИ;
252. **Резниченко Надежда Александровна**, студент, ДГТУ;
253. **Репинский Владимир Николаевич**, профессор, к.т.н., доцент, МТУСИ;
254. **Решетникова Ирина Витальевна**, к.т.н, доцент, СКФ МТУСИ;
255. **Родзевич Антон Игоревич**, сержант, командир учебной группы, ВУНЦ ВВС «ВВА»;
256. **Родионов Александр Сергеевич**, к.т.н., доцент каф. СПОИ, СКФ МТУСИ;
257. **Родякин Павел Александрович**, студент, СКФ МТУСИ;
258. **Рожин Сергей Николаевич**, студент, СКФ МТУСИ;
259. **Роза Андрей Николаевич**, адъюнкт, подполковник, ВУНЦ ВВС «ВВА»;
260. **Ромашкин Данил Олегович**, студент, Ростовский Государственный Экономический Университет (РИНХ);

261. **Руденко Николай Валерьевич**, доцент, к.т.н., доцент кафедры «Радиоэлектроника» ДГТУ;
262. **Румянцев Константин Евгеньевич**, заведующий кафедрой ИБТКС, д.т.н., профессор, Институт компьютерных технологий и информационной безопасности (ИКТИБ) Южного федерального университета (ЮФУ);
263. **Русанов Роман Игоревич**, студент, ДГТУ;
264. **Рыбалко Игорь Петрович**, доцент каф. СССК, СКФ МТУСИ;
265. **Сагдеев Александр Константинович**, к.т.н., преподаватель учебного военного центра Института военного образования, СПбГУТ им. проф. М.А. Бонч-Бруевича;
266. **Саламан Андрей Сергеевич**, студент, МТУСИ;
267. **Салютина Татьяна Юрьевна**, д.э.н., профессор, зав. кафедрой экономики связи, МТУСИ;
268. **Самаке Киндиа**, аспирант кафедры ИБиА, МТУСИ;
269. **Самсонов Денис Андреевич**, студент, СКФ МТУСИ;
270. **Саркисов Артём Брониславович**, аспирант кафедры «Информационная безопасность автоматизированных систем», Северо-Кавказский Федеральный Университет;
271. **Саттарова Ёкутой Юсуфовна**, преподаватель информатики, Ташкентский институт инженеров железнодорожного транспорта;
272. **Светлана Викторовна Гусишная**, студент, СКФ МТУСИ;
273. **Светличная Наталия Олеговна**, к.ф.н., доцент каф. ОНП, СКФ МТУСИ;
274. **Семеняка Максим Викторович**, аспирант, Харьковский национальный университет радиоэлектроники;
275. **Сергей Дмитриевич Ерохин**, к.т.н., доцент, декан факультета ИТ, МТУСИ;
276. **Сечко Татьяна Евгеньевна**, студент, ДГТУ;
277. **Сидоренко Евгений Николаевич**, старший преподаватель, СПбГУТ им. проф. М.А. Бонч-Бруевича, Институт военного образования, учебный военный центр;
278. **Сидоров Владислав Олегович**, студент, ДГТУ;
279. **Синева Ирина Сергеевна**, к.ф.-м.н., доцент, профессор МТУСИ;
280. **Смирнов Даниил Андреевич**, ефрейтор, старший оператор роты (научной), ВУНЦ ВВС «ВВА»;
281. **Смоляков Виктор Николаевич**, к.т.н., доцент, доцент кафедры СПОИ, СКФ
282. **Соболев Юрий Владимирович**, старший преподаватель, ПГУТИ;
283. **Сосновский Иван Александрович**, к.т.н., доцент каф. СССК, СКФ МТУСИ;
284. **Степанов Михаил Сергеевич**, аспирант кафедры ССиСК, МТУСИ;
285. **Стрий Любовь Алексеевна**, профессор, д.э.н., профессор кафедры менеджмента и маркетинга, Одесская национальная академия связи им. А.С. Попова;
286. **Стромин Александр Сергеевич**, студент, Северо-Кавказский федеральный университет;
287. **Струев Дмитрий Александрович**, адъюнкт, Академия Федеральной службы охраны Российской Федерации;
288. **Суворов Александр Борисович**, к.т.н., доцент, начальник НИО, СКФ МТУСИ;
289. **Суворова Татьяна Виссарионовна**, д.ф-м.н., профессор, РГУПС;
290. **Судаков Станислав Андреевич**, студент, ЮФУ;
291. **Сукиязов Александр Гургенович**, к.т.н., профессор, профессор кафедры «Радиоэлектроника», ДГТУ;
292. **Сулейманов Алмаз Авхатович**, аспирант, МТУСИ;

293. **Сулейманов Руслан Надирович**, студент, ДГТУ;
294. **Сущенко Михаил Иванович**, доцент, к.т.н., СКФ МТУСИ;
295. **Таджиев Нажмиддин Саидахматович**, магистрант кафедры «Информационная безопасность», Ташкентский университет информационных технологий;
296. **Тарасов Евгений Сергеевич**, старший преподаватель кафедры ОПД ТС, УрТИСИ ФГОБУ ВПО «СибГУТИ»;
297. **Тарики Надия**, аспирант, Харьковский национальный университет радиоэлектроники;
298. Ташев Камил Ахматович, к.т.н., декан факультета «Компьютерный инжиниринг», Ташкентский университет информационных технологий;
299. **Твердов Антон Павлович**, студент, СКФ МТУСИ;
300. **Терехова Юлия Сергеевна**, старший преподаватель кафедры экономики связи, МТУСИ
301. **Тимошин Алексей Владимирович**, студент, СКФ МТУСИ;
302. **Титов Вячеслав Юрьевич**, к.т.н., младший научный сотрудник научно-технического отдела, Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации;
303. **Тищенко Евгений Николаевич**, доцент, д.э.н., СКФ МТУСИ;
304. **Тошматов Шункоржон Тошпулатович**, старший преподаватель, З.Ташкентский университет информационных технологий;
305. **Трипута Владимир Николаевич**, студент, Ростовский государственный экономический университет (РИНХ);
306. **Тумаков Максим Дмитриевич**, студент, Академия Федеральной службы охраны Российской Федерации;
307. **Туракулов Искандар Нуритдинович**, доцент, к.т.н., Самаркандский государственный университет;
308. **Туракулова Азиза Искандаровна**, научный исследователь, Ташкентский государственный педагогический университет;
309. **Турсунов Шерзод Абдукодирович**, заведующий кафедрой «Менеджмент и маркетинг», Ташкентский университет информационных технологий;
310. **Тюренков Максим Вадимович**, аспирант кафедры экономики связи, МТУСИ;
311. **Умарова Умида Бойсариевна**, научный исследователь, Ташкентский государственный педагогический университет;
312. **Усошина Елена Александровна**, программист-разработчик I категории, ООО "Датум Групп;
313. **Фадеев Александр Николаевич**, аспирант, МТУСИ;
314. **Фатхулин Тимур Джалилевич**, аспирант, МТУСИ;
315. **Федотов Виталий Викторович**, начальник отдела развития, Ростовский филиал ОАО «Ростелеком»;
316. **Фенчук Михаил Михайлович**, аспирант, МТУСИ;
317. **Филиппова Дарья**, студент, СКФ МТУСИ;
318. **Фокин Илья Александрович**, студент, Академия Федеральной службы охраны Российской Федерации;
319. **Фролова Юлия Аркадьевна**, студент, СПбГУТ им. проф. Бонч-Бруевича;
320. **Фрунзе Валерия Александровна**, студент, Ростовский государственный экономический университет (РИНХ);

321. **Хабибулин Александр Викторович**, студент 4 курса направления Прикладная информатика в экономике, Северо-Кавказский федеральный университет;
322. **Хакимов Зафар Туляганович**, к.т.н., проректор по науке, Ташкентский университет информационных технологий;
323. **Халбаева Муаззам Зафаровна**, студент, Ташкентский университет информационных технологий;
324. **Харченко Виктор Викторович**, к.т.н, доцент, подполковник, ВУНЦ ВВС «ВВА»;
325. **Харченко Лидия Николаевна**, студент, ДГТУ;
326. **Хасанов Миркомил Мирхидоятович**, ст. преподаватель, Ташкентский Государственный технический университет;
327. **Хасоян Гурген Сергеевич**, студент, СКФ МТУСИ;
328. **Хорольский Евгений Михайлович**, к.т.н., научный сотрудник научно-технического отдела, Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации;
329. **Цепляева Алена Викторовна**, студент, УрТИСИ ФГОБУ ВПО «СибГУТИ»;
330. **Черкасов Александр Евгеньевич**, Академия Федеральной службы охраны Российской Федерации;
331. **Чернышев Николай Николаевич**, к.т.н., доцент, Донецкий национальный технический университет;
332. **Чикалов Андрей Николаевич**, к.т.н, доцент, доцент кафедры СПОИ, СКФ МТУСИ;
333. **Чудин Денис Алексеевич**, курсант, Уральский юридический институт МВД России;
334. **Чучупалова Валерия Алексеевна**, студент, СКФ МТУСИ;
335. **Шаакбарова Барно Рафиковна**, преподаватель, Ташкентский государственный педагогический университет;
336. **Шалабаева Исламгуль Айболатовна**, магистрант специальности Информационные системы, Западно-Казахстанский инженерно-гуманитарный университет;
337. **Шаравова Ольга Ивановна**, к.э.н., доцент кафедры экономики связи, МТУСИ;
338. **Шарипходжаева Фатма**, к.ф-м.н., доцент, доцент каф. «Информатики и методики ее преподавания», Ташкентский государственный педагогический университет;
339. **Шарыпова Татьяна Николаевна**, к.э.н., зав. кафедрой ЭиУ, СКФ МТУСИ;
340. **Шатилина Юлия Геннадиевна**, студент, СКФ МТУСИ;
341. **Швидченко Андрей Виталевич**, студент, СКФ МТУСИ;
342. **Швидченко Светлана Александровна**, доц. к.т.н., ДГТУ;
343. **Шевченко Светлана Алексеевна**, студент, Московский государственный университет приборостроения и информатики, Ставропольский филиал;
344. **Шевчук Петр Сергеевич**, д.т.н., профессор, СКФ МТУСИ;
345. **Шипицина Марина Сергеевна**, студент, СКФ МТУСИ;
346. **Шишкин Вадим Викторинович**, к.т.н., доцент, профессор кафедры ИВК, Ульяновский Государственный Технический Университет;
347. **Шишкин Вадим Викторинович**, к.т.н., профессор, директор Института авиационных технологий и управления Ульяновского государственного технического университета;
348. **Шоков Андрей Викторович**, аспирант, ДГТУ;
349. **Шокова Юлия Александровна**, доцент, к.ф.-м.н., ДГТУ;
350. **Шомахамедов Жамолиддин Фазлитдинович**, магистрант кафедры «Информационная безопасность», Ташкентский университет информационных технологий;

351. **Шполянская Ирина Юрьевна**, д.э.н., зав. кафедрой Информационных систем и Прикладной информатики, Ростовский государственный экономический университет (РИНХ);
352. **Шубин Дмитрий Николаевич**, инженер, студент магистратуры, МТУСИ;
353. **Шульженко Роман Алексеевич**, студент, СКФ МТУСИ;
354. **Щаднев Антон Вадимович**, студент, РГЭУ;
355. **Щербань Игорь Васильевич**, профессор кафедры, д.т.н., доцент, СКФ МТУСИ;
356. **Щербань Оксана Георгиевна**, к.т.н., доцент, доцент кафедры, Институт высоких технологий и пьезотехники, ЮФУ;
357. **Юлдашев Умит Юлдашевич**, д.т.н., профессор, профессор каф. «Информатики и методики ее преподавания», Ташкентский государственный педагогический университет;
358. **Юрчевская Наталья Николаевна**, студент, СКФ МТУСИ;
359. **Юхнов Василий Иванович**, к.т.н., доцент, заведующий кафедрой МТС, СКФ МТУСИ;
360. **Якубов Максадхон Султаниязович**, профессор, д.т.н., Ташкентский университет информационных технологий.

АВТОРСКИЙ УКАЗАТЕЛЬ