ISSN 2221-7975

ТРУДЫ

СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА
ОРДЕНА ТРУДОВОГО КРАСНОГО ЗАНМЕНИ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СВЯЗИ И ИНФОРМАТИКИ»
ЧАСТЬ II

РОСТОВ-НА-ДОНУ
2017

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

ТРУДЫ

СЕВЕРО-КАВКАЗСКОГО ФИЛИАЛА

МОСКОВСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

СВЯЗИ И ИНФОРМАТИКИ

Часть II

Подготовлены по результатам
Международной научно-практической конференции
«ИНФОКОМ-2017»
16 – 18 мая 2017 года

Ростов-на-Дону
2017

УДК 621.396.1

ББК 32
Т 78

Т 78 Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть II - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2017, 442с.

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 X-ой Международной научно-практической конференции «ИНФОКОМ-2017», которая проходила 16-18 мая 2017 г. в СКФ МТУСИ. Сборник объединяет статьи по актуальным научным направлениям создания, совершенствования, перспективного развития современных технологий обработки и передачи информации, а также инфокоммуникационных технологий в сфере менеджмента, экономики, и образования.

Вторая часть сборника содержит материалы статей работы 2 и 3 секций конференции по направлениям, соответственно:

- «Информационная безопасность»
- «Инфокоммуникационные технологии в сфере образования, экономики и менеджмента»

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: Опарин А.Ю., Сафронов А.И

© СКФ МТУСИ, 2017

Подписано в печать 24.05.2017
Формат 60x84/8. Печать офсетная. Тираж 50 экз.
Полиграфический центр «Университет» СКФ МТУСИ,
Ростов-на-Дону, 344002, ул. Серафимовича, 62

СОДЕРЖАНИЕ

ЧАСТЬ I

СЕКЦИЯ №1
СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

***П.П. Акулин, *О.А. Сафарьян, **Н.В. Болдырихин** Технологическая сингулярность **.....20**

***Ф.А. Алтунин, *В.М. Кносаль, *Р.В. Давыдов, **Н.В. Болдырихин** Анализ методов классификации трафика **.....23**

Д.Х. Аль Ясири Исследование протоколов маршрутизации в сетях с коммутацией пакетов **.....27**

У.Б. Амирсаидов Метод распределения потоков в облачных IMS **.....34**

А.М. Бабычев, Н.В. Будылдина Методика определения параметров потоков в мультисервисной телекоммуникационной сети с учетом эффекта самоподобия **.....43**

Е.В. Бармина, Ф.П. Филиппов, Н.И. Ильиных Термодинамическое моделирование поведения Al_2O_3 с добавками SiC и ZrO_2 в широком интервале температур **.....49**

И.М. Безруков Аппроксимация и сжатие классическим и модифицированным методами Прони импульсной характеристики канала связи **.....58**

Н.В. Болдырихин, И.П. Рыбалко, И.А. Сосновский, И.С. Гирин Применение динамических моделей при описании сетевого оборудования в задачах мониторинга **.....70**

А.В. Бородин Исследование материалов перспективных для использования в волноводной и интегральной оптике **.....73**

П.С. Бражуненко, О.П. Иевлев Исследование вероятностных характеристик сигнального трафика сетей IMS в целях предотвращения перегрузок SIP- сервера **.....77**

И.А. Брежный, Е.А. Ревякина, Е.М. Уколов Перспективы развития отрасли электроэнергетики с применением геоинформационных систем **.....84**

Е.В. Букрина Промышленный интернет вещей – инновационный сегмент экосистемы телекоммуникационного оператора **.....87**

А.Н. Буренин, К.Е. Легков, В.В. Оркин Постановка задачи управления функционированием информационной системы специального назначения **.....92**

В.С. Волков, К.А. Шимельфених Построение беспроводных сетей широкополосного доступа, основанных на стандарте IEEE 802.16, на распределенных инфраструктурах **.....98**

В.Е. Герасименко, Е.А. Карпов, А.В. Лаухин Перспективы применения телекоммуникационных технологий в диагностике аритмических и ишемических болезней сердца в телемедицине **.....109**

Е.А. Горохова Моделирование алгоритма распознавания наземных объектов на борту беспилотных летательных аппаратов **.....114**

***Н.О. Горшенин, *И.В. Щербань, К.Д. Грабовый** Распределенная система измерения и контроля параметров почвы **.....122**

И.Д. Григорьев, В.Г. Орлов Механизмы качества обслуживания в VDL Mode 4 **.....129**

И.Д. Григорьев, В.В. Трофлянин, А.А. Кальфа Исследование средств качества обслуживания операционной системы VRP Huawei **.....133**

В.А. Данилов, Ю.В. Жабинский, А.С. Усик Вероятностные характеристики узкополосного случайного процесса на выходе инерционно-нелинейного преобразователя **139**

В.А. Данилов, В.Л. Львов Амплитудное подавление частотно-модулированных помех в ВЧ-диапазоне **145**

В.А. Данилов, Л.В. Данилова Эффективнось непараметрических обнаружителей слабых сигналов при негауссовских помехах узкополосного типа..... **148**

Д.В. Денисов, М.С. Самков, К.С. Сухоева, Д.Э. Королёв Техническая реализация многослойных линзовых антенн Люнеберга **153**

Д.В. Денисов, К.А. Санникова, Д.Э. Королев Рассеяние электромагнитных волн сотовых диапазонов на многослойной сферической модели **161**

Д.В. Денисов, К.С. Сухоева, Д.А. Максимов, К.А. Санникова Измерение параметров материалов..... **170**

Д.В. Денисов, В.С. Чащин О применимости методов генерации электромагнитных волн с ненулевым орбитальным угловым моментом в системах радиосвязи **176**

В.В. Евстафьев, Н.В. Руденко, К.А. Кашуба, А.П. Зуйков, И.А. Ситьков Возможности маршрутизации информационных потоков в сетях связи следующего поколения..... **180**

А.В. Елисеев, С.Н. Овсянников, А.Г. Прыгунов Управление параметрами линейного дискретного фильтра на основе нечеткой экспертной системы **187**

М.А. Елфимов, Н.В. Руденко, В.В. Евстафьев, Н.А. Коньшина, В.А. Федотов, М.К. Баженов Электроснабжение инфокоммуникационных систем, размещаемых на низкоорбитальных дирижаблях **196**

И.А. Енгибарян, А.В. Ермолаев, *О.А. Сафарьян, *А.И. Тютюнникова Оценка эффективности использования свойств эмерджентности в инфокоммуникационных системах..... **200**

А.В. Ермолаев, К.А. Артынов, И.Ю. Сулименко, И.В. Решетникова Анализ технологий VSAT **205**

В.В. Ершов, Н.В. Руденко, К.А. Решетникова, Д.С. Боковеев О целесообразности использования вертикально-осевых ветроэнергетических установок для базовых станций сотовой связи..... **207**

***А.П. Зверев, И.П. Рыбалко, М.А. Дерканосов** Программное средство управления маршрутизацией в подвижных радиосетях спасательных формирований МЧС на основе экспертной системы..... **213**

***А.П. Зверев, И.П. Рыбалко** Использование БПЛА для МЧС России **220**

С.В. Зеленский, К.А. Батенков Исследования вероятностно-временных характеристик видеоприложений **226**

Н.И. Ильиных, И.А. Малкова, Е.А. Волгарев Исследование поведения системы Al-N при нагревании в широком интервале температур **230**

М.О. Киреев, *Е.В. Глушак Исследования факторов, влияющих на параметры качества технологии широкополосного доступа ADSL **233**

***Н.Е. Кириленко, *С.О. Красников, К.Д. Бадыштова, *И.В. Щербань** Решение задачи поиска осцилляторных паттернов в составе зашумленных сигналов..... **236**

М.А. Клевакин, Д.В. Кусайкин О новых способах генерации электромагнитных волн оптического диапазона с ненулевым орбитальным угловым моментом в ВОСП **238**

[*]В.М. Кносаль, [*]Ф.А. Алтунин, [*]Р.В. Давыдов, [**]Н.В. Болдырихин Анализ математических моделей сетей связи, используемых в задачах мониторинга **245**

В.Г. Кобак*, Д.А. Жуковский*, Н.И. Кривошей Исследование модифицированной модели уитли с различными методами формирования элитных особей **248**

В.Г. Кобак*, А.Г. Жуковский, А.А. Манин, А.А. Пешкевич* Использование гибридного алгоритма при решении задачи коммивояжёра небольшой размерности **252**

В.Г. Кобак*, А.Г. Жуковский, В.М. Поркшеян* Решение однородной минимаксной задачи исландской моделью, где в качестве островов выступает модифицированная модель Голдберга **257**

В.Г. Кобак*, А.Г. Жуковский, В.М. Поркшеян* Сравнение эвристических алгоритмов при решении неоднородной минимаксной задачи **262**

А.В. Колосков, А.С. Шпилько, Н.В. Болдырихин Анализ технологии CWDM **267**

С.И. Конева, Ю.Е. Михайленко Модернизация волоконно-оптической линии связи на участке Ростов-на-Дону – Куйбышево **269**

С.И. Конева, В.Г. Кабакова Модернизация ЛВС Кропотскинского почтамта УФПС Краснодарского края - филиала ФГУП «Почта России» **273**

С.И. Конева, А.С. Кузьменко Разработка WiMAX-сети в Веселовском ЛТЦ Азовского МЦТЭТ Ростовского филиала МРФ «Юг» ПАО «Ростелеком» **277**

И.С. Коновалов, В.А. Фатхи, В.Г. Кобак Исследование влияния параметров модифицированной модели Голдберга генетического алгоритма на точность решения задачи покрытия множеств **281**

Я.Б. Константинова, Н.О. Светличная Информационные методы прогнозирования свойств сегнетоэлектриков. Фазовый переход в сегнетоэлектриках **287**

Н.А. Коньшина, Н.В. Руденко, В.В. Ершов*, М.А. Елфимов, Т.Э. Тимирбулатова*, Е.М. Мищук О целесообразности размещения инфокоммуникационных систем на низкоорбитальных дирижаблях **292**

В.Т. Куанышев, А.Б. Папаев, И.А. Зубарев Использование информационных технологий при моделировании чрезвычайных явлений **297**

Д.В. Кусайкин, С.В. Коновалов, М.А. Клевакин Об эффективности применения форматов модуляции RZ-DQPSK, RZ-BPSK и 16QAM в современных ВОСП **302**

Д.В. Кусайкин, Р.И. Хурматов Классификация типов оптических волокон с уменьшенными потерями на макроизгибах **308**

М.А. Лукиенко, П.В. Лобзенко Автоматизированная система удаленного контроля и управления **319**

В.Л. Львов, Е.В. Игначкова, К.В. Львов Оценка структурной живучести сети связи по узловым сечениям **324**

А.А. Манин, Н.В. Болдырихин, *С.В. Коробенко, И.А. Сосновский Минимизация технологического риска при эксплуатации комплексов связи на основе разработки информационной системы контроля и управления подготовкой сотрудников **328**

И.А. Молоковский, М.Г. Каличак Алгоритм маршрутизации ad-hoc сетей в условиях неоднородной среды **335**

Д.А. Овчинников, С.А. Баранов Интроскопия поверхности земли электромагнитными волнами при использовании беспилотных летательных аппаратов **340**

Э.Л. Портнов, Т.Д. Фатхулин Анализ методов подавления шумовых явлений в современных DWDM-системах связи **345**

Г.А. Птицын, Д.Н. Безумнов Математическая модель интенсивности межузлового потока между двумя транспортными узлами **350**

А.С. Пузанов, К.А. Батенков, М.В. Стремоухов Имитационное моделирование сети связи с отказами с помощью программы Riverbed..... **354**

А.В. Рахимьянов, П.В. Лобзенко Android приложение для эффективного запоминания изучаемого материала **366**

И.Г. Ремез Актуализация основных стратегических направлений развития инфокоммуникаций в Свердловской области..... **372**

И.П. Рыбалко, В.Г Караченцев, Е.А. Цибульский Характеристика технологии IEEE 802.3bz 2.5 GBASE-T И 5 BASE-T..... **377**

А.И. Сафронов Исследование полосно-пропускающего фильтра на копланарной линии, возбуждающей поверхностные магнитостатические волны..... **380**

В.О. Семенец, М.П. Трухин Способы противодействия радиоуправляемым устройствам. **394**

***Н.Ю. Семиряд, **Н.В. Болдырихин** Анализ принципов организации параллельных вычислений..... **398**

И.С. Синева, Д.С. Зайченко Генетические алгоритмы в задачах помехоустойчивого кодирования **402**

В.Н. Смоляков, Г.В. Детко Разработка сети беспроводного доступа на основе технологии LTE в Крыловском районе Краснодарского края силами Крыловского ЛТЦ ПАО «Ростелеком»..... **416**

В.Н. Смоляков, Д.А. Ланко Модернизация локальной вычислительной сети ООО «Вилмари» город Москва **422**

В.Н. Смоляков, В.В. Чернышев Модернизация локальной вычислительной сети типографии «Lucky Pack» город Ростов-на-Дону **427**

С.В. Соколов, М.В. Полякова, О.И. Соколова Решение проблемы адаптивной фильтрации на основе нерегулярных точных наблюдений..... **432**

О.В. Сумарокова Сравнение характеристик помехоустойчивости системы OFDM в различных режимах модуляции поднесущих **437**

А.П. Сухоев, Н.И. Ильиных Исследование температурной зависимости показателя преломления SiO_2 ..... **439**

И.Н. Таов, А.А. Манин Сравнение современных стандартов видеонаблюдения **447**

Е.С. Тарасов Исследование эффективности алгоритма сжатия кодовой последовательности сформирванной текстовым сообщением **450**

Э.Р. Тлекова Развитие инфокоммуникационных технологий для высокоскоростных железных дорог: от GSM-R к LTE-R **462**

В.В. Трофлянин, М.Н. Беленькая Исследование средств передачи потокового видео по сети..... **474**

А.А. Уманов, Н.Г. Бикбулатова Исследование Dataflow-архитектуры **479**

Н.Б. Усманова Представление и формализация процессов взаимодействия в распределенных сетевых структурах..... **487**

Д.С. Федоров, *В.И. Юхнов Антенна базовой станции на основе кольцевой антенной решетки..... **492**

В.В. Федотов, Б.П. Борисов Применение сверхплотных ленточных оптических кабелей при генеральном планировании и строительстве сетей связи **499**

В.В. Харченко, В.В. Бурдюг Использование метаматериалов для улучшения направленных свойств антенных систем **503**

К.Ш. Хушмуродов, М.П. Трухин Факторы, влияющие на сбои электропитания персонального компьютера **508**

В.Г. Черемных, В.С. Невельский, Д.В. Астрецов Исследование возможности перехвата сигналов излучаемых клавиатурой компьютера **513**

Г.Н. Черпаченко, П.В. Лобзенко Клиент-северное приложение для регистрации состояния информационной сети **520**

А.А. Шадрин, М.П. Трухин, И.В. Соловаров Восстановление частоты несущего колебания MSK -сигнала **525**

А.М. Шаповалов, А.Ю. Опарин Автоматизация или гуманизация экономики будущего **529**

М.В. Юферев, А.Н. Езин Фреймворк как основной инструмент разработки Web-приложения **532**

П.В. Явтушенко, А.Ю. Опарин Проблемы и перспективы развития современных средств отображения информации **541**

КРАТКИЕ СВЕДЕНИЯ ОБ АВТОРАХ **552**

АВТОРСКИЙ УКАЗАТЕЛЬ **572**

ЧАСТЬ II

СЕКЦИЯ №2
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ю.А. Безуглый, А.В. Вершенник, А.В. Попова, Е.В. Сухорукова Анализ методов аутентификации **20**

Ю.А. Безуглый, А.В. Вершенник, А.В. Попова, Е.В. Сухорукова Основные угрозы аутентификации **25**

Н.В. Белан, И.В. Карасев, Л.А. Луганская Сравнение ансамблей многофазных ортогональных сигналов **29**

Н.П. Борисенко, А.М. Цыганов, М.А. Куликов Генерация s-блоков с заданными параметрами с использованием параллельных вычислений **35**

Б.П. Борисов, А.И. Янкина Анализ аппаратных средств защиты информации в сетях передачи данных **39**

А.Э. Боярчук, *В.И. Юхнов, *П.С. Шевчук Анализ угроз безопасности организации **43**

А.В. Вершенник, М.Н. Корчемкина, Н.А. Куприянов, Е.В. Сухорукова Анализ условий обеспечения подлинности информации при ее передаче по каналам ССОП ЕСЭ РФ **49**

А.В. Вершенник, М.Н. Корчемкина, Н.А. Куприянов, Е.В. Сухорукова Анализ методов компьютерной стеганографии **54**

А.С. Галкин, Д.О. Маркин Распределенное тестирование веб-приложений методом фаззинга на основе технологий веб-прокси и активных данных **61**

М.Г. Гизатуллин, Д.В. Варакосов Некоторые особенности реализации угрозы несанкционированного доступа к системе по беспроводным каналам связи **72**

И.С. Гирин, Е.А. Стаценко, И.А. Сосновский Анализ методов защиты информации в беспроводных сетях стандарта 802.11 ..... **77**

О.В. Гончарова, А.А. Гончаров Информационная безопасность современного молодежного общества: тенденции и угрозы **79**

А.С. Жук[1], В.А. Головской[2] Анализ вычислительной сложности решения задачи о мультипликативном рюкзаке **82**

А.С. Жук[1], В.А. Головской[2] Синтез иерархической системы защиты информации от несанкционированного доступа на основании модели Белла-ЛаПадулы **91**

Э.Т. Ишдавлетова, К.А. Ролдугина Обеспечение информационной безопасности в условиях модернизации и развития почтовых услуг на базе ИКТ **98**

А.Г. Кирхеев[1], В.А. Головской[2] К вопросу обеспечения безопасности информации мобильного устройства **104**

С.М. Краснопеев, А.А. Юркин Расследование инцидентов информационной безопасности на основе анализа образа оперативной памяти **107**

А.Ю. Кудряшова , А.Н. Руднев Исследование и разработка метода оценки информационной безопасности сетевых хранилищ **115**

С.И. Кузнецов, С.П. Тесля, Е.В. Сухорукова, А.В. Вершенник Вариант изменения логической структуры адресного пространства информационно-коммуникационных сетей **125**

А.А. Полков, А.С. Совенко Некоторые аспекты практической реализации электронной цифровой подписи **133**

А.А. Полков, Д.С. Совенко Обзор способов программной реализации линейного преобразования **136**

Н.В. Путилин[1], В.А. Головской[2], В.А. Крутов[1] Комплексный подход к построению и модернизации сетей радиосвязи специального назначения **141**

Н.И. Сидняев, С.А. Говор Исследование планирования эксперимента при построении моделей со случайным дрейфом параметров регрессионной модели **146**

В.Н. Смоляков, Р.М. Кильдишов Модернизация системы информационной безопасности офиса контактного центра Теле2-Ростов программно-аппаратными средствами **156**

В.Н. Смоляков, В.В. Сильченко Разработка системы защиты информации ЛВС Руднянского ЛТЦ Волгоградского филиала МРФ «Юг» ПАО «Ростелеком» **162**

М.Г. Усынин, А.Ю. Опарин Защита информации и информационная безопасность **168**

А.Н. Чикалов, А.И. Янкина Переполнение буфера в стеке. методы обнаружения и борьбы с данным видом эксплойта **176**

О.В. Швачко, И.С. Деркачев Вопросы обеспечения защиты персональных данных в информационных системах **180**

Д.А. Яковлев, И.С. Синева Часто встречаемые ошибки при проектировании и реализации сетевых протоколов для обмена данными **184**

СЕКЦИЯ №3
«ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБРАЗОВАНИЯ, ЭКОНОМИКИ И МЕНЕДЖМЕНТА»

А.С. Артеменкова, А.И. Момот Применение системы бережливого производства на предприятиях почтовой связи **190**

А.Х. Бабаян, П.В. Лобзенко Интерактивное обучающее приложение по дисциплине «Технология программирования» **197**

***Д.А. Безуглов, **А.П. Кузин, **С.А. Швидченко** Обнаружение контуров изображений в мультимедийных приложениях на основе дискретного вейвлет-преобразования **200**

Э.А. Бинеев Особенности структуры дисциплины БЖД по направлению ИТСС **209**

А.Э. Боярчук, *В.И. Юхнов, *П.С. Шевчук Повышение эффективности систем управления проектами **211**

С.А. Быстров Задача идентификации личности по голосу: анализ подходов к решению **217**

Н.А. Вернигорова, И.В. Головина Проблема импортозамещения в инфокоммуникациях **221**

И.В. Водовозов, Д.А. Васинев Разработка узла доступа к транспортной сети с коммутацией пакетов для применения в учебном процессе **225**

М.Г. Гизатуллин, Ф.И. Тураев Некоторые аспекты реализации медиаобразовательных технологий в рамках организации образовательного процесса по учебной дисциплине «Основы информационной безопасности в органах внутренних дел» **228**

Е.И. Гниломёдов, И.И. Шестаков Оценка применимости компонентов разветвленных сетей стандарта ITU-T G.984 архитектуры FTTX, для организации учебного процесса с целью формирования профессиональных компетенций выпускников в соответствии с ФГОС ВО 3+ **242**

О.В. Гончарова, А.Ю. Опарин Здоровье педагога – залог профессионального долголетия **249**

А.М. Данилова, Ш.А. Турсунов Организация управления инвестиционными процессами в сфере информационно-коммуникационных технологий **251**

Н.В. Данилова Оценка параметров в модели стохастической волатильности **256**

Д.Е. Демидов, Л.Н. Евдакова Перспективы и проблемы развития отрасли инфокоммуникаций в России **258**

Ю.Н. Денисенко, Ю.А. Олейникова «Сарафанный» маркетинг как инструментарий брендинга **265**

В.Ю. Денисов, И.С. Синева Применение и инструменты Business intelligence **271**

С.А. Докучаев, Г.С. Костецкая, Н.О. Светличная О формировании общепрофессиональной компетенции бакалавров в области информационных технологий и вычислительной техники при изучении общенаучных дисциплин (на примере кейс-метода) **276**

С.А. Докучаев, Г.С. Костецкая О междисциплинарном взаимодействии при обучении бакалавров в области инфокоммуникаций (на примере одной задачи математической физики) **279**

Л.И. Долинер, Н.Г. Бикбулатова Электронный курс как базовый компонент обучения в современном ВУЗе **282**

А.С. Доткулова, М.С Мосева Метод интеллектуальной верификации логических связей модулей ООП в соответствии с ФГОС ВО. **287**

Л.Н. Евдакова Роль самостоятельной работы в формировании компетенций у студентов инфокоммуникационных вузов **294**

И.В. Калиенко, И.С.Абрамов, Н.И.Абрамова Разработка методических рекомендаций по исследованию тиристоров на лабораторной установке «Электронные приборы» кафедры «Радиоэлектроника» ДГТУ **300**

Е.А. Коломиец, А.М. Коршун Совершенствование внеаудиторной самостоятельной работы обучающихся на базе информационных технологий **309**

Б.Б. Конкин Информационно-коммуникационные технологии в обучении **314**

Д.В. Костюченко, П.М. Табунщикова Культура речи в жизни IT -специалистов и всего человечества **319**

В.Г. Лисицин Проблемы организации маркетинговых коммуникаций в малом бизнесе **322**

Р.А. Момот Особенности формирования процессов венчурного инвестирования в России **326**

М.Л. Мухитдинова , В.А. Каримова Анализ процесса управления запасами предприятия на основе метода совмещенного ABC и XYZ анализа **330**

***В.А. Погорелов, *А.О. Семилеткин, **С.А. Швидченко** Исследование метода параметрической идентификации динамической системы в условиях действия помех **335**

М.А. Пташинский, А.И. Момот Особенности перехода на версию инновационного стандарта ИСО 9001-2015 ..... **341**

Е.Г. Ротова, А.И. Момот Использование процессного подхода при осуществлении закупочной деятельности предприятия **346**

А.А. Санников, В.Т. Куанышев Информационные технологии и обработка больших массивов данных в сфере образования **351**

Е.А. Свирщ Информационная компетентность экономистов **354**

Т.В. Сидорина Обеспечение безопаности на предприятиях почтовой связи **358**

Е.А. Скоробогатова Влияние инфокоммуникационных услуг на эффективность деятельности Сбербанка **364**

И.А. Степская, С.А. Уколова, А.И. Момот О ценка конкурентоспособности услуги по приему коммунальных платежей УФПС Ростовской области – Филиала ФГУП «Почта России» **368**

В.Н. Трофименко, А.В. Павлова, К.В. Пащенко Имитационное моделирование контура угловой стабилизации самолета **373**

Д.Л. Устименко, Е.А. Гатилова Актуальные проблемы компьютерного дизайна в современных инфокоммуникационных технологиях **377**

В.В. Федотов, Е.Н. Тищенко, А.А. Яковенко Построение системы информационной поддержки жизненного цикла проектирования и производства наукоемкой телекоммуникационной продукции на базе единого информационного пространства в виде виртуального предприятия между ПАО «Ростелеком» и ведущими производителями, проектировщиками ТК материалов и оборудования, строительными ТК компаниями **380**

П.Ч.Е. Федотова, Н.В. Будылдина Реализация в России индустриальных интернет вещей **384**

О.И. Шаравова , М.П. Белянчикова, И.А. Новикова Результаты сравнительной оценки финансового положения крупнейших российских операторов подвижной связи **.....388**

А.А. Яковенко, М.А. Галухин Трансформации современного общества и инновации в управлении персоналом **.....395**

А.А. Яковенко, Е.П. Косарева Планирование как механизм реализации целей социально-экономического развития современного общества**.....401**

А.А. Яковенко А.А. Пятина Инновации и риски в отрасли связи **.....407**

А.А. Яковенко, О.О. Шадрунова Статистическое исследование бедности и социального неравенства в российском обществе **.....412**

КРАТКИЕ СВЕДЕНИЯ ОБ АВТОРАХ.....419

АВТОРСКИЙ УКАЗАТЕЛЬ.....439

CONTENTS

PART I

SECTION 1
STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

***P.P. Akulin, *O.A. Safaryan, **N.V. Boldyrikhin** Technological singularity **20**

***F.A. Altunin, *V.M. Knosal, *R.V. Davydov, **N.V. Boldyrikhin** Analysis of traffic classification methods **23**

J.H. Al-Yasiri Investigation of routing protocols in packet switched networks **27**

U. Amirsaidov Method for flow distribution in cloud-based IMS **34**

A.M. Babychev, N.V. Budyldina Methodology for determining parameters of flows of multi-service telecommunication network with regard to the effect of self-design **43**

E.V. Barmina, A.P.Philippov, N.I. Ilinykh Thermodynamic modeling of the behavior of Al_2O_3 with additives of SiC and ZrO_2 in a wide range of temperatures **49**

I.M. Bezrukov Approximation and compression of impulse response of the communication channel by classical and modified Prony's method **58**

N.V. Boldyrikhin, I.P. Rybalko, I.A. Sosnovsky, I.S. Girin Application of dynamic models in description of network equipment in monitoring problems **70**

A.V. Borodin Study of perspective materials to use in guided-wave optics and integrated optics **73**

P.S. Brajunenko, O.P. Ievlev The study of probabilistic characteristics of signal traffic for the preventing SIP-server overloads in IMS **77**

I.A. Brezhny, E.A. Revyakina, E.M. Ukolov Perspectives of development of the electric power industry with application of geoinformation systems **84**

E.V. Bukrina Indastrial internet of things is an innovative segment of telecommunications operator ecosystem **87**

A.N. Burenin, K.E. Legkov, V.V. Orkin Problem formulation of information system for special purposes functioning management **92**

V.S. Volkov, K.A. Schimelfenikh Constructions of a wireless broadband networks based on the standard IEEE 802.16 on distributed infrastructures **98**

V.E. Gerasimenko, E.A. Karpov, A.V. Laukhin Prospects of application of telecommunication technologies in diagnostics of arithmic and ischemic heart diseases in telemedicine **109**

E.A. Gorokhova Modeling of the algorithm for recognition of ground object on board the unmanned aeria vehicle **114**

***N.O. Gorshenin, *I.V. Shcherban, K.D. Grabovy** Distributed measurement and control system of soil parameters **122**

I.D. Grigoryev, V.G. Orlov Quality of service mechanisms in VDL Mode 4 ..... **129**

I.D. Grigoryev, V.V. Troflyanin, A.A. Kalfa Quality of service methods researching in operating system VRP Huawei **133**

V.A. Danilov, Y.V.Zhabinskiy, A.S. Usik Probabilistic characteristics of narrow-band random process the output of the inertial-non-linear converter **139**

V.A. Danilov, V.L. Lvov Amplitude suppression of frequency-modulated noise in the HF-range **145**

V.A. Danilov, L.V. Danilova The efficiency of nonparametric detector of weak signals with not gaussian interferences of narrowband type **148**

D.V. Denisov, M.S. Samkov, K.S. Sukhoeva, Korolev D.E. Technical realization of multilayer luneberg lens antenna **153**

D.V. Denisov, K.A. Sannikova, D.E. Korolev Dispersion of electromagnetic waves of the cellular ranges on multi-layer spherical model **161**

D.V. Denisov, K.S. Sukhoeva, D.A.Maksimov, K.A. Sannikova Measurement of the materials parameters **170**

D.V. Denisov, V.S. Chaschin The applicability of vortex beams generation methods for radio communication systems **176**

V.V. Evstafiev, N.V. Rudenko, K.A. Kashuba, A.P. Zuikov, I.A Sitkov Possibilities of information routing by streaming next-generation communication networks **180**

A.V. Eliseev, S.N. Ovsyannikov, A.G. Prigunov The control parameters of linear discrete filter based on fuzzy expert system **187**

M.A. Elfimov, N.V. Rudenko, V.V. Evstafyev, N.A. Konshina, V.A. Fedotov, M.K. Bazhenov Electrical supply of infocommunication systems, located on low-orbital directions **196**

I.A. Engibaryan, A.V. Yermolayev, *O.A. Safar'yan, A.I. Tyutyunnikova Efficiency estimation of usage of emergentness properties in infokommunication systems **200**

A.V. Yermolaev, K.A. Artynov, I.Y. Sulimenko, I.V. Reshetnikova Analysis of technologies VSAT **205**

V.V. Ershov, N.V. Rudenko, K.A. Reshetnikova, D.S. Bokoveev About the purpose of the use of vertical-axial wind-power plants for basic stations cellular communication **207**

***A.P. Zverev, I.P. Rybalko, M.A. Derkanosov** Routing in mobile radio networks of the savior-enforcement forces the Ministry of emergency situations on the basis of expert system **213**

***A.P. Zverev, I.P. Rybalko** The use of UAVS for emergency situations of Russia **220**

S.V. Zelensky, K.A. Batenkov The study of probabilistic-temporal characteristics of video applications **226**

N.I. Ilinykh, I.A. Malkova, E.A. Volgarev Investigation of the behavior of the Al-N system in heating in a wide temperature interval **230**

M.O. Kireev*, E.V. Glushak Study of factors influencing the quality parameters of broadband access technologies ADSL **233**

***N.E. Kirilenko, * S.O. Krasnikov, K.D. Badyshtova, * I.V. Shcherban** The solution of the problem for searching an oscillatory patterns in the noised signals **236**

M.A. Klevakin, D.V. Kusaykin The new ways to generate vortex beams in fiber optic transmission systems **238**

***V.M. Knosal, *F.A. Altunin, *R.V. Davydov, **N.V. Boldyrikhin** Analysis of mathematical models of communication networks used in monitoring problems **245**

V.G. Kobak*, D.A. Zhukovskiy*, N.I. Krivoshey* A study of a modified model of wheatley with different methods of formation of elite individuals **248**

V.G. Kobak*, A.G. Zhukovskiy, A.A. Manin, A.A. Peshkevich* Using hybrid algorithms for solving traveling salesman problem of low dimension **252**

V.G. Kobak*, A.G. Zhukovskiy, V.M. Porksheyan* T he homogeneous solution of the minimax problem the icelandic model, where the islands speaks a modified Goldberg`s model... **257**

V.G. Kobak*, A.G. Zhukovskiy, V.M. Porksheyan* Comparison of heuristic algorithms for the minimax solution of the inhomogeneous problem **262**

A.V. Koloskov, A.S. Shpilko, N.V. Boldyrikhin CWDM technology analysis **267**

S.I. Koneva, Yu.E. Mikhaylenko Modernization of fiber optic line on the site Rostov-na-Donu – Kuibyshev **269**

S.I. Koneva, V.G. Kabakova Modernization of the LAN Kropotkinskaja post office UFPS Krasnodar region - filial FGUP «Russian Post» **273**

S.I. Koneva, A.S. Kuzmenko Development of a WiMAX network in Veselovska NO MTSTAT Azov of the Rostov branch of the «South» JSC «Rostelecom» **277**

I.S. Konovalov, V.A. Fathi, V.G. Kobak Research of influence of parameters of the modified model, Goldberg's genetic algorithm on the accuracy of solving the problem of covering sets **281**

Y.B. Konstantinova, N.O. Svetlichnaya Information methods for predicting properties of ferroelectrics. Phase transitions in ferroelectrics **287**

N.A. Konshina, N.V. Rudenko, V.V. Ershov *, M.A. Elfimov, T.E. Tamirbulatova*, E.M. Mischuk About the performance of accommodation of infocommunication systems on low-orbital directions **292**

V.T. Kuanyshev, A.B. Papaev, I.A. Zubarev The use of information technology in the modeling of natural phenomena **297**

D.V. Kusaykin, S.V. Konovalov, M.A. Klevakin About applications of RZ-DQPSK, RZ-BPSK and 16QAM modulation formats in modern optical networks **302**

D.V. Kusaykin, R.I. Khurmatov Classification of bend-insensitive optical fibers **308**

M.A. Lukienko, P.V. Lobzenko An interactive tutorial on the subject "Technology of programming" **319**

V.L. Lvov, E.V. Ignachkova, K.V. Lvov Amplitude suppression of frequency-modulated noise in the HF-range **324**

A.A. Manin, N.V. Boldyrikhin, * S.V. Korobenko, I.A. Sosnovsky Minimization of technological risk in operation of communication complexes based on development of information system of control and management of preparation of employees **328**

I.A. Molokovskiy, M.G. Kalichak Ad-hoc networks' routing algorithm within heterogeneous environment conditions **335**

D.A. Ovchinnikov, S.A. Baranov Introscopy of the earth's surface by electromagnetic waves with the use of unmanned aerial vehicles **340**

E.L. Portnov, T.D. Fatkhulin Analysis of noise reduction methods in modern DWDM communication systems **345**

G.A. Ptitsyn, D.N. Bezumnov Mathematical model of internodal transport flow intensity between two transport nodes **350**

A.S. Puzanov, K.A. Batenkov, M.V. Stremoukhov Imitative modeling of the communication network with rejections with the Riverbed program **354**

A.V. Rahimjanov, P.V. Lobzenko An Android application for efficient memorization of the studied material **366**

I.G. Remez Actualization of the basic strategic directions of infocommunications development in Sverdlovsk region **372**

I.P. Rybalko, V.G. Karachentsev, E.A. Tsibulsky Technology characteristic IEEE 802.3bz 2.5 GBASE-T И 5 BASE-T **.....377**

A.I. Safronov Investigation of a band-pass filter, based on a magnetostatic surface waves excitating coplanar line**.....380**

V.O. Semenets, M.P. Trukhin Methods of counteraction to radio-controlled devices **.....394**

***N.Y. Semiryad, **N.V. Boldyrikhin** Analysis of the principles of parallel computing organization **.....398**

I.S. Sineva, D.S. Zaichenko Genetic algorithtms in the noise proof coding **.....402**

V.N. Smolyakov, G.V. Detko Development of wireless access network on LTE technology in Krylovsk district of Krasnodar territory Krylovskogo LETS PJSC Rostelecom **.....416**

V.N. Smolyakov, D.A. Lanko Modernization of local computer network LLC "Vilmari" city Moscow **.....422**

V.N. Smolyakov, V.V. Chernyshev Modernization of the local computer network of the printing house "Lucky Pack" city of Rostov-on-Don**.....427**

S.V. Sokolov, M.V. Polyakova, O.I. Sokolova Solution problem of adaptive filtration by the acyclic correct observations**.....432**

O.V. Sumarokova Comparison of the features of the ofdm interference system in various modes of modulation of substating**.....437**

A.P. Sukhoev, N.I. Ilinykh Investigation of temperature dependence of the refractive index of SiO_2**.....439**

I.N. Taov, A.A. Manin Comparison of video surveillance standards**.....447**

E.S. Tarasov Research efficiency compression algorithm code sequence formed text messages **..450**

E.R. Tlekova The Development of infocommunication technologies for high-speed railways: from GSM-R to LTE-R **.....462**

V.V. Troflyanin, M.N. Belenkaya Researching of video stream transmission instruments over the network **.....474**

A.A. Umanov, N.G.Bikbulatova Dataflow architecture research **.....479**

N. Usmanova Representing and formalizing the processes of interactions in distributed network structures **.....487**

D.S. Fedorov, *V.I. Yuhnov Ring antenna array as base station antenna **.....492**

V.V. Fedotov, B.P. Borisov The use of ultra-dense tape optical cables general the planning and construction of communication networks**.....499**

V.V. Kharchenko, V.V. Burdyug The use of metamaterials for improving the directional properties of antenna systems**.....503**

K.Sh. Khushmurodov, M.P. Trukhin The factors, influencing failures of power supply of the personal computer**.....508**

V.G. Cheremnykh, V.S. Nevelskiy, D.V. Astretsov Investigation of the possibility of interfering signals radiated by the keyboard by the computer**.....513**

G.N. Cherpachenko, P.V. Lobzenko The client and the application for registration of the state information network **.....520**

A.A. Shadrin, M.P. Trukhin, I.V. Solovarov Frequency recovery of MSK signal **.....525**

A.M. Shapovalov, A.Yu. Oparin Automation or humanizing economy of the future**.....529**

M.V. Yuferev, A.N.Ezin Framework as the main tool for developing a web application**.....532**

P.V. Yavtushenko, A.Yu. Oparin The modern displaying devices development problems and prospects **541**

BRIEF INFORMATION ABOUT THE AUTHORS **552**

AUTHOR INDEX **572**

PART II

SECTION 2
INFORMATION SECURITY

J.A. Bezugly, A.V. Vershennik, A.V. Popova, E.V. Sukhorukova The authentication methodology analysis **20**

J.A. Bezugly, A.V. Vershennik, A.V. Popova, E.V. Sukhorukova The main threats to authentication **25**

N.V. Belan, I.V. Karasev, L.A. Luganskaya Comparison of ansembles of multiphase orthogonal signals **29**

N.P. Borisenko, A.M. Tsyganov, M.A. Kulikov Generation of s-blocks with the specified parameters using parallel computing **35**

B.P. Borisov, A.I. Yankina Analysis of hardware information protection equipment in data-networks **39**

E.A. Boyarchuk, *I.V. Yukhnov, *P.S. Shevchuk Analysis of security threats to organizations **43**

A.V. Vershennik, M.N. Korchemkina, N.A. Kupriyanov, E.V. Sukhorukova Analysis of the conditions ensuring the authenticity of information, during transmission through the channels of the MTSIP UTN of the Russian Federation **49**

A.V. Vershennik, M.N. Korchemkina, N.A. Kupriyanov, E.V. Sukhorukova Analysis of methods of computer steganography **54**

A.S. Galkin, D.O. Markin Distributed testing of web-applications by fazzing method based on web-proxy and active data technologies **61**

M.G. Gizatullin, D.V. Varakosov Some features of realization of threat of unauthorized access to system through wireless channels of communication **72**

I.S. Girin, E.A. Statsenko, I.A. Sosnovsky Analysis of protection methods in wireless networks of 802.11 standard **77**

O.V. Goncharova, A.A. Goncharov Information security of modern youth society: tendencies and threats **79**

A.S. Zhuck[1], V.A. Golovskoy[2] The analysis of the computational complexity of solving the problem on the multiple knapsack **82**

A.S. Zhuck[1], V.A. Golovskoy[2] Synthesis of a hierarchical system of information protection from unauthorized access on the basis on the Bell–LaPadula model **91**

E.T. Ishdavletova, K.A. Roldugina E nsuring information security in the context of modernization and development of postal services on the basis of ICT **98**

A.G. Kirheev[1], V.A. Golovskoy[2] To the problem of information security mobile device **104**

S.M. Krasnopeev, A.A. Yurkin Investigation incidents of information security, based on analysis image of main storage **107**

A.Y. Kudriashova, A.N. Rudnev Researching and developing of method for assessing information security network storage **115**

S.I. Kuznetsov, S. P. Tesla, E.V. Sukhorukova, A.V. Vershennik The option of changing the logical structure of the address space information and communication networks **125**

A.A. Polkov, A.S. Sovenko Some aspects of practical realization of digital signature. **133**

A.A. Polkov, A.S. Sovenko Overview of ways for the software implementation of linear transformation **136**

N.V. Putilin[1], V.A. Golovskoy[2], Krutov V.A.[1] Comprehensive approach to building and modernization of special radio networks **141**

N.I. Sydnyaev, S.A. Govor Study of experiment planning when building models with random drift parameters of the regression model **146**

V.N. Smolyakov, R.M. Kildishev Modernization of the system of information security office contact center Tele2 - Rostov software and hardware **156**

V.N. Smolyakov, V.V. Silchenko Development of the information protection system for LANTS of Rudnyansky letter of Volgograd branch of MYFF "South" PJSC "Rostelecom" **162**

M.G. Usynin, A.Yu. Oparin Information protection and information security **168**

A.N. Chikalov, A.I. Yankina Buffer overflow on the stack. methods of detection and fight against this type of exploit **176**

O.V. Shvachko, I.S. Derkachev The issues on the protection of personal data in information systems **180**

D.A. Yakovlev, I.S. Sineva Common mistakes in design and implementation of the network protocols for data exchange **184**

SECTION 3
INFOCOMMUNICATION TECHNOLOGIES IN MANAGEMENT, ECONOMY AND EDUCATION

A.S. Artemenkova, A.I. Момот Application of the lean production system at the enterprises of postal communication **190**

A.H. Babayan, P.V. Lobzenko A n interactive tutorial on the subject "Technology of programming" **197**

***D.A. Bezuglov, **A.P. Kuzin, **S.A. Shvidchenko** Contour detection of images for multimedia applications based on the discrete wavelet transform **200**

E.A. Bineev Features of the structure of the discipline Life safety in the direction of ITCS **209**

A.E. Boyarchuk, *V.I. Yukhnov, *P.S. Shevchuk Improving the efficiency of the system project management **211**

S.A. Bystrov Personal identity identification: analysis of approaches to solution **217**

N.A. Vernigorova, I.V. Golovina The problem of import substitution in infocommunications **221**

I.V. Vodovozov, D.A. Vasinev Developing of the access node to the packet switching network for using in an education process **225**

M.G. Gizatullin, F.I. Turaev S ome aspects of realization of media educational technologies within organization of educational process for the subject matter «Basis of information security in interior» **228**

Y.I. Gnilomyodov, I.I. Shestakov Estimation of the applicability of the components of the elected networks of the ITU-T G.984 standard architecture FTTX, for the organization of the training process for the formation of the professional competencies of graduates in accordance with the federal state educational standard of higher education 3+ **242**

O.V. Goncharova, A.Yu. Oparin The health of the teacher is the key to professional longevity **249**

A.M. Danilova, Sh.A. Tursunov Organization of investment processes management **251**

N.V.Danilova Estimation of parameters in the stochastic volatility model **256**

D.E. Demidov, L.N. Evdakova Development prospects and problems of infocommunication branch in russia **258**

Yu.N. Denisenko, Yu.A. Oleinikova "Word of mouth" marketing as a tool of branding **265**

V.Yu. Denisov, I.S. Sineva Business intelligence: usage and tools **271**

S.A. Dokuchaev, G.S Kostetskaya, N.O. Svetlichnaya To the question of forming general vocational competences of bachelors in the field of information technologies and computing techniques when studying general science group subjects (on the example of case-method) **276**

S.A. Dokuchaev, G.S Kostetskaya T o the question of interdisciplinary interaction in educating bachelors of infocommunication industry (on the example of a problem of mathematical physics) **279**

L.I. Doliner, N.G. Bikbulatova E-course as a basic component of learning in modern university **282**

Dotkulova A.S., Moseva M.S. Method of intellectual verification of logical connections of modules of educational program in accordance with new educational standards. **287**

L.N.Evdakova The role of self-working in the infocommunication university students competences formation **294**

I.V. Kalienko, I.S. Abramov, N.I. Abramova Development of methodical recommendations study of thyristors in a laboratory setting "Electronic devices" of the department "Electronics" DGTU **300**

E.A. Kolomiets, A.M. Korshun Improving of the students out-of-class individual work based on information technologies **309**

B.B. Konkin Infocommunications technologies used in education **314**

D.V. Kostyuchenko, P.M. Tabunshchikova Culture of speech in the life of it-specialists and all of humanity **319**

V.G. Lisitsin Problems of organization marketing communications in a small business **322**

R.A. Момот Peculiarities of forming venture processes investments in russia **326**

M.L. Mukhitdinova, V.A. Karimova The analysis of process of the enterprise stocks management on the basis of the combined ABC and XYZ analysis method **330**

***V.A. Pogorelov, *A.O. Semiletkin, S.A. Shvidchenko** The research method of parametric identification of dynamic systems in conditions of interference **335**

M.A. Ptashinskiy, A.I. Момот F eatures of transition to version of innovation standard ISO 9001-2015 **341**

E.G. Rotova, A.I. Момот Use of the process approach when performing purchasing activity of the enterprise **346**

A.A. Sannikov, V.T. Kuanyshev Information technologies and processing big data in education **351**

E.A. Svirsch Information competence of economists **354**

T.V. Sidorina Providing of security on enterprises of postal connection **358**

E.A. Skorobogatova Infocommunication services influence for efficiency of Sberbank activity **.364**

I.A. Stepskaya, S.A. Ukolova, A.I. Момот Evaluation of the competitiveness of services for the receipt of utility bills in the organization «Post of Russia» **368**

V.N. Trofimenko, A.V. Pavlova, K.V. Pashchenko Of the plane imitating modelling of the contour of angular stabilization **373**

D.L. Ustimenko, E.A. Gatilova Actual problems of computer design in the modern information and communication technologies **377**

V.V. Fedotov, E.N. Tishchenko, A.A. Yakovenko Building a system of information support of life cycle design and production of science-intensive telecommunication products based on a common information space in the form of a virtual enterprise between PJSC Rostelecom and leading manufacturers and designers of TC materials and equipment, construction of TC companies **380**

P.C.E. Fedotova, N.V. Budyldina Realization industrial internet of thing in Russia **384**

O.I. Sharavova, M.P. Belyanchikova, I.A. Novikova The results of the comparative evaluation of the financial situation of the largest russian operators mobile **388**

A.A. Yakovenko, M.A. Galukhin Modern society transformations and human resources management innovations **395**

A.A. Yakovenko, E.P. Kosareva Planning as a mechanism of implementation of social and economic development goals of the contemporary society **401**

A.A. Yakovenko, A.A. Pyatina Innovations and risk in the communications industry **407**

A.A.Yakovenko , O.O. Shadrunova Statistical study of poverty and social inequality in the russian society **412**

BRIEF INFORMATION ABOUT THE AUTHORS **419**

AUTHOR INDEX **439**

Ю.А. Безуглый, А.В. Вершенник, А.В. Попова, Е.В. Сухорукова

АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия

Ключевые слова: обеспечение подлинности, аутентификация, методы аутентификации.

В статье представлены основные понятия и опреление аутентификации, уточнена и систематизирована классификация методов аутентификации.

J.A. Bezugly, A.V. Vershennik, A.V. Popova, E.V. Sukhorukova

THE AUTHENTICATION METHODOLOGY ANALYSIS

Military Academy of telecommunications named. Marshal Of The Soviet Union S. M. Budyonny, Saint-Petersburg, Russia

Keywords: security authentication, authentication, authentication methods.

The article presents the basic concepts and the definition of authentication, refined and systematized the classification of authentication methods.

В настоящее время передача данных по незащищенным каналам связи создаёт потенциальную возможность для действий злоумышленников. В информационных системах хранится, обрабатывается, циркулирует различная информация, потеря или искажение которой может нанести существенный вред. Поэтому для обеспечения информационной безопасности, одной из важных задач является использование методов и средств для того, чтобы проверяющая сторона убедилась в подлинности проверяемой стороны [1-4].

Для достижения этих целей используют процедуры идентификации и аутентификации. Несмотря на близость этих понятий, обозначают они принципиально разные вещи.

Идентификация — процедура распознавания субъекта по его идентификатору (некоторой информации — числу, строке символов).

Аутентификация (подтверждение подлинности) — процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации.

Таким образом, идентификация — это всего лишь поиск идентификатора в базе данных учетных записей, а аутентификация — это проверка соответствия между

субъектом и предъявляемым им идентификатором. Чтобы доказать свою подлинность, субъект должен предъявить нечто, называемое фактором аутентификации. Строго говоря, фактор аутентификации — это определенный вид уникальной информации, предоставляемый субъектом системе при его аутентификации [5].

Существует четыре основных типа аутентификационной информации:

1) Пользователь знает уникальную информацию. Самый яркий пример – парольная аутентификация.
2) У пользователя есть некий предмет, обладающий уникальными характеристиками или содержимым (смарт-карты, токены и т.д.).
3) Аутентификационная информация – неотъемлемая часть пользователя. Данный тип называется общим термином «биометрическая аутентификация». В качестве примеров выступают отпечатки пальцев, радужной оболочки глаза и другие способы.
4) Аутентификация посредством электронной подписи.

Процедура аутентификации состоит из двух этапов:

1) При первом взаимодействии пользователя с защищаемой информацией у него берется некий эталонный образец аутентификационной информации. Он хранится у модуля аутентификации – субъекта системы, проверяющего аутентификацию.
2) Каждый раз при выполнении аутентификации необходимо ввести данную аутентификационную информацию, которая сравнивается с эталоном. В случае совпадения пользователь считается подлинным и получает доступ к информационным ресурсам в соответствии с выделенными ему правами.

Эталон может храниться и в «чистом» виде, и в преобразованном. Например, если в качестве метода аутентификации используется один из биометрических способов, эталон свертывается в кодовое значение, точно так же будет каждый раз свертываться и введенная пользователем аутентификационная информация. Такое преобразование задействует меньший объем памяти для хранения эталона и требует меньшее время для сверки с ним введенной информации.

Аутентификация бывает односторонней (когда, например, сервер проверяет пользователя) и взаимной (когда участники информационного обмена проверяют друг друга).

Для повышения стойкости аутентификации зачастую используются несколько методов аутентификации (например, смарт-карта и пин-код или пароль и отпечаток пальца). Если аутентификация проводится на основе предъявления нескольких видов аутентификационной информации, она называется многофакторной.

Рассмотрим основные типы аутентификации.

Парольная аутентификация.

Является наиболее распространенным вариантом проверки подлинности пользователей ввиду простоты использования. Но у нее есть и существенные недостатки:

1) Зачастую пароль легко подобрать, так как он легко предугадываем, например:
   - В нем фигурирует какая-то информация о пользователе (имя, дата рождения и т.д.) или же он эквивалентен имени пользователя.
   - Пароль – слово или фраза. Такой пароль взламывается путем «словарной атаки» - перебора всех слов согласно словарю выбранного языка.
   - Пароль очень короткий и взламывается простым перебором.

2) Существует множество утилит подбора паролей. Их основное назначение – помочь пользователю вернуть возможность работы с информацией при утере пароля, но злоумышленники также нередко пользуются этим способом.
3) Пароль может быть получен путем насилия над пользователем.
4) Пароль может быть подсмотрен или перехвачен при вводе.

Парольная аутентификация бывает двух типов: по одноразовым и многоразовым паролям. Многоразовые используются гораздо чаще, но их легче взломать. Основной же сферой применения одноразовых паролей является финансовая, так как одноразовый пароль гораздо труднее перехватить, а при каждой следующей попытке аутентификации нужно будет вводить новый пароль.

Аутентификация с помощью уникального предмета

Как правило, данный метод обеспечивает более серьезную защиту, чем парольная аутентификация.

Предметы, которые используются для аутентификации, можно разделить на две группы:

1) «Пассивные» - предметы, которые просто содержат аутентификационную информацию, причем она может храниться как в открытом, так и в зашифрованном виде. В последнем случае для получения доступа к хранящимся данным необходимо ввести пин-код, что делает такой предмет средством двухфакторной аутентификации.
2) «Активные» предметы. Они обладают достаточными вычислительными ресурсами, чтобы самостоятельно участвовать в процессе аутентификации (токены, микропроцессорные смарт-карты). При удаленной аутентификации пользователя можно обеспечить строгую аутентификацию (секретная информация, позволяющая проверить подлинность пользователя, не передается в открытом виде).

У аутентификации с использованием уникальных предметов есть и некоторые недостатки:

1) Предмет может быть похищен.
2) В большинстве случаев необходимо специальное оборудование.
3) В теории возможно изготовление копии или эмулятора предмета.

Биометрическая аутентификация

Данный тип аутентификации основан на уникальности некоторых характеристик человека. Наиболее часто используемыми являются следующие характеристики:

1) Отпечатки пальцев.
2) Узор радужной оболочки глаза и структура сетчатки глаза.
3) Черты лица.
4) Форма кисти руки.
5) Голос.
6) Тепловая карта лица.
7) Форма и способ подписи.

Погрешность при сравнении с образцом устанавливается заранее на основе оптимального соотношения коэффициентов ложного принятия (FAR) и ложного отказа (FRR) (данные величины должны быть минимальны). Эти коэффициенты обратно зависимы. Надежными можно назвать системы, в которых погрешность FAR настроена примерно на величину 0,01-0,001%, а FRR – 3-5%.

Средства биометрической аутентификации также имеют недостатки:

1) За продолжительное время некоторые характеристики могут измениться (в результате ожогов, порезов, ампутации и т.д.), и в таком случае аутентификация может и не пройти.
2) База эталонов может быть изменена злоумышленником.
3) Возможно применение муляжа.
4) Если биометрические данные крадут или компрометируют, их практически невозможно сменить.
5) Биометрические характеристики уникальны, но их нельзя сохранить в секрете.

Аутентификация при помощи электронной подписи

Существуют следующие виды электронной подписи:

1) Простая электронная подпись – электронная подпись, которая посредством использования паролей, кодов или иных средств подтверждает факт формирования подписи определенным лицом.
2) Неквалифицированная электронная подпись – электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет определить лицо, подписавшее документ, обнаружить факт внесения изменений в документ после момента его подписания и создается с использованием средств электронной подписи.
3) Квалифицированная электронная подпись – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

Ключ проверки электронной подписи указан в квалифицированном сертификате.

Для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

Технология электронной подписи имеет широкие перспективы внедрения во всех сферах жизни современного общества, связанных с передачей и обработкой информации. В отличие от собственноручной подписи, электронная подпись позволяет передавать подписанный документ по каналам связи без пересылки материального носителя документа и сохранять при этом возможность проверки его подлинности. Кроме того, электронную подпись очень сложно подделать. На данный момент не известно ни одного случая успешной подделки электронной подписи, созданной в соответствии с международными или российскими стандартами. В случае же, если подпись не подделана, не похищена и не передана другому лицу, она позволяет однозначно идентифицировать создателя документа как подлинного. Помимо этого, подписать электронной подписью можно не только весь документ, но и только отдельные его части.

Наряду с этим существует и ряд недостатков. Например, если закрытый ключ, используемый для подписания документа, будет передан кому-либо, доказать, что подпись подлинна, будет невозможно. Если же этот ключ будет похищен, то определить, когда были подписаны документы – до или после похищения – будет практически невозможно, так как создатель документа может по своему усмотрению менять любые параметры и свойства документа, а также и время его передачи. Еще одним недостатком является наличие посредника – так как ключ представляет собой последовательность нулей и единиц, он крайне неудобен для восприятия. Да и не способен человек считать эту последовательность с электронного носителя. Значит, существует необходимость

доверять тому оборудованию, которое будет использовано для работы с подписью. Наконец, у электронной подписи есть свой срок действия, который оговаривается при ее создании. Это накладывает определенные ограничения на ее использование, так как, если подписать документ, скажем, за день до истечения ее срока действия, то через сутки он утратит свою юридическую значимость.

Таким образом, различные методы аутентификации обладают своими особенностями работы и применения, своими достоинствами и недостатками. У каждого из них есть свои сферы применения и свои перспективы. В зависимости от ситуации может быть наиболее предпочтительным тот или иной метод, но главным остается одно – каждый из методов имеет свои уязвимости и поэтому требует доработки и улучшения.

СПИСОК ЛИТЕРАТУРЫ

1. *Мартынова Л. Е., Умницын М. Ю., Назарова К. Е., Пересыпкин И. П.* Исследование и сравнительный анализ методов аутентификации // Молодой ученый. — 2016. — №19. — С. 90-93.
2. *Стародубцев Ю.И., Чукариков А.Г., Корсунский А.С., Сухорукова Е.В.* Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны. В сборнике: Интегрированные системы управления сборник научных трудов научно-технической конференции. 2016. С. 199-206.
3. *Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В.* Проблема формирования системы динамической защиты государственных информационных систем / В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 239-243.
4. *Евграфов А.А., Шугуров Д.Е., Сухорукова Е.В., Закалкин П.В.* Способ защиты бизнес-процессов, использующих удаленные информационные ресурсы, посредством одношаговой аутентификации / Проблемы экономики и управления в торговле и промышленности. 2013. № 3. С. 60-67.
5. *Комаров А.* Современные методы аутентификации // Т –Comm. - № 6. – 2008. – с. 13 – 16.
6. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – кн. 1,2.
7. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атака через Интернет. НПО «Мир и семья-95», 1997.
8. *Мельников В.В.* Защита информации в компьютерных системах. – М.; Финансы и статистика, 1997.
9. *Олейник В.* Основные открытия XX века в области криптографии // Acta Academia, Chisinau: Evrica, 2000. - С.23-38.
10. *Охрименко С.А., Черней Г.А.* Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // НТИ. Серия 1. Организация и методика информационной работы. – 1996, № 5. - С.5-13.
11. *Черней Г.А.* Проблемы аутентификации в информационных системах. – Кишинев: Реклама, 2001. – 112 с.

Ю.А. Безуглый, А.В. Вершенник, А.В. Попова, Е.В. Сухорукова

ОСНОВНЫЕ УГРОЗЫ АУТЕНТИФИКАЦИИ

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия

Ключевые слова: обеспечение подлинности, аутентификация, угрозы аутентификации.

Процедуры удаленной аутентификации подвержены многим негативным факторам, что требует защиты данных процедур и требует тщательного их изучения. В статье рассмотрены условия обеспечения процедур удаленной аутентификации, уточнена и систематизирована классификация угроз, направленных на нарушение процедур аутентификации.

J.A. Bezugly, A.V. Vershennik, A.V. Popova, E.V. Sukhorukova

THE MAIN THREATS TO AUTHENTICATION

Military Academy of telecommunications named. Marshal Of The Soviet Union S. M. Budyonny, Saint-Petersburg, Russia

Keywords: security authentication, authentication threats authentication.

The procedure of remote authentication is susceptible to many negative factors that require the protection of data procedures and requires careful study. The article considers the terms of the security procedures for the remote authentication, refined and systematized classification of threats aimed at the disruption of the authentication procedures.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности (ИБ), и в ходе технического прогресса эта зависимость будет возрастать.

Решение задач ИБ затрудняется из-за внедрения новых методов и средств передачи информации, обусловленными тенденциями развития современных систем и средств связи, основными из которых являются:

увеличение пропускной способности систем связи (СС);

широкое использование возможностей сети ЕСЭ для передачи информации;

разработка и использование методов повышения безопасности сетевых технологий.

При этом одной из основных задач является обеспечение целостности информации, а также подтверждение подлинности и авторства каждого массива данных [1-3].

Аутентификация пользователя – это проверка, действительно ли проверяемый пользователь является тем, за кого он себя выдает. Различные методы аутентификации необходимы, чтобы разграничить и ограничить доступ к данным. После прохождения процесса аутентификации пользователь получает доступ согласно политики доступа, а также набор прав, которые для данного пользователя выделил администратор.

В настоящее время достаточно много существует механизмов и средств современных систем аутентификации, но при этом достаточно сложно определить на сколько сможет тот или иной механизм повысить защищенность процесса удаленной аутентификации при информационном обмене пользователей в условиях воздействия внешнего нарушителя.

Обобщенная схема аутентификации пользователя при его доступе к автоматизированной системе (АС) представлена на рисунке 1. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации его пропускает и в дальнейшем должна определить его полномочия (авторизация). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

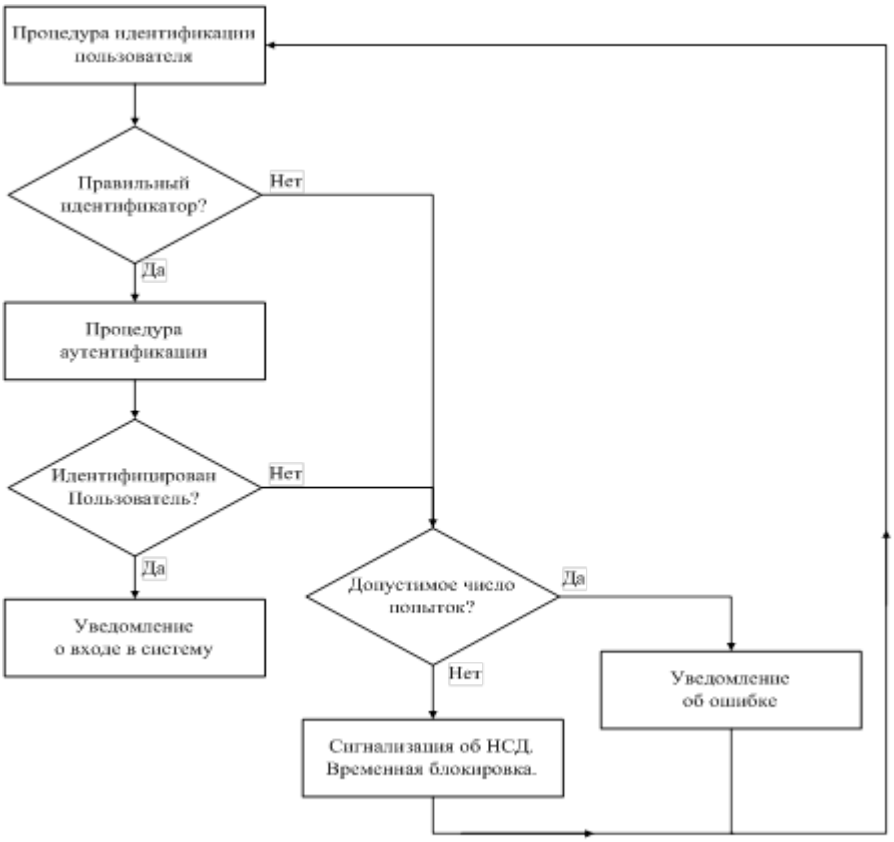


Рисунок 1. Обобщенная схема аутентификации

Данная процедура широко используются на практике в различных автоматизированных системах (АС) для определения аутентичности пользователей или процессов запущенных от их имени.

Система обеспечения информационного обмена распределена географически и задачи проверки объектов взаимодействия в данных условиях определяется по

предоставлению аутентификационной информации через открытые каналы сети связи общего пользования Единой сети электросвязи Российской Федерации.

Основными угрозами аутентификации являются [4-9]:

1) Пассивное наблюдение.

   Данный способ наиболее прост в реализации и трудно обнаружим, но при использовании криптографических протоколов аутентификации атака не является действенной. Если сообщения зашифрованы и ключи не скомпрометированы, этот вид угрозы бесполезен.

2) Воздействие на обменную информацию.

   При этом виде угроз злоумышленник перехватывает передаваемую информацию, изменяет ее и отсылает получателю. В результате получатель уверен, что имеет дело с подлинными данными, отправленными авторизованным пользователем, в то время как получает подмененную информацию. Данный вид угроз опасен тем, что нарушает целостность данных, что влечет за собой их прямые потери.

3) Изменение структуры протокола.

   Сущность данной угрозы проста: злоумышленник видоизменяет структуру протокола аутентификации, в результате чего законные участники не могут завершить протокол. Последствия могут быть разными: от отказа в обслуживании авторизованных пользователей до получения нарушителем доступа к ресурсам информационной системы.

4) Видоизменение механизмов принятия решений.

   Примером данного вида угроз является изменение программы проверки подписи, принятия решений об аутентичности и так далее. Эта угроза опасна в первую очередь потому, что обнаружить ее возможно только при реализации самозащиты механизмов обеспечения безопасности и наличии доверительной компьютерной базы.

4) Криптоанализ. Это наиболее известный метод атаки на любые модели защиты, использующие криптографические операции.

5) Перехват обменной информации - несанкционированное чтение информации. Если применяются криптографические методы защиты для построения протоколов аутентификации, нарушитель не сможет воспользоваться перехваченной информацией, не имея необходимых ключей.

6) Повтор сообщений - повторная передача ранее регистрированных сообщений. Часто получатель должен быть уверен в том, что моменты формирования, передачи и приема сообщения очень близки друг к другу. Это означает, что отправитель в момент приема сообщения получателем находится на другом конце канала связи. Если получатель не может в этом убедиться, его легко ввести в заблуждение, что зачастую приводит к серьезным последствиям.

7) Маскарад - попытка выдать себя за другого в целях получения несанкционированного доступа к информационным ресурсам или расширения полномочий. По сути, является нарушением состояния аутентификации.

8) Дезорганизация - незаконное изменение адресной части передаваемой информации. В результате дезорганизация может привести к нарушению целостности технологических процессов обработки данных (в частности, отказ в обслуживании) и, соответственно, к значительным материальным потерям.

9) Манипуляция - незаконная замена, вставка, удаление или переупорядочение данных в информационных потоках. Она похожа на манипуляцию, но есть и отличия. Основное заключается в том, что если у дезорганизации нет четкой цели, то при манипуляции данными злоумышленник ставит цель заранее.
10) Отказ от обязательств. Состоит в отказе от ранее принятых или переданных сообщений (взятых на себя обязательств). Отказ от обязательств наиболее распространен в системах электронной торговли и банковских информационных системах, когда пользователь отказывается от проведенных ранее транзакций. Развитие технологий, в особенности появление криптографических средств, позволило решить данную проблему. Основным шагом вперед стало применение электронной цифровой подписи, позволяющее фиксировать авторство сообщения без возможности отказа от него.
11) Подбрасывание ключей - самая распространенная атака на протоколы, основанная на криптографии с открытыми ключами. Она заключается в следующем: злоумышленник представляет свой публичный ключ вместо публичного ключа легального пользователя; если он подписывает сообщение своим секретным ключом, получатель решит, что его подписал законный участник процесса обмена данными. Эта атака является особо опасной для финансово-банковских систем, так как в конечном итоге может быть проведена незаконная транзакция.
12) Атака рефлексией с параллельным протоколом. Реализуется следующим образом: нарушитель начинает встречный протокол и посылает те же вопросы, которые он получает. Например, если кто-то запрашивает пароль, можно ему же параллельно адресовать это вопрос. Если злоумышленник получает ответ, то он возвращает его, и этот ответ будет принят как верный.
13) Главный в центре (MITM, Man In The Middle). Состоит в том, что нарушитель ведет диалог одновременно с каждым из участников, а они думают, что сообщаются напрямую.

Таким образом, процедуры удаленной аутентификации подвержены многим негативным факторам, что требует защиты данных процедур и требует тщательного их изучения. Необходимость исследования удаленной аутентификации диктуется также недопустимо низким уровнем эффективности существующих средств защиты процедур аутентификации при целенаправленном воздействии нарушителя. Это обусловлено тем, что в условиях целенаправленных воздействий нарушителя, многие параметры сети, такие как вероятность ошибки на бит, скорость передачи данных, задержки на каждом узле, преднамеренное изменение аутентифицирующих последовательностей, не обеспечивают корректную работу процедур аутентификации.

СПИСОК ЛИТЕРАТУРЫ

1. *Стародубцев Ю.И., Чукариков А.Г., Корсунский А.С., Сухорукова Е.В.* Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны. В сборнике: Интегрированные системы управления сборник научных трудов научно-технической конференции. 2016. С. 199-206.
2. *Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В.* Проблема формирования системы динамической защиты государственных информационных систем / В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и

образовании сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 239-243.
3. *Евграфов А.А., Шугуров Д.Е., Сухорукова Е.В., Закалкин П.В.* Способ защиты бизнес-процессов, использующих удаленные информационные ресурсы, посредством одношаговой аутентификации / Проблемы экономики и управления в торговле и промышленности. 2013. № 3. С. 60-67.
4. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – кн. 1,2.
5. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атака через Интернет. НПО «Мир и семья-95», 1997.
6. *Мельников В.В.* Защита информации в компьютерных системах. – М.; Финансы и статистика, 1997.
7. *Олейник В.* Основные открытия XX века в области криптографии // Acta Academia, Chisinau: Evrica, 2000. - С.23-38.
8. *Охрименко С.А., Черней Г.А.* Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // НТИ. Серия 1. Организация и методика информационной работы. – 1996, № 5. - С.5-13.
9. *Черней Г.А.* Проблемы аутентификации в информационных системах. – Кишинев: Реклама, 2001. – 112 с.

Н.В. Белан, И.В. Карасев, Л.А. Луганская

СРАВНЕНИЕ АНСАМБЛЕЙ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ

ФГАОУ ВПО Северо-Кавказский федеральный университет, Ставрополь, Россия

Ключевые слова: собственные вектора, Эрмитова матрица, ансамбль многофазных ортогональных сигналов, структурная скрытность, модели сигналов.

В статье рассмотрены ансамбли многофазных ортогональных сигналов, получаемые путем их моделирования собственными векторами Эрмитовых матриц. Представлены результаты расчетов количества уникальных ансамблей многофазных ортогональных сигналов, сделан вывод о целесообразности увеличения количества структур сигналов при рассмотрении Эрмитовых матриц со всеми ненулевыми диагональными коэффициентами.

N.V. Belan, I.V. Karasev, L.A. Luganskaya

COMPARISON OF ANSEMBLES OF MULTIPHASE ORTHOGONAL SIGNALS

Federal State Educational Institution of Higher Professional Education
North-Caucasian Federal University, Stavropol, Russia

Keywords: eigenvectors, Hermite matrix, ensemble of multiphase orthogonal signals, structural stealth, signal models.

In this article, there are ensembles of multiphase orthogonal signals obtained by their simulation by the eigenvectors of Hermitian matrices. The results of calculations of the number of unique ensembles of multiphase orthogonal signals are presented, it is concluded that it is advisable to increase the number of signal structures when considering Hermitian matrices with all nonzero diagonal coefficients.

Как известно из [1-4, 5, 10] для обеспечения структурной скрытности сигналов-переносчиков информации необходим ансамбль ортогональных сигналов (АОС) большого объема. На сегодняшний день известно множество способов получения АОС [1-4], однако, не каждый из этих способов позволяет решить в полной мере данную задачу.

Вариантом повышения структурной скрытности, по мнению авторов, является получение представительного количества ансамблей сигналов, моделируемых собственными векторами Эрмитовой матрицы (ЭМ). При этом, для примера, в данной работе рассматриваются ЭМ четвертого порядка (N=4) с количеством диагональных коэффициентов от 3 до 6, рассчитываются собственные вектора (СВ) ЭМ, являющиеся моделями ансамблей многофазных ортогональных сигналов (АМФОС). После этого оценивается количество фаз в сигнале, то есть количестве структур сигналов, и на основе оценки делается вывод о целесообразности или нецелесообразности стохастического применения полученных сигналов.

Задачей статьи является сравнительный анализ возможностей способа получения АМФОС на основе СВ ЭМ при различном количестве ненулевых диагональных коэффициентов ЭМ.

Целью статьи является обоснование преимуществ способа получения АМФОС, моделируемых СВ ЭМ с ненулевыми диагональными коэффициентами.

Определим условия проведения экспериментов:

- расчеты СВ осуществляются для бидиагональной ЭМ четвертого порядка (N=4);
- во всех экспериментах изменениям подвергается фаза одного диагонального коэффициента - $A_{1,2}$.

В ЭМ вида (1) диагональные коэффициенты представлены в показательной форме, где $A_{1,2}=A_{2,1}=100$, $A_{2,3}=A_{3,2}=14$, $A_{3,4}=A_{4,3}=100$ – это фиксированные для анализа значения модулей, а $\varphi_{i,j}$ – значения аргументов, определяющих фазу, диагональных коэффициентов ЭМ.

$$M = \begin{pmatrix} 0 & A_{1,2}\cdot e^{i\cdot\varphi_{1,2}} & 0 & 0 \\ A_{2,1}\cdot e^{i\cdot\varphi_{2,1}} & 0 & A_{2,3}\cdot e^{i\cdot\varphi_{2,3}} & 0 \\ 0 & A_{3,2}\cdot e^{i\cdot\varphi_{3,2}} & 0 & A_{3,4}\cdot e^{i\cdot\varphi_{3,4}} \\ 0 & 0 & A_{4,3}\cdot e^{i\cdot\varphi_{4,3}} & 0 \end{pmatrix} \quad (1)$$

Проанализируем АМФОС, получаемые в результате ввода в ЭМ (1) трех диагональных коэффициентов $A_{1,2}$, $A_{2,3}$, $A_{3,4}$.

Результаты эксперимента представлены в таблице 1.

Таблица 1 – АМФОС, полученные при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

№	Значения сигналов S1 – S4			
S1	$0{,}008 \cdot e^{i \cdot 88}$	$-0{,}055 \cdot e^{i \cdot (-106)}$	$0{,}68 \cdot e^{i \cdot 0}$	$-0{,}67 \cdot e^{i \cdot 179}$
S2	$0{,}68 \cdot e^{i \cdot 0}$	$-0{,}67 \cdot e^{i \cdot 179}$	$-0{,}008 \cdot e^{i \cdot (-92)}$	$0{,}055 \cdot e^{i \cdot 74}$
S3	$0{,}008 \cdot e^{i \cdot 88}$	$0{,}055 \cdot e^{i \cdot 74}$	$0{,}68 \cdot e^{i \cdot 0}$	$0{,}67 \cdot e^{i \cdot (-1)}$
S4	$0{,}68 \cdot e^{i \cdot 0}$	$0{,}67 \cdot e^{i \cdot (-1)}$	$-0{,}008 \cdot e^{i \cdot (-92)}$	$-0{,}055 \cdot e^{i \cdot (-106)}$

На рисунках 1 – 2 изображены визуализированные по данным из таблицы 1 модели АМФОС.

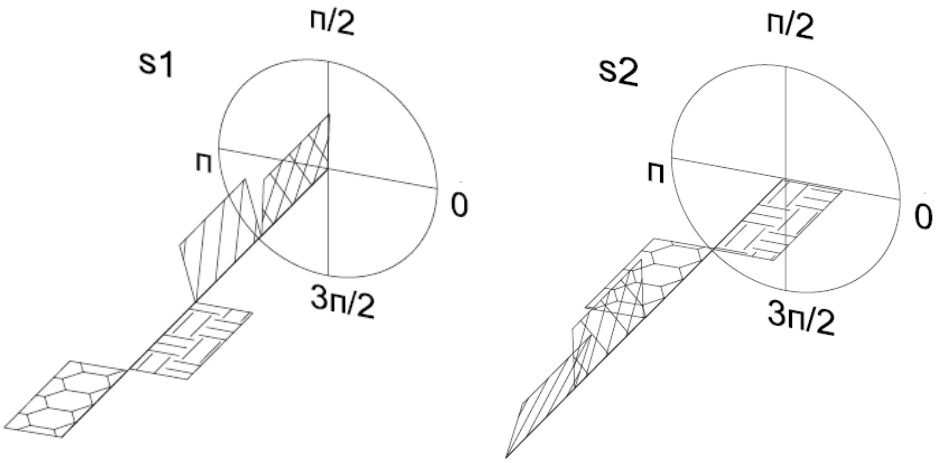


Рисунок 1 – Модели сигналов S1 и S2 при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

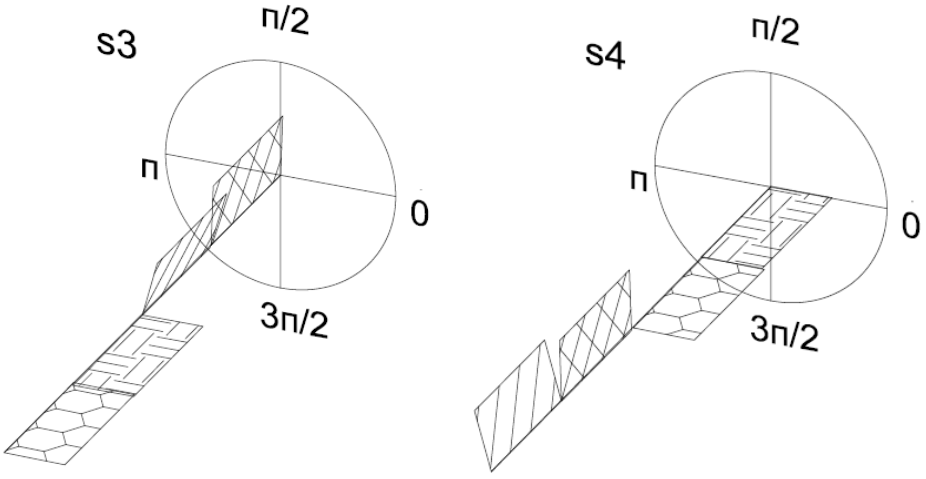
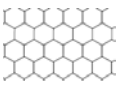


Рисунок 2 – Модели сигналов S3 и S4 при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

Штриховка моделей сигналов S1 – S4 соответствует значениям их фаз.

0^0  -1^0, 179^0 -92^0, 88^0 -106^0, 74^0

Д

для оценки количества получаемых АМФОС для матрицы вида (1) составим формулу:

$$K = N \cdot T \cdot D, \quad (2)$$

где K – общее количество уникальных АМФОС;

N – порядок матрицы;

T – количество возможных комбинаций изменения фаз коэффициентов ЭМ;

D – количество используемых фаз диагонального коэффициента ЭМ.

Для N=4, T=6, D=90, используя формулу (1) получим:

$$K = 4 \cdot 6 \cdot 90 = 2160.$$

По результатам расчетов составим таблицу 2.

Таблица 2. Результаты расчетов количества уникальных АМФОС

Порядок матрицы, N	Количество уникальных АМФОС, К
4	$2.112 \cdot 10^3$

Из результатов проведенного эксперимента следует вывод: в АМФОС, полученных при вводе трех диагональных коэффициентов в ЭМ присутствуют сигналы с повторяющимися значениями амплитуд при разных значениях фаз, что может снижать количество структур получаемых сигналов.

Далее проанализируем АМФОС, полученные в результате ввода в бидиагональную ЭМ вида (2) шести коэффициентов со следующими значениями амплитуд: $A_{1,2}=A_{2,1}=100$, $A_{2,3}=A_{3,2}=14$, $A_{3,4}=A_{4,3}=100$, $A_{1,3}=A_{3,1}=25$, $A_{2,4}=A_{4,2}=90$, $A_{1,4}=A_{4,1}=0{,}5$.

$$M1 = \begin{pmatrix} 0 & A_{1,2} \cdot e^{i \cdot \varphi_{1,2}} & A_{1,3} \cdot e^{i \cdot \varphi_{1,3}} & A_{1,4} \cdot e^{i \cdot \varphi_{1,4}} \\ A_{2,1} \cdot e^{i \cdot \varphi_{2,1}} & 0 & A_{2,3} \cdot e^{i \cdot \varphi_{2,3}} & A_{2,4} \cdot e^{i \cdot \varphi_{2,4}} \\ A_{3,1} \cdot e^{i \cdot \varphi_{3,1}} & A_{3,2} \cdot e^{i \cdot \varphi_{3,2}} & 0 & A_{3,4} \cdot e^{i \cdot \varphi_{3,4}} \\ A_{4,1} \cdot e^{i \cdot \varphi_{4,1}} & A_{4,2} \cdot e^{i \cdot \varphi_{4,2}} & A_{4,3} \cdot e^{i \cdot \varphi_{4,3}} & 0 \end{pmatrix} \quad (3)$$

Результаты эксперимента представлены в таблице 3.

Таблица 3 – АМФОС, полученные при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

№	Значения сигналов S1 – S4			
S1	$0{,}52 \cdot e^{i \cdot (-8)}$	$-0{,}43 \cdot e^{i \cdot 168}$	$0{,}6 \cdot e^{i \cdot 0}$	$-0{,}4 \cdot e^{i \cdot (-171)}$
S2	$0{,}41 \cdot e^{i \cdot 17}$	$-0{,}55 \cdot e^{i \cdot (-169)}$	$-0{,}4 \cdot e^{i \cdot 177}$	$0{,}59 \cdot e^{i \cdot 0}$
S3	$0{,}62 \cdot e^{i \cdot 0}$	$0{,}4 \cdot e^{i \cdot 0}$	$-0{,}51 \cdot e^{i \cdot (-169)}$	$-0{,}41 \cdot e^{i \cdot (-165)}$
S4	$0{,}39 \cdot e^{i \cdot 15}$	$0{,}56 \cdot e^{i \cdot 8}$	$0{,}45 \cdot e^{i \cdot (-1)}$	$-0{,}57 \cdot e^{i \cdot 0}$

На рисунках 3 – 4 изображены визуализированные модели АМФОС, представленные в таблице 2.

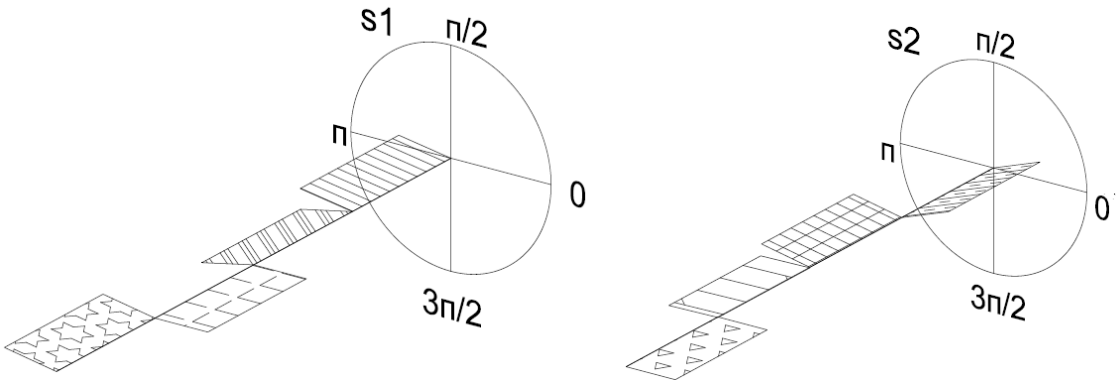


Рисунок 3 – Модели сигналов S1 и S2при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

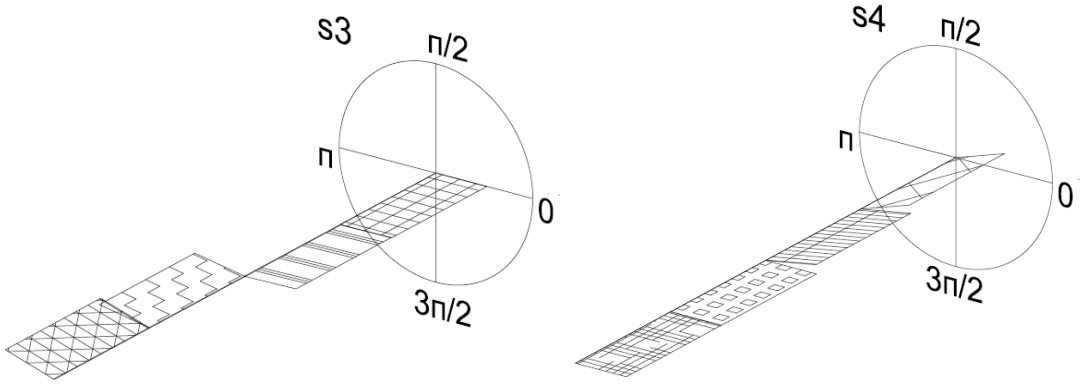


Рисунок 4 – Модели сигналов S3 и S4 при значении фазы $\varphi=15^0$ коэффициента $A_{1,2}$

Для моделей сигналов, представленных на рисунках 3 – 4 штриховка задана произвольно, без учета фактических значений фаз и амплитуд элементов сигналов.

Используя формулу (2) и значение T= 62 получим:

$$K = 4 \cdot 62 \cdot 90 = 22320. \quad (4)$$

По результатам расчетов составим таблицу 4.

Таблица 4. Результаты расчетов количества уникальных АМФОС

Порядок матрицы, N	Количество уникальных АМФОС, К
4	$2.232 \cdot 10^4$

Из исследований, проведенных при использовании в бидиагональной ЭМ шести коэффициентов, следует вывод:

- получены АМФОС с неповторяющимися амплитудами при одинаковом значении фаз;
- значения фаз элементов получаемых сигналов при использовании в бидиагональной ЭМ шести коэффициентов меняются в более широком числовом диапазоне, по сравнению со случаем использования в бидиагональной ЭМ трех коэффициентов.

Оценим преимущества второго способа над первым, для это выполним расчеты по формуле:

$$\Delta = 22320 - 2160 = 20160. \quad (5)$$

Таким образом, имеет смысл использовать для получения АМФОС ЭМ с шестью диагональными коэффициентами, так как полученные сигналы отличаются большим разнообразием фаз, что способствует повышению их структурной скрытности.

СПИСОК ЛИТЕРАТУРЫ

1. *Пашинцев В.П., Малофей О.П., Жук А.П.* Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн. – М.: Физматлит, 2010. – 195 с.
2. *Бабков В.Ю., Вознюк М.А., Никитин А.Н.* Системы связи с кодовым разделением каналов. – СПб.: СПбГУТ, 1999. – 120 с.
3. *Сухарев Е.М.* Общесистемные вопросы защиты информации: Коллективная монография. Кн. 1.– М.: Радиотехника, 2003. – 296 с.
4. *Жук А.П., Голубь Ю.С., Иванов А.С.* Методика стохастического формирования ансамблей дискретных ортогональных многоуровневых сигналов. // Информационное противодействие угрозам терроризма. 2011. N 6. С. 109-113.
5. *Осмоловский С.А.* Стохастические методы защиты информации. – М.: «Радио и связь», 2003. – 320 с.
6. *Короленко П.В., Рыжикова Ю.В.* Моделирование и обработка случайных сигналов и конструкций. – М.: МГУ, 2012. – 69 с.
7. *Вохник О.М., Зотов А.М., Короленко П.В.* Моделирование и обработка стохастических сигналов и структур: Учебное пособие. М.: Университетская книга, 2013, 125 с.
8. *Жук А.П., Черняк З.В., Сазонов В.В.*. О целесообразности использования ортогональных ансамблей сигналов с изменяющейся размерностью в системе CDMA // Инфокоммуникационные технологии. Том 6, N 4, 2008.
9. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.
10. *Залогин Н.Н., Кислов В.В.* Широкополосные хаотические сигналы в радиотехнических и информационных системах. – М.: Радиотехника, 2006. – 208 с.

Н.П. Борисенко, А.М. Цыганов, М.А. Куликов

ГЕНЕРАЦИЯ S-БЛОКОВ С ЗАДАННЫМИ ПАРАМЕТРАМИ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

Академия Федеральной службы охраны Российской Федерации, Орел, Россия

Ключевые слова: кластер, s-блок, линейный криптоанализ, диференциальный криптоанализ.

В тезисах представлен способ генерации криптографическистойких s-блоков. Приведен алгоритм внедрения данного способа в вычислительную кластерную систему. Обоснован выбор кластера как метода повышения скорости генерации криптографическистойких s-блоков путем распараллеливания сложных вычислений.

N.P. Borisenko, A.M. Tsyganov, M.A. Kulikov

GENERATION OF S-BLOCKS WITH THE SPECIFIED PARAMETERS USING PARALLEL COMPUTING

Academy of Federal Guarding Service of Russian Federation, Orel, Russia

Key words: cluster, s-box, linear cryptanalysis, differential cryptanalysis.

This article is devoted to the way of generation of the Cryptographically persistent s-blocks. The article describes an algorithm of implementation that way to computing cluster system. It tells about the cluster choice as a method of rate increasing of Cryptographically persistent s-blocks generation by way of Parallelization of complex computings.

Все современные алгоритмы шифрования представляют собой суперпозицию линейного и нелинейного шифрования. В качестве нелинейной части алгоритма шифрования выступают s-блоки. S-блоки, как узлы замены, применяются в действующих стандартах шифрования, таких как ГОСТ 34.12-2015 и американский стандарт AES. Для того, чтобы алгоритмы шифрования удовлетворяли требованиям, предъявляемым к практически недешифруемым шифрам, необходимо использовать в качестве нелинейной части криптостойкие s-блоки, которая оценивается с помощью существующих методов криптоанализа. Различают два основных метода криптоанализа дифференциальный и линейный. Дифференциальный криптоанализ - это атака на основе выборочного шифротекста. При этом анализируются изменения меры несовпадений двух открытых текстов на основных этапах криптопреобразования. В качестве меры несовпадения двух двоичных векторов используется расстояние Хэмминга. Линейный анализ направлен на поиск корреляции некоторых битов в открытых текстах. Каждый из этих подходов в итоге формирует набор параметров, анализ которых позволяет оценить криптойстойкость анализируемого s-блока.

Стойкость к дифференциальному анализу оценивается дифференциальным коэффициентом, который вычисляется по формуле:

$$p_g = 2^{-n} * \max_{\alpha,\beta \in V_n^x} |\{x \in V_n \mid g(x \oplus \alpha) \oplus g(x) = \beta\}|, [1]$$

где V_n – s-блок размерности n, $V_n^x = V_n\{0\}$, $g(x)-$ подстановка из V_x

g(x)-подстановкаизV_x.

Стойкость к линейному анализу оценивается линейным коэффициентом, который вычисляется по формуле:

$$\delta_g = \max |c(l_\alpha, l_{\beta \circ g})|, [1]$$

где$c(f_1, f_2)$ $c(f_1, f_2)$- функция корреляции булевых векторов, l_g - функция корреляции вектора x и α,

$l_{a \circ b}$ - функция корреляции векторов g и β.

Кроме этих параметров, для оценки криптостойкости s-блоков также вычисляются полином Жегалкина, степень нелинейности и другие характеристики.

Основная проблема криптоанализа s-блоков заключается в сложности алгоритмов, вычисляющих эти параметры. Как видно из представленных выше формул, вычислительная сложность расчета параметров изменяется в зависимости от размера s-блока по закону 2^n, где n – размерность s-блока. Это означает, что при достаточно больших размерах ($n \geq 8$), вычисление параметров только одного s-блока будет занимать уже ощутимое для человека время, а именно для n=8 несколько секунд. Когда же возникает необходимость вычислить характеристики нескольких s-блоков, то затрачиваемое время может оказаться недопустимо большим. Для уменьшения времени вычисления предлагается распараллелить процесс расчета параметров.

В настоящее время существуют две архитектуры вычислительных систем: системы с общей памятью и системы с распределенной памятью. Система с общей памятью предполагает использование всеми процессорами системы общей памяти. Такие системы строятся на базе одной ПЭВМ. Система с распределенной памятью наоборот предполагает использование каждым процессором системы своего отдельного участка памяти. Основной особенностью этих систем является возможность объединения нескольких ПЭВМ в одну систему под управлением центральной ПЭВМ. По этому принципу строятся современные высокопроизводительные кластеры.

Кластер – это слабосвязанная система связи узлов, в основе которой используется одна из стандартных технологий на базе шинной архитектуры или коммутатора. Его предназначение состоит в распределении вычислительной нагрузки между своими узлами, для уменьшения времени выполнения задачи. Одним из преимуществ по производительности кластера над системой с общей памятью является полная масштабируемость. Это означает, что можно объединить сколь угодно большое число ПЭВМ, и вместе они будут производительнее любого суперкомпьютера на базе одной ПЭВМ.

В современном мире, чтобы ускорить обработку информационных потоков, было разработано много моделей. Одной из самых популярных является модель, основанная на «передачи сообщений» (message passing). Реализована она была в стандарте MPI (Message Passing Interface). Данный стандарт представляет собой библиотеку, функции которой обеспечивают передачу сообщений между параллельными процессами, и управляет ими.

Кластер имеет массивно-параллельную структуру (MPP), преимущества данной архитектуры (Рис.1) в том, что она легко масштабируется, и «относительно дешевая»: стоимость 1 GFLOPS значительно меньше, чем у высокопроизводительных систем, использующих другие технологии. Также, неоспоримым преимуществом является использование в качестве аппаратной составляющей кластера обычные ПЭВМ, не оборудованные ни каким специальным аппаратным обеспечением.

В силу того, что MPP архитектура и архитектура обычного персонального компьютера отличаются, то и написание программного обеспечения требует отдельных особенностей. Поэтому для программирования под данную архитектуру были созданы различные библиотеки, позволяющие упростить разработку программ. Одна из таких библиотек реализует стандарт MPI (message passing interface). В эту библиотеку входят функции, позволяющие инициализировать и закрывать MPI процессы, выполнять обмен между процессами фиксировать время выполнения процессов, блокировать передачу, выполнять синхронный, асинхронный обмен данными, а также обмен данными с блокировкой.

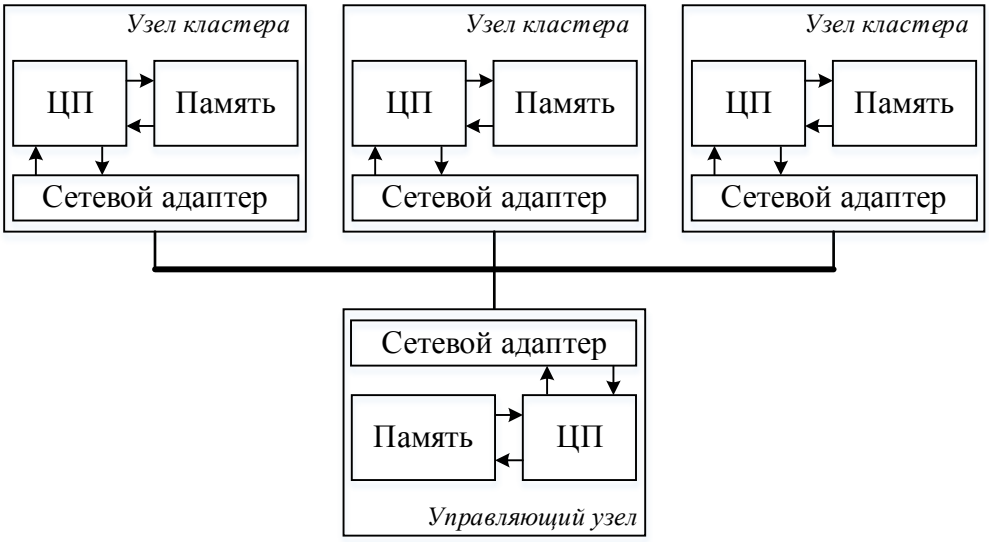


Рис.1. Обобщенная архитектура системы MPP

Также необходимо отметить, что для построения нестационарных кластеров (т.е. сети компьютеров, являющихся узлами кластера не постоянно, а возможно даже разово) уже существуют специализированные бесплатные дистрибутивы на основе ОС Linux, например, PelicanHPC GNU Linux. Преимущество данной системы в легкости развертывания: дистрибутив уже имеет в своем составе набор необходимых библиотек для управления параллельными процессами и программирования, имеется уже настроенная служба ssh с возможностью беспарольного доступа узлов к хосту по открытому ключу RSA. Также существует возможность указать виртуальный раздел в оперативной памяти, который будет использоваться как устройство хранения используемых программ. Это позволяет ускорить операции с файлами, а также не хранить на жестком диске данные. Кроме того, использования данного продукта обеспечивает хорошую масштабируемость комплекса (количество узлов варьируется от 2 до 65536).

Алгоритм применения кластера для генерации криптографическистойких s-блоков.

Необходимость использования кластера вытекает из того что, для генерации s-блоков будут применяться линейный и дифференциальный криптоанализы. Кроме того, необходимо осуществлять перебор всех элементов множества s-блоков, количество которых зависит от их размерности. А также рассчитать основные характеристики s-блока, такие как нелинейность, степень полинома Жегалкина, стойкость к дифференциальному и линейному анализу. Из-за высокой арифметической сложности генерация криптостойких s-блоков на одной ЭВМ в приемлемые сроки невозможна. Решение данной проблемы было найдено в возможности распараллеливания алгоритма генерации. В итоге, подав алгоритм на кластер возможно получить уменьшение во времени выполнения задачи пропорционально количеству узлов кластера. За основу взят метод генерации s-блоков с использованием специального линейного и специального дифференциального анализов[1]. Алгоритм построен таким образом, чтобы максимально разгрузить хостовую часть кластера, тем самым выделяя ей только функцию генерирования s-блоков, записи их в базу данных, а также сортировку базы данных и поиск в ней s-блоков. Основная же вычислительная сложность будет приходиться на сами узлы кластера. Данный подход позволит не только увеличить производительность системы, но и повысит отказоустойчивость, так как хостовой компьютер не будет перегружен, и может продолжить работу с разгруженными узловыми компьютерами, при этом загруженные узлы продолжат выполнять свою задачу.

Для успешного решения поставленной задачи необходимо наличие:

1. Базы данных s-блоков, для хранения сгенерированных s-блоков (пустая, либо уже имеющая записи);
2. Настроенный кластер на n узлов;
3. Программа, реализованная под кластер, выполняющая генерацию.

Распараллеленный алгоритм генерации s-блоков:

1. Выбор криптостойкого s-блока;
2. Генерация на его основе случайных s-блоков в количестве равном $C_{2^n}^2$ на хостовой машине;
3. Запись всех сгенерированных s-блоков в файл;
4. Инициализация параллельных процессов, присвоение каждому процессу номера rank;
5. Считывание i-го диапазона i-ым узлом;
6. Фиксация характеристик исходного s-блока в переменных;
7. Считывание конкретного s-блока каждым узлом из своего диапазона;
8. Вычисление на каждом узле характеристик конкретного s-блока и исходного;
9. Сравнение характеристик исходного s-блока со значением, хранящимся в переменных;
10. Если характеристики сгененрированного превзошли характеристики исходного, то передача s-блока вместе с его характеристиками на хостовую машину;
11. Присвоение переменным значений характеристик полученного s-блока;
12. Иначе к шагу 7;
13. Запись каждым узлом лучших s-блоков в файл;
14. Передача хосту сигнала о завершении вычислений каждым узлом;
15. Если все узлы завершили работу, то:
    1. Считывание файлов, созданных узлами;

2. Выбор среди записанных там s-блоков, лучшего;
3. Запись этого s-блока в базу данных;

16. Иначе ждать сигнала о завершении всеми узлами работы
17. Использование вновь полученного s-блока в качестве исходного.

Выводы по работе.

Таким образом, благодаря развитию в области операционных систем, а именно в области высокопроизводительных кластеров, стало возможным, в пределах допустимого времени, решать многие арифметически сложные задачи. Одной из таких задач является генерация криптостойких s-блоков. Использование возможности распараллеливания базового алгоритма генерации позволит улучшить производительность, а соответственно уменьшить время работы алгоритма в количество раз, равное числу узлов кластера, по сравнению с решением такой же задачи, но на одной машине. Данная работа направлена на улучшение метода генерации s-блоков, с целью их дальнейшего использования в отечественных криптографических системах, ГОСТах в области криптографии. Более криптостойкие s-блоки позволят создавать более стойкие к криптоанализу алгоритмы шифрования, что необходимо ввиду последних тенденций развития области высокопроизводительных систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Andrey Menyachikhin*. Spectral-linear and spectral-difference methods for generating cryptographically strong S-boxes. Pre-proceedings, 5th Workshop on Current Trends in Cryptology (CTCrypt 2016), June 6-8, 2016, pp 232 – 253.

Б.П. Борисов, А.И. Янкина

АНАЛИЗ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ.

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: криптографические методы защиты информации, аппаратные средства, защита информации, eToken, смарт-карта, несанкционированный доступ.

В статье рассмотрена проблема борьбы с несанкционированным доступом при помощи аппаратных средств защиты информации в сетях передачи данных.

B.P. Borisov, A.I. Yankina

ANALYSIS OF HARDWARE INFORMATION PROTECTION EQUIPMENT IN DATA-NETWORKS.

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

Keywords: cryptographic methods of information protection, hardware, information protection, eToken, smart card, unauthorized access.

The article deals with the problem of combating unauthorized access by means of hardware information protection in data transmission networks.

С развитием разработки, усложнением и появлением новых средств автоматизации процессов обработки информации возникают новые каналы утечки информации системах защиты информации. В этом случае, имеет место возможность уничтожения или искажения информации.

Одним из основных аппаратных средств обнаружения и борьбы с несанкционированным доступом являются **аппаратные средства защиты информации** - это компьютеры и их составные части (процессоры, мониторы, кабели, линии связи и т.п.);

Расширенной группой аппаратных средств являются средства или криптографические методы защиты информации (КМЗИ) такие как:

1. специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
2. генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
3. устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
4. специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты.

КМЗИ-это та же PGP (компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске), только реализованная на уровне «железа». Обычно такие устройства представляют собой платы, модули и даже отдельные системы, выполняющие различные алгоритмы шифрования. Ключи в данном случае тоже «железные»: чаще всего это смарт-карты или идентификаторы Touch Memory. Ключи загружаются в устройства напрямую, обходя память и системную шину компьютера, что делает невозможным перехват полезных данных. Используются шифраторы для кодирования данных внутри закрытых систем, и для передачи информации по открытым каналам связи. По такому принципу работает, в частности, система защиты КРИПТОН-ЗАМОК, выпускаемая зеленоградской фирмой

АНКАД. Эта плата устанавливается в слот PCI, позволяет на низком уровне распределять ресурсы компьютера в зависимости от значения ключа, вводимого еще до загрузки BIOS материнской платой. Именно тем, какой ключ введен, определяется вся конфигурация системы – какие диски или разделы диска будут доступны, какая загрузится ОС и т. д.

Так же работа любых электронных устройств сопровождается электромагнитными излучениями, что делает систему уязвимой и имея современные технические средства злоумышленник с легкостью может перехватить создаваемые вашей аппаратурой наводки и извлечь из них полезный сигнал. Источником электромагнитных излучений являются компьютеры, активные элементы локальных сетей и кабели. Следующий шаг — экранирование помещений, установка активного сетевого оборудования в экранированные шкафы и использование специальных, радиогерметизированных компьютеров (с корпусами из специальных материалов, поглощающих электромагнитные излучения). Помимо этого, в подобных комплексах обязательно применение сетевых фильтров и использование кабелей с двойным экранированием. Если же обрабатываемые данные сверхсекретны, в дополнение к полной радиогерметизации применяют еще и генераторы шума. Эти электронные устройства маскируют побочные излучения компьютеров и периферийного оборудования, создавая радиопомехи в широком диапазоне частот.

Вторая группа аппаратных средств реализует физические сканы различных объектов, к примеру:

1) **eToken** - Электронный ключ eToken - персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП). eToken выпускается в форм-факторах USB-ключа, смарт-карты или брелока. Модель eToken NG-OTP имеет встроенный генератор одноразовых паролей. Модель eToken NG-FLASH имеет встроенный модуль flash-памяти объемом до 4 ГБ. Модель eToken PASS содержит только генератор одноразовых паролей. Модель eToken PRO (Java) аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП. Дополнительно eToken могут иметь встроенные бесконтактные радиометки (RFID-метки), что позволяет использовать eToken также и для доступа в помещения.

Модели eToken следует использовать для аутентификации пользователей и хранения ключевой информации в автоматизированных системах, обрабатывающих конфиденциальную информацию, до класса защищенности 1Г включительно. Они являются рекомендуемыми носителями ключевой информации для сертифицированных СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.)

2) **Смарт-карты доступа** – аппаратный декодер, применяемый для генерирования ключей декодирования на основе публично доступных данных. Чип смарт-карты (либо иного аппаратного форм-фактора) содержит в себе специализированную микропрограмму и, опционально, микроаппаратное обеспечение, задачей которого является вычисление ключа декодирования зашифрованных данных на основе предоставляемых в открытый доступ зашифрованных версий ключа. Область применения не ограничена, на сегодняшний день применяется в основном для организации условного доступа к потоковым данным, таким как системы цифрового телевидения. Данный способ сокрытия данных не несёт в себе задачи полной невозможности получения данных в случае компрометирования одного ключа: за счёт того, что ключ кодирования-декодирования

меняется случайным образом каждые несколько секунд, обладание одним экземпляром ключа приведёт к получению доступа к незначительно малой части данных. Включение дополнительных мер ограничения, таких как программная привязка декодирующей смарт-карты к конкретному экземпляру подключённого аппаратного обеспечения, повышает стойкость системы шифрования т.к. получение доступа к небольшой по размерам смарт-карты не даст доступа к данным, принимаемым иным приёмником.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба и образуют систему защиты.

Технические средства защиты информации при-меняются для решения следующих задач:

- проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

Однако, никакие аппаратные и любые другие решения не смогут со 100% вероятностью предотвратить проникновение злоумышленника в систему и защитить информацию от несанкционированного доступа в любой организации. Проводимый анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты - административных, аппаратных, программных и прочих.

Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной и неконкурентоспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Главное при определении мер и принципов защиты информации не только квалифицированно определить границы разумной безопасности и затрат на средства защиты, а так же поддержание системы в работоспособном состоянии и приемлемого риска с другой.

СПИСОК ЛИТЕРАТУРЫ

1. *Проскурин В.Г.* и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. – М.: Радио и связь, 2000.
2. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др.- М.: Радио и связь, 1999.

3. *Хисамов Ф.Г. Макаров Ю.П.* Оптимизация аппаратных средств криптографической защиты информации //Системы безопасности. - 2004. – февраль-март №1 (55). –стр.108.

А.Э. Боярчук, *В.И. Юхнов, *П.С. Шевчук

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Ростовский филиал государственного казенного образовательного учреждения высшего образования «Российская таможенная академия», г. Ростов-на-Дону, Россия

* Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: стратегический подход, предвидение, внутренний аудит, вредоносные программы, группы факторов.

Рассмотрен вопрос анализа внутренних угроз при разработке стратегии развития организации. Предвидение, стратегическое управление и последующие решения руководства составляют основу Форсайта как технологии стратегического планирования. Угрозы классифицированы на восемь групп. Для каждой из групп дана краткая характеристика.

E.A. Boyarchuk, *I.V. Yukhnov, *P.S. Shevchuk

ANALYSIS OF SECURITY THREATS TO ORGANIZATIONS

Rostov branch of the state educational institution of higher education "Russian customs Academy", Rostov-on-don, Russia

* North Caucasus branch of the order of the red banner of Labour of the Federal state budgetary educational institution of higher professional education "Moscow technical University of communications and Informatics", Rostov-on-don, Russia

Key words: strategic approach, foresight, internal audit, vredo-Nonie program, groups of factors.

Considered the analysis of internal threats in the development of strategy development of the organization. Foresight, strategic management and the subsequent management decisions are the basis of foresight technology and strategic planning. Threats are classified into eight groups. For each of the groups was given a brief description.

Персонал современных образовательных организаций является важнейшим ресурсом, определяющим экономические факторы ограничения при изучении внутренней среды в процессе разработке стратегии [4]. Анализ функционирования этого ресурса должен проводиться с применением стратегического подхода, который заключается в предвидении еще не проявившихся закономерностей и умении соответствующим образом разрабатывать стратегию их влияния.

Эффективное функционирование системы стратегического управления организацией особенно актуально в период финансового кризиса и дефицита федерального и консолидированного бюджетов России. Формирование системы стратегического управления организацией позволит:

- изменить подход к среднесрочному прогнозированию в организации;
- обеспечить его связь с прогнозированием долгосрочных тенденций развития;
- обеспечить координацию разработки, реализации долгосрочных стратегии и программ развития, а также отдельных отделов и секторов организации, их взаимную интеграцию по целям, срокам и мероприятиям.

Предвидение, стратегическое управление и последующие решения руководства составляют основу Форсайта как технологии стратегического планирования [2].

Содержание внутренних угроз безопасности можно классифицировать на группы следующим образом.

Первая группа - это руководитель, директор, он находится на верхнем уровне. От его действий зависит вся сформированная концепция стратегического развития безопасности учреждения. От его кардинальных, твердых и правильных решений зависит безопасность на всех направлениях (экономическая, противопожарная, информационная и др.). Директор курирует деятельность управления организационной работы, информационного и документационного обеспечения, управления инновационного развития, ресурсного центра автоматизации управленческой деятельности и электронных образовательных технологий.

Вторая группа - это руководители высшего звена, заместители директора, советники. От их скоординированных совместных действий, контроля над выполнением функций структурными подразделениями, обладания навыками и профессионализма зависит как успешная реализация концепций в области безопасности, так и ошибочные действия или бездействие.

Причиной может быть не безрезультатное управление учреждением и некомпетентность руководителей, а недостатки корпоративного процесса в принятии решений. Таким образом, целью корпоративного управления должно быть снижение серьезных ошибок при принятии решений. Руководители в большей степени должны быть направлены на поиск, разработку и внедрение новых стратегий, на обсуждение вопросов управления рисками и в меньшей степени - на анализ уже достигнутых результатов.

Особого внимания заслуживает и передача управления учреждением лицу, замещающему, исполняющему обязанности директора. При принятии управления организацией исполняющему обязанности директора необходимо учитывать целый комплекс нормативных и правовых аспектов.

В этот механизм входят моральные, этические и субъективные критерии собственной персоны. То есть исполняющий обязанности директора должен позаботиться о том, чтобы при принятии управления не ущемлялись права работников,

административного и управленческого аппарата и, конечно, интереса учреждения в целом. Исполняющий обязанности директора должен четко представлять объемы и пределы своей профессиональной компетенции. Это в первую очередь затрагивает право как конституционный инструмент и этические основы.

Нужно отметить, что многие действия исполняющего обязанности директора, если они неэтичные и неправомерные, также являются и нелегальными. Однако бывают исключения, когда принятое решение является абсолютно легальным, но совершенно неэтичными, и наоборот: есть ситуации, когда действие считается нелегальным, но не противоречит законам этики. Из этого можно сделать вывод, что, принимая решения в конкретной ситуации, о неком плане действий, исполняющий обязанности директора должен обдумать текущий вопрос, взвесить, не только проанализировать правовые аспекты, но и во многом учесть этические нормы - это касается конфиденциальной информации. Прежде всего нужно учесть существующие на сегодняшний день регламентирующие правовые акты и нормы действующего законодательства.

Третья группа - это сотрудники службы безопасности. На сотрудников службы безопасности возлагаются функции по поддержанию на высоком уровне и продвижению корпоративной безопасности, обеспечению охраны всех объектов учреждения, его работников, студентов, слушателей, имущества, материальных ценностей и денежных средств. Сотрудники службы безопасности должны вести разработку и осуществление мероприятий, направленных на организацию и поддержание контрольно-пропускного режима (осуществлять контроль над изготовлением, учетом, хранением, выдачей, использованием и уничтожением электронных пропусков; устанавливать порядок допуска работников, студентов, лиц сторонних организаций, посетителей и транспортных средств на объекты учреждения), своевременно предотвращать причины, способствующие его нарушению; пресекать попытки несанкционированного проникновения на объекты (следить за функционированием системы охранной сигнализации, видеонаблюдения, СКУД (системы контроля управления доступом)).

Также в обязанности сотрудников входит выявление причин и условий, способствующих нарушению нормальной деятельности всех структур института; фактов, свидетельствующих о наличии конфликта интересов работников учреждения при осуществлении учебного процесса и финансово-хозяйственной деятельности; проведение профилактики и пресечение противоправных действий на объектах; проведение внеплановых проверок подразделений организации на предмет выявления фактов коррупции, ставших известными службе безопасности на основании письменного (устного) обращения гражданина.

Взаимодействие с правоохранительными органами в целях выполнения возложенных на службу задач также является обязанностью сотрудников службы безопасности.

Существенное значение имеет противодействие сотрудников службы безопасности вероятным корпоративным захватам, данная деятельность подробно описана в литературе [1; 2].

От профессионализма, ответственного подхода к работе и лояльного отношения сотрудников безопасности к учреждению зависит выполнение возложенных на них руководством обязанностей и получение качественного результата.

Четвертый класс - сотрудники отдела внутреннего аудита. Внутренний контроль в рамках проверки экономических процессов управления в учреждении осуществляется отделом внутреннего аудита на основании действующего законодательства, инструкций, положений и нормативных актов. От эффективности работы отдела зависит стабильность в хозяйственной деятельности, а это значит, что если налажен внутренний контроль, то у бухгалтеров, в чьи обязанности входит контролировать всю хозяйственную деятельность и совершаемые финансовые операции, меньше обременительной и беспокойной работы. Снижается риск внешних аудиторских проверок, повышается исполнительность, дисциплина, улучшается контроль и порядок ведения деятельности; добросовестная работа отдела внутреннего аудита значительно снижает возможность нарушения действующего законодательства, правил ведения и составления финансовой отчетности и учета. В целом это отражается на результатах производственно-хозяйственного управления, экономической стабильности управления рисками и на имидже учреждения в деловых кругах.

Несомненно, основной целью внутреннего аудита является объективная и независимая оценка управления рисками, а также осуществление контроля корпоративного управления. Для обеспечения независимости и непредвзятости внутреннего аудита необходимо эффективно выстроить функции подчинения подразделений. По сложившейся практике начальник отдела службы внутреннего аудита подчиняется непосредственно директору.

Пятая группа - сотрудники отдела кадров. Если служба безопасности узнает о человеке только в случае причастности его к правонарушению и собирает данные по частям, отправляя запросы в различные отделы и инстанции, то отдел кадров может предоставлять более обширную информацию.

Качество информации определяет качество управления, ведь в современных условиях только уделяя достаточное внимание работе с документами и информации, можно добиться эффективного управления, так как управленческое решение базируется на информации, на служебном документе.

Через отдел кадров проходят каждый трудоустраивающийся, а также документы, содержащие конфиденциальную информацию и персональные данные, не подлежащие разглашению. Эта информация представляет интерес для конкурентов и криминальных лиц, тем самым влияя, как и служба безопасности, на корпоративную безопасность учреждения. Только сотрудники, которые обладают профессионализмом и интуицией, при подборе персонала смогут выявить неблагонадежных, слабых духом, несмотря на пол, уровень образования, служебное положение и классовую принадлежность соискателей.

Шестая группа - финансовый отдел. Управление экономической безопасностью находится в компетенции сотрудников финансового отдела (бухгалтерия, планово-экономический отдел и др.). В финансовом отделе хранится, обрабатывается и используется информация обо всех потоках финансовой деятельности учреждения.

Финансовый отдел управляет финансовыми операциями учреждения, контролирует поступление денежных средств на расчетный счет и порядок их расходования; выполняет операции по кредитованию, ведет расчеты и контроль денежных потоков; составляет бюджет и анализирует фактическое его выполнение; выполняет расчет плановой себестоимости продукции; готовит отчеты о деятельности учреждения, предоставляя их руководству, государственным и местным органам.

Финансовая деятельность учреждения формируется и накапливается в единой базе. Право подписи финансовых документов (платежных документов, счетов-фактур и др.) подлежит четкой проверке и контролю. Документооборот и документирование электронных и иных документов, в которых указаны данные, имеющие юридическую силу, регламентируются законом «Об информации, информационных технологиях и о защите информации».

Седьмая группа - сотрудники управления (отдела) информационных технологий. Этот фактор наиболее уязвим в сфере неразглашения и хранения всей информации в учреждении. Для обеспечения оперативного доступа сотрудников к базам данных необходимо создавать электронную службу протоколов и, следовательно, сервер банка документов.

При наличии доступа ко всем научным статьям, разработкам, планам, хранящимся в электронном виде, электронным базам, персональным рабочим станциям (компьютерам) сотрудников может произойти как осознанная утечка, так и утечка в случае непрофессионализма либо из-за халатного отношения к выполняемым обязанностям. Должное внимание сотрудниками управления должно уделяться внешним атакам на информационные ресурсы.

Анализ обстановки за 2016 год, позволяет сделать некоторые выводы относительно развития ситуации в сфере компьютерной безопасности в 2017 году. Ожидается рост количества вредоносных программ для устройств, работающих под управлением ОС семейства Linux. Будет увеличиваться число атак на уязвимые устройства с использованием протоколов Telnet и SSH, разнообразие используемых злоумышленниками вредоносных программ, будут совершенствоваться их функциональные возможности. Будут расти интенсивности DDoS-атак на различные сетевые узлы и IT-инфраструктуру отдельных интернет-сервисов. Высокую опасность представляют троянцы-шифровальщики для устройств под управлением ОС Windows, Linux, Android и macOS. Используемые ими алгоритмы шифрования будут усложняться, а количество энкодеров наиболее распространенных семейств возрастет. Можно ожидать рост числа разновидностей и общего количества вредоносных программ для мобильной платформы Google Android. Будут совершенствоваться способы доставки опасного программного обеспечения. Вложения в электронных письмах нередко содержат файлы, использующие известные уязвимости в офисных приложениях. Можно не сомневаться в том, что ассортимент используемых методов заражения компьютеров пользователей вредоносными программами будет расширяться и в 2017 году.

В управлении информационными технологиями (УИТ), как правило, имеется разнообразный пакет антивирусных среств, средств от НСД, межсетевых экранов (файрволов) и других средств борьбы.

Восьмая группа - комплекс студенческих общежитий. Одним из приоритетных направлений стала безопасность взрослого и подросткового населения (это связано и преступлениями насильственного характера, и с незаконным оборотом наркотиков, и с несоблюдением правил пожарной безопасности).

Так как все образовательные учреждения имеют общежития для проживания несовершеннолетних и совершеннолетних студентов, то стоит обратить внимание на статистику правонарушений в отношении и среди подростков.

Зачастую неправомерные действия по отношению к детям и подросткам можно было бы предотвратить, если бы соблюдались элементарные правила безопасного поведения.

Это далеко не все группы угроз, а наиболее уязвимые и входящие в группу корпоративного риска.

При проведении более глубокого анализа в группу корпоративного риска можно включить и сотрудников второстепенных отделов (девятая группа), не имеющих прямого отношения к носителям конфиденциальной информации или безопасности организации, но своими действиями могущих принести ущерб организации, сопоставимый с утечкой дорогостоящей информации.

Стоит рассмотреть примеры таких сотрудников. Это люди, зависимые от азартных игр, имеющие дорогостоящие хобби, долговые обязательства, любящие отдых «не по карману» и др. Решая личные финансовые проблемы, не сопоставимые с финансовыми возможностями, они становятся растратчиками казенных средств (взяв как бы в долг из кассы и потратив на собственные нужды), наносят серьезный урон корпоративной безопасности.

Проанализировав группы угроз, потенциально являющихся в основном внутренними угрозами безопасности организации, необходимо обратиться к современным методам прогнозирования последствий подобных ситуаций [7]. Это направление может служить основой для дальнейшей разработки данной проблематики.

СПИСОК ЛИТЕРАТУРЫ

1. *Балашов А. И.* Организация защиты от корпоративных захватов как компонент экономической безопасности предприятия // Евразийский юридический журнал. 2012. № 6(49). С. 149-152.
2. *Балашов А.* //., *Козырев А. А.* Форсайт как технология стратегического планирования // Управленческое консультирование. 2015. № 7(79). С. 45-56.
3. *Балашов А. И.* Организация защиты от корпоративных захватов как компонент экономической безопасности предприятия // Вопросы управления. 2011. № 4(17). С. 187-194.
4. *Квинт В. Л.* Разработка стратегии: мониторинг и прогнозирование внутренней и внешней среды // Управленческое консультирование. 2015. № 7(79). С. 6-11.
5. *Козырев А. А.* Мотивация потребителей. СПб. : Михайлов, 2003. - 384 с.
6. *Козырев А. А.* Система мотивации трудовой деятельности государственных служащих // Управленческое консультирование. 2010. № 4(40). С. 30-37.
7. *Макаров В. Л., Бахтизин А. Р.* Современные методы прогнозирования последствий управленческих решений // Управленческое консультирование. 2015. № 7(79). С. 12-24.

А.В. Вершенник, М.Н. Корчемкина, Н.А. Куприянов, Е.В. Сухорукова

АНАЛИЗ УСЛОВИЙ ОБЕСПЕЧЕНИЯ ПОДЛИННОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ ССОП ЕСЭ РФ

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия

Ключевые слова: обеспечение подлинности, внешний нарушитель, внутренний нарушитель, анализ угроз.

В статье рассмотрены условия обеспечения подлинности информации при ее передаче по каналам ССОП ЕСЭ РФ, уточнена и систематизирована классификация угроз, типов и условий атак, направленных на нарушение подлинности информации.

A.V. Vershennik, M.N. Korchemkina, N.A. Kupriyanov, E.V. Sukhorukova

ANALYSIS OF THE CONDITIONS ENSURING THE AUTHENTICITY OF INFORMATION, DURING TRANSMISSION THROUGH THE CHANNELS OF THE MTSIP UTN OF THE RUSSIAN FEDERATION

Military Academy of communications. Marshal Of The Soviet Union S. M. Budyonny
Saint-Petersburg, Russia

Key words: assurance of authenticity, the external intruder, insider threat, threat analysis.

The article deals with the conditions of ensuring the authenticity of information, during transmission through the channels of the MTSIP UTN of the Russian Federation, clarified and systematized the classification of threats, conditions and types of attacks aimed at authentication violation information.

Осуществляемый в настоящее время в Российской Федерации переход к информационному обществу приводит к тому, что подавляющее большинство процессов в ключевых отраслях экономики и сфере государственного управления реализуются или планируются к реализации в ближайшем будущем с использованием информационных технологий. В различных информационных системах уже сейчас хранятся и обрабатываются значительные объемы информации, в том числе касающейся вопросов государственной политики и обороны, финансовой и научно-технической сферы, частной жизни граждан [1-6].

В то же время глобализация современных информационно-коммуникационных сетей и информационных систем, вынужденное применение при их построении иностранного оборудования и заимствованного программного обеспечения, имеющего уязвимости, а также то, что взаимодействие органов государственной власти, безопасности, обороны и правопорядка осуществляется посредством сетей связи общего пользования единой сети электросвязи Российской Федерации (ЕСЭ РФ), в сочетании с

интенсивным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях, формируют новые угрозы безопасности [1-6].

Объектами воздействия становятся как элементы информационно-телекоммуникационных систем, так и циркулирующая в них информация. Одной из важных задач является обеспечение ее подлинности при передаче по каналам сети связи общего пользования (ССОП) Единой сети электросвязи Российской Федерации (ЕСЭ РФ).

Классификация угроз, типов и условий атак, направленных на нарушение подлинности информации, представлена на рисунке 1.

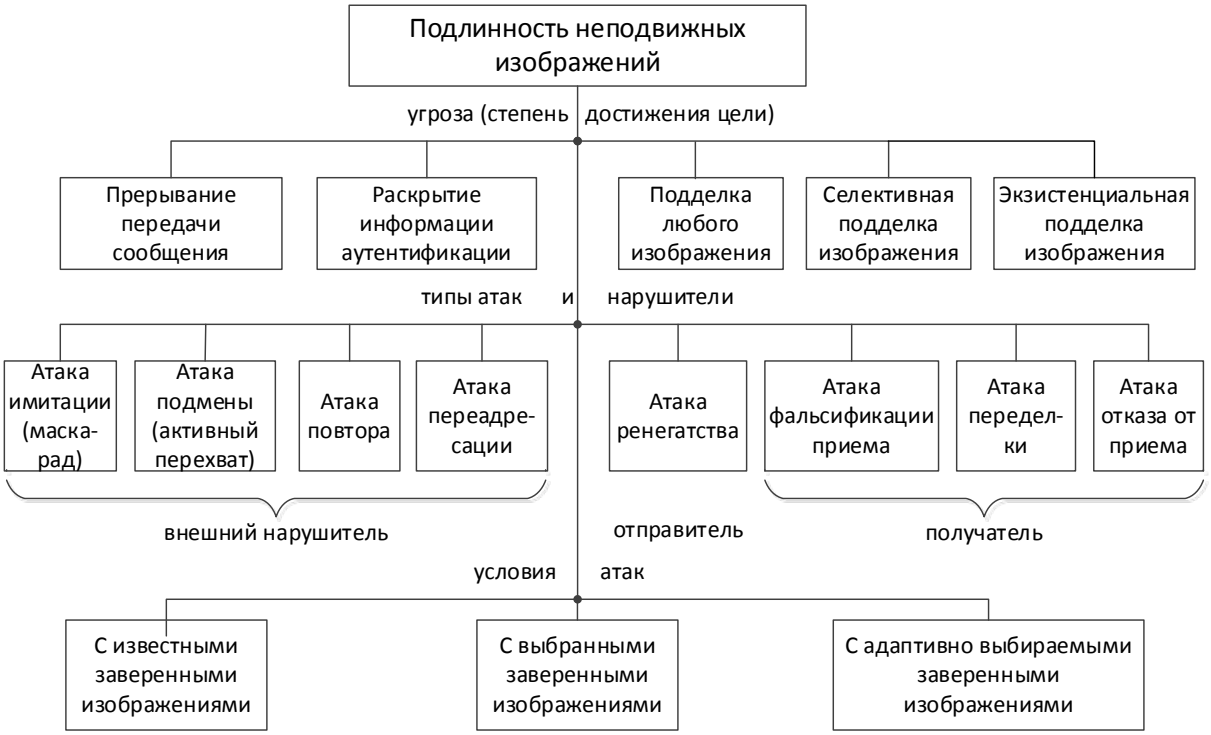


Рис.1. Классификация угроз, типов и условий атак на подлинность неподвижных изображений

По признаку принадлежности к информационно-телекоммуникационной системе все типы нарушителей делятся на две группы:

внешние нарушители – физические лица, не имеющие права доступа в помещения, в которых расположены технические средства, а также доступа к самой информационной системе (ИС);

внутренние нарушители – физические лица, имеющие право доступа в помещения, в которых расположены технические средства, а также доступ непосредственно к самой ИС (легальный пользователь).

Внешний нарушитель может обладать следующей информацией и данными об ИС:

- знаниями функциональных особенностей ИС;
- высоким уровнем знаний в области технических средств;
- сведениями о средствах защиты информации (в том числе применяемых в ИС);
- данными об уязвимостях ИС, включая данные о недокументированных возможностях технических средств ИС;
- информацией о возможных и существующих способах (методах) реализации атак;

– знаниями в области программирования и вычислительной техники.

Состав и характеристики имеющихся у внешнего нарушителя средств существенно определяются имеющимися у него возможностями по их приобретению или разработке. Возможности нарушителя по использованию имеющихся средств зависят от реализованной в информационной системе политики безопасности.

Внешний нарушитель может использовать следующие средства доступа к защищаемой информации:

– средства, подключаемые к сетям связи общего пользования;
– средства активации аппаратных закладок;
– имеющиеся в свободной продаже программные средства прослушивания каналов передачи данных;
– имеющиеся в свободной продаже программные средства модификации данных при их передаче по каналам связи;
– специальные программные средства для осуществления несанкционированного доступа, в том числе вредоносное программное обеспечение.

Возможности внутреннего нарушителя ИС существенным образом зависят от действующих в системе ограничительных факторов, основными из которых являются организационные, режимные, инженерно-технические и другие меры.

Нарушитель этой категории может обладать следующей информацией и данными об ИС:

– атрибутами, обеспечивающими доступ к некоторому подмножеству ресурсов (например, паролем, легальным именем доступа);
– сведениями о структуре, функциях, принципах, механизмах действия и правилах работы технических средств и средств защиты информации в объеме эксплуатационной документации;
– знаниями функциональных особенностей ИС;
– сведениями о ресурсах ИС: порядок и правила создания, хранения и передачи информации, форматы сообщений, структура и свойства информационных потоков;
– данными об уязвимостях ИС, включая данные о недокументированных возможностях технических средств ИС;
– данными о реализованных в системе и средствах защиты информации принципах и алгоритмах;
– сведениями о возможных для ИС каналах атак;
– информацией о способах атак.

Этот нарушитель обладает следующими средствами доступа к ресурсам ИС:

преодоления (обхода) средств и системы защиты информации, систем контроля доступа;

– использования специальных программных средств (в том числе вредоносного ПО) или уязвимостей легально используемого ПО;
– использования специализированных средств съема (добывания) информации по техническим каналам;
– использование средств специальных воздействий;
– внедрения аппаратных закладных устройств.

Внешний нарушитель потенциально может пытаться реализовать атаки имитации, подмены, повтора или переадресации неподвижных изображений. При атаке имитации нарушитель пытается сформировать похожую аутентификационную последовательность (т.е. ложную) или кодограмму и аутентифицироваться как легальный субъект/объект. При атаке подмены нарушитель записывает в сообщение ложную информацию, и затем от имени пользователя А пытается навязать ее пользователю В. В атаке повтора нарушитель, перехватив сообщение от пользователя А, изменяет время его доставки пользователю В. В атаке переадресации пытается навязать перехваченное сообщение от пользователя А другим корреспондентам системы связи.

Подлинность информации в условиях взаимного недоверия сторон может быть обеспечена, если отправитель сообщений заверяет их с использованием только ему известного ключа, а получатель способен убедится в подлинности и авторстве принятого сообщения с использованием известного ему ключа проверки. Системы, стойкие к атакам ренегатства, переделки и подмены, должны быть построены так, чтобы из ключа проверки нельзя было бы вычислить ключ отправителя.

При использовании средств защиты подлинности неподвижных изображений рассмотрим следующие степени достижения нарушителем цели. В случае прерывания передачи сообщения информация уничтожается или становится недоступной либо непригодной для использования. В этом случае нарушается доступность информации. Примером таких нарушений может быть воздействие нарушителя на элементы сети с целью их уничтожения или приведение в нерабочее состояние. При полном раскрытии информации аутентификации нарушитель узнает конфиденциальную информацию аутентификации вида ключ, пароль и т. п. и от его имени способен сфабриковать любое сообщение. Возможно также, что нарушитель не способен раскрыть информацию аутентификации, но может от имени отправителя подделывать любые сообщения. При выборочной подделке нарушитель в состоянии сфабриковать только отдельные изображения. При экзистенциальной подделке нарушитель не в состоянии выбирать фабрикуемое изображение, а навязывает «вслепую», надеясь на случайное формирование выгодного ему ложного изображения с информацией.

Ограничения и особенности воздействий внешнего нарушителя на каналы передачи неподвижных изображений представлены в таблице 1.

Таблица 1.

Ограничения и особенности воздействий внешнего нарушителя на каналы передачи информации

Виды воздействий	Ограничения	Особенности
Перехват и анализ	Время анализа ограничено временем актуальности передаваемой информации.	Низкая избыточность защищаемых сообщений

Продолжение таблицы 1

Ввод ложных сообщений или ложной информации в сообщение	Время воздействия ограничено временем актуальности сообщения	Большое число возможных попыток воздействия Допустимость навязывания ложных сообщений с некоторой погрешностью

Рассмотрим особенности модели внутреннего нарушителя, в качестве которого могут выступать недобросовестный легальный пользователь или получатель неподвижных изображений. Для этих потенциальных нарушителей характерна возможность реализации любой атаки, включая адаптивный выбор заверяемых корреспондентов неподвижных изображений. Например, в качестве внутреннего нарушителя может выступать отправитель сообщения. Он может подготовить два различных сообщения, передать получателю первое из них, а впоследствии отречься от него, утверждая, что он якобы передавал второе, а получатель подменил его на первое. Такая атака со стороны внутреннего нарушителя-отправителя называется атакой ренегатства и потенциально возможна. В качестве внутреннего нарушителя может выступать и получатель сообщения. Получатель может отказаться от факта приема сообщения, внести в него изменения или фальсифицировать прием сообщения. Внутренний нарушитель, имея легальные права доступа к системам связи, способен тщательно подготовиться к атаке и является наиболее опасным видом нарушителя. К его ограничениям относится малое число попыток обмана.

В настоящее время существует два наиболее распространенных пути обеспечения подлинности информации в электронной среде:

1) применение средств электронной подписи ЭП или других криптографических средств, что не снимает проблему перехвата сообщений;

2) обеспечение доверенности среды передачи, хранения, получения и обработки информации [7], что значительно затруднено в условиях использования каналов сети связи общего пользования Единой сети электросвязи Российской Федерации.

Эти обстоятельства усложняют обеспечение конфиденциальности, целостности и доступности информации, передаваемой в современных информационно-телекоммуникационных системах.

Таким образом, обеспечение защищенности неподвижных изображений при различных атаках нарушителя является сложной многогранной задачей, требующей тщательного выбора и синтеза методов обеспечения подлинности.

СПИСОК ЛИТЕРАТУРЫ

1. *СухоруковаЕ.В., Корсунский А.С., Стародубцев Ю.И., Чукариков А.Г.* Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны. Сборник научных трудов (часть вторая) научно-технической конференции «Интегрированные системы управления». 2016 г. - с. 199 – 207.
2. *Стародубцев Ю.И., Евграфов А.А., Сухорукова Е.В.* Проблема формирования системы показателей для оценки защищенности информационно-телекоммуникационных сетей.

/ Проблемы экономики и управления в торговле и промышленности. 2014. № 3. С. 80-86.
3. *Стародубцев Ю.И., Сухорукова Е.В., Чукариков А.Г.* Методика выявления критически важных элементов информационно-телекоммуникационных систем. / Проблемы экономики и управления в торговле и промышленности. 2014. № 1. С. 95-101.
4. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. http://www.scrf.gov.ru/documents/6/113.html (дата обращения 24.12.2016 г.).
5. *Стародубцев Ю.И., Сухорукова Е.В., Закалкин П.В.* Мониторинг корпоративных сетей. / Проблемы экономики и управления в торговле и промышленности. 2016. № 1 (13). С. 70-74.
6. *Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В.* Проблема формирования системы динамической защиты государственных информационных систем. / Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 239-243.
7. *Финько О.А., Елисеев Н.И.* Установление подлинности информации, полученной из недоверенной среды. Информационные технологии, связь и защита информации МВД России – 2012, 2. стр. 54-55. http://www.mvd.informost.ru/2012/pdf2/doc/1-18.pdf

А.В. Вершенник, М.Н. Корчемкина, Н.А. Куприянов, Е.В. Сухорукова

АНАЛИЗ МЕТОДОВ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия

Ключевые слова: компьютерная стеганография, цифровая стеганография, методы стеганографии.

В статье рассмотрены методы компьютерной стеганографии, уточнена их классификация, представлена суть основных методов, рассмотрены их достоинства и недостатки.

A.V. Vershennik, M.N. Korchemkina, N.A. Kupriyanov, E.V. Sukhorukova

ANALYSIS OF METHODS OF COMPUTER STEGANOGRAPHY

Military Academy of communications. Marshal Of The Soviet Union S. M. Budyonny
Saint-Petersburg, Russia

Keywords: video steganography, digital steganography, steganography techniques.

The article considers the methods of computer steganography, refined their classification, the essence of the main methods and discusses their advantages and disadvantages.

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой [1,2]. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии.

Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования и передачи информации в той или иной среде, а также средств реализации этих методов.

Большинство методов компьютерной стеганографии базируется на двух принципах.

Первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности.

Второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в исходных файлах.

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначимых фрагментов среды и замена существующей в них информации на информацию, которую предполагается защитить. Поскольку в компьютерной стеганографии рассматриваются среды, поддерживаемые средствами вычислительной техники и соответствующими сетями, то вся информационная среда, в конечном итоге, может представляться в цифровом виде. Таким образом, незначимые для кадра информационной среды фрагменты в соответствии с тем или иным алгоритмом или методикой заменяются (смешиваются) на фрагменты скрываемой информации.

Для методов компьютерной стеганографии можно ввести следующую классификацию (рисунок 1).

Рисунок 1. Классификация методов компьютерной стеганографии

По назначению методы компьютерной стеганографии могут быть направлены на сокрытие информации, организацию срытых каналов, аутентификацию; защита прав на цифровые объекты [3-8].

Сокрытие информации подразумевает под собой создания имитации отсутствия данной информации в системе или канале передачи. Данный метод используется в основном для передачи и хранения зашифрованной скрытой информации.

Скрытый канал - это коммуникационный канал, пересылающий информацию методом, который изначально был для этого не предназначен. Техника скрытых каналов основывается на факте, что любое изменение состояния какого-то объекта несет информацию [3-8].

По способу выбора контейнера методы делятся на: суррогатный, селективный, конструирующий [3-6].

В методах суррогатной (безальтернативной) стеганографии отсутствует возможность выбора контейнера и для сокрытия сообщения выбирается первый попавшийся контейнер, зачастую не совсем подходящий к встраиваемому сообщению. В

этом случае, биты контейнера заменяются битами скрываемого сообщения таким образом, чтобы это изменение не было заметным. Основным недостатком метода является то, он позволяет скрывать лишь незначительное количество данных.

В методах селективной стеганографии предполагается, что спрятанное сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящий из них для конкретного сообщения [3-6].

В методах конструирующей стеганографии контейнер генерируется самой стегосистемой.

По способу доступа к информации методы делятся на методы с потоковым доступом и с произвольным доступом [3-8].

Методы, использующие потоковые контейнеры, работают с потоками непрерывных данных (например, интернет-телефония). В этом случае скрываемые биты необходимо в режиме реального времени включать в информационный поток. О потоковом контейнере нельзя предварительно сказать, когда он начнется, когда закончится и насколько продолжительным он будет. Более того, объективно нет возможности узнать заранее, какими будут последующие шумовые биты. Существует целый ряд трудностей, которые необходимо преодолеть корреспондентам при использовании потоковых контейнеров. Наибольшую проблему при этом составляет синхронизация начала скрытого сообщения [4].

Методы, которые используются для контейнеров с произвольным доступом, предназначены для работы с файлами фиксированной длины (текстовая информация, программы, графические или звуковые файлы). В этом случае заранее известны размеры файла и его содержимое. Скрываемые биты могут быть равномерно выбраны с помощью подходящей псевдослучайной функции. Недостаток таких контейнеров состоит в том, они обладают намного меньшими размерами, чем потоковые, а также то, что расстояния между скрываемыми битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный шум будет иметь экспоненциальное распределение длин интервала [4].

По способу организации контейнера методы делятся на методы с систематической и несистематической организацией контейнеров.

В систематически организованных контейнерах можно указать конкретные места стеганограммы, где находятся информационные биты самого контейнера, а где - шумовые биты, предназначенные для скрываемой информации.

При несистематической организации контейнера такого разделения сделать нельзя. В этом случае для выделения скрытой информации необходимо обрабатывать содержимое всей стеганограммы.

По используемым принципам различают следующие методы компьютерной стеганографии: встраивание информации, встраивание цифровых водяных знаков (ЦВЗ), встраивание заголовков.

Встраивание информации с целью ее скрытой передачи заключается в размещении информации внутри стегоконтейнеров. В настоящее время наиболее распространенным является метод замены наименьших значащих битов или LSB-метод. Он заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях или аудио- и видеофайлах.

В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого изображения. Указанный метод реализуется при помощи двух различных алгоритмов и их возможных модификаций. В первом случае информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Во втором - имеющийся диапазон частот делится на несколько каналов и передача производится между этими каналами.

При встраивании заголовков стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла. Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

По типу используемого ключа методы делятся на бесключевые, с секретным ключом, с открытым ключом, смешанные [3].

Бесключевое шифрование - это некоторое преобразование исходного текста таким образом, при котором получатель, в отличии от нарушителя, может восстановить преобразованный текст.

Система с открытым ключом (или асимметричное шифрование, асимметричный шифр) - система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ.

В системе с секретным ключом используется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Смешанные стегосистемы используют преимущества двух основных криптосистем: симметричной и асимметричной криптографии. Основной недостаток асимметричной криптографии состоит в низкой скорости из-за сложных вычислений, используемых в алгоритмах, в то время как симметричная криптография традиционно показывает высокую скорость работы. Однако симметричные криптосистемы имеют один существенный недостаток - её использование предполагает наличие защищённого канала для передачи ключей.

По принципу сокрытия данных методы компьютерной стеганографии делятся на форматные и неформатные [3-8].

Форматные методы сокрытия - это методы (системы), основанные на особенностях формата хранения графических данных [3]. Разработка таких методов сводится к анализу формата с целью поиска служебных полей формата, изменение которых в конкретных условиях не скажется на работе с графическим изображением. Все форматные методы обладают общим недостатком - для них возможно построение полностью автоматического алгоритма, направленного на обнаружение факта сокрытия.

Неформатные методы - это методы, использующие непосредственно сами данные, которыми изображение представлено в этом формате. Применение неформатных методов неизбежно приводит к появлению искажений, вносимых стеганографической системой, однако при этом они являются более стойкими к атакам как пассивных, так и активных противников.

По типу информационной среды методы делятся на текстовые, звуковые,

изображения и видео [3-8].

В текстовой информационной среде различают методы стеганографической обработки:

- методы искажения формата текстового документа;
- синтаксические методы;
- семантические методы;
- методы генерации стеганограмм с помощью скрываемого сообщения.

Сокрытие данных путем изменения формата текстовых файлов проводится так, чтобы стандартные текстовые редакторы не смогли выявить признаков присутствия дополнительной информации. Стегосистемы обычно манипулируют интервалами между словами и предложениями или же пробелами в конце текстовых строк.

При синтаксическом методе сокрытие информации происходит путем изменения количества пробелов, табуляции, изменение межстрочных интервалов, использование невидимых символов, регистр букв и т.д.

Семантические методы стеганографии аналогичны синтаксическим методам. Для этих методов элементарными лингвистическими компонентами считаются отдельные слова, поэтому сокрытие данных реализуется путем непосредственной замены слов.

В звуковой информационной среде различают методы стеганографической обработки:

- метод наименьших значащих битов;
- методы широкополосного кодирования;
- метод сокрытия в эхо-сигнале;
- фазовые методы сокрытия;
- музыкальные стегосистемы [3].

Метод наименьших значащих битов. При преобразовании звукового сигнала в цифровую форму всегда присутствует шум дискретизации, который не вносит существенных искажений. “Шумовым” битам соответствуют младшие биты цифрового представления сигнала, которые можно заменить скрываемыми данными.

Методы широкополосного кодирования используют те же принципы, что методы сокрытия данных в изображениях. Их суть заключается в незначительной одновременной модификации целого ряда определенных битов контейнера при сокрытии одного бита информации.

Метод сокрытия в эхо-сигнале. При небольших временных сдвигах эхо-сигнал практически не различим на слух. Поэтому, если ввести определенные временные задержки, величина которых не превышает порог обнаружения, то, разбивая исходный звуковой сигнал на сегменты, в каждый из них можно ввести соответствующий эхо-сигнал [3].

Фазовые методы сокрытия применяются как для аналогового, так и для цифрового сигнала. Они используют тот факт, что плавное изменение фазы на слух определить нельзя. В таких методах защищаемые данные кодируются либо определенным значением фазы, либо изменением фаз в спектре.

Музыкальные стегосистемы обеспечивают сокрытие информации в музыкальной среде по аналогии с импровизацией музыкальных произведений. Целью является внесение изменений, которые сохраняют мелодию основного произведения, соответствуют всем правилам построения данного произведения и при этом кодируют скрываемое сообщение,

не искажая главной темы произведения.

Сокрытие данных в изображении и видео.

В настоящее время создано достаточное количество методов сокрытия информации в цифровых изображениях и видео, что позволило провести их систематизацию и выделить следующие группы:

- методы замены во временной (пространственной) области;
- методы сокрытия в частотной области изображения;
- широкополосные методы;
- статистические методы;
- методы искажения;
- структурные методы [3-8].

Отдельно следует выделить методы замены. К ним относятся: метод замены наименьшего значащего бита, метод случайного интервала, метод псевдослучайной перестановки, метод блочного сокрытия, методы замены палитры, метод квантования изображений. Общий принцип данных методов заключается в замене избыточной, малозначимой части изображения битами секретного сообщения.

Суть широкополосных методов состоит в значительном расширении полосы частот сигнала, более чем это необходимо для передачи реальной информации.

Статистические методы скрывают информацию путем изменения некоторых статистических свойств изображения. Они основаны на проверке статистических гипотез. Суть метода заключается в таком изменении некоторых статистических характеристик контейнера, при котором получатель сможет отличить модифицированное изображение от не модифицированного [3-8].

Методы искажения, в отличие от предыдущих методов, требуют знания о первоначальном виде контейнера. Схема сокрытия заключается в последовательном проведении ряда модификаций контейнера, которые выбираются в соответствии с секретным сообщением.

Структурный метод, в котором сокрытие информации проводится на содержательном уровне с использованием структурных и информационных параметров изображения. По существу, он является развитием известной стеганографической технологии - семаграмм. Суть метода заключается в проведении последовательных преобразований фрагментов графического изображения, которые в конечном итоге приводят к формированию скрываемого текста.

Таким образом, в настоящее время существует достаточно большое количество стеганографических методов, которые могут быть эффективно использованы для решения таких задач, как защиты информации от несанкционированного доступа, аутентификации сообщений, управления сетевыми ресурсами, камуфляжа программного обеспечения и др.

СПИСОК ЛИТЕРАТУРЫ

1. *Стародубцев Ю.И., Чукариков А.Г., Корсунский А.С., Сухорукова Е.В.* Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны. В сборнике: Интегрированные системы управления сборник научных трудов научно-технической конференции. 2016. С. 199-206.

2. *Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В.* Проблема формирования системы динамической защиты государственных информационных систем / В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 239-243.
3. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* «Цифровая стеганография». .- М: Солон-Пресс, 2002.-272с.
4. *Ленков С.В., Перегудов Д.А., Хорошко В.А.,* «Методы и средства защиты информации». - К.: Арий, 2008. - 464 с.
5. *Коханович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006.-288с.
6. *Гавриш В.А.*Практическое пособие по защите коммерческой тайны. Таврида 1994г.-112с.
7. *Хорошко В.А., Шелест Н.Е.* Введение в компьютерную стеганографию. НАУ 2000.-140с.
8. *Петраков А.В.* Основы практической защиты информации. Радио и связь 1999г.-368с.

А.С. Галкин, Д.О. Маркин

РАСПРЕДЕЛЕННОЕ ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ МЕТОДОМ ФАЗЗИНГА НА ОСНОВЕ ТЕХНОЛОГИЙ ВЕБ-ПРОКСИ И АКТИВНЫХ ДАННЫХ

Академия ФСО России, Орел, Россия

Ключевые слова: фаззинг, распределенное тестирование, веб-прокси, прокси-сервер, активные данные.

В работе описана система распределенного тестирования удаленных веб-приложений, использующая сеть узлов, построенных по технологии веб-прокси-серверов, в основе которых лежит концепция активных данных. Предложен способ тестирования веб-приложений методом фаззинга, заключающейся в использовании данной распределенной сети для обмена активными данными, содержащими активные скрипты, осуществляющие тестирование целевого веб-приложения и дальнейшую передачу активных данных по распределенной сети.

A.S. Galkin, D.O. Markin

DISTRIBUTED TESTING OF WEB-APPLICATIONS BY FAZZING METHOD BASED ON WEB-PROXY AND ACTIVE DATA TECHNOLOGIES.

FSO Academy, Orel, Russia

Keywords: fazzing, distributed testing, web-proxy, proxy-server, active data.

In the work it is described the testing system for remote web-applications, that uses the network of web-proxy server technology built nodes, which are based on the active data conception. It offers the fazzing method for testing web-applications, that uses current distributed network for active data interchange, containing active scripts, performing the testing of a target web-application and further transmission of active data through the distributed network.

Современные системы анализа защищенности (САЗ), как правило, строятся на основе агентно-ориентированных подхода, когда в исследуемой сети имеется ряд программных или программно-аппаратных агентов, позволяющих собирать информацию об информационном взаимодействии сети и параметрах этого взаимодействия. Еще одним вариантом построения такой системы является средство, установленное на выделенной ЭВМ, позволяющее осуществлять тестирования удаленных ресурсов. В случае, когда исследуемый удаленный ресурс обладает средствами противодействия анализу его защищенности, эффективность тестирования значительно снижается, поскольку такой ресурс начинает блокировать запросы от САЗ. Решением данной проблемы может быть использование прокси-серверов или анонимных сетей для реализации задачи тестирования защищенности.

В данной работе предлагается новый подход по реализации распределенного тестирования защищенности удаленных веб-ресурсов, основанный на применении концепции активных данных [1, 2] в географически распределенной сети, построенной на базе технологий веб-прокси. Технологической базой данной сети являются географически распределенные веб-сервера, содержащие скрипты, позволяющие принимать сетевые пакеты и выполнять обрабатывать код, содержащийся внутри них, при этом в процессе обработки, данный код может формировать очередной запрос, содержащий свой собственный код либо измененную по определенному алгоритму его копию.

1. Классификация прокси-серверов и обоснование использования технологии веб-прокси

При организации географически распределенной сети вместо одного прокси-сервера между компьютером пользователя и удаленными информационными ресурсами находится сеть прокси-серверов. Их классификация представлена на рисунке 1.

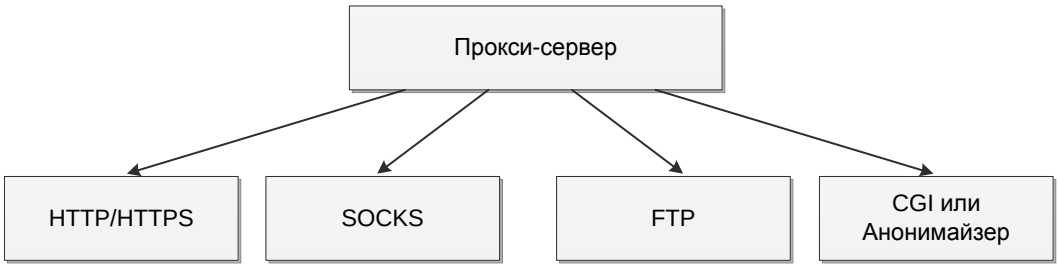


Рис. 1 Классификация прокси-серверов по типу

Выделяют отдельную категорию прокси-серверов – веб-прокси-серверы, представляющие собой веб-приложения, установленные на веб-сервере (например на базе Perl, Python или PHP-скриптов). Анализ веб-прокси и исследование их устойчивости проведены в работах [3-5]. В настоящее время существует несколько готовых решений веб-прокси-серверов, к которым относятся CGIProxy (на базе CGI-скриптов и OpenSSL); Glype Proxy (на базе PHP); PHProxy; Zelune (на базе PHP); Cohula (на базе Java).

Построение распределенных сетей на базе веб-прокси является достаточно тривиальной задачей, однако она не получила широкого распространения в связи с рядом проблем, связанных с ограниченной функциональностью веб-серверов. К таким проблемам относятся:

– низкая скорость соединения между веб-прокси и удаленными ресурсами;

– наличие скриптов в коде удаленного информационного ресурса, которые исполняются на клиентской стороне и должны в "прозрачном" режиме передаваться через веб-прокси.

В то же время использование веб-прокси, в отличие от классических программно-аппаратных платформ, имеет ряд преимуществ:

– может быть использована арендованная или бесплатная программно-аппаратная платформа, не требующая существенных материальных и временных затрат для развертывания;

– установка и настройка программного обеспечения веб-прокси не требует глубоких специальных знаний и позволяет в сжатые сроки получить работоспособный прокси-сервер;

– существует большое количество доступных программно-аппаратных платформ – хостингов, которые могут быть использованы в качестве веб-прокси за сравнительно низкую плату или вовсе бесплатно.

Совокупность данных факторов предопределяет высокую доступность технологии веб-прокси, а современные технические возможности веб-серверов и серверных расширений, позволяющих обрабатывать Perl, Python, PHP и другие скрипты, предоставляют широкие возможности для разработчиков.

2. Построение географически распределенной сети на базе веб-прокси-серверов

Веб-прокси, выступающий в качестве посредника между пользователем или САЗ и информационными ресурсами глобальной сети, позволяет частично решить задачу распределенного доступа и обойти ограничения локальной сети, однако он достаточно уязвим к обнаружению и блокированию как со стороны администраторов локальной сети пользователя, так и со стороны ресурсов глобальной сети.

Схема доступа к удаленным ресурсам посредством распределенной сети на базе веб-прокси представлена на рисунке 2. Сеть представляет собой совокупность логически связанных между собой веб-узлов с веб-прокси-серверами и один управляющий узел. Веб-прокси представлен скриптом или набором скриптов, разработанных на PHP и Perl и предназначенных для обработки поступающих на веб-сервер специальным образом сформированных запросов и последующей передачи их следующему веб-узлу в цепочке маршрута в распределенной сети.

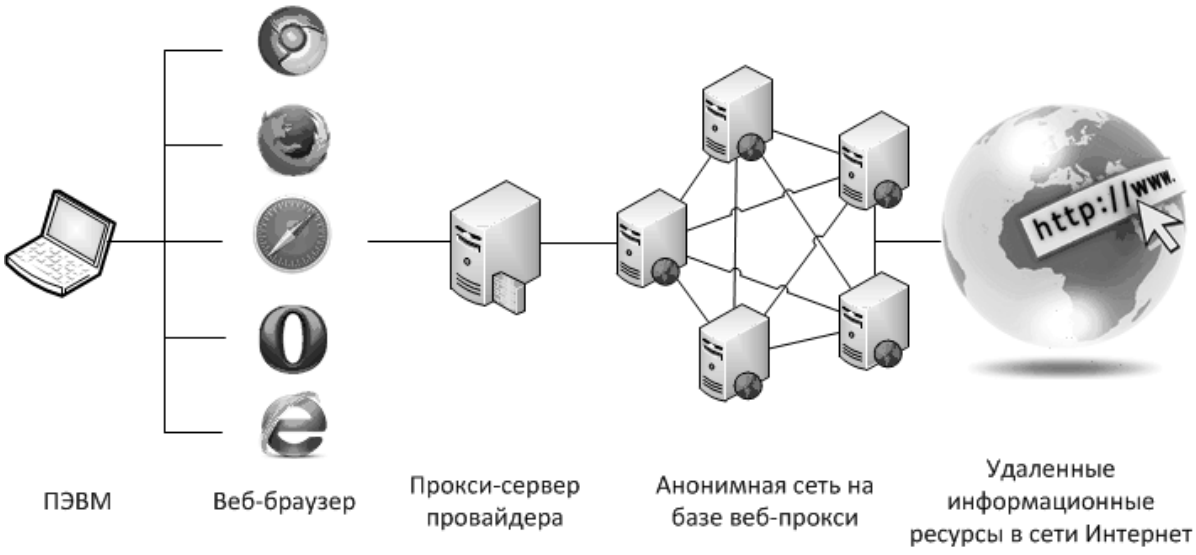


Рис. 2 Структура распределенной сети на основе технологии веб-прокси

Каждый узел содержит сценарий на языке Perl. Данный сценарий выполняет две функции в разных параллельных потоках. Первая функция – отправка запроса от управляющего узла на следующий узел в маршруте и реализация тем самым передачи данных по логическому маршруту в распределенной сети. Вторая функция реализует процесс тестирования удаленного веб-ресурса и отправку отчета на управляющий узел.

Технология веб-прокси являются подходящим инструментом, не требующим разработки дополнительных механизмов реализации концепции терминальных программ. При передаче данных по такой сети на базе веб-прокси в качестве полезной нагрузки в данных приложения HTTP могут быть заложены инструкции в виде скрипта. Такой скрипт, попав на i-й удаленный узел – веб-прокси, после его исполнения может решать ряд задач, включая тестирование удаленных веб-приложений либо активную маршрутизацию, например:

- сгенерировать новый маршрут следования передаваемых данных;
- сгенерировать новый исполняемый скрипт с необходимыми функциями;
- выполнить запрос к удаленному узлу(ам) или осуществить информационный обмен со сменой протокола доступа (например, по протоколу Telnet, SSH и др.).

Пример построения маршрута продвижения активных данных по распределенной сети на основе веб-прокси представлен на рисунке 3.

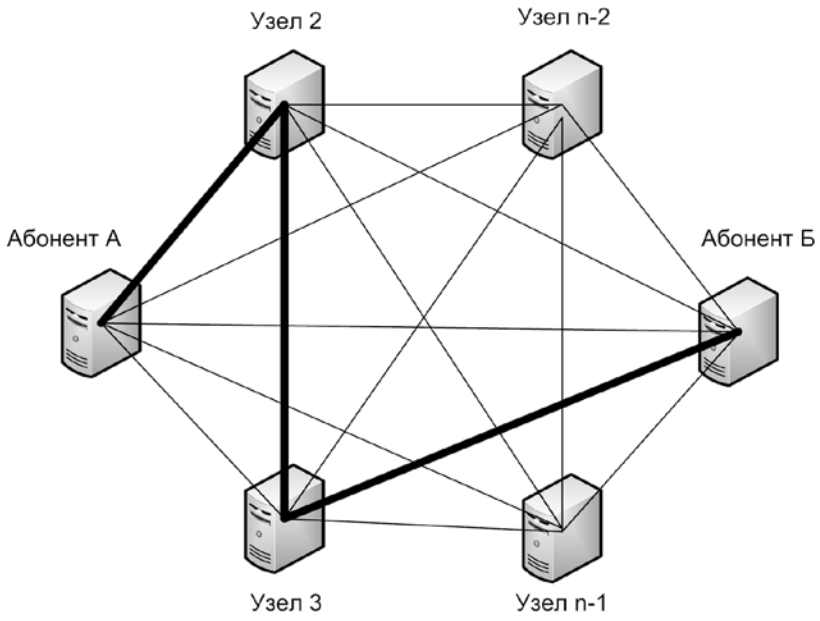


Рис. 3 Пример построения маршрута продвижения активных данных по распределенной сети на основе веб-прокси

Принцип работы сети на базе веб-прокси заключается в следующем.. Пусть абонент А желает связаться с абонентом Б. У абонента А хранится полный список узлов сети. Он формирует маршрут пересылки запроса, а также скрипт с активными данными, например, shell-код, реализующий алгоритм фаззинга веб-приложения, и отсылает запрос с активными данными на первый узел из этого списка. В нашем случай параметром является абонент Б. К примеру, запрос пришел на узел 2. Узел 2 выступает в роли прокси-сервера. Узел 2 выполняет активные данные, определяет адрес следующего узла, на основе алгоритма активных данных и отправляет запрос с теми же либо модифицированными активными данными очередному узлу из маршрута. Эти операции проводятся до тех пор, пока запрос не достигнет получателя.

3. Алгоритмы функционирования управляющего узла, веб-прокси-серверов и скрипта, осуществляющего фаззинг удаленного веб-приложения

Элементы представленных алгоритмов реализованы в веб-приложении [7]. На рисунке 4 представлен алгоритм работы управляющего узла. Реализация прототипа данного узла расположена по адресу: http://nsk.nikitka.net/host/.

Узел управления состоит из четырех разделов: раздел настроек, информационный раздел, раздел запуска теста, раздел отображения отчета.

При запуске веб-интерфейса произойдет автоматическая загрузка списка доступных прокси-серверов. В настройках узла управления предусмотрено:

- редактирование списка шлюзов;
- два способа построения маршрутов: случайно или вручную;
- дополнительные опции создания отчета.

Рис. 4 Алгоритм работы управляющего узла

Если выбрано случайное построение маршрута, то маршрут будет формироваться случайным образом из всех доступных узлов. Пример такого порядка построения маршрута представлен на рисунке 5, иначе маршрут выбирается из списка сохраненных маршрутов, или создается новый. Пример представлен на рисунке 6.

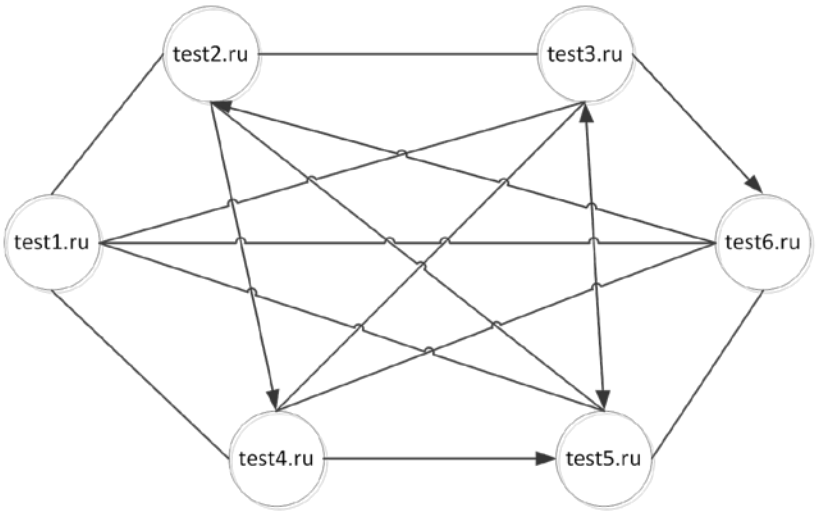


Рис. 5 Пример построения случайного маршрута

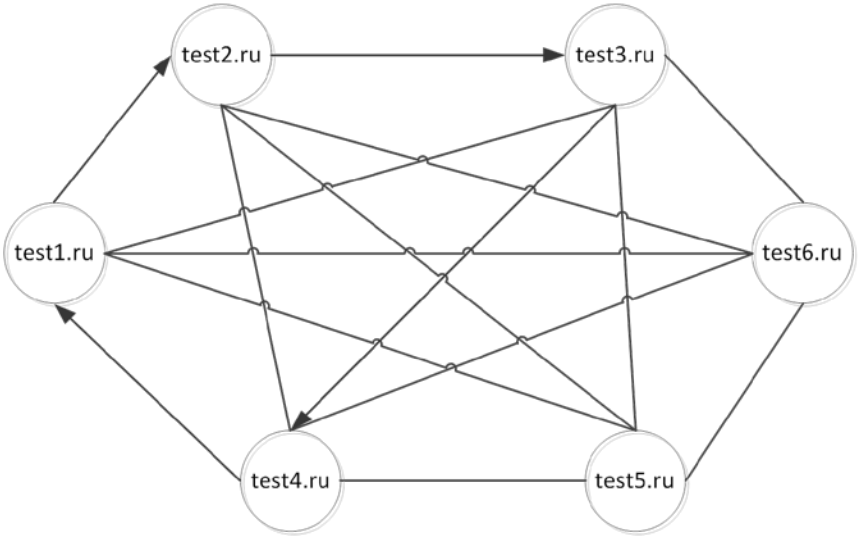


Рис. 6 Пример построения заданного маршрута

После выбора маршрута необходимо ввести URL ресурса, в отношении которого будет осуществляться тестирование.

Исходный код скрипта веб-прокси-сервера представлен ниже.

```
my $target = param("target");
my $way = param("way");
my $N = param("N");
my $N_c = param("N_c");
my $text = param("text");
my $n = param("n");
eval $mytext;
```

На рисунке 7 представлен алгоритм работы скрипта веб-прокси-сервера.

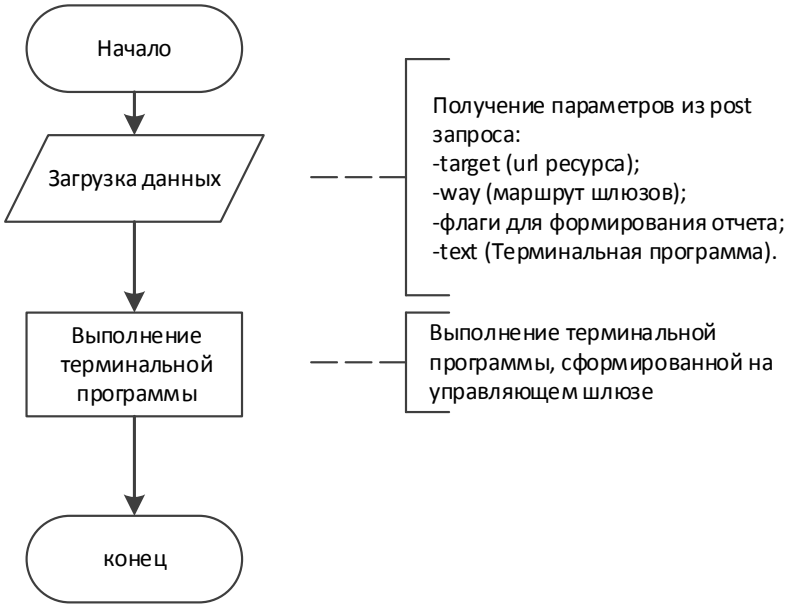


Рис. 7 Алгоритм работы скрипта веб-прокси-сервера

Функция EVAL осуществляет анализ и выполнение выражения переданного в нее, как если бы оно представляло собой автономную программу на Perl. Выполнение производится в контексте текущей исполняемой программы, что позволяет использовать любые переменные, подпрограммы и определения форматов, которые используются в данной программе. Значение, возвращаемое функцией, представляет собой значение последнего выражения внутри EVAL. Допускается использование оператора return как в обычной подпрограмме.

На рисунке 8 представлен алгоритм используемой терминальной программы-активных данных для тестирования удаленного веб-приложения.

Веб-прокси предназначен для приема, обработки и выполнения терминальной программы, а так же для отправки ее на очередной узел маршрута. Веб-прокси-сервер начинает работать после получения HTTP-запроса с активными данными.

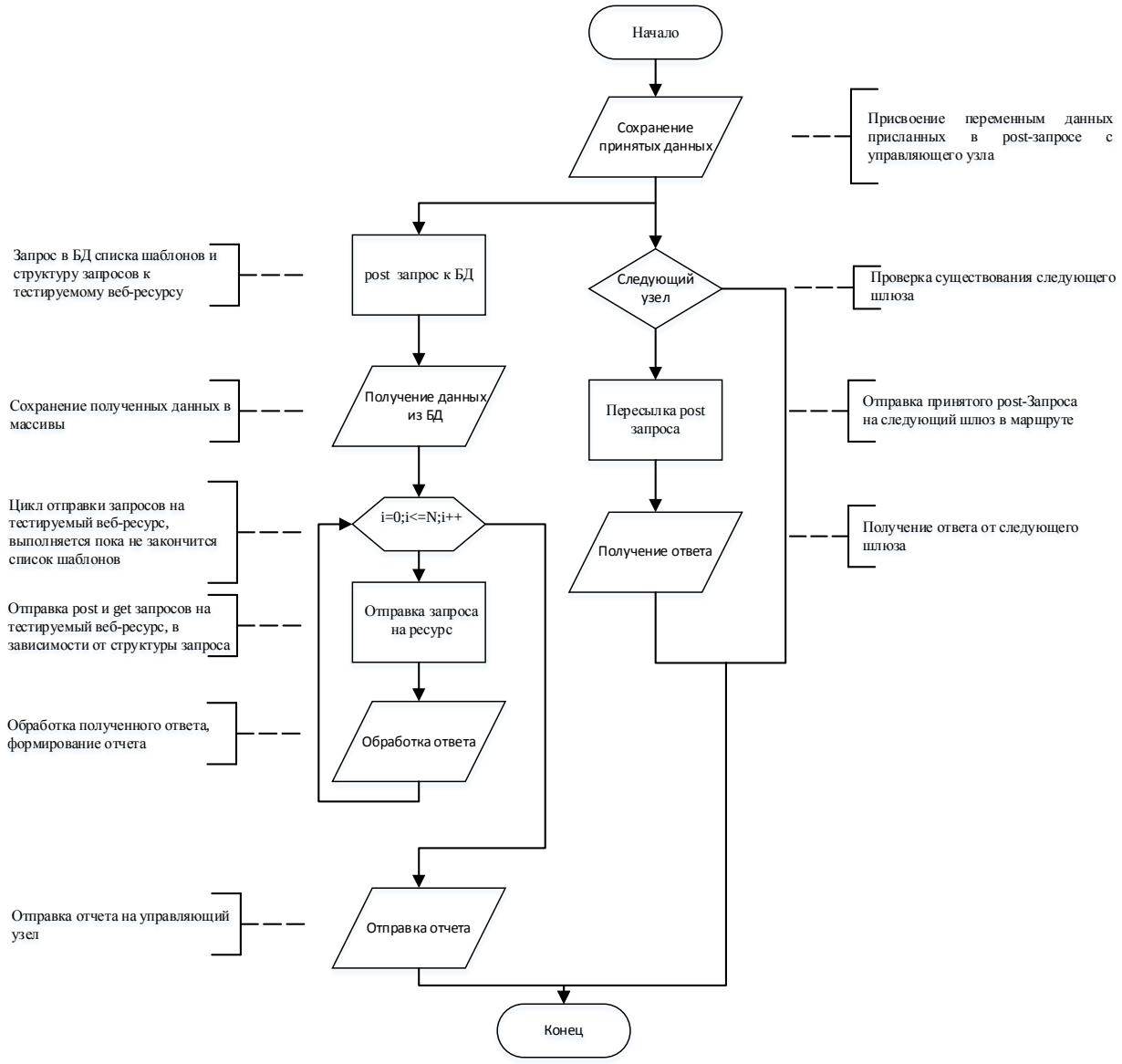


Рис. 8 Алгоритм работы терминальной программы

4. Эксперимент по распределенному тестированию удаленного веб-приложения методов фаззинга на основе технологий веб-прокси и активных данных

Сущность эксперимент состояла в том, чтобы с помощью построенной распределенной сети на базе технологии веб-прокси и активных данных реализовать тестирование удаленного веб-ресурса. Общая схема представлена на рисунке 9.

Управляющий узел рассылает по выбранному маршруту данные для проведения теста (HTTP-запрос + exploit). Каждый узел в маршруте принимает запрос, обрабатывает и передает на следующий узел в маршруте, вместе с этим в отдельном потоке начинается тестирование удаленного веб-ресурса.

Сценарий на узле маршрута обращается к базе данных и получает структуру запросов к тестируемому веб-ресурсу, а так же набор шаблонов, для подстановки их в запросы.

Тестирование осуществлено в сети Интернет.

В состав испытательного стенда входят:

– тестируемый веб-ресурс, расположенный по адресу http://nsk.nikitka.net/testsite/;

– прототипа управляющего, расположенный по адресу: http://nsk.nikitka.net/host/;

– географически распределенная сеть на базе веб-прокси из 18 узлов.

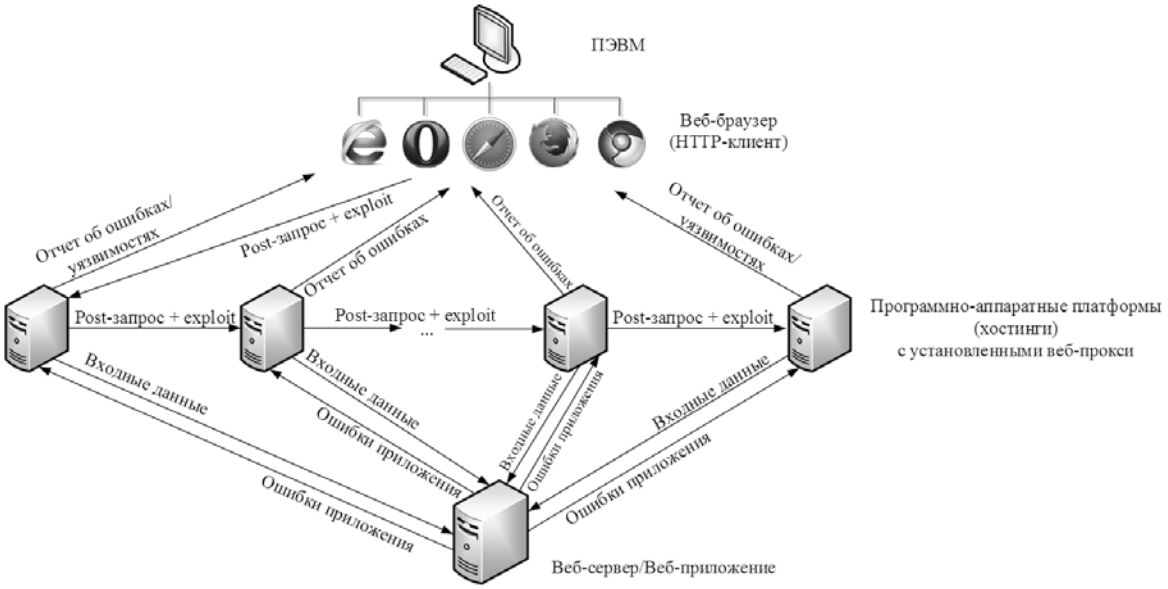


Рис. 9 Общая схема работы распределенного фаззера

В состав географически распределенной сети входят узлы веб-сервера в городе Новосибирск: s01.nsk.nikitka.net, s02.nsk.nikitka.net, …, s09.nsk.nikitka.net, и узлы веб-сервера в Москве: s01.msk.nikitka.net, s02.msk.nikitka.net, …, s09.msk.nikitka.net.

Обновление скриптов на узлах осуществлялось с использованием веб-приложения [6].

Образец отчета представлен на рисунке 10.

[s01.nsk.nikitka.net/fuzz.pl]!Время получения запроса =[14:46:34.707] [s01.nsk.nikitka.net/fuzz.pl]

Время{14:46:35.119} Запрос[s01.nsk.nikitka.net/fuzz.pl]: firstname=' OR 1=1 -- &lastname=' OR 1=1 -- &form=submit

Время{14:46:35.299} Ответ: [html_get] Welcome ' OR 1=1 -- ' OR 1=1 -- !

Время{14:46:35.299} Запрос[s01.nsk.nikitka.net/fuzz.pl]: firstname=" OR 1=1 -- &lastname=" OR 1=1 -- &form=submit

Время{14:46:35.538} Ответ: [html_get] Welcome " OR 1=1 -- " OR 1=1 -- !

Время{14:46:35.538} Запрос[s01.nsk.nikitka.net/fuzz.pl]: firstname=OR 1=1 -- &lastname=OR 1=1 -- &form=submit

Время{14:46:35.744} Ответ: [html_get] Welcome OR 1=1 -- OR 1=1 -- !

Время{14:46:35.744} Запрос[s01.nsk.nikitka.net/fuzz.pl]: firstname=' OR 'a'='a -- &lastname=' OR 'a'='a -- &form=submit

Время{14:46:35.971} Ответ: [html_get] Welcome ' OR 'a'='a -- ' OR 'a'='a -- !

Время{14:46:35.971} Запрос[s01.nsk.nikitka.net/fuzz.pl]: firstname=' OR 1=1 -- &lastname=' OR 1=1 -- &form=submit

Время{14:46:36.207} Ответ: [html_post] Welcome ' OR 1=1 -- ' OR 1=1 -- !

Рис. 10 Раздел отображения отчета

В состав тестируемого веб-ресурса входит 6 форм, каждая из которых содержит определенную уязвимость.

Список уязвимостей:

– HTML Injection-Reflected (GET);
– HTML Injection-Reflected (POST);
– HTML Injection-Stored (Blog);
– PHP Code Injection;
– SQL Injection (GET);
– SQL Injection (POST).

В ходе эксперимента проверено 12 шаблонов, с помощью трех узлов сети. Каждый узел проверяет 4 шаблона из 12 на 6 формах тестового сайта, таким образом, в отчете от каждого узла 24 записи.

Основные результаты работы опубликованы в научной статье в рецензируемом научном журнале "Вопросы кибербезопасности" [3], получено 2 свидетельства о государственной регистрации программы для ЭВМ №№ 2016619070 [7] и 2016617298 [6]. Результаты апробированы на двух конференциях международного и всероссийского масштаба [4, 5].

Выводы

Для реализации распределенной системы тестирования защищенности удаленных ресурсов достаточно эффективным инструментом может являться технологии веб-прокси-серверов, объединенные в единую сеть и реализующую концепцию активных данных. Применение такого подхода позволяет снизить вероятность раскрытия параметров средства тестирования и, соответственно, повысить эффективность тестирования и анализа защищенности удаленных ресурсов.

В работе предложены алгоритмы функционирования узла управления и веб-прокси-серверов. Данные алгоритмы позволяют осуществить управления логической географически распределенной сетью из веб-прокси-серверов, а также, используя принцип активных данных и терминальных программ, реализовать распределенное тестирования защищенности удаленного ресурса.

Проведенное исследование показывает, что использование распределенного средства тестирования защищенности удаленных веб-приложений на базе веб-прокси-серверов позволяет эффективно оценивать из защищенность и обнаруживать некоторые уязвимости.

СПИСОК ЛИТЕРАТУРЫ

1. *Кулешов С.В., Цветков О.В.* Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы № 6, 2014 г. С.12-19.
2. *Кулешов С. В.* Терминальные программы "цифровой" передачи и обработки данных, энергетическая и информационная эквивалентность // Информационно-измерительные и управляющие системы. 2007. Т. 5. № 9. С. 10-15.

3. *Галкин А.С.,* Исследование устойчивости анонимной сети на основе технологий Web-прокси / Д. О. Маркин, П. А. Архипов, А. С. Галкин // Вопросы кибербезопасности. – 2016. – № 2 (15). – С. 21–28.
4. *Галкин А.С.*, Построение анонимной сети на базе технологии Web-прокси / Д. О. Маркин, А. С. Галкин, П. А. Архипов // Перспективные информационные технологии (ПИТ 2016): труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2016. – С. 284–288. ISBN 978-5-93424-758-5.
5. *Галкин А.С.,* Принципы построения анонимной сети на основе технологии Web-прокси / Д. О. Маркин, А. С. Галкин, П. А. Архипов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции [Текст] + [Электронный ресурс] / под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2016. – С. 81–86. ISBN 978-5-89838-886-10.
6. *Свидетельство о государственной регистрации программы для ЭВМ № 2016617298* Российская Федерация. Автоматизированная система управления содержанием удаленных информационных ресурсов / Д. О. Маркин, С. М. Макеев, В. Д. Ленчук, А. А. Охрименко, Р. В. Шапкин ; заявл. 04.05.2016; зарегистрировано в Реестре программ для ЭВМ 29.06.2016 г.
7. *Свидетельство о государственной регистрации программы для ЭВМ № 2016619070* Российская Федерация. Программное средство обеспечения анонимного защищенного доступа к удаленным сетевым ресурсам / Д. О. Маркин, Ф. А. Лаврик, И. А. Сенотрусов, А. С. Галкин, П. А. Архипов ; заявл. 22.06.2016; зарегистрировано в Реестре программ для ЭВМ 12.08.2016 г.

М.Г. Гизатуллин, Д.В. Варакосов

НЕКОТОРЫЕ ОСОБЕННОСТИ РЕАЛИЗАЦИИ УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМЕ ПО БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ

Уральский юридический институт МВД России, Екатеринбург, Россия

Ключевые слова: информационная безопасность, система, канал связи, несанкционированный доступ, угроза, источник угрозы, объект воздействия.

В статье, внимание авторов акцентировано на анализе достаточно актуальной на сегодняшний день угрозы безопасности информации – угрозы несанкционированного доступа к системе по беспроводным каналам связи, которая в большей степени проявляется и наносит вред информационным системам, например, организаций, учреждений, предприятий.

M.G. Gizatullin, D.V. Varakosov

SOME FEATURES OF REALIZATION OF THREAT OF UNAUTHORIZED ACCESS TO SYSTEM THROUGH WIRELESS CHANNELS OF COMMUNICATION

Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg, Russia

Keywords: information security, system, communication channel, unauthorized access, threat, threat source, object of influence.

In article, the attention of the author is focused on the analysis of threat to security of information rather urgent today – threats of unauthorized access to system through wireless channels of communication which is more shown and does harm to information systems, for example, of the organizations, institutions, the enterprises.

Рассматривая современное общество, нельзя не отметить факт того, что существующие на сегодняшний день инфокоммуникационные технологии, использующиеся повсеместно различными категориями потребителей (пользователей различного контента) во всех сферах деятельности с целью удовлетворения их информационных потребностей развиваются достаточно стремительно.

Интегральный подход к обеспечению информационной безопасности в существующих инфокоммуникационных системах и сетях связи предполагает в первую очередь выявление всевозможных угроз и атак.

Целью исследования является анализ совокупности условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (угрозы несанкционированного доступа к системе по беспроводным каналам связи), которые могут нанести вред информационным системам, например, организаций, учреждений, предприятий с точки зрения таких позиций, как описание угрозы, источник угрозы, объект воздействия, последствие реализации угрозы.

В качестве задач исследования можно выделить следующие:

1. Дать общее представление (описание) угрозы несанкционированного доступа к системе по беспроводным каналам связи.
2. Проанализировать угрозу несанкционированного доступа к системе по беспроводным каналам связи.

При решении поставленных задач использованы методы системного анализа, методы теории защиты информации.

Владея терминологией в области обеспечения информационной безопасности нельзя не выделить такие достаточно «актуальные» во всех смыслах термины, как «Угроза», «Угроза безопасности информации». В общем смысле, под угрозой понимается потенциальная причина нежелательного инцидента, который может нанести вред системе или организации [1]. Под угрозой же безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Проанализируем достаточно актуальную и часто встречаемую угрозу – угрозу несанкционированного доступа к системе по беспроводным каналам связи [3] с точки

зрения следующих аспектов:

- описание угрозы;
- источник угрозы;
- объект воздействия;
- последствие реализации угрозы.

Также дадим определения ряду терминов, необходимых для общего представления рассматриваемой проблемы.

Под несанкционированным доступом к информации понимается доступ к информации (ресурсам информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам информационной системы) с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам [4].

Под нарушителем безопасности информации понимается физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах [5].

Угроза несанкционированного доступа к системе по беспроводным каналам связи заключается в возможности получения нарушителем доступа к ресурсам всей информационной системы через используемые в ее составе беспроводные каналы передачи данных.

Угроза несанкционированного доступа к системе по беспроводным каналам связи обусловлена слабостями протоколов идентификации (аутентификации) (таких как, например, WEP, WPA, WPA2), используемых для авторизации пользователей при подключении к точке беспроводного доступа.

Реализация угрозы несанкционированного доступа к системе по беспроводным каналам связи возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации (аутентификации) беспроводных сетей, а также нахождения в точке приема сигналов беспроводной сети.

В общем смысле, под потенциалом нарушителя понимается мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

Различают следующие потенциалы нарушителя:

- высокий;
- средний;
- низкий.

Высокий потенциал нарушителя подразумевает наличие возможностей уровня предприятия (группы предприятий, государства) по разработке и использованию специальных средств эксплуатации уязвимостей.

Средний потенциал нарушителя подразумевает наличие возможностей уровня группы лиц (организации) по разработке и использованию специальных средств эксплуатации уязвимостей.

Низкий потенциал нарушителя подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

В общем смысле, под источником угрозы безопасности информации понимается субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

В качестве источника угрозы несанкционированного доступа к системе по беспроводным каналам связи (тип нарушителя и его минимально необходимый функционал (потенциал)) может выступать внешний нарушитель с низким потенциалом.

Под внешним нарушителем понимают нарушителя, находящегося вне информационной системы на момент начала реализации угрозы. Для реализации угрозы в информационной системе внешний нарушитель должен тем или иным способом получить доступ к процессам, проходящим в информационной системе. При этом дальнейшие свои действия внешний нарушитель выполняет от имени созданного им нового или существующего в системе субъекта.

Объектами воздействия реализации угрозы несанкционированного доступа к системе по беспроводным каналам связи являются:

– сетевой узел;
– учетные данные пользователя;
– сетевой трафик;
– аппаратное обеспечение.

Необходимо также выделить последствие реализации угрозы несанкционированного доступа к системе по беспроводным каналам связи – нарушение конфиденциальности.

Необходимо также отметить, что организации, учреждения, предприятия в рамках организации своей деятельности должны осуществлять взаимоувязанные правовые, организационные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры [6] по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

В заключение необходимо отметить, что не все основополагающие вопросы по реализации рассмотренной угрозы несанкционированного доступа к системе по беспроводным каналам связи, которая может нанести вред информационным системам, например, организаций, учреждений, предприятий и ее анализу вошли в статью в связи с большим необходимым объемом представления информации.

Представленный в статье материал может быть использован в образовательном процессе образовательных организаций высшего образования различных Федеральных министерств и подведомственных им агентств (Министерство внутренних дел Российской Федерации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерство образования и науки Российской Федерации (Федеральная служба по надзору в сфере образования и науки), Министерство связи и массовых коммуникаций Российской Федерации (Федеральное агентство связи), Министерство транспорта Российской Федерации (Федеральное агентство железнодорожного транспорта) и т.д.) для формирования у обучающихся знаний, умений, навыков и (или) опыта деятельности

(компетенций) при выполнении практических, лабораторных и исследовательских работ по учебным дисциплинам (модулям, курсам), реализации дипломных проектов (работ), выпускных квалификационных работ и т.д., «затрагивающих» область обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27013-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 16.09.2014 № 1084-ст) [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 09.03.2017).
2. Национальный стандарт РФ ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 № 531-ст) [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 09.03.2017).
3. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. – URL:http://www.fstec.ru/ (дата обращения: 09.03.2017).
4. Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29.12.2005 № 479-ст) [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 09.03.2017).
5. Национальный стандарт РФ ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 № 531-ст) [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 09.03.2017).
6. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 05.12.2016 № 646 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).

И.С. Гирин, Е.А. Стаценко, И.А. Сосновский

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ СТАНДАРТА 802.11

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: WIFI, безопасность, беспроводные сети, методы защиты.

Рассматриваются методы защиты в сетях доступа на основе беспроводных сетей WiFi.

I.S. Girin, E.A. Statsenko, I.A. Sosnovsky

ANALYSIS OF PROTECTION METHODS IN WIRELESS NETWORKS OF 802.11 STANDARD

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

Keywords: WIFI, security, wireless networks, security methods.

Methods of protection in access networks based on wireless WiFi networks are considered.

Стандарт Wi-Fi разработан на основе IEEE 802.11, используется для широкополосных беспроводных сетей связи [1-3]. Изначально технология Wi-Fi была ориентирована на организацию точек быстрого доступа в Интернет для мобильных пользователей. Преимущества беспроводного доступа очевидны, а технология Wi-Fi изначально стала стандартом, которого придерживаются производители мобильных устройств. Постепенно сети Wi-Fi стали использовать малые и крупные офисы для организации внутренних сетей и подсетей, а операторы создавать собственную инфраструктуру предоставления беспроводного доступа в Интернет на основе технологии Wi-Fi. Таким образом, в настоящее время сети Wi-Fi распространены повсеместно и зачастую имеют зоны покрытия целых районов города.

Беспроводная технология связи более уязвима, нежели подключение по Ethernet-кабелю, в связи с этим нужны более надежные средства защиты сети такие как [1,2]:

- Длинный и сложный пароль для входа в меню настроек роутера.
- Надежный пароль для подключения к Wi-Fi сети.
- Выбор безопасного типа шифрования.
- Использование MAC-фильтра.
- Настройки доступа в операционной системе.

Длинный и сложный пароль для входа в меню настроек роутера.

Одной из самых распространенных ошибок пользователей является легкий пароль, открывающий большие возможности для проведения разного рода атак, устранение этой уязвимости к отсеиванию огромного количества взломщиков со слабой квалификацией.

Надежный пароль для подключения к Wi-Fi сети.

Данная процедура так же усложнит процесс завладения личными данными. Рекомендуется использовать различные символы, разной языковой раскладки, цифры и буквы верхнего и нижнего регистра.

Выбор безопасного типа шифрования.

Тип шифрования WEP появился ещё в 90-х и был первым вариантом защиты Wi-Fi сетей: позиционировался он как аналог шифрования в проводных сетях и применял шифр RC4. Существовало три распространенных алгоритма шифровки передаваемых данных — Neesus, Apple и MD5 — но каждый из них не обеспечивал должного уровня безопасности. В данный момент такой тип шифрования для wifi использовать не рекомендуется, т.к. он не является криптостойким [1,2].

Шифрованием WPA имеет преимущество по сравнению с уязвимым шифром RC4 здесь используется шифрование AES, где длина пароля – величина произвольная (8 – 63 бита). Данный тип шифрования обеспечивает нормальный уровень безопасности и вполне подходит для простых WIFI маршрутизаторов. При этом существует две его разновидности:

- Тип PSK (Pre-Shared Key) – подключение к точке доступа осуществляется с помощью заранее заданного пароля.
- Enterprise – пароль для каждого узла генерируется автоматически с проверкой на серверах RADIUS.

Как и у шифрования WPA, тип WPA2 имеет два режима работы: PSK и Enterprise.

Преимущества шифрования WPA2 перед WPA [1,2]:

а) Корпоративный режим (коммерческие, правительственные, образовательные структуры):
   - Аутентификация: IEEE 802.1X/EAP.
   - Шифрование: TKIP/MIC.
   - Аутентификация: IEEE 802.1X/EAP.
   - Шифрование: AES-CCMP.

б) Персональный режим (небольшие компании, домашние и персональные системы):
   - Аутентификация: PSK.
   - Шифрование: TKIP/MIC.
   - Аутентификация: PSK.
   - Шифрование: AES-CCMP.

Использование MAC-фильтра.

Каждое устройство, оснащенное сетевым адаптером, имеет уникальный MAC адрес. Для того чтобы повысить защиту сети рекомендуется устанавливать фильтр таких адресов. Другими словами, в настройках маршрутизатора вы можете разрешить подключение только доверенным устройствам, указав их адреса [1,2].

Настройки доступа в операционной системе.

В первую очередь необходимо включить доступ с парольной защитой. При этом система самостоятельно генерирует сложный пароль.

СПИСОК ЛИТЕРАТУРЫ

1. *Пролетарский А.В., Баскаков И.В., Федотов Р.А.* и др., Беспроводные сети Wi-Fi(2-е изд.). - М.: НОУ "ИНТУИТ". - 2016г. С – 284.
2. *Олифер В.Г. , Олифер Н.А.,* Основы компьютерных сетей. (1-е изд.). –СПб:Питер, 2009.
3. *Шулева Н.О., Болдырыхин Н.В.* Сравнительный анализ технологий стандарта IEEE 802.11X // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. -2014. -№ 1. -С. 165-166.

О.В. Гончарова, А.А. Гончаров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННОГО МОЛОДЕЖНОГО ОБЩЕСТВА: ТЕНДЕНЦИИ И УГРОЗЫ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова:информационная безопасность, электронные методы воздействия, компьютерные вирусы, спам, естественные угрозы.

В статье рассмотрены проблемы и актуальные тенденции информационной безопасности. Так же представлены основные задачи информационной безопасности.

O.V. Goncharova, A.A. Goncharov

INFORMATION SECURITY OF MODERN YOUTH SOCIETY: TENDENCIES AND THREATS

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

Keywords: information security, electronic techniques, computer viruses, spam, natural threats.

The article considers problems and trends of information security. It is also presented the main objectives of information security.

Каким образом мы можем определить информационную безопасность, и что она означает для потребителей? В первую очередь это защита различных данных и направлена на сохранение информационных ресурсов и личностных прав в информационной сфере.

В современном обществе информационная сфера имеет два направления:

- информационно-техническое;
- информационно-психологическое.

Информационно-техническое, повествует нам о искусственно созданном человеком мире технологий и техники.

Информационно-психологическое напротив, повествует нам о естественном мире живой природы, в том числе включающую самого человека.

Информационная безопасность — это защищенность данных.

В качестве стандартной модели безопасности часто приводят следующую модель из трёх категорий:

- Конфиденциальность: Обеспечение доступа к информации только авторизованным льзователям.
- Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.
- Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

1. Действия, осуществляемые авторизованными пользователями. Сюда входят: кража или уничтожение данных; повреждение данных пользователей.
2. Электронные методы воздействия, осуществляемые хакерами. Хакеры – это квалифицированные специалисты, с большим опытом работы в разработке и изучении программного обеспечения, языков программирования и всего, что связано с компьютерными программами.
3. Компьютерные вирусы. Это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.
4. Спам. Ненужные адресату электронные послания, рекламные письма и т. п., рассылаемые отдельными фирмами по Интернету или электронной почте.
5. 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.

Таким образом, в современных условиях наличие достойной системы информационной безопасности становится одним из важнейших условий конкурентоспособности и даже жизнеспособности компании.

Проблема обеспечения информационной безопасности детей в сети ИНТЕРНЕТ становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем».

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых студентов.

В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию.

Какие же опасности ждут студента в Интернет? Прежде всего, можно выделить следующие:

Суицид-сайты, на которых дети получают информацию о «способах» расстаться с жизнью;

1. Сайты-форумы потенциальных самоубийц;
2. Нарко-сайты. Интернет пестрит новостями о “пользе” употребления марихуаны, рецептами и советами изготовления “зелья”;
3. Сайты, разжигающие национальную рознь и расовое неприятие: экстремизм, национализм, фашизм;
4. Сайты порнографической направленности;
5. Сайты знакомств. Виртуальное “убивает” коммуникативные навыки подростка; секты.
6. Даже с точки зрения безопасности и сохранности вашего имущества, общение в сетях надо контролировать!

Это далеко не весь список угроз Интернета. Любой студент может попасть на такие сайты случайно: кликнув по всплывшему баннеру или перейдя по ссылке. Есть дети, которые ищут подобную информацию специально, и естественно, находят.

Кроме этого, появились психологические отклонения, такие как компьютерная и Интернет-зависимость, игромания (зависимость от компьютерных игр).

Для обеспечения безопасности в интернете можно выделить несколько правил.

1. Персональная информация. Сайты для обеспечения полного доступа предлагают пройти регистрацию с введением персональных данных. Неблагонадежные источники могут использовать эти сведения в корыстных целях.
2. Вредоносные сообщения. Необходимо настороженно относиться к письмам из неизвестных источников. Эти письма могут содержать вредоносные программы.
3. И главное – помнить, что собеседник не всегда тот, кем хочет казаться.

СПИСОК ЛИТЕРАТУРЫ

1. *Е.Б. Белов, В.П. Лось* - Основы информационной безопасности. 2015г.
2. *А.А. Малюк* - Информационная безопасность. 2016г.

А.С. Жук[1], В.А. Головской[2]

АНАЛИЗ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ РЕШЕНИЯ ЗАДАЧИ О МУЛЬТИПЛИКАТИВНОМ РЮКЗАКЕ

[1]Некоммерческое частное образовательное учреждение высшего образования «Кубанский институт информзащиты», Краснодар, Россия

[2]Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: защита информации, задача о рюкзаке, мультипликативный рюкзак, вычислительная сложность.

В статье разработана классификация мультипликативных векторов согласно сложности решения задачи об обобщенном рюкзаке. Проведен анализ вычислительной сложности алгоритма нахождения решения задачи для введенных классов векторов. Детально рассмотрен класс, при котором решение задачи об обобщенном мультипликативном рюкзаке будет иметь экспоненциальную сложность, введены условия, при которых исключается образование классов понижающих сложность решения задачи. Доказаны условия, при которых задача о мультипликативном рюкзаке является задачей полного перебора.

A.S. Zhuck[1], V.A. Golovskoy[2]

THE ANALYSIS OF THE COMPUTATIONAL COMPLEXITY OF SOLVING THE PROBLEM ON THE MULTIPLE KNAPSACK

[1]Kuban Institute of Informprotection, Krasnodar, Russia

[2]North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: information security, the task about a knapsack, multiple knapsack, computational complexity.

In the article the classification of multiplier vectors according to the complexity of solving the problem of a generalized backpack. The analysis of computational complexity of the algorithm for finding the solution of the problem for the introduced classes of vectors. Detail class, in which the solution of the generalized multiplicative backpack will have exponential complexity imposed by the conditions under which excluded education classes to reduce the complexity of the solution. Proved the conditions under which the problem of multiplicative backpack is the task of complete enumeration.

Цель статьи: сформулировать условия, при которых обобщенный мультипликативный вектор будет иметь экспоненциальную вычислительную сложность.

Введение

Создание эффективных моделей систем защиты информации на основе задачи об укладке рюкзака является интенсивно разрабатываемым направлением [1-8]. Как известно [1, 9, 10], в основе всех стандартных рюкзачных систем защиты информации (РСЗИ) лежит NP-полная задача об укладке рюкзака или ранца K_S. Здесь и далее рассматривается возможность построения системы защиты информации на основе задачи о мультипликативном рюкзаке.

Математическая модель задачи мультипликативного ранца

Стандартная математическая модель мультипликативной задачи о ранце K_{MS} может быть сформулирована следующим образом [3]. Пусть заданы ранцевый вектор размерности n, $n \geq 3$, из n натуральных чисел, a_i, $i = 1..n$ ($1..n$ – отрезок натуральных чисел от 1 до n) с заданными свойствами, например, простые числа заданного отрезка

$$A = (a_1, a_2, ..., a_n),$$

и некоторое натуральное число V. Требуется установить, существуют ли для заданного V такие значения $\alpha_i \in \{0,1\}$, для которых справедливо следующее равенство:

$$\prod_{i=1}^{n} a_i^{\alpha_i} = V . \qquad (1)$$

Очевидно, что для любого мультипликативного входа (A, V) представление (1) либо невозможно, либо имеется единственное такое представление, либо имеется более одного представления, что соответствует возможностям преобразования открытого текста с помощью такого ранца. Если каждый вход ранца имеет одно единственное представление со спектром (тень входа (A, V))

$$w = (\alpha_1, \alpha_2, ..., \alpha_n),$$

то для нахождения этого решения проверяется делимость числа V на i-й справа компонент вектора A. Если число V делится нацело на a_i, то в i-ю справа позицию записываем 1, затем заменяем число V на частное и переходим к следующему компоненту вектора A. Если же V не делится на a_i, то в i-ю позицию записываем 0 и снова переходим к следующему компоненту. Эта процедура завершится не более, чем за n шагов, т.к. A состоит из n компонент.

Еще раз отметим, что при условии, что элементы вектора являются простыми числами некоторого промежутка, алгоритм нахождения решения задачи о мультипликативном ранце имеет линейную сложность $o(n)$ в зависимости от размерности исходного вектора.

Так, например, если мультипликативный ранец A = (2, 3, 5, 7), то для значения V = 42 имеем следующий спектр w = (1, 1, 0, 1), т.к. $V = 42 = 2^1 * 3^1 * 5^0 * 7^1$. Здесь значение V = 42 порождено спектром w = (1, 1, 0, 1) из ранца A = (2, 3, 5, 7). Очевидно, что для данного двоичного ранца имеет место неравенства $1 \leq V \leq 210$ относительно величины V.

Теперь перейдем к рассмотрению математической модели нестандартной мультипликативной задачи о ранце.

Математическая модель задачи обобщенного мультипликативного ранца

Пусть имеются набор A_{MP} = (a_1,a_2,...,a_n) из n предметов с заданными объемами α_i, $\alpha_i \in N$, $i = 1..n$ (назовем его обобщенным мультипликативным ранцем) и некоторое натуральное число V. Требуется установить, существуют ли для заданного V такие значения

$$\alpha_i \in Z_p = \{0, 1, ..., p-1\},$$

для которых справедливо равенство

$$\prod_{i=1}^{n} a_i^{\alpha_i} = V \text{ или } A_{MP}{}^{wp} = V, \quad (2)$$

где Z_p – множество значений обобщенного мультипликативного спектра для компонент вектора A_{MP}, $p \geq 2$,

$$w_p = (\alpha_1, \alpha_2, ..., \alpha_n), \alpha_i \in Z_p.$$

Отметим, что в данной задаче $p \in N, p \geq 2$, – любое натуральное число и представляет собой так называемое пороговое значение для степеней. В частности, если $p = 2$, то имеем двоичный спектр и двоичную задачу о мультипликативном рюкзаке. Для простоты изложения будем считать, что значения компонент рюкзачного вектора A_{MP} расположены в возрастающем порядке и $a_1 \neq 1$.

Так, например, если $A_{MP} = (2,3,5,7), p = 5,$ то для значения $V = 48020$ имеем следующий обобщенный спектр $w_5 = (2,0,1,4)$, т.к. $V = 48020 = 2^2 * 3^0 * 5^1 * 7^4.$ Здесь значение $V = 48020$ порождено спектром $w_5 = (2,0,1,4)$ из ранца $A_{MP} = (2,3,5,7)$.

Очевидно, что для указанного мультипликативного ранца (здесь пороговое значение $p = 5$) имеют место неравенства $1 \leq V \leq 1944810000$ относительно величины V.

Предварительно рассмотрим вопрос представления заданного значения V в виде произведения (2) компонент вектора A_{MP}, при условии, что его компоненты либо не могут повторяться, как это требуется в известных источниках по построению ранцевых систем защиты информации с открытым ключом [1-3, 8], либо могут повторяться, как предлагается в данной работе. Причем при моделировании систем защиты информации на основе заданного мультипликативного ранца нас будет интересовать случай, когда имеется не более одного представление для заданного натурального значения V.

Решением для мультипликативного входа (A_{MP}, V) назовем подмножество компонентов A_{MP}, для которых имеет место равенство (2). При этом, если для подобного вектора рассматриваются решения над Z_p, то этот вектор назовем обобщенным мультипликативным ранцевым вектором. Обобщенный мультипликативный ранцевый вектор A_{MP} будем называть инъективным, если для произвольного значения V вход (A_{MP}, V) обладают не более, чем одним решением – с повторениями или без него. Очевидно, что количество $\mu(A_{MP})$ всех различных числовых входов (A_{MP}, V) для мультипликативного ранцевого вектора A_{MP} определяется равенством: $\mu(A_{MP}) = p^n$. При этом, если для подобного вектора рассматриваются решения с коэффициентами

повторений компонент вектора A_{MP} из Z_p, то этот инъективный вектор назовем обобщенным ранцевым вектором и обозначим его через A_p.

В частности, если $p = 2$, то это означает, что $A_2 = A$.

Так, например, для $p = 3$ вектор $A_3 = (2,3,5,7,11,13)$ является обобщенным мультипликативным инъективным ранцевым вектором размерности 6.

Определим понятие инъективности мультипликативного рюкзачного вектора так же, как и для аддитивного случая.

Рюкзачный вектор $A = (a_1,a_2,...,a_n)$ называется инъективным, если для любого числа V мультипликативная задача о ранце со входом (A, V) имеет не более одного решения.

Рюкзачный вектор $A = (2, 3, 5, 7)$ является инъективным, в чем легко убедиться. В более общем случае можем утверждать, что, если все элементы вектора $A = (a_1,a_2,...,a_n)$ простые числа, то данный вектор инъективен. Данное утверждение следует из основной теоремы арифметики.

Определение сложности решения задачи

Сформируем алгоритм поиска решения задачи о рюкзаке с входом (A_{MP},V) для произвольного значения V и приведенного выше вектора $A_3 = (2,3,5,7,11,13)$. Перед началом выполнения зададим значения $w_p = (0, 0, ..., 0)$.

1.1. Разделим значение V на компонент 13. Если $13|V$, то перепишем в V значение $\frac{V}{13}$, увеличиваем α_6 на 1, и переходим к выполнению пункта 1.2, иначе переходим к выполнению пункта 2.1.

1.2. Разделим значение V на компонент 13. Если $13|V$, то перепишем в V значение $\frac{V}{13}$, увеличиваем α_6 на 1, иначе оставляем V прежним, и переходим к выполнению пункта 2.1.

2.1 Разделим значение V на компонент 11. Если $11|V$, то перепишем в V значение $\frac{V}{11}$, увеличиваем α_5 на 1, и переходим к выполнению пункта 2.2, иначе переходим к выполнению пункта 3.1

2.2. Разделим значение V на компонент 11. Если $11|V$, то перепишем в V значение $\frac{V}{11}$, увеличиваем α_5 на 1, иначе оставляем V прежним, и переходим к выполнению пункта 3.1…

Подобным образом обрабатываем i-ю компоненту рюкзачного вектора и заполняем соответствующий элемент вектора спектра. В итоге у нас получается, что на каждой итерации число V уменьшается. После исследования каждого элемента рюкзачного вектора A_{MP} необходимо рассмотреть полученное значение V. Если $V = 1$, то мы нашли решение для рюкзака с входом (A_{MP},V), иначе не существует вектора $w_p = (\alpha_1,\alpha_2,...,\alpha_n)$ такого что $\prod_{i=1}^{n} a_i^{\alpha_i} = V$.

Легко заметить, что вычислительная сложность данного алгоритма линейна, причем $s(A_{MP}) = o(n * p)$. Заметим, что все компоненты приведенного вектора – простые числа. В более общем случае можно утверждать, что если все компоненты рюкзачного обобщенного мультипликативного вектора – простые числа, то вычислительная сложность данного алгоритма линейная функция, зависящая от начальных значений *n,p,* $s(A_{MP}) = o(n * p)$. Кроме того, вектор, сформированный подобным образом, будет обобщенно инъективным, что следует из основной теоремы арифметики [10].

Рассмотрим рюкзачные векторы размерности n такие, что $A_p = (a_1, a_2, ..., a_n), \forall i, j = 1..n:$ НОД(a_i, a_j)=1. Обозначим такие векторы A_p^n, а множество всех таких векторов через A_p^{n*}.

Отметим, что существует рюкзачный вектор, который инъективен, но не принадлежит множеству векторов A_p^{n*}, и алгоритм, разработанный для рассмотренных выше классов, не будет работать для такого вектора.

Например, $M = (4,25,1000)$. Решим задачу о рюкзаке со входом (M,V), воспользовавшись алгоритмом, разработанным выше для векторов Ap_p и A_p^n. Перед началом выполнения зададим значения $w_p = (0,0,0)$, $V = 10000$, $p = 3$.

1. Разделим значение V на компонент 1000. $1000 | V$, следовательно, перепишем в V значение 10, увеличиваем α_3 на 1. Теперь имеем $w_p = (0,0,1)$, $V = 10$.
2. Разделим значение V на компонент 25. ~~$25 | V$~~, следовательно, сразу переходим к выполнению пункта 3.
3. Разделим значение V на компонент 4. ~~$4 | V$~~, следовательно, завершаем исследование.

Получено $V \neq 1$, значит, руководствуясь примененным алгоритмом, принимается решение об отсутствии решений. Тем не менее, существует решение $p = 4^2 * 25^2 = 10000, \; w = (2,2,0)$. Получается, что для решения задачи с входом $(M,10000)$ приведенный выше алгоритм не подходит. Для получения значения $w = (2,2,0)$ необходимо перебрать все возможные $\mu(M) = p^n = 3^3$ вариантов.

Но приведенный выше вектор инъективен, в чем легко убедиться, перебрав все возможные значения V, для которых будет существовать решение задачи $(M,10000)$.

Теперь на основе рассмотренного вектора $A = (4,25,1000)$ введем условия, при которых алгоритм решения задачи со входом (A_{MP}, V) имеет экспоненциальную вычислительную сложность относительно начальных данных n и p для обобщенного мультипликативного вектора $A_{MP} = (a_1, a_2, ..., a_n)$.

Рассмотрим множество мультипликативных векторов вида

$$A_p^{0*} = \left\{ A_p^{\,0} = (a_1, a_2, ..., a_n) \mid \forall i \in \{1...n\} \; \exists j \neq i, \; j \in \{1...n\}, НОД(a_i, a_j) \neq 1 \right\}.$$

Очевидно, что для данных векторов нет возможности подобрать алгоритм полиномиальной сложности, позволяющий решить задачу о мультипликативном рюкзаке со входом $(A_p^{\,0}, V)$.

Тем не менее, существуют рюкзачные векторы такие, что подобрать алгоритм полиномиальной сложности для решения задачи о мультипликативном рюкзаке сложная задача, но возможно подобрать алгоритм, понижающий сложность решения данной задачи.

Например, рассмотрим множество векторов

$$A_p^{1*} = \left\{ A_p^{1} = (a_1, a_2, ..., a_n) \mid \exists! k, \forall\, j \in \{1...n\} : НОД\left(a_k, a_j\right) = 1; \right.$$
$$\left. \forall\, i \in \{1...n\}, i \neq k, \exists\, j \neq i, j \neq k, j \in \{1...n\}, НОД\left(a_i, a_j\right) \neq 1 \right\}.$$

Заметим, что, вычислив изначально наибольший общий делитель каждой пары компонент вектора, сокращается поиск решения задачи о мультипликативном рюкзаке из-за удаления компоненты a_k из полного перебора. Это позволит уменьшить вычислительную сложность алгоритма решения данной задачи до $s\left(A_p^{1}\right) = o\left(n^2 + p + p^{n-1}\right)$

.

Подобным образом определим следующие множества векторов:

$$A_p^{2*} = \left\{ A_p^{2} = (a_1, a_2, ..., a_n) \mid \exists! k_1, \exists! k_2, НОД\left(a_{k_1}, a_{k_2}\right) = 1, \forall\, j \in \{1...n\},\ j \neq k_1,\ j \neq k_2 : \right.$$
$$НОД\left(a_{k_1}, a_j\right) = 1, НОД\left(a_{k_2}, a_j\right) = 1; \forall\, i \in \{1...n\}, i \neq k_1, i \neq k_2,\ \exists\, j \neq i,\ j \in \{1...n\}, НОД\left(a_i, a_j\right) \neq 1 \Big\};$$
$$A_p^{l*} = \left\{ A_p^{l} = (a_1, a_2, ..., a_n) \mid \exists! k_1, ..., \exists! k_l, \forall m \in \{1...l\} : \forall\, j \in \{1...n\},\ j \neq k_m : НОД\left(a_{k_l}, a_j\right) = 1; \right.$$
$$\left. \forall\, i \in \{1...n\}, i \neq k_1, ..., i \neq k_l\ \exists\, j \neq i,\ j \in \{1...n\}, НОД\left(a_i, a_j\right) \neq 1 \right\}.$$

Очевидным образом определяется вычислительная сложность алгоритмов решения задач о мультипликативном рюкзаке для векторов каждого из указанных классов:

$$s\left(A_p^{2}\right) = o\left(n^2 + 2p + p^{n-2}\right), \quad s\left(A_p^{l}\right) = o\left(n^2 + lp + p^{n-l}\right).$$

Отметим, что увеличивая значения *l* до значения *n*, получаем уже описанный выше класс A_p^{n*} с вычислительной сложностью $s\left(A_p^{n}\right) = o\left(n^2 + lp\right)$. Квадратичная сложность обусловлена необходимостью подсчета наибольшего общего делителя каждой пары компонент.

В целях разработки системы защиты от несанкционированного доступа интерес представляет класс векторов A_p^{0*}, такой, что алгоритм нахождения решения соответствующей мультипликативной задачи о рюкзаке будет иметь экспоненциальную сложность. Важно, что главный интерес исследований представляют такие векторы, что решение задачи с соответствующим входом может быть найдено только полным перебором.

Рассмотрим следующий пример. Пусть $K = (4,25,1000,9,49,9261)$, где p = 3. Для входа (K,10000) количество всех возможных наборов элементов исходного вектора $\mu(K) = p^n = 3^6 = 729$. Однако, в данном случае достаточно проверить делимость числа 10000 на цифры первой тройки. Если хоть на одно делится нацело, перебираем комбинации первой тройки. Иначе комбинации второй тройки. Вычислительная сложность в таком случае будет равна $\mu(K) = 2 * p^{\frac{6}{2}} = 2 * 3^3 = 54$, то есть нам достаточно перебрать 54 набора для первой тройки, чтобы найти решение для входа $(K,10000)$. В

общем случае падение сложности будет равно $s(A_p^n) = o(np^{\frac{n}{2}})$. Таким образом, использование этих указанных классов следует исключить при проектировании рюкзачного вектора для конкретной рюкзачной системы защиты информации.

Сформулируем условия, которые позволят избежать данной ситуации. Для этого введем дополнительные объекты. Введем отношение на нашем множестве.

Известно, что бинарное отношение R на множестве X называется отношением эквивалентности, если оно обладает следующими свойствами [10]:

1. Рефлексивность: X: xRx.
2. Симметричность: X: если xRy, то yRx.
3. Транзитивность: X: если xRy и yRz, то xRz.

Пусть задано отношение вида

$$aRb = [(NOD(a,b) \neq 1 \vee (\exists c \in A_p{}^0, NOD(a,c) \neq 1 \wedge NOD(b,c) \neq 1)].$$

Докажем, что данное отношение является отношением эквивалентности. Для этого проверим выполнимость следующих трех свойств:

1. Отношение R рефлексивно, если $\forall a \in A^0{}_p : (aRa)$. Тогда, по свойству НОД: $NOD(a,a) = a$, перезапишем наше отношение в виде: $aRa = [NOD(a,a) \neq 1 \vee (\exists c \in A_p{}^0, NOD(a,c) \neq 1)]$ получаем, что a находится в отношении R с самим собой.
2. Отношение R симметрично, если $\forall a,b \in A^0{}_p : (aRb) \Rightarrow (bRa)$. Тогда, используя свойство НОД: $NOD(a,b) = NOD(b,a)$, получим, что $\forall a,b : (aRb) \Rightarrow (bRa)$.
3. Бинарное отношение R, заданное на множестве F называется транзитивными если

$$\forall a,b,c \in A : (aRb) \wedge (bRc) \Rightarrow (aRc). \quad (3)$$

Рассмотрим наше отношение. Для начала выберем произвольные элементы вектора, составим три отношения и составим предикат вида: $(aRb)(bRc) \rightarrow (aRc)$. Распишем каждую пару, в соответствии с нашим отношением

$$\begin{aligned} aRb &= (NOD(a,b) \neq 1 \vee NOD(a,c) \neq 1 \wedge NOD(b,c) \neq 1); \\ bRc &= (NOD(b,c) \neq 1 \vee NOD(b,a) \neq 1 \wedge NOD(a,c) \neq 1); \\ aRc &= (NOD(a,c) \neq 1 \vee NOD(a,b) \neq 1 \wedge NOD(b,c) \neq 1). \end{aligned} \quad (4)$$

Подставим выражение (4) в (3), получим выражение:

$$\begin{aligned} aRb = [(NOD(a,b) \neq 1 \vee NOD(a,c) \neq 1 \wedge NOD(b,c) \neq 1) \wedge (NOD(b,c) \neq 1 \vee NOD(b,a) \neq 1 \wedge \\ \wedge NOD(a,c) \neq 1)] \Rightarrow (NOD(a,c) \neq 1 \vee NOD(a,b) \neq 1 \wedge NOD(b,c) \neq 1) \end{aligned} \quad (5)$$

Упростим выражение (5), проведя замены:

$$\begin{aligned} x &= NOD(a,b) \neq 1; \\ y &= NOD(b,c) \neq 1; \\ z &= NOD(a,c) \neq 1. \end{aligned} \quad (6)$$

Подставив (6) в (5), получим:

$$(x \vee zy) \wedge (y \vee xz) \Rightarrow (z \vee xy), \quad (7)$$

$$xy \vee xz \vee zy \vee zxy \Rightarrow z \vee xy. \quad (8)$$

Воспользуемся формулами поглощения:

$$z(x \vee y) \vee xy \Rightarrow z \vee xy. \quad (9)$$

Построим таблицу истинности для выражения (9).

Таблица 1 – Таблица истинности

№	x	y	z	$x \vee y$	$z(x \vee y)$	xy	$z(x \vee y) \vee xy$	$z \vee xy$	$F(x,y,z)$
1	**0**	**0**	**0**	0	0	0	0	0	1
2	**0**	**0**	**1**	0	0	0	0	1	1
3	**0**	**1**	**0**	1	0	0	0	0	1
4	**0**	**1**	**1**	1	1	0	1	1	1
5	**1**	**0**	**0**	1	0	0	0	0	1
6	**1**	**0**	**1**	1	1	0	1	1	1
7	**1**	**1**	**0**	1	0	1	1	1	1
8	**1**	**1**	**1**	1	1	1	1	1	1

Полученная функция $F(x,y,z)$ тождественно истинна. Это означает, что введенный предикат является тавтологией. Таким образом, мы доказали, что наше отношение является отношением эквивалентности.

Так как отношение является отношением эквивалентности, то оно разбивает наше множество на классы эквивалентности. Например, вектор K разбит на два класса, вектор $M = (4,25,1000,10000)$ образует один класс эквивалентности. Тогда справедливо следующие утверждение: для того чтобы вычислительная сложность мультипликативной задачи о рюкзаке определялась по формуле $O\left(p^n\right)$ для любого алгоритма ее решения, необходимо и достаточно, чтобы отношение R разбивало множество только на один класс эквивалентности.

Другими словами, необходимо, чтобы элементы a_i подмножества $I \subset A$, находились в отношении с элементами только этого подмножества и таких подмножеств должно быть не более одного.

В результате проанализирована вычислительная сложность решения задач о мультипликативном рюкзаке для различных классов рюкзаков и введены условия, при которых задача о рюкзаке является задачей полного перебора.

Заключение

Рассматривается задача о мультипликативном обобщенном рюкзаке. Разработана классификация мультипликативных обобщенных рюкзачных векторов. Введено отношение эквивалентности над мультипликативным рюкзачным вектором класса A_p^{0*}. На основании этого отношения разработана математическая модель такого мультипликативного рюкзачного вектора, что решение задачи с соответствующим входом возможно только с использованием полного перебора без использования эвристик.

Введены условия формирования мультипликативных обобщенных рюкзачных векторов экспоненциальной вычислительной сложности решения соответствующей задачи о рюкзаке. Далее необходимо сформировать функцию преобразования вектора из одного класса в другой, удовлетворяющую определенным условиям. Построение подходящей функции позволит разработать математическую модель системы защиты от несанкционированного доступа к иерархическим данным.

СПИСОК ЛИТЕРАТУРЫ

1. *Осипян В.О.* Об одном обобщении рюкзачных криптосистем. – Изв. вузов. Сев.-Кавк. регион. Техн. науки. – 2003. Приложение №5, С. 18-25.
2. *Осипян В.О.* О полиалфавитной криптосистеме с обобщенным рюкзаком.– Изв. вузов. Сев.-Кавк. регион. Техн. науки. – 2004. – Спецвыпуск, С. 65-66.
3. *Осипян В.О.* Моделирование систем защиты информации, содержащих диофантовы трудности. Разработка методов решений многостепенных систем диофантовых уравнений. Разработка нестандартных рюкзачных криптосистем. – LAP. 2012. – 344с.
4. *Осипян В.О., Карпенко Ю.А., Жук А.С., Арутюнян А.Х.* Диофантовы трудности атак на нестандартные рюкзачные системы защиты информации // Известия ЮФУ. Технические науки. – 2013, №12 (149), С.209-216.
5. *Осипян В.О., Мирзаян А.В., Карпенко Ю.А., Жук А.С., Арутюнян А.Х.* Математическая модель системы защиты информации на основе диофантова множества // Чебышевский сборник. – 2014, №1 (49), С.146-154.
6. *Осипян В.О., Жук А.С.* Условия инъективности мультипликативного обобщенного рюкзачного вектора, научная статья / Специальная связь и безопасность информации (ССБИ-2016): Сборник трудов. Международная научно-практическая конференция. Краснодар. Издательство: Краснодарский центр научно-технической информации (ЦНТИ), 2016 г. – С. 92-97.
7. *Дурнев В.Г., Зеткина О.В., Зеткина А.И., Мурин Д.М.* О coNP-полноте задачи «Инъективный рюкзак» // Прикладная дискретная математика. – 2016, №3 (33), С.85-92.
8. *Шевляков Т.Н.* Мультипликативная рюкзачная криптосистема // Вестник ОмГУ. –2011, №4, С.23-25.
9. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995. – 318с.
10. *Айерлэнд К.* Классическое введение в современную теорию чисел. Роузен М. – М.: Мир, 1987, 416 с.

А.С. Жук[1], В.А. Головской[2]

СИНТЕЗ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОСНОВАНИИ МОДЕЛИ БЕЛЛА-ЛАПАДУЛЫ

[1]Некоммерческое частное образовательное учреждение высшего образования «Кубанский институт информзащиты», Краснодар, Россия

[2]Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: защита информации, несанкционированный доступ, иерархическая система, распределение ключей, модель Белла-Лападулы, ориентированный ациклический граф, верификация.

В статье рассмотрены иерархические системы защиты информации от несанкционированного доступа и методы распределения ключей в таких системах. Проанализированы иерархические системы защиты с криптографическим распределением ключей «сверху-вниз» и «снизу-вверх», приведены общие недостатки данных систем. Приведена математическая модель предлагаемой к разработке иерархической системы защиты информации от несанкционированного доступа на основании модели Белла-Лападулы.

A.S. Zhuck[1], V.A. Golovskoy[2]

[1]Kuban Institute of Informprotection, Krasnodar, Russia

[2]North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

SYNTHESIS OF A HIERARCHICAL SYSTEM OF INFORMATION PROTECTION FROM UNAUTHORIZED ACCESS ON THE BASIS ON THE BELL–LaPADULA MODEL

Keywords: information security, unauthorized access, hierarchical system, distribution of keys, Bell-LaPadula model, a directed acyclic graph, verification.

The article considers a hierarchical system of information protection from unauthorized access and methods of distribution of keys in such systems. Analyzed hierarchical system of protection with a cryptographic key distribution «top-down» and «bottom-up», given the common disadvantages of these systems. The mathematical model proposed for development of a hierarchical system of information protection from unauthorized access on the basis of the Bell-Lapadula model.

Современный этап развития информационных технологий характеризуется, в том числе, актуальностью вопросов обеспечения информационной безопасности [1-3]. Согласно исследованиям, проводимым ведущими аналитическими и исследовательскими компаниями [2, 3], наиболее актуальную угрозу информационной безопасности представляют случаи несанкционированного доступа (НСД) к служебной информации сотрудниками и выполнения ими неправомерных операций над ней. В связи с этим актуальной технической задачей является проектирование безопасной системы защиты от НСД.

Для решения указанной задачи используются различные правовые, организационные, аппаратные и программные средства обеспечения информационной безопасности, в которых ключевым звеном является «модель доступа». Среди различных используемых на практике моделей доступа принято выделять следующие основные типы: дискреционная модель, мандатная модель, ролевая модель. Все современные системы защиты от НСД реализуют, как правило, синтез данных моделей, с различными уникальными свойствами, определяемыми областью применения системы защиты.

В настоящей работе, в частности, рассматривается задача организации доступа к файловым хранилищам. Цель статьи: описать предлагаемую к разработке модель иерархической системы защиты информации от несанкционированного доступа.

Современные тенденции развития технических средств хранения и обработки данных подразумевают использование облачных хранилищ и распределенных систем. С увеличением объемов хранимой и обрабатываемой информации в таких системах принято использовать современные методы и средства работы с большими данными (big data) [4]. Концептуальный подход таких методов заключается в систематизации рассматриваемой информации. Для обеспечения быстродействия алгоритмов big data многие методы подразумевают иерархическую структуру данных. Таким образом, в данной статье рассматриваются иерархические системы защиты данных.

Следует отметить, что современные информационные системы с выделенными файловыми хранилищами подразумевают доступ к информации удаленными пользователями, что обуславливает использование сетевых технологий при проектировании рассматриваемых информационных систем. В подобных системах для осуществления защиты информации от НСД принято использовать технологию распределения ключей [5, 6].

Реализация подобной системы может быть осуществлена с использованием одной из следующих технологий:

- административное распределение ключей;
- иерархическое шифрование;
- криптографическое распределение ключей.

Авторами статьи проводятся исследования, имеющие своей целью повышение уровня защищенности иерархических систем с криптографическим распределением ключей от НСД.

Все существующие алгоритмы криптографического распределения ключей подразделяются на два типа [5]:

- «снизу-вверх»
- «сверху-вниз».

Основной подход в алгоритмах распределения ключей типа «снизу-вверх» заключается в том, что для доступа к информации каждый из пользователей имеет ключ, причем ключ пользователя с более высоким приоритетом содержит в себе ключи всех подчиненных пользователей. Подобные системы применяют симметричные алгоритмы шифрования для контроля доступа субъекта к объектам.

Основной подход в алгоритмах распределения ключей типа «сверху-вниз» заключается в том, что для доступа к информации каждый из пользователей имеет ключ, причем ключ пользователя с более высоким приоритетом содержится в ключах всех подчиненных пользователей. Но подчиненные пользователи не могут получить доступ к информации предков, а пользователь с высоким приоритетом может на основе ассиметричных алгоритмов шифрования получить доступ к ключам всех подчиненных пользователей.

Краткая характеристика основных алгоритмов обеспечения доступа с криптографическим распределением ключей приведена таблице № 1 [7].

Таблица № 1. Алгоритмы обеспечения доступа.

Алгоритм	Время взлома, MIPS-лет	Размер ключей	Вычисление ключей	Применимость	Недостатки
J. Yeh	Задача разложения больших чисел/ $3*10^7$	Секретных — $N = 1024$ Открытых — $L = 1024$	Возведение в степень, умножение: $O(r*l*p*\ln N) = O(69{,}3*l*p)$	В любых иерархических структурах	Невозможно расширение системы, трудоемкая операция возведения в степень
Хэш-функций	Стойкость хэш-функции/ $3{,}7*10^3$	Секретных — длина блока хэш-функции, $N = 512$	Вычисление хэш столько раз, сколько уровней: $O(N*p*l) = O(512*p*l)$	В древовидных иерархических структурах	Вычисление хэш-функций столько раз, сколько уровней
Hwang	Алгоритм шифрования Triple DES/ 10^{18}	Секретных — $N = 128$ Открытых — неограничен, $L^r = 128^r$	Деление и шифрование столько раз, сколько уровней, $n = 128^r/16$: $O(p*l*(n*\ln n*\ln\ln n)) = = O(p*l*2{,}58\mathrm{E}^{22})$	В любых иерархических структурах	Вычисление симметричного алгоритма столько раз, сколько уровней. Размер секретных ключей уменьшается в зависимости от уровня, открытых — растет
Комбинированный	Задача разложения больших чисел/ $3*10^7$	Секретных — $N = 1024$ Открытых — $L = 384$	Деление и умножение столько раз, сколько уровней: $O(p*2*l*(n*\ln n*\ln\ln n)) = = O(p*l*759)$ $n = N/16$	В древовидных иерархических структурах. Ключи группы, уровня	Размер секретных ключей незначительно уменьшается в зависимости от уровня

Существуют комплексные алгоритмы, реализующие каждый из этих подходов, например, описанный последним в таблице.

Отметим следующее важное свойство: в каждом из указанных алгоритмов каждому субъекту ставится в соответствие некоторое число, например, простое число p для алгоритма Дж. Иеха. Данное число будет использоваться для синтеза новой системы защиты иерархической информации.

Каждый из алгоритмов имеет свои преимущества и недостатки, и соответственно, свою преобладающую область применения. Но сформулируем задачу, которую не решает ни один из рассмотренных алгоритмов. Для этого рассмотрим самый распространенный пример мандатной модели управления доступом, систему Белла-Лападулы [8-11]: информационная система с множеством разделяемых объектов доступа из множества $O = \{o_1, o_2, ..., o_m\}$ и множеством субъектов доступа из множества $S = \{s_1, s_2, ..., s_n\}$. Так же отметим, что в качестве субъектов могут выступать как конкретные пользователи, так и роли.

Каждому объекту и субъекту ставится в соответствие число из множества $M = \{m_1, m_2, .., m_k\}$, называемое меткой доступа (мандатом), при этом значение метки тем ниже, чем ниже уровень конфиденциальности. Каждый субъект может получить право на выполнение одной из операций чтения, записи, удаления (r, w, d) некоторого объекта. Далее, если субъект s_i с мандатом m_{s_i} пытается получить доступ к объекту o_j с меткой m_{o_i}, то диспетчер доступа выполняет одну из следующих операций:

– если $m_{s_i} \le m_{o_i}$, то субъекту выдается право чтения, но не право записи;

– если $m_{s_i} \ge m_{o_i}$, то субъекту выдается право записи.

Теперь проверим выполнимость указанных условий в рассматриваемой иерархической системе защиты от НСД. Очевидно, что пользователь *S* всегда имеет право на запись и чтение файлов подчиненного пользователя. Но при этом существует вероятность утечки информации от пользователя *S* к его потомкам, то есть существует вероятность неправомерного информационного потока от пользователя *S* к его потомкам, и несанкционированный доступ потомков к этой информации.

Таким образом, можно сделать следующий вывод. Несмотря на то, что криптографическое распределение ключей позволяет обеспечить безопасность информации пользователя *S* от пользователей, не имеющих к ней доступ, иерархическая система управления доступом изначально не предназначена для решения задачи защиты информации, обрабатываемой пользователем *S,* от недобросовестных действий самого пользователя. Например, пользователь *S* имеет техническую возможность передать своему потомку информацию, к которой тот не имеет доступа. С учетом того, что именно несанкционированный обмен информацией между внутренними пользователями системы является главной причиной нарушений информационной безопасности в организациях [2, 3], цель проводимого исследования представляется актуальной.

Перед формулированием предложения по синтезу системы необходимо отметить, что требуется модифицировать именно иерархическую систему управления доступом, математическая модель которой представляет собой ориентированное дерево, в котором каждой вершине поставлен в соответствие некоторый субъект безопасности.

Далее сформулируем общие требования к системе управления доступом к иерархической информации, на основании которых будет осуществляться поиск подходящей математической модели решения задачи.

1. Пользователь системы должен иметь доступ к информации только согласно своим полномочиям.
2. Коалиция пользователей не должна иметь доступ к информации не подчиненных им пользователей.
3. Вычисление ключей пользователей на любом уровне не должно приводить к замедлению работы автоматизированной системы обработки информации.
4. Система должна иметь возможность расширения, как в глубину, так и в ширину, без перерасчета остальных параметров ключей остальных пользователей.

С учетом требования к быстродействию системы удобно использовать задачу, основанную на математическом аппарате, моделирующем реальную систему иерархического доступа. Исходя из этого, выдвигается предложение использовать задачу верификации вершины графа для определения конкретного субъекта доступа. Задача

верификации достаточно часто используется для тестирования работающих систем путем составления графа состояний системы и определения нахождения системы в указанном состоянии [12, 13]. Предлагается модификация данной задачи для определения конкретного субъекта по составленной математической модели защиты иерархической информации. Напомним, что данная модель является графом, задающим отношение приоритета для субъектов доступа, являющееся строгим отношением порядка на множестве всех пользователей (ролей) информационной системы с выделенным файловым хранилищем.

Для построения требуемой модели системы рассмотрим информационную систему с субъектами доступа из некоторого множества S. В качестве субъектов могут выступать как конкретные пользователи, так и роли пользователей в более общем случае. На множестве пользователей задано отношение нелинейного порядка (рефлексивное, антисимметричное, транзитивное) $R: S_i R S_j \leftrightarrow$ пользователь S_i превосходит в полномочиях пользователя S_j и имеет доступ ко всем данным этого пользователя. Отношение R таково, что граф, задающий его, представляет собой дерево, где все субъекты доступа системы располагаются на различных уровнях доступа (рисунок 1).

Отметим, что в данной модели в качестве субъектов доступа в зависимости от конкретной реализации могут выступать как пользователи системы, так и роли.

Введем метки доступа $M = \{m_1, m_2, .., m_k\}$ такие, что $(S_i R S_j) \to (m_{s_i} < m_{s_j})$. Каждому субъекту доступа поставим в соответствие объект доступа в виде каталога, для которого в дальнейшем необходимо спроектировать структуру доступа к внутренней информации. Для каждого субъекта S_i существует единственный путь доступа от вершины S_0 к соответствующей вершине, обозначим его P_i. Обозначим через $P = \{P_1, ..., P_n\}$ множество всех возможных путей P_i на данном графе.

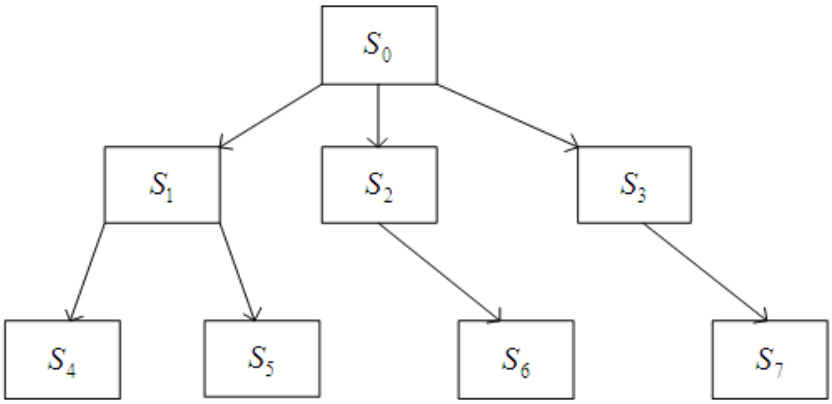


Рисунок 1. Иерархия субъектов доступа

Введем некоторую функцию $F: P \to N$, про которую известно, что она получает значения из множества натуральных чисел и является односторонней функцией. Далее введем предикат $Q = Q(F(P_i), p_i)$, который при выполнении некоторого условия над

значением функции пути для данного пользователя и значения p_i (система Иеха) для него же принимает истинное значение.

Теперь опишем модель доступа субъекта S_i к объекту O_j. При авторизации пользователя как субъекта доступа он получает значения P_i, p_i. Далее при попытке получения доступа на запись будет проверена выполнимость предиката $Q = Q\left(F\left(P_j\right), p_i\right)$. Таким образом, будет смоделирована задача верификации вершины графа. Если предикат для заданных значений становится тавтологией, то доступ на запись разрешается.

Отметим, что доступ на чтение осуществляется на основе любого из приведенных ранее алгоритмов криптографического распределения ключей в иерархических системах защиты информации.

В результате модифицирована иерархическая системы защиты информации с криптографическим распределением ключей посредством введения дополнительной защиты от разглашения конфиденциальной информации на основе условий Белла-Лападулы. Предлагается использование задачи верификации вершин графа для определения права доступа на запись к информации подчиненных пользователей.

Важно, что системы доступа к иерархической информации уже используются на практике, например, в модели доступа Белла-Лападулы реализуется доступ к иерархической информации. Но в подобных системах есть два недостатка [4, 6]. Во-первых, на множестве субъектов доступа реализовано отношение линейного порядка, что не позволяет смоделировать пользователей информационных систем в реальных организациях. Во-вторых, в подобных системах небезопасной является операция удаления объекта доступа. В проектируемой системе данные недостатки устранены за счет общих принципов построения любых систем защиты иерархической информации с криптографическим распределением ключей.

Дальнейшее направление исследования предполагает следующее:

1. Подбор односторонней функции $F\left(P_i\right)$, которая на основе пути графа получает численное значение.
2. Математическое обоснование возможности использования подобранной функции.
3. Подбор предиката $Q = Q\left(F\left(P_i\right), p_i\right)$, реализующего решение задачи верификации вершины графа.
4. Математическое моделирование иерархической системы защиты от НСД и разглашения информации ограниченного доступа с криптографическим распределением ключей.
5. Доказательство выполнимости указанных выше требований к системе.
6. Доказательство безопасности построенной системы.
7. Информационной моделирование указанной системы.
8. Реализация выделенных в предыдущем пункте подпрограмм.

В статье приведен анализ некоторых существующих моделей построения систем защиты информации от несанкционированного доступа. Проанализированы модели иерархических систем с криптографическим распределением ключей и различными применяемыми алгоритмами. Определен недостаток всех указанных моделей. Предложено решение по устранению данного недостатка путем синтеза иерархической модели и мандатной модели Белла-Лападулы. На основании требований, предъявляемых к

системам контроля управления доступом, предложена математическая модель указанной системы на основании задачи верификации вершины графа.

СПИСОК ЛИТЕРАТУРЫ

1. DARPA to release research on security ratings for software in 2016 [Электронный ресурс]. – Режим доступа: https://insidecybersecurity.com/share/4169 (дата обращения 30.03.2017).
2. KasperskySecurityBulletin. Основная статистика за 2011 год [Электронный ресурс]. – Режим доступа: URL: http://www.securelist.com/ru/analysis/208050741/rss/analysis (дата обращения 30.03.2017).
3. Код Безопасности [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/company/news/SC-analytic-2011 (дата обращения 30.03.2017).
4. *Min Chen, Shiwen Mao, Yin Zhang, Leung C.M.* Big data. Related technologies, challenges, and future prospects. – Springer, 2014. – 100 p.
5. *Лернер В.Д.* Криптографическое распределение ключей для защиты информации в иерархических системах // Информационно-управляющие системы. – 2012, №5 (60), С.37-43.
6. *Щеглов А.Ю.* Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие. – СПб: Университет ИТМО, 2014. – 95 с.
7. *Kayem Anne V.D.M., Akl S.G., Martin P.* Adaptive cryptographic access control. – Springer, 2010. – 152 p.
8. *Bell D.E.* Looking Back at the Bell-LaPadula Model // 21st Annual Computer Security Applications Conference. Tucson, Arizona, USA. – 2005. P. 337-351.
9. *Усов С.В.* О связи между объектно-ориентированной дискреционной и субъектно-объектной мандатной моделями безопасности // Математические структуры и моделирование. – 2016, №4 (40), С.151-163.
10. *Девянин П.Н.* Необходимые условия нарушения безопасности информационных потоков по времени в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. – 2015, № 8, С. 81-83.
11. *Щеглов К.А., Щеглов А.Ю.* Непротиворечивая модель мандатного контроля доступа // Известия высших учебных заведений. Приборостроение. – 2014, Т. 57, № 4, С. 12-15.
12. *Карпов Ю.Г.* MODEL CHECKING. Верификация параллельных и распределенных программных систем, БХВ-Петербург, 2010, 560 с.
13. *Bayer C., Katoen J.-P.* Principles of model checking. – MIT Press, 2008. – 975 p.

Э.Т. Ишдавлетова, К.А. Ролдугина

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ МОДЕРНИЗАЦИИ И РАЗВИТИЯ ПОЧТОВЫХ УСЛУГ НА БАЗЕ ИКТ

Ташкентский университет информационных технологий, Ташкент, Узбекистан

Ключевые слова: информационно – коммуникационные технологии, информационная система, модернизация, почтовая связь, нормативно – правовая база Республики Узбекистан, АО «Узбекистон почтаси».

В статье рассмотрено внедрение информационных технологий в различных отраслях Республики Узбекистан, а также модернизация и развитие почтовых услуг на базе ИКТ.

E.T. Ishdavletova, K.A. Roldugina

ENSURING INFORMATION SECURITY IN THE CONTEXT OF MODERNIZATION AND DEVELOPMENT OF POSTAL SERVICES ON THE BASIS OF ICT

Tashkent University of Information Technologies, Tashkent, Uzbekistan

Keywords: information and communication technologies, information system, modernization, postal service, regulatory and legal base of the Republic of Uzbekistan, "Uzbekiston Pochtasi".

In this article is considered the introduction information technologies in the different industries of Republic of Uzbekistan, and also modernization and development of postal services on the basics of ICT.

Мир информационно-коммуникационных технологий стал неотъемлемой частью повседневной жизни. Соответственно меняется форма ведения деятельности органов государственной власти и управления при оказании различных услуг физическим и юридическим лицам путем применения информационно-коммуникационных технологий по реализации их функций и задач.

Весь мировой опыт показывает, что в настоящее время в глобальной экономике все более возрастающую роль и значение приобретает сектор информационно-коммуникационных технологий, включающий в себя производство компьютерных и телекоммуникационных технологий, разработку программного обеспечения и предоставление на их основе широкого спектра интерактивных услуг. Не следует забывать, что развитие ИКТ напрямую влияет на уровень конкурентоспособности страны, позволяет собирать и обобщать огромные массивы информации, открывает широкие возможности для управления на стратегическом уровне».

В связи с актуальностью задач, важно отметить, что в республике осуществляется широкий комплекс целенаправленных организационно-правовых мер по формированию национальной системы информатизации, массовому внедрению и использованию во всех сферах экономики и жизни общества современных информационных технологий, средств компьютерной техники и телекоммуникаций, полному удовлетворению растущих информационных потребностей граждан, созданию благоприятных условий для вхождения в мировое информационное сообщество и расширению доступа к мировым информационным ресурсам.

В частности, приняты и успешно реализуются ряд нормативно-правовых актов. В частности, Законы Республики Узбекистан «Об информатизации», «Об электронной цифровой подписи», «Об электронном документообороте» и другие подзаконные нормативно-правовые акты.

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».

Стратегия развития Национальной информационно-коммуникационной системы Республики Узбекистан, осуществляемая по всем направлениям развития информационно-коммуникационных технологий, демонстрирует положительную тенденцию.

Для достижения в стране поставленных целей по развитию ИКТ сформирована мощная нормативно-правовая база, в частности: приняты законы «Об информатизации», «Об электронной цифровой подписи», «Об электронном документообороте», «Об электронных платежах» и др. Отдельно позвольте отметить, что в настоящее время разработан и внесен в Парламент проект закона «Об электронном правительстве»; в рамках принимаемых мер по развитию Национальной информационно-коммуникационной системы за последние три года принято более 20 постановлений и указов Президента Республики Узбекистан, 30 правительственных решений, затрагивающих вопросы широкого внедрения информационных систем, интерактивных услуг и организации обучения в сфере ИКТ.

Правительством республики уделяется особое внимание вопросам ускоренного развития и широкого внедрения в отраслях реальной экономики информационно-коммуникационных технологий и программных продуктов и на этой основе повышения эффективности управления, снижения издержек производства, обеспечения прозрачности финансово-хозяйственной деятельности хозяйственных объединений и крупных предприятий, повышения их конкурентоспособности на внутреннем и внешних рынках.

В заключение позвольте остановиться на перспективных направлениях развития отрасли ИКТ по следующим блокам:

В области развития рынка программных продуктов:

- Стимулирование развития производства отечественного программного обеспечения.
- Создание современных информационных систем для автоматизации производственных и управленческих процессов, особенно для малого бизнеса.

В области развития телекоммуникационной инфраструктуры:

– Расширение сети широкополосного доступа.
– Создание современных дата-центров для обработки «больших данных».
– Развитие сети мобильной связи по технологии 4G LTE.

В области электронного правительства:

– Развитие решений информатизации государственных органов.
– Совершенствование деятельности создаваемых центров «одно окно».
– Создание условий для эффективного использования открытых данных.

В области национального контента

– Насыщение информационного пространства национального сегмента Интернета информационными ресурсами, основанными на познании богатой истории Узбекистана, национальных традиций и духовных ценностей народа.
– Создание современных отечественных веб-ресурсов, обеспечивающих удовлетворение информационных и интеллектуальных потребностей населения.

Почтовая сеть представляет собой крупный сектор мирового бизнеса и в частности, бизнеса отдельно взятой страны, что делает ее заманчивой для преступных элементов. Почтовые службы всего мира работают в условиях постоянно растущего числа посягательств со стороны криминальных структур.

Для почтовых служб всех стран мира, как и для любой коммерческой деятельности, наиболее важным фактором успеха является высокое качество обслуживания клиентов.

Клиенты хотят иметь гарантию, что пересылаемые ими отправления прибудут по назначению в целости и сохранности и в установленный срок.

Почтовая гарантия не может быть обеспечена без почтовой безопасности и её составной части - информационной безопасности, так как почтовая безопасность является одной из опор качества.

Эффективность и целостность физической сети должна постоянно улучшаться благодаря скоординированным и комплексным действиям стран-членов для противостояния проблемам, возникающим на пути прохождения почтовых отправлений.

В Дохинской почтовой стратегии для достижения эффективного взаимодействия инфраструктуры почтовых сетей были запланированы следующие программы: повышение качества службы, надежности и эффективности почтовых сетей; повышение сохранности и безопасности почтовых отправлений и содействие упрощению таможенных процессов; разработка соответствующих стандартов и правил; стимулирование использования инфокоммуникационных технологий (ИКТ) для облегчения доступа к услугам и улучшения показателей работы; способствование совершенствованию методов адресации в национальных почтовых системах.

Безусловно, при этом следует учитывать снижение объемов на некоторых сегментах международных почтовых рынков и необходимость приспосабливаться к изменяющимся условиям, упрощать спектр услуг и продуктов.

Электронная сеть предполагает внедрение самых новых технологий для обеспечения безопасности передачи информации и создания высокоэффективных, скоростных и надежных информационных систем.

Развитие финансовых систем также должно опираться на функциональную совместимость и безопасность информационных систем. По всем указанным

направлениям национальный оператор почтовой связи Республики Узбекистан имеет определенные результаты, поскольку с момента его создания постоянно ведет работы по автоматизации технологических процессов, управления производством и предприятием в целом.

За последние годы структура информационных систем в почтовой связи приобрела четкий вид и стала более универсальной во всех филиалах предприятия, подразделяясь на информационные системы для управленческих (статистика, бухгалтерия, налоговый учет, финансовый анализ, кадровый учет, документооборот и т. д.) и технологических процессов и системы для автоматизации предоставления услуг потребителям.

В почтовой связи создана корпоративная мультисервисная коммуникационная сеть предприятия с возможностями масштабирования и развития, которая позволяет обеспечить защиту информации и поддержку современных цифровых сервисов.

Почтовая связь в мире идет в ногу со временем и постоянно модернизирует существующие технологии, программные продукты и подходы к управлению сетью объектов почтовой связи. Все это обусловлено желанием максимально исключить влияние человеческого фактора на информационный поток, которым сопровождаются физические почтовые отправления, и приведением базы данных сети объектов почтовой связи к единому стандарту.

Почтовый сектор вынужден обновляться в целях разработки инновационных, интегрированных и доступных решений в области развития.

Стратегическая конференция ВПС 2015 г. в Женеве: подтвердила, что в предстоящие несколько лет Всемирный почтовый союз и назначенные операторы стран-членов будут располагать потенциалом, способным создать условия для глобального социально-экономического преобразования. Это произойдет благодаря принятию и выполнению плана деятельности, заложенного в Стамбульскую почтовую стратегию и направленного на успешное использование совместными усилиями членами ВПС преимуществ функционального взаимодействия различных информационных систем и систем передачи данных.

Взаимодействие информационных систем позволяет не только улучшить доступ к почтовым услугам и повысить качество службы, но и обеспечить эффективность процессов и удовлетворенность клиентов, а также эффективность управления предприятием за счет обеспечения руководителей и специалистов максимально полной, оперативной и достоверной информацией.

Подводя итог сказанному выше, следует отметить, что важным условием успешной реализации задач является интерес центральных органов исполнительной власти страны к деятельности почтового сектора. При этом целесообразно определить и распределить ответственность за реализацию Всемирной почтовой стратегии между назначенным оператором, правительством и регулятором.

Правительство должно содействовать привлечению инвестиций в почтовый сектор, чтобы национальный почтовый оператор был в состоянии внедрять инновационные, интегрированные решения для удовлетворения потребностей клиентов, выполнять свои социальные обязательства и обеспечивать стабильное развитие.

Регулятор обязан нести ответственность за установление справедливой конкуренции на рынке, а назначенный оператор — удовлетворять потребности клиентуры почтовых услуг.

Необходима достаточная поддержка со стороны государственных органов в проведении реформы, а также реализация стратегий на основе Дохинской почтовой стратегии, а также будущей Стамбульской стратегии, которая станет отправной точкой при разработке приоритетной деятельности членов ВПС и их региональных союзов и будет реализовываться посредством планов регионального развития.

Безусловно, Стамбульская почтовая стратегия будет использована странами-членами при разработке своей национальной почтовой стратегии и политики, чтобы каждое государство быстрее осуществляло преобразования и шло в ногу с изменениями, если оно стремится сохранить свою значимость.

Одним из основных приоритетов АО «Узбекистон почтаси» является модернизация сети почтовой связи, развитие и внедрение новых видов услуг на базе ИКТ. В АО «Узбекистон почтаси» создана корпоративная сеть, на базе которой функционируют автоматизированные системы: Автоматизированная система электронные денежные переводы; «Гибридный денежный перевод»; Автоматизированная система учета выплаты пенсий и пособий; Автоматизированная информационная система приема платежей; Автоматизированная система по контролю за прохождением регистрируемых почтовых отправлений; «Автоматизированная система обмена рекламации по посылкам IBIS»; Автоматизированная информационная система «PRIME»; Автоматизированной системы приема подписки, оформления и обработки заказов на периодические издания; Автоматизированная информационная система «Ragby»; «Автоматизированная система составления плана направлений международных посылок»; Система контроля автотранспорта «GPS трекер»; АРМ Билинг; Система дистанционного обучения.

В 2002 году на основании приказа АО «Узбекистон почтаси» начато создание корпоративной компьютерной сети (ККС) АО "Узбекистон почтаси".

Проект ККС АО разработан филиалом «Intal Telekom» ОАК «Узбектелеком». Сама сеть создана на базе арендуемых у филиала «ЦРБ» АК «Узбектелеком» каналов и принята в эксплуатацию в начале 2003 года.

В целях активного внедрения и контроля ИБ разработана и утверждена «Политика информационной безопасности АО «Узбекистон почтаси», и в филиалах в приказном порядке назначены ответственные лица по ИБ и переработаны должностные инструкции ответственных лиц по ИБ в филиалах.

Для ознакомления работников Общества и почтовых объектов с новым направлением «Информационная безопасность», проведены ряд совещаний в филиалах с демонстрацией видеоролика, посвященного вопросам информационной безопасности, проведены занятия по соответствующим темам с лицами, ответственными за данный участок деятельности.

На всех персональных компьютерах установлены идентификаторы, налажена работа по учету и контролю пользователей домена «post.uz», упорядочена система выдачи адресов электронной почты. Разработан план перехода филиалов на новую схему подключения к сети Интернет через корпоративную сеть АО «Узбекистон почтаси», также внедрена единая биллинговая система для распределения доступа к сети Интернет.

В заключении можно отметить, что гарантом обеспечения информационной безопасности предприятия, является строгое соблюдение предписаний политики, инструкций и правил, затрагивающих вопросы приема, передачи, хранения информации и

осуществление регулярной и периодической проверки и контроля соблюдения указанных правил всеми сотрудниками организации.

С точки зрения бурного развития информационных технологий, требуемого при этом обеспечение информационной безопасности в почтовой связи, необходимо обращать постоянное внимание на следующие вопросы:

- при разработке нормативных документов уделять особое внимание вопросам защиты и хранения конфиденциальной информации;
- проводить регулярные занятия по вопросам обеспечения информационной безопасности и повышению квалификации сотрудников АО «Узбекистон почтаси» и её филиалов;
- приобретение необходимого технического оборудования и программных средств защиты информации в зависимости от категории уязвимости внедряемых перспективных задач и услуг;
- осуществлять регулярный обмен знаниями в сфере информационной безопасности, как местными, так и с зарубежными коллегами.

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Кабинета Министров 19 мая 2005 года № 128 «О Программе модернизации сети почтовой связи, внедрения и развития новых видов услуг на базе информационно-коммуникационных технологий до 2010 года»
2. Постановление Президента Республики Узбекистан от 21 марта 2012 года № ПП-1730«О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий»
3. Информационные технологии и вычислительные системы / Под ред. *С.В. Емельянова*. – М.: Изд-во УРСС, 2004
4. *Исакова А.И.* Основы теории управленческих информационных систем. – Томск: ТУСУР, 2005

А.Г. Кирхеев[1], В.А. Головской[2]

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ МОБИЛЬНОГО УСТРОЙСТВА

[1]Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище им. генерала армии С.М. Штеменко», Краснодар, Россия

[2]Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: безопасность информации, уязвимость операционной системы, операционная система Android, вредоносное программное обеспечение.

Рассмотрены угрозы безопасности информации мобильного устройства под управлением операционной системы Android, приведены результаты анализа способов проникновения вредоносного программного обеспечения на мобильные устройства.

A.G. Kirheev[1], V.A. Golovskoy[2]

TO THE PROBLEM OF INFORMATION SECURITY MOBILE DEVICE

[1]Krasnodar Higher Military School named after S.M. Shtemenko, Krasnodar, Russia

[2]North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: information security, weakness of operation system, operation system Android, malicious software.

Considered threats to the security of the mobile device information on Android operating system, the results of the analysis of the ways malicious software on mobile devices are presented.

В условиях интенсивного роста уровня киберпреступности одним из распространенных криминальных направлений является использование уязвимостей операционных систем мобильных устройств для доступа к данным, на них хранящимся, и неправомерное их использование [1-3]. Наличие уязвимостей ОС Android [4] в комплексе с несовершенной модерацией приложений сервисом Play маркет [3] может способствовать получению злоумышленником, действующим удаленно, данных пользователя с помощью специально созданного или модифицированного официального приложения известных компаний.

Кроме нарушения конфиденциальности данных, хранящихся на мобильном устройстве, рассматриваются угрозы получения геолокационных данных пользователя, персональных данных, не хранящихся в памяти устройства, – захвата управления ресурсами мобильного устройства вообще. Под ресурсами мобильного устройства понимаются хранящиеся на нем данные, его аппаратные и программные средства.

Для обеспечения безопасности ресурсов мобильного устройства были выработаны требования к защищенной мобильной операционной системе [5]. Однако обеспечение выполнения указанных требований разработчиками ОС для мобильных устройств видится затруднительным. Авторами проводятся исследования, имеющие целью создание приложения, обеспечивающего безопасность ресурсов мобильных устройств под управлением ОС Android. С целью создания указанного приложения проведен анализ возможных путей проникновения вредоносного программного обеспечения (ВПО) на мобильные устройства.

Традиционно, для рассмотрения уязвимостей рассматривается четыре уровня ОС Android, отвечающие за функционирование самой ОС и обеспечивающие выполнение процессов [6]:

1. Ядро Linux (kernel). Так как ОС Android создана на базе Linux, ядро данной системы имеет набор базовых функций и открытый исходный код. Ядро выполняет такие задачи, как соблюдение прав доступа и осуществление контроля выполнения процессов, то есть, приложения не могут получить доступ к данным другого приложения, пока ядро не даст разрешение. Каждое приложение, в свою очередь, является отдельным пользователем, который имеет свои права доступа к данным, которые использует приложение.
2. Библиотеки (Native Libraries), необходимые для ОС Android. Например, библиотека 3D graphics отвечает за правильное отображение трехмерной графики, а Media codecs – за воспроизведение видео файлов.
3. Android Framework. К этому уровню относится набор инструментов разработки приложений для ОС Android (PowerManager, ActivityManager, NotificationManager и т.д.).
4. Приложения (Applications). ОС Android обеспечивает функционирование приложений двух типов: системные (предустановленные производителем устройства) и приложения, которые пользователь имеет возможность устанавливать самостоятельно из различных источников. Первые приложения находятся в папке /system/app, вторые – в папке /data/app.

Одним из вариантов проникновения ВПО на мобильные устройства является его установка под видом известных приложений либо установка приложений, модифицированных злоумышленниками.

Злоумышленник имеет возможность инициировать установку ВПО следующими способами [6, 7]:

- Используя приложение PackageInstaller.
- Используя приложение Play маркет.
- Используя команду «adb install».

После установки приложения ему присваивается свой собственный идентификатор пользователя (UID) и создается папка, где хранятся исходные данные приложения. Безопасность данных обеспечивается с помощью песочницы, которая с помощью

разграничения прав доступа к приложению разрешают самому приложению читать собственные файлы и запрещают делать это другим процессам и приложениям. Еще одним важным аспектом защиты при установке приложений является определение прав доступа к функциям мобильного устройства (сообщения, звонки, камера, микрофон и другие), которые далее записываются в файл AndroidManifest.xml.

Разрешения (permission) в ОС Android также работают на уровне ядра, например, – android.permission.INTERNET [8]. Когда приложение во время установки запрашивает доступ к этому разрешению, ОС Android добавляет это приложение в группу «inet». Аналогично реализуются и другие разрешения. Список соответствия таких разрешений и групп хранится в файле frameworks/base/data/etc/platform.xml. Следовательно, если приложение запросит доступ к интернету, то оно должно пройти проверку, которую осуществляет ядро ОС Android, убеждающееся в процессе, что приложение находится в группе с идентификатором INET. Только после проверки ядро дает разрешение на выход в интернет, при соблюдении требований ядра.

Для обеспечения безопасности ресурсов мобильного устройства под управлением ОС Android ведутся исследования, направленные на создание специализированного приложения. Данное приложение должно будет осуществлять проверку дистрибутива приложения на предмет определения его легальности, немодифицированности и отсутствия ВПО, а также анализировать генерируемый трафик.

Для создания приложения необходимо решить следующие задачи:

- исследование функционирования ОС Android и модифицированных приложений;
- исследование алгоритмов работы антивирусных программ и сканеров уязвимостей;
- анализ достоинств и недостатков антивирусных программ и сканеров уязвимостей;
- разработка метода проверки дистрибутива приложения на предмет определения его легальности, немодифицированности и отсутствия ВПО;
- разработка оптимального алгоритма реализации разработанного метода;
- создание приложения для ОС Android, реализующего разработанный метод.

СПИСОК ЛИТЕРАТУРЫ

1. Internet Organised Crime Threat Assessment, report 2016 [Электронный ресурс] // Официальный сайт Европолиции. – Режим доступа: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016, свободный. – загл. с экрана.
2. *Dunn J.E.* Android's 5 biggest security flaws 2015 [Электронный ресурс] – Режим доступа: http://www.techworld.com/security/androids-5-biggest-security-flaws-2015-3622116, свободный. – загл. с экрана.
3. *Михайлов Д.М.* Выявление признаков негласного слежения за местоположением абонентов в сетях беспроводной связи // Спецтехника и связь. – 2013, № 2, с. 42–47.
4. Банк данных угроз безопасности информации [Электронный ресурс] // Федеральная служба по техническому и экспортному контролю. – Режим доступа: https//www.bdu.fstec.ru/vul/2016-01160, свободный. – загл. с экрана.
5. *Бокова О.И., Михайлов Д.М., Фроимсон М.И.* Выработка и анализ требований к защищенной мобильной операционной системе // Вестник Воронежского института МВД России. – 2013, № 4, с.242–247.

6. *Enck W., Ongtang M., McDaniel P.* Understanding Android Security, IEEE Security & Privacy. – 2009, vol.7, Issue № 1, p. 50–57.
7. *Казимир В.В., Карпачев И.И.* Функциональная безопасность архитектуры мобильной операционной системы Android // Вісник Чернігівського державного технологічного університетую. – 2015, № 1 (77), с. 127–134.
8. Разработчикам Android [Электронный ресурс] – Режим доступа: http://developer.android.com/reference/android/manifest.permission.html, свободный. – загл. с экрана.

С.М. Краснопеев, А.А. Юркин

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АНАЛИЗА ОБРАЗА ОПЕРАТИВНОЙ ПАМЯТИ

Академия ФСО России, Орел, Россия

Ключевые слова: инцидент информационной безопасности, оперативная память, расследование, анализ.

В работе проведен анализ способов расследования инцидентов информационной безопасности, описана функциональная модель расследования инцидентов информационной безопасности. Предложен способ обнаружения инцидентов информационной безопасности на основе анализа образа оперативной памяти.

S.M. Krasnopeev, A.A. Yurkin

INVESTIGATION INCIDENTS OF INFORMATION SECURITY, BASED ON ANALYSIS IMAGE OF MAIN STORAGE

FSO Academy, Orel, Russia

Key words: incident of information security, main storage, investigation, analysis.

The article includes analysis of metod investigation incidents of information security, description of functional model of investigation incidents of information security. In the article method of exposure incidents of information security, based on analysis image of main storage, is offered.

Защита информации, содержащейся в государственных информационных системах, обеспечивается путем выполнения требований к организации защиты информации, одним из которых является выявление и расследование всех инцидентов информационной безопасности. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007, инцидент

информационной безопасности – одно или серия нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации бизнес-операции и угрожают информационной безопасности [1].

При расследовании инцидентов обнаруживается какие уязвимости информационной безопасности содержит информационная система, проявляются последствия негативного воздействия нарушителя на систему и оценивается вероятность возникновения возможных инцидентов в самой информационной системе.

Развитие информационных систем и увеличение числа инцидентов в них требует их оперативного обнаружения и всестороннего рассмотрения причин возникновения, с целью минимизации последствий произошедшего. Улучшить достоверность и оперативность расследований можно с помощью нескольких вариантов. К техническим вариантам относится использование большего количества источников важной для расследования информации, каковыми являются:

- энергонезависимые носители информации (накопители на жестких магнитных дисках, флеш-накопители);
- энергозависимые носители информации (оперативное запоминающее устройство);
- лог-файлы сетевого оборудования (систем обнаружения атак и др.);
- сетевой трафик.

Анализ энергонезависимых источников информации и анализ лог-файлов являются распространенными способами расследования, для которых уже рассмотрены существующие алгоритмы и функциональное программное обеспечение (ПО). Анализ сетевого трафика – полностью изучен с технической точки зрения, но при расследовании инцидентов не распространен. А вот создание копий оперативной памяти (ОП) и последующий его анализ – относительно новый метод, ещё не нашедший полного и повсеместного использования, не смотря на то, что программы для данных анализов существуют: The Volatility Framework, Belkasoft Evidence Center, Elcomsoft Forensic Disk Decryptor, Passware Kit Forensic и др.

Помимо использования большего количества источников важной для расследования информации необходимо рассматривать и средства проведения расследований. Определенное количество распространенных средств являются платными, не являются русскоязычными, имеют большое количество ошибок.

Можно отметить, что ОП является наилучшим объектом для расследования инцидентов информационной безопасности, так как все действия в операционной системе (ОС) осуществляются в ней, а именно:

- процессы и потоки;
- функционирование вредоносного программного обеспечения (включая руткит-технологии);
- настройка сетевых портов, URL-адреса, IP-адреса;
- манипуляции с открытыми файлами;
- контент, создаваемый пользователями (пароли, буфер обмена);
- ключи шифрования, посредством которых можно быстро расшифровать что находится в криптоконтейнерах TrueCrypt, BitLocker и PGP Disk;
- программные и аппаратные конфигурации;
- ключи реестра для Windows и журналы регистрации событий;

Оперативная память является наилучшим местом для выявления активности вредоносного программного обеспечения. С помощью анализа дампа оперативной памяти возможно:

- выявление каких-либо несовместимостей в ОС;
- просмотр конфигурации операционной системы;
- обход упаковщиков, обфускаторов, руткитов и подобных инструментов сокрытия вредоносного кода.

Посредством анализа оперативной памяти возможно отслеживание недавней активности в ОС:

- анализ недавних действий пользователя;
- отслеживание активности вредоносного программного обеспечения.

Также, в энергозависимой памяти обнаруживаются сведения о последних изменениях файлов. В ОП определенный промежуток времени находятся страницы с веб-сайтов, даже если в браузере включен режим защиты приватности, отключен кеш и сохранение истории посещений. Также, можно найти существенный объём системной информации, загруженные ветки реестра, распакованные и расшифрованные версии защищенных программ, информацию о совершенных сетевых соединениях. Некоторые типы вредоносного программного обеспечения, такого, как средства несанкционированного доступа на основе технологии подгружаемых модулей ядра ОС (LKM rootkit), загружаются непосредственно в память, не модифицируя файлы или каталоги. Сетевой червь Code Red является хорошим примером таких вредоносных программ, которые не записываются предварительно в файл, а загружаются непосредственно в оперативное запоминающее устройство системы и запускаются на исполнение. В случае нахождения на ЭВМ вредоносного программного обеспечения при анализе образа ОП его можно легко обнаружить.

Функциональную модель расследования инцидентов информационной безопасности можно представить рисунком 1. При этом необходимо учитывать, что сами действия сотрудников организации и специалистов по расследованию инцидентов информационной безопасности должны быть отражены в политике безопасности организации.

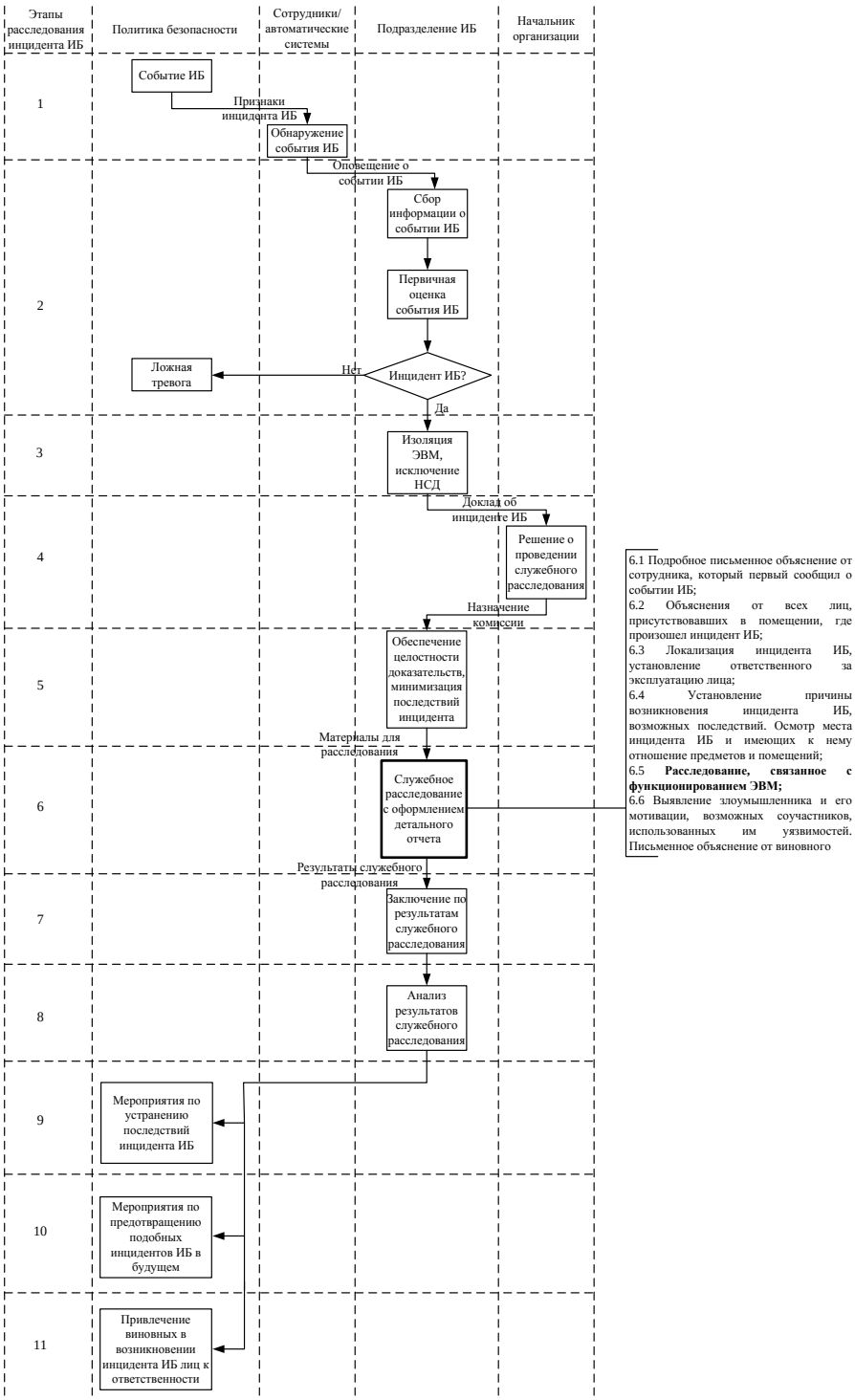


Рис. 1 Функциональная модель процесса расследования инцидентов информационной безопасности

Расследование инцидента информационной безопасности в ходе проведения служебного расследования, связанного с функционированием ЭВМ можно разделить на два этапа: сбор данных и их анализ.

В качестве данных будет выступать образ оперативной памяти.

В ходе снятия дампа ОП необходимо изолировать ЭВМ без выключения питания, так как ОП является энергозависимым источником информации для проведения

расследования. После решения начальника организации о проведении служебного расследования, из числа наиболее подготовленных сотрудников организации составляется комиссия по расследованию инцидента ИБ. Сотрудник подразделения ИБ, входящий в состав комиссии и являющимся специалистом в расследовании инцидентов ИБ (далее – специалистом), должен произвести следующий порядок действий:

1. Снять дамп ОП с анализируемой ЭВМ. При этом возможны следующие случаи:
   А. В случае полного доступа к ОС (компьютер без пароля) специалист должен произвести:
   - подобр флеш-носителя, способного полностью вместить содержимое ОП и необходимое специальное ПО;
   - установку на данный флеш-носитель специального ПО Belkasoft Live RAM Capturer;
   - подключение флеш-носителя к анализируемой ЭВМ и запуск утилиты Belkasoft Live RAM Capturer непосредственно с флеш-носителя, результатом чего будет получение дампа ОП на флеш-носителе;
   - копировать полученный образ ОП на рабочее место специалиста.

   Б. При невозможности получения доступа к ОС исследуемой ЭВМ (компьютер закрыт паролем) также имеется несколько вариантов работы:
   - на исследуемом ЭВМ имеется порт FireWire:
     - подключить рабочее место специалиста к исследуемому компьютеру с использованием кабеля FireWire;
     - запустить на рабочем месте специалиста специальное ПО (Inception или pyfw), результатом чего будет получение дампа ОП на рабочем месте специалиста.
   - на анализируемом ЭВМ отсутствует порт FireWire:
     - подключить карту-адаптер с интерфейсом PCMCIA, CardBus или ExpressCard;
     - подключить рабочее место аналитика к исследуемому ЭВМ с помощью кабеля FireWire;
     - запустить на рабочем месте специалиста специальное ПО (Inception или pyfw), результатом чего будет получение дампа ОП на рабочем месте специалиста.
2. Минимизировать последствия инцидента информационной безопасности на ЭВМ. Необходимо выключить питание ЭВМ, не производить на нём никаких работ.
3. Проанализировать дамп ОП:
   - создать копию дампа оперативной памяти, тем самым обеспечив целостность доказательств произошедшего инцидента ИБ;
   - произвести анализ образа ОП с помощью разработанного специального ПО.
4. Оформить детальный отчет о результатах анализа дампа ОП с указанием:
   - выявленного инцидента информационной безопасности;
   - причины возникновения инцидента ИБ;
   - возможных виновных лиц;
   - причиненного ущерба от данного инцидента ИБ;
   - рекомендаций по устранению данного инцидента ИБ и его последствий;
   - рекомендаций по предотвращению подобных инцидентов в будущем.

Далее специалист должен доложить о результатах своего расследования членам назначенной комиссии, которая в свою очередь доводит служебное расследование до

конца с организационной точки зрения, оформляет заключение по результатам служебного расследования. Далее проводятся мероприятия по результатам служебного расследования, представленные этапами 8-11 на функциональной модели.

При получении дампа ОП необходимо брать во внимание определенные моменты. Большое количество программных продуктов функционируют в пользовательском режиме и для расследования абсолютно не подходят. Определенное ПО, например компьютерные игры, системы безопасности, а также вредоносные программы, скрывают свои процессы при помощи отладочных модулей. Они могут увидеть и пресечь попытку просмотреть информацию из защищенных областей ОП. При этом вместо искомой информации в защищенной области выводятся нули или некорректная информация. При плохом раскладе возникает некорректная работа ЭВМ, в следствии которого питание выключается. При этом анализ энергозависимой информации становиться недоступным. Для исключения данного случая необходимо пользоваться специальным ПО, например CaptureGUARD Gateway, WindowsSCOPE, цена которого очень велика. Возможно использовать Belkasoft Live RAM Capturer, который помимо бесплатного распространения имеет удобный графический интерфейс, прост в работе и является российской разработкой, а не иностранным аналогом. Обмануть активные виды защиты от отладки возможно с помощью средств, функционирующих в привилегированном режиме ядра ОС, каковым является Belkasoft Live RAM Capturer.

Также, необходимо учитывать, что любая утилита для сбора данных, запущенная на уровне пользователя или ядра операционной системы, естественным образом изменяет состояние исследуемой системы. Запуская любую утилиту в работающей системе, мы создаем минимум один процесс, который может быть записан в область, где до этого возможно хранились данные, имеющие значение для расследования. При создании нового процесса менеджер памяти операционной системы резервирует для этого процесса область памяти, при этом данные, которые находились в этот момент в свободной области памяти или в области подкачки файловой системы, могут быть в дальнейшем перезаписаны данными нового процесса. Поэтому нужно использовать программу с минимальным объемом занимаемой оперативной памяти.

Идеальным решением данных проблем представлялось бы наличие определенного устройства для компьютеров, построенных на платформе Intel, которое позволяло бы записать образ содержимого оперативной памяти на внешний носитель без использования функций операционной системы. Подобное решение существует для компьютерных систем на платформе Sparc, где копия содержимого всего ОЗУ может быть создана с помощью встроенного программного обеспечения OpenBoot. К сожалению, в настоящее время не существует подобных решений для ЭВМ, построенных на базе платформ Intel и AMD.

Исходя из всех достоинств и недостатков специального ПО для получения дампа ОП была выбрана Belkasoft Live RAM Capturer.

Полученный дамп ОП возможно изучить с помощью программных средств: Belkasoft Evidence Center (Россия), Elcomsoft Forensic Disk Decryptor (Россия), Passware Kit Forensic (Россия), Guidance EnCase (США), The Volatility Framework. Но, несмотря на множество существующих программ для анализа инцидентов информационной безопасности, они являются или платными, или функционирующими с ошибками, или рассматривающими узкое направление анализа, или в них отсутствует графический

интерфейс и их использование является неудобным. В связи с этим актуальным является написание программного средства для анализа образов ОП на предмет расследования инцидентов информационной безопасности. Наиболее подходящим для решения данной задачи является язык Python. В данный момент ведется разработка данного программного средства и уже получен ряд результатов. В качестве примера был проанализирован зараженный образ оперативной памяти Zeus. Было обнаружено, что с ЭВМ происходило постороннее TCP-соединение по адресу 193.104.41.75, которое было вызвано исполняемым файлом svchost.exe. На специализированных сайтах было установлено, что данный IP адрес находится в блэк листах и содержит ВПО типа троян.

После того, как специалист получил и сделал резервную копию дампа оперативной памяти анализируемой ЭВМ, он приступает к его анализу с помощью разработанного специального ПО. Задача специалиста произвести анализ данных, выдаваемых программным средством.

Работа специального ПО основывается на работе программы The Volatility Framework-2.4. Данная программа представляет собой большую и многофункциональную библиотеку для анализа ОП. Для удобного анализа образа ОП необходимо создать программное средство, предоставляющее весь алгоритм действий специалиста, от которого требуется только проанализировать выходную информацию и сделать вывод о случившемся инциденте ИБ. Данное программное средство будет функционировать в программной среде Jupyter Notebook которая поставляется в ПО Anaconda. Данная программная среда предназначена для функционирования программ, написанных на языке Python, в работе будет использоваться версия 2.7. Кроме того программная среда Jupyter Notebook обладает возможностью оформления удобного графического интерфейса, что делает использование специального ПО более удобным. Необходимо заметить, что для работы программной среды Jupyter Notebook необходим веб-браузер. В ходе опытного исследования, было установлено, что лучше всего для этой цели подходит веб-браузер Mozilla Firefox.

Таким образом, для функционирования специального ПО необходимо установить следующие компоненты:

- веб-браузер Mozilla Firefox;
- ПО Anaconda;
- модуль The Volatility Framework-2.4;
- модуль Pandas;
- модуль Graphviz;
- модуль Hierarchymagic.

Алгоритм расследования инцидентов ИБ на основе анализа образа ОП можно представить следующим образом:

1. Подключение необходимых для анализа дампа ОП библиотек;
2. Открытие исследуемого образа ОП;
3. Получение информации о типе ОС был установлен на анализируемой ЭВМ (в случае, если специалисты, снимающий дамп ОП с анализируемой ЭВМ, и специалист, анализирующий данный образ, разные люди);
4. Внесение типа ОС анализируемой ЭВМ в программу;
5. Просмотр запущенных процессов во время снятия дампа ОП;

6. Обнаружение скрытых процессов путем вывода сводной таблицы с указанием процессов и таблиц с указанием того, где процесс обнаруживается, а где нет;
7. Просмотр процессов, в том числе и скрытых с помощью руткит технологий. Получение информации о названии процесса, идентификаторе процесса, родительском идентификаторе процесса, количестве потоков процесса, количестве дескрипторов, идентификаторов сеанса, какое адресное пространство использовалось процессом (32- или 64-битное), даты и времени когда процесс начался и когда завершился;
8. Просмотр TCP соединений, которые были задействованы в момент получения дампа ОП с указанием адреса, с которого производилось подключение, адреса, к которому производилось подключение, идентификатора процесса, который инициировал данное подключение;
9. Просмотр TCP соединений, которые были активны и завершены к моменту снятия дампа оперативной памяти с указанием адреса, с которого производилось подключение, адреса, к которому производилось подключение, идентификатора процесса, который инициировал данное подключение;
10. Просмотра процесса и родительского идентификатора процесса по идентификатору самого процесса;
11. Просмотр всех процессов, которые были порождены процессом с указанным идентификатором с получением информации о названии процесса, идентификаторе процесса, родительском идентификаторе процесса, количестве потоков процесса, количестве дескрипторов, идентификаторов сеанса, какое адресное пространство использовалось процессом (32- или 64-битное), даты и времени когда процесс начался и когда завершился;
12. Графическое представление дерева процессов с указание идентификатора процесса, его названия, информации о его состоянии (запущен или в какое время завершился);
13. Проверка автозагрузки ОС;
14. Просмотр подозрительных перехватов в процессах, скрытых или инжектированных кодов в процессах, dll;
15. Просмотр мьютекстов.

Направлениями дальнейшего исследования является:

- доработка алгоритма расследования инцидентов ИБ на основе анализа образа оперативной памяти;
- доработка прототипа программного средства расследования инцидентов ИБ на основе анализа образа оперативной памяти;
- обоснование эффективности применения разработанного прототипа программного средства.

СПИСОК ЛИТЕРАТУРЫ

1. *ГОСТ Р ИСО/МЭК ТО 18044-2007* "Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности"
2. *Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters* "The Art of Memory Forensics"

А.Ю. Кудряшова , А.Н. Руднев

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ ХРАНИЛИЩ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: информационные технологии, сетевые хранилища, информационная безопасность, показатели надёжности информации, показатели качества информации, сетевая безопасность.

В статье исследован уровень безопасности сетевых хранилищ на примере конкретного хранилища, рассчитаны показатели надёжности и качества информации, разработана методика оценки информационной безопасности хранилищ данных.

A.Y. Kudriashova, A.N. Rudnev

RESEARCHING AND DEVELOPING OF METHOD FOR ASSESSING INFORMATION SECURITY NETWORK STORAGE

Moscow technical university of communications and informatics, Moscow, Russia

Keywords: information technology, network storage, information security, reliability of information, quality of information, network security.

This paper investigates the security of the network storage on the example of concrete vault, designed reliability and quality of information, developed a method for evaluation of information security for data warehouse.

Эффективное ведение бизнеса в наше время невозможно без применения технических решений и средств коммуникации. Каждая коммерческая организация прежде всего обеспечивает себя современным компьютерным и сетевым оборудованием. Но с течением времени появляется всё больше новых технологий и перспективных решений, что приводит к необходимости анализа существующего технического обеспечения и его совершенствования. Одним из перспективных является использование современных хранилищ данных

На сегодняшний день хранилища данных приобретают все большую популярность среди организаций в различных сферах деятельности. Они, безусловно, удобны для хранения и обработки большого количества информации. Но насколько безопасно загружать информацию в сетевые хранилища? Соответствует ли их уровень безопасности возможному классу конфиденциальности обрабатываемой информации?

Чтобы оценить запрашиваемый уровень безопасности хранилища, необходимо использовать какой-либо метод оценки. Для достоверности результата оценки он должен

включать в себя исследование всех технических аспектов сети и самого сетевого хранилища. Именно созданию подобного метода посвящена данная статья.

Для разработки метода оценки информационной безопасности сетевых хранилищ данных в целом, исследован уровень безопасности хранилища данных определенной организации. Причем, в данной статье предлагается рассмотреть понятие информационной безопасности как совокупность критериев сетевой безопасности. надежности сети и достоверности информации.

На основе полученных результатов исследования создан метод оценки информационной безопасности для всех сетевых хранилищ с возможностью предложения внесения определенных корректировок для достижения высокого уровня безопасности.

Для исследования было выбрано сетевое хранилище данных «Высшей школы бизнеса, инновационных технологий и интеллектуальных систем» («ВШ БИТИС МТУСИ»). В целях обеспечения выполнения своих основных функций в «ВШ БИТИС» было разработано и внедрено в 2011 году сетевое хранилище данных «Контингент». В качестве СУБД в ПК использовался Microsoft SQL Server. Система была разработана в идеологии файл-сервер.

Для того чтобы оптимизировать структуру сетевого хранилища с помощью внесения определённых корректировок, на первом этапе необходимо изучить саму структуру и рассчитать определённые показатели качества и надёжности.

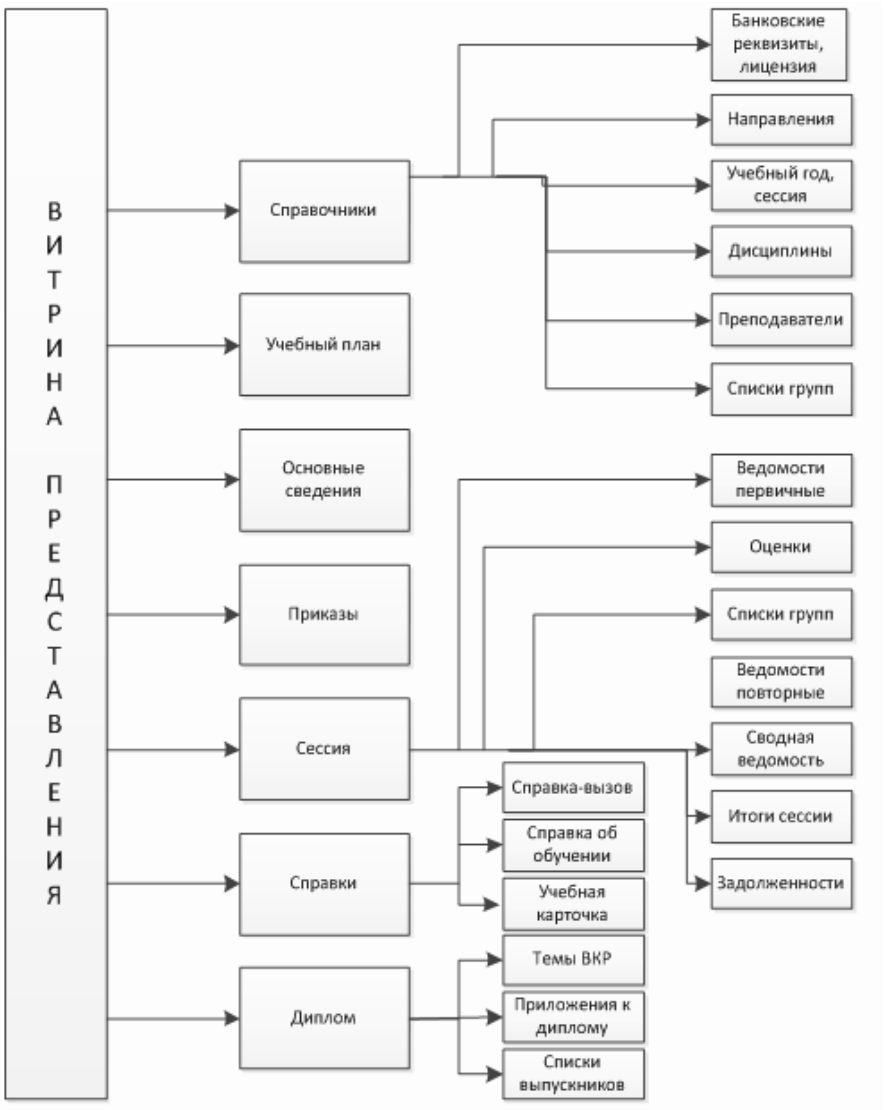


Рисунок 1 – Структура хранилища данных «Контингент»

Что касается архитектуры данного хранилища данных, то оно является централизованным хранилищем с зависимыми вторичными витринами, а значит его архитектура - «звезда». [1]

Вторичные витрины зависят в первую очередь от составляющей «Список студентов», на основе которой формируются многие отчёты и документы.

Уровень доступа к данным обеспечен Microsoft SQL Server 2010, уровень информационного доступа - с помощью интерфейса Microsoft Access 2010, а уровень администрирования обеспечивается входом в систему под аккаунтом администратора, для обычных пользователей функции администрирования недоступны.

Анализ данных по технологии OLAP также производится с использованием инструментария Microsoft SQL Server 2010, а представление результатов пользователю осуществляется через витрины хранилища данных. [2]

Необходимо также исследовать комплекс технических средств, кабельную и сетевую системы, программное обеспечение. Рассмотрим их. [3]

Занимаемая площадь организации «ВШ БИТИС» составляет 150 кв.м. Помещение разделено на 3 комнаты с общим коридором. Кабельная сеть проложена между фальш-потолком и плитой перекрытия между первым и вторым этажом.

При монтаже СКС использован кабель фирмы Rexant, стандарта UTP (неэкранированная витая пара) категории 5 для горизонтальной, административной подсистем и подсистемы рабочего места. Для организации «последней мили» использован одномодовый оптоволоконный кабель.

В организации «ВШ БИТИС» установлен маршрутизатор Cisco 2901,коммутатор CiscoSF200E-24. К коммутатору подключен сервер БД и рабочие станции. У коммутатора имеется станция управления. В помещении установлено 20 рабочих станций.

Корпоративная сеть предприятия представлена на рисунке 2.

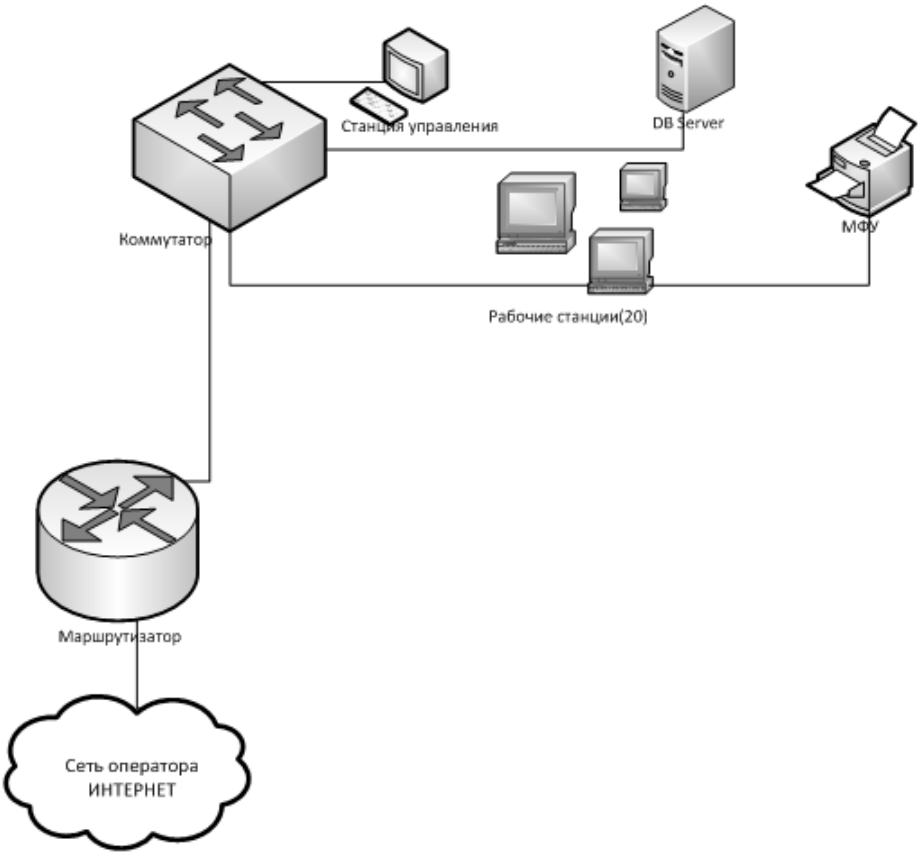


Рисунок 2- Сетевая система «ВШ БИТИС МТУСИ»

На сетевых устройствах установлено программное обеспечение, представленное в таблице 1.

Таблица 1 - Программное обеспечение сетевого оборудования

Устройство	**ПО**
DB-сервер	ОС:Ubuntu Server 14.4 LTS Инструменты: Oracle SQL Server 2012
WS (рабочие станции)	Windows 8.1 Enterprise
Терминал	Windows 8.1 Professional
Маршрутизатор	Cisco IOS 15.0(1)

Приведем результаты анализа:

1. При построении кабельной и сетевой систем соблюдены следующие стандарты:
   - EIA/TIA-569
   - ГОСТ Р 53246-2008
   - IEEE 802.1x
   - DoD standard 5200.28-STD "Orange Book"
2. Аппаратное обеспечение удовлетворяет требованиям производительности сети, его модернизация не требуется.
3. Программное обеспечение соответствует возможностям аппаратного обеспечения, в данное время установленные программные продукты актуальны, производитель ПО не прекращает их поддержку.

После исследования структуры заданного сетевого хранилища и комплекса технических средств необходимо рассчитать показатели качества и внести корректировки при необходимости.

В соответствие с техническими требованиями, предъявляемыми к безопасной работе системы организации, максимальное суммарное время простоев за 5 лет работы сети не должно превышать 5 часов, что соответствует значению коэффициента готовности 0,999.

На основании свойства простейшего потока отказов, предположим, что поток отказов Пуассоновский, а время восстановления элемента распределено по экспоненциальному закону. Были рассчитаны коэффициенты готовности для каждого элемента сети на основе заданных значений интенсивности отказов, представленных в таблице 2. [5]

Таблица 2 - Значения интенсивности отказов и восстановлений

	Элементы сети	**Интенсивность отказов (час$^{-1}$)**	**Интенсивность восстановления (час$^{-1}$)**
1	Рабочая станция	0,0008	1
2	Среда передачи	0,0001	1
3	Коммутатор	0,0003	1
4	Сервер	0,0006	1

Расчет коэффициентов готовности каждого элемента представлен в таблице 3.

Таблица 3 - Коэффициенты готовности элементов сети

Элементы сети	**Коэффициент готовности, Кг (5 лет)**
Рабочая станция	0,9992
Среда передачи	0,9999
Коммутатор	0,9997
Сервер	0,9994

Согласно структурной схеме надежности сети, представленной на рисунке 3, путем перемножения коэффициентов готовности каждого элемента сети, мы получили значение коэффициента готовности всей сети.

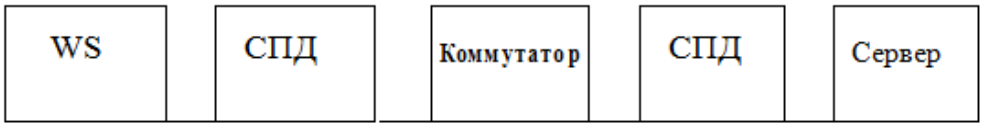


Рисунок 3 – Структурная схема надежности сети

Таким образом, были получено значение 0,997, что не соответствует требованию к максимальному суммарному времени простоев, описанному ранее.

Для повышения надежности введём резервные элементы в «ненагруженном» режиме, когда резервный элемент начинает работать только после отказа основного элемента. [6]

Зарезервируем с кратностью 1 каждый из рассматриваемых элементов сети и рассчитаем коэффициент готовности.

Расчёт коэффициента готовности каждого элемента сети после резервирования представлен в таблице 4.

Таблица 4 - Коэффициенты готовности элементов сети после резервирования

Элементы сети	**Коэффициент готовности, Кг (5 лет)**
Рабочая станция	0,99994572
Среда передачи	0,99995436
Коммутатор	0,99999876
Сервер	0,99998674

Коэффициент готовности за 5 лет для данной системы после резервирования составит 0,99988558.

Таким образом, полученный коэффициент готовности после резервирования удовлетворяет заданному условию для суммарного времени простоя системы, не превышающего 5 часов за 5 лет.

Теперь рассмотрим критерий достоверности и качества информации в хранилище данных.

Достоверность информации количественно оценивается вероятностью отсутствия ошибочных символов в объеме Q символов обрабатываемой информации. Визуальный самоконтроль оператора при работе с хранилищем относится к методам внутри операционного контроля. [7]

В соответствие с техническими требованиями, предъявляемыми к работе хранилища, достоверность информации должна быть > 0.999.

1) Модель достоверности для операции заведения карточки студента представлена на рисунке 4.

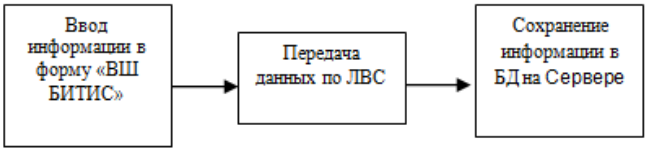


Рисунок 4 - Модель достоверности операции заведения карточки студента

2) Вероятность искажения единицы информации при ручном вводе с клавиатуры $1*10^{-3}$
3) Вероятность обнаружения ошибок при самоконтроле оператора по экрану 0.8
4) Интенсивность сбоев сервера 0.00008 [1/час]
5) Интенсивность сбоя 0.001 [1/час]
6) Объем вводимых символов Q представлен в таблице 4.

Таблица 4 - Объем вводимых данных для каждого поля.

Наименование поля	**Длина, байт**
ФИО студента	8
Год рождения	4
Специальность	4
Группа	4
Номер зачетной книжки	4
Паспортные данные	32
Адрес	32
Телефон	4
Оценки (по курсам, дисциплинам)	128
Доп. информация	64
Итого	284

Вероятность искажения единицы обрабатываемой информации при ручном вводе с клавиатуры - 0,001

Рассчитаем вероятность искажения информации после выполнения ручной операции ввода при условии независимой посимвольной. [7]

$q = 1 - (1 - q_1)^Q = 1 - (1 - 0{,}001)^{284} = 0{,}2$

Рассчитаем достоверность информации [7]:

$p = 1 - q = 1 - 0{,}2 = 0{,}8$

Теперь рассмотрим расчет достоверности машинных операций. Модели достоверности для операций передачи информации на сервер БД, представленной на рисунке 5.

Рисунок 5- Модель операций передачи информации на сервер БД

Рассчитаем вероятности отсутствия ошибки после операции в случае машинной обработки информации. Для этого сначала рассчитаем время обработки t передачи пакета длиной 284 байт=2272 бит по узлам сети с учетом следующих исходных данных [7]:

1. Пропускная способность сегмента 100Base-TX – 95 Мбит/с.
2. Пропускная способность коммутатора Cisco SF200E-24– 94,5 Мбит/с.
3. Среднее время доступа к жесткому диску сервера – 8,5мс.
4. Средняя скорость записи – 3 Гбит/с.

$$t_{среда\ передачи} = \frac{2272}{95*10^6} = 0{,}000023\,\text{с}$$

$$t_{switch} = \frac{2272}{94{,}5*10^6} = 0{,}000024\text{с}$$

$$t_{srv} = 0{,}0085 + \frac{2840}{3*10^9} = 0{,}00850095\text{с}$$

Интенсивности отказов элементов:

$\lambda_1 = \lambda_3 = 0{,}0001$ [1/час];

$\lambda_2 = 0{,}0003$[1/час];

$\lambda_3 = 0{,}0006$ [1/час].

Тогда вероятности отсутствия ошибки в каждом из блоков будут следующими:

$P1 = (e^{-10*0{,}0001*0{,}000023})^2 = 0{,}9999998$

$P2 = e^{-10*0{,}0003*0{,}000024} = 0{,}9999962$

$P3 = e^{-10*0{,}0006*0{,}00850095} = 0{,}9999491$

Теперь можно рассчитать полную вероятность отсутствия ошибки:

$P = \prod_3^1 p_i = 0{,}9999470$

Однако при расчёте показателя достоверности информации при ручном вводе было получено значение 0,8. Так как после вычислений, приведённых выше, достоверность информации не удовлетворила необходимому условию, введем схему контроля ошибок при ручном вводе, представленную на рисунке 6.

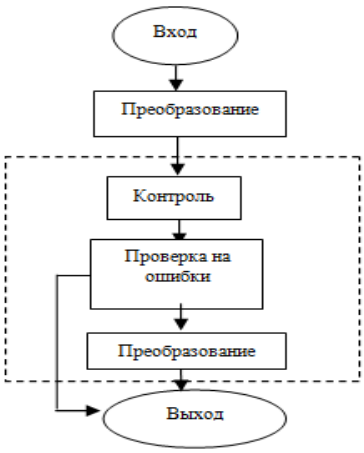


Рисунок 6 - Схема алгоритма однократной операции с внутриоперационным контролем и дополнительной корректирующей

Вероятность обнаружения ошибок при самоконтроле оператора по монитору– 0,8.

Вероятность внесения ошибки после выполнения корректирующей операции – 0,001.

Количество операций контроля -1

Рассчитаем вероятность отсутствия искаженного символа на выходе операции ручного ввода при единичном самоконтроле оператора по экрану видеотерминального устройства[7]:

$$P_1 = 1 - q_1(1 - k + kr)^N = 1 - 0{,}001(1 - 0{,}8 + 0{,}8 \cdot 0{,}001) = 0{,}9997992$$

Таким образом, для достижения значения достоверности 0,999 операции ввода данных с клавиатуры применим однократный контроль[8],[9].

Полученное значение достоверности информации при ручном вводе удовлетворяет заданному требованию значения достоверности 0,999, стоит отметить, что в случае достоверности для операций передачи информации на сервер БД (машинные операции) значение изначально удовлетворило требованию.

Проанализируем уровень сетевой безопасности. На рисунке 7 наглядно показаны установленные средства сетевой безопасности.

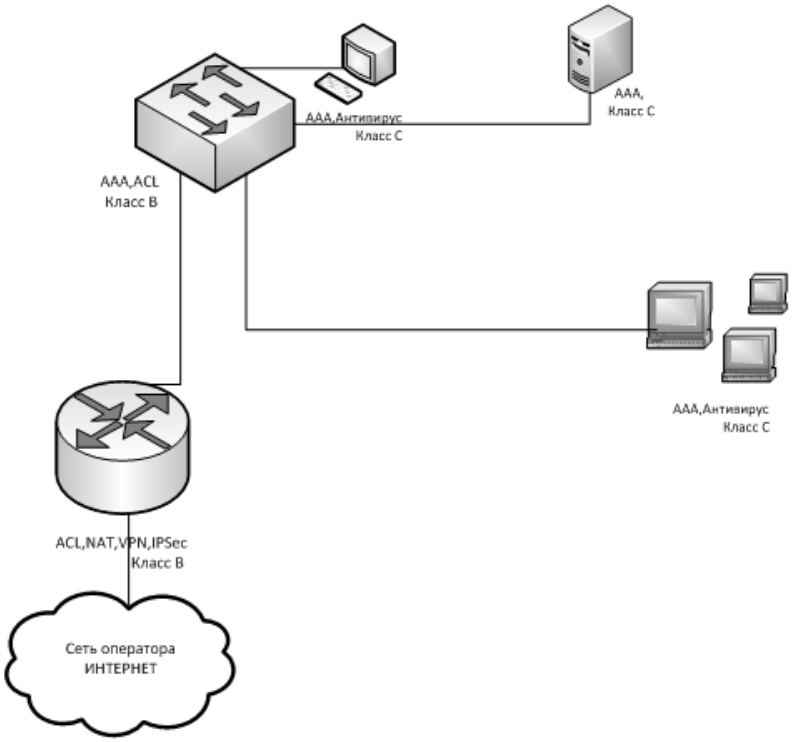


Рисунок 7 - Средства сетевой безопасности и классы безопасности в соответствие с DoD standard 5200.28

В связи с наличием конфиденциальной информации в хранилище были проанализированы средства сетевой безопасности, выявлены и исправлены недочёты системы:

1) На участке последний мили необходимо реализовать только трансляция сетевых адресов и межсетевой экран для повышения эффективной работы коммутатора.
2) Необходимо установить блокирование клавиатур на станциях управления и серверах.
3) Активное сетевое оборудование следует поместить в телекоммуникационный шкаф, доступ к нему ограничить с помощью замка и датчика определения вскрытия.
4) Безопасность доступа к настройкам сетевых устройств обеспечить ограничением доступа через управляющие программы эмуляции терминала SSH к управляющей консоли устройства.
5) Предусмотреть журналы контроля доступа.
6) Необходимо предусмотреть автономную систему контроля управления доступом (включающую персональные идентификаторы).[10],[11]

Таким образом, в предлагаемой методике оценки информационной безопасности сетевых хранилищ данных предлагается оценивать уровень безопасности по следующим критериям:

1) Оптимальности структуры хранилища данных
2) Надёжность комплекса технических средств
3) Достоверности информации в хранилище при ручном и машинном вводе данных
4) Наличия средств и мер сетевой безопасности, их соответствия уровню конфиденциальности хранимой информации.

Пользуясь результатами исследования возможно сформулировать требования к структуре хранилища, организации инфокоммуникационного обмена, требования к составу оборудования и программных средств.

В продолжение разработки методики планируется исследование других показателей качества системы с возможностью их корректировки при несоответствии заявленным требованиям, например, анализ сетевого трафика на наличие аномалий и рекомендации по его фильтрации.[12]

СПИСОК ЛИТЕРАТУРЫ

1. *Маклаков С.В.* Проектирование реляционных хранилищ данных / Маклаков С. В. – М., Диалог-МИФИ, 2006. - 456 с.
2. *Архипенков С.Д.* Хранилища данных. От концепции до внедрения/ Архипенков С.Д., Голубев Д.В. – М.:Диалог-МИФИ, 2002. -528 с.
3. *Коломоец Г.П.* Организация компьютерных сетей / Г.П. Коломец - М.: Наука, 2003. - 712с.
4. *Биячуев Т.Я.* Безопасность корпоративных сетей / Т.Я. Биячуев - М.: Академия, 2009. - 512 с
5. *Воронцов Ю.А.* Технико-экономическое обоснование эффективности проектов информационных систем. Учебное пособие / Ю. А. Воронцов. - М.: МТУСИ, 2011. - 50 с.
6. *Стрелец И.А.* Сетевая экономика / И. А. Стрелец - СПб.: Научная мысль, 2007. - 320 с.
7. *Менаске Д.А* .Производительность Web-служб. Анализ, оценка и планирование: [пер. с англ.] / Д. А. Менаске, В. А. Ф. Алмейда СПб.: ДиаСофтЮП, 2003. - 480 с
8. *Беленькая М.Н.* Администрирование в информационных системах / М. Н. Беленькая, С. Т. Малиновский, Н.В. Яковенко - М.: Горячая линия-Телеком, 2011. - 400 с.
9. *Кукушкин С.С.* Теория конечных полей и информатика: т.1 Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках, М.: МО РФ, 2003. 284с.
10. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.:КУДИЦ-ОБРАЗ, 2001 368 с.
11. *Руднев А.Н., Васьковский А.С.* Скрытие видеоинформации некриптографическими методами при потоковой передаче. Нелинейный мир, 2012, №8.
12. *Руднев А.Н. Шелухин О.И.* Потоковое видео в системах радиодоступа монография . «Горячая линия -Телеком» 2013 г.ISBN 978-5-9912-0303-6 308с.

С.И. Кузнецов, С.П. Тесля, Е.В. Сухорукова, А.В. Вершенник

ВАРИАНТ ИЗМЕНЕНИЯ ЛОГИЧЕСКОЙ СТРУКТУРЫ АДРЕСНОГО ПРОСТРАНСТВА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЕЙ

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия

Ключевые слова: информационная безопасность, защита, информационно-телекоммуникационная сеть, логическая структура адресного пространства.

В статье предлагается способ повышения защищенности элементов распределенных ИТКС за счет усложнения процедуры определения адресов и выявления взаимосвязей удаленных сегментов ИТКС при анализе трафика в некоторой точке сети связи общего пользования.

S.I. Kuznetsov, S. P. Tesla, E.V. Sukhorukova, A.V. Vershennik

THE OPTION OF CHANGING THE LOGICAL STRUCTURE OF THE ADDRESS SPACE INFORMATION AND COMMUNICATION NETWORKS

Military Academy of telecommunications named. Marshal Of The Soviet Union S. M. Budyonny, Saint-Petersburg, Russia

Key words: information security, protection, information and telecommunication network, the logical structure of the address space.

The article proposes the way to improve the security elements of the distributed information and telecommunication systems due to the complexity of the procedure of determining the addresses and correlate remote segments of ITKs when analyzing the traffic at some point of the communication network of General use.

Обеспечение безопасности информационно-телекоммуникационных сетей (ИТКС) предполагает их защиту со стороны внешних угроз, направленных на нарушение нормального функционирования.

Одними из наиболее опасных и самых распространенных внешних угроз являются сканирование сети и отказ в обслуживании, в частности DDos атаки. Реализация этих угроз прямо или косвенно приводит к нарушению безопасности информации, а также вскрытию структуры (топологии) сети (логической структуры адресного пространства ИТКС).

Полностью защититься от DDoS-атак на сегодняшний день невозможно. В настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния [1, 2, 3, 4]. Среди многообразия способов защиты выделяют: защиту от преднамеренных деструктивных воздействий; управление

демаскирующими признаками ИТКС; разработку базовых защищенных информационных технологий и т.д.

Необходимо отметить, что любой атаке предшествует стадия предварительного информирования (рекогносцировки), которая направлена на сбор информации, необходимой для выбора методов и средств дальнейшей реализации атаки. Для этого нарушитель может использовать специальные программные средства, при помощи которых можно определить существующие информационные потоки, схему адресации узлов, типы используемых сетевых сервисов и др.

Так, возможность определения открытых адресов отправителя и получателя, дает возможность вскрытия логической структуры адресного пространства ИТКС. Множество оборудования отображает типы физического оборудования, которым представлены узлы ИТКС (ПЭВМ, межсетевой экран, маршрутизатор, коммутатор и т. п.), марки его производителя и версии оборудования, которое будет являться демаскирующими признаками оборудования элемента ИТКС. Для формирования такого множества нарушитель будет проводить активное сканирование идентифицированных узлов и анализ их трафика (адреса отправителей в IP-заголовках позволяют определить является ли узел конечным или промежуточным, а другие поля заголовков – службы, порты и программное обеспечение). Кроме того, информация о структуре ИТКС может быть получена путем получения доступа (несанкционированного доступа к телекоммуникационному оборудованию или перехвата идентификационных признаков) к таблицам маршрутизации и путем ведения активной сетевой разведки. Активная разведка может вестись при помощи дополнительных возможностей утилиты ping (например, путем задания специальных параметров ping позволяет просмотреть маршрут – список узлов, по которому проходил пакет с запросом до указанного узла), при помощи специализированных утилит, а также при помощи других методов разведки (например, поиск информации о структуре в информационных ресурсах сети связи общего пользования).

Прямым демаскирующим признаком является идентификатор узла, по которому возможно определить его местоположение. При помощи сетевого сервиса whois по идентификатору узла можно получить информацию об адресе его расположения (почтовый адрес организации, где расположен узел) и другую информацию

Таким образом, возникает противоречие между необходимостью открытой передачи адресов пакетов сообщений по каналам связи с требованиями по обеспечению безопасности, т.к. выявление корреспондирующих субъектов и каналов связи создает предпосылки для осуществления деструктивных воздействий на элементы распределенной ИТКС.

В связи с этим, актуальной является задача разработки способов, расширяющих арсенал средств и способов и устройств защиты информации в компьютерных системах и сетях на этапе предварительного информирования (рекогносцировки).

Для решения данной задачи авторами статьи предлагается вариант изменения логической структуры адресного пространства информационно-коммуникационных сетей, который позволит сформировать у нарушителя устойчивых ложных стереотипов относительно структуры ИТКС и алгоритмов ее функционирования и т.д.

Целью предлагаемого варианта является повышение безопасности элементов распределенных ИТКС за счет усложнения процедуры определения адресов и выявления

взаимосвязей удаленных сегментов ИТКС при анализе трафика в некоторой точке сети связи общего пользования.

Вариант изменения логической структуры адресного пространства реализуется следующим образом.

Для передачи информации между удаленными сегментами распределенной ИТКС (например, ЛВС1 и ЛВС2) посредством протоколов взаимодействия устанавливают канал связи, под которым, в данном случае, понимают информационный поток от отправителя к получателю.

Информационный поток от ЛВС1 к ЛВС2 передают через соответствующие маршрутизаторы и сеть связи общего пользования. В общем случае эту модель можно упростить и представить в виде оконечного коммуникационного оборудования корреспондентов (отправителя и получателя пакетов сообщений), а также канала связи между ними.

В процессе установления соединения отправителю и получателю необходимо произвести согласование сетевых адресов. Для этого у всех корреспондентов предварительно задают базу, включающую *IP*-адреса первого сетевого адаптера $A1_{ск}$ и индивидуальные ключи Хэш-функции ПК взаимодействия, за них принимают все элементы, не своей ЛВС.

Пример базы адресов и ключей Хэш-функций, представленной в виде таблицы, показан на рисунке 1.

Первый столбец в таблице означает порядковый номер адреса отправителя, получателя или транзита в базе адресов. Во втором и четвертом столбцах представлены соответствующие значения адресов отправителя и получателя.

Усл №	Адреса взаимодействующих ПК $A_{ск1}$	Дополнит информ.	Адреса взаимодействующих ПК $A_{2ск}$	Дополнит информ.	Ключ хэш-функции ПК F(x)
1	2	3	4	5	6
1	196.128.12.1	$A_{отпр}$	196.128.78.1	$A_{обр.отпр}$	011011001010
2	196.128.15.1	$A_{тр3}$	196.129.13.18	$A_{обр.тр3}$	110110111011
3	196.132.14.3	$A_{тр2}$	196.132.19.16	$A_{обр.тр2}$	001011010101
4	196.148.15.7	$A_{тр1}$	196.148.17.2	$A_{обр.тр1}$	011100100011
5	196.133.12.18		196.133.14.7		100111000011
6	196.134.77.6	$A_{получ}$	196.134.52.24	$A_{обр.получ}$	111001011111

Рис. 1 – Пример базы адресов и Хэш–функций отправителя и получателя

IP-адрес, имеющий длину 4 байта (32 бита), отображают в таблице в наиболее употребляемом виде представления IP адреса – в десятичной форме. В третьем и пятом столбцах размещают дополнительную информацию об адресах. Например, в них указывают обозначение текущих адресов отправителя $A_{отпр}$ и получателя $A_{получ}$, а также обратных адресов отправителя $A_{обр.отпр}$ и получателя $A_{обр.получ}$, и элементов транзита $A_{трN}$и $A_{обр.трN}$. В шестом столбце записана назначенного для каждого ПК взаимодействия (под элементами взаимодействия понимаются элементы отправителя, получателя или транзита) Хэш-функция, применяемая для идентификации абонента.

Пример базы контрольного времени, представленной в виде таблицы, показан на рисунке 2 и 3. Первый столбец в таблице означает порядковый номер адреса отправителя, получателя или транзита в базе адресов. В третьем и пятом столбцах рисунка 2 представлены соответствующие значения времени отправления пакета и времени получения отчета.

Усл №	Дополнит информ.	Время отправления $t_{отпр}$	Дополнит информ.	Время получения уведомления $t_{отчета}$	Дополнит информ.	Контрольное время $t_{отчета}$
1	2	3	4	5	6	7
1	$A_{отпр}$					
2		10:23:18:42		10:23:18:82		40 мс
3		10:23:18:50		10:23:19:03		53 мс
4		10:23:18:58		10:23:18:95		37 мс
5		10:23:18:64		10:23:19:12		48 мс
6	$A_{получ}$					

Рис. 2 – Пример базы расчета контрольного времени до взаимодействующего элемента в оперативно-запоминающем устройстве

Усл №	Дополнит информ.	Контрольное время $t_{отчета}$	Дополнит информ.	Контрольное время $t_{Контр}$ до получателя	Дополнит информ.	Контрольное время $t_{контр.ср\ до}$ получателя
1	2	3	4	5	6	7
1	$A_{отпр}$					
2		40 мс		53 мс	$A_{тр3}$	93 мс
3		53 мс		33 мс	$A_{тр2}$	86 мс
4		37 мс		41 мс	$A_{тр1}$	78 мс
5		48 мс		65 мс		113 мс
6	$A_{получ}$					

Рис. 3 – Пример базы расчета пунктов транзита информации в оперативно-запоминающем устройстве

Значение времени, имеющее длину 4 байта (32 бита), отображают в таблице в наиболее употребляемом виде представления времени – ЧЧ:ММ:СС:МсМс. В третьем и пятом столбцах рисунка 3 представлены соответствующие значения контрольного времени отчета, и контрольного времени до получателя от ПК транзита. Значение времени, имеющее длину 1 байта (8 бит), отображают в таблице в виде представления времени в миллисекундах. В седьмом столбце представлено значение суммы времени пятого и третьего столбцов, в миллисекундах, имеющее длину 1 байт (8 бит). Во втором и четвертом и шестом столбцах размещают дополнительную информацию об адресах. Например, в них указывают соответствие адресу отправителя $A_{отпр}$, получателя $A_{получ}$, или элементу транзита $A_{трN}$.

Пример базы пакетов сессии, представлен в виде таблицы на рисунке 4.

Первый столбец в таблице означает порядковый номер адреса отправителя, получателя или транзита в базе адресов. В третьем столбце представлено значение отношения времени от отправителя до получателя через элемент транзита, по отношению к сумме общего времени до получателя через все пункты транзита, определяемое по формуле, представленной ранее.

Усл №	Дополнит информ.	Контрольное время $t_{ср.контрN.квант}$	Количество пакетов ΔS_N	Дополнит информ.
1	2	3	4	5
1	$A_{отпр}$	$t_{ср.контр.общ}$ = 297 мс	$\Delta K = 3$; $\Delta S = 2000$	
2	$A_{тр3}$	$t_{ср.контр3.Квант} = 3$	$\Delta S_1 = 666$	
3	$A_{тр2}$	$t_{ср.контр2.Квант} = 3$	$\Delta S_2 = 1222$	
4	$A_{тр1}$	$t_{ср.контр1.Квант} = 3$	$\Delta S_3 = 1998$	
5				
6	$A_{получ}$			

Рис. 4 – Пример базы расчета количества пакетов через транзитные

Значение времени, имеющее длину 1 байт (8 бита), отображают в таблице виде времени в миллисекундах. В четвертом столбце представлено значение расчетного количества пакетов сессии, через каждый транзитный пункт. Значение имеет длину 4 байта (32 бита) и отображается в таблице в десятичном виде. Во втором и пятом столбцах размещают дополнительную информацию об адресах. Например, в них указывают соответствие адресов отправителю $A_{отпр}$, получателя $A_{получ}$, или ПК транзита $A_{трN}$.

Все составляющие пакетов сообщений представляют собой электромагнитные сигналы в цифровой (двоичной) форме. Рассматриваемые ниже действия над ними заключаются в соответствующих преобразованиях сигналов, при которых изменяются их параметры (общее число бит и последовательность их нулевых и единичных значений).

На начальном этапе подключают два сетевых адаптера к сети связи общего пользования с динамической адресацией в выделенном диапазоне IP-адресов для организации связи, через различные точки доступа (под которыми подразумеваются точки доступа различных провайдеров услуг связи сети общего пользования). Формируют в постоянно запоминающих устройства базу данных, включающую адреса всех элементов взаимодействия и их индивидуальные ключи (инициализирующие векторы) Хэш-функции. При установке и настройке устройства системные администраторы могут задавать адреса, согласовав свои действия по засекреченным каналам телефонной или документальной связи. В базе данных обозначают текущий адрес отправителя $A_{отпр}$ и обратный отправителя $A_{обр.отпр}$ сообщений (адреса первой $A_{1ск}$ и второй $A_{2ск}$ сетевого адаптера соответственно) . Затем записывают данные в постоянно-запоминающем устройстве. Аналогичные действия производятся на всех элементах взаимодействия.

Первоначально необходимо произвести согласование адресов всех рабочих станций между собой, для этого у отправителя формируют пакет согласования. Затем формируют промежуточный пакет, для чего в зарезервированное поле пакета согласования включают

обратный адрес отправителя $А_{обр.отпр}$, составляющий 32 бита информации, предварительно зафиксированный в таблице. В информационной части пакета указывается принадлежность этого пакета к пакетам согласования.

После чего кодируют любым из известных способов кодирования полученный промежуточный пакет и рассчитывают значение Хэш-функции от исходного пакета, затем включают рассчитанное значение Хэш-функции от пакета согласования, в отведенные для этого 32 бита информации в окончании информационной части пакета. Затем преобразуют его в формат TCP/IP. Преобразование заключается в добавлении IP-заголовка и TCP-заголовка к кодированному пакету данных. Полученный в результате пакет является пакетом согласования. Далее делают запрос на прокси-сервер. В результате чего получают цепочку свободных IP-адресов, состоящую из определенного количества взаимодействующих прокси серверов (например – три). Исходный пакет полностью инкапсулируется в новый (внешний) IP-пакет и для продвижения пакета по сети используется заголовок нового IP-пакета. Для полученных адресов происходит тройное инкапсулированние, то есть сначала инкапсулируется пакет для третьего сервера, затем для второго и только потом для первого. В поля адреса отправителя включают адрес третьего сервера, в поля адреса получателя включают поочередно все известные адреса элементов взаимодействия, кодируют пакет и добавляют заголовок внешнего IP-пакета. В поля адреса отправителя включают адрес второго сервера, в поля адреса получателя прописывается адрес третьего сервера. Полученный пакет кодируют, путем добавления ключей и служебной информации. Добавляют заголовок внешнего IP-пакета и т.д. В поля адреса отправителя включают адрес первого сервера, в поля адрес получателя включают адрес второго сервера. Снова кодируют полученный пакет путем добавления ключа и служебной информации. Добавляют заголовок внешнего IP-пакета. В поля адрес отправителя включают адрес отправителя $А_{отпр}$, в поля адрес получателя включают адрес первого сервера. Кодируют пакет, путем добавления ключа и служебной информации. Закодированный пакет передают первому серверу и т.д.

Во время создания пакета сервер устанавливает свой IP-адрес. Передают сформированные информационные пакеты сообщений всем ПК взаимодействия, записывают время отправления каждого пакета $t_{отпр}$ в базе данных оперативно-запоминающего устройства.

После приема у получателя пакета согласования из его заголовка выделяют адреса отправителя $А_{отпр}$, выделяют из постоянно-запоминающего устройства ключ Хэш-функции, соответствующую данному адресу и находят ее значение от информационной части пакета, предварительно выделив из него 32 бита информации из конца информационной части пакета, включающих данное значение Хэш-функции, рассчитанной у отправителя пакета и сравнивают их (например, побитно) со значением Хэш-функции, рассчитанной от пакета согласования. При несовпадении значений Хэш-функции принятый пакет не анализируют, т.к. его отправитель не является санкционированным участником информационного обмена. При совпадении значений из принятого пакета сообщений выделяют кодированные данные путем отделения IP-заголовка и декодируют их, из первых 32 бит информации пакета согласования выделяют значение обратного IP-адреса отправителя, и записывают его в постоянно-запоминающее устройство.

Для подтверждения факта получения от отправителя пакета у получателя формируют уведомляющий пакет сообщений. Для чего аналогично, как и у отправителя формируют уведомляющий информационный пакет (отчет о доставке), представляющий собой уведомление о получении пакета согласования. Затем к пакету добавляют обратный адрес ПК взаимодействия $A_{2ск}$ ($A_{обр.трN}$ или $A_{получ.обр}$), составляющий 32 бита информации, предварительно зафиксированный в таблице получают промежуточный пакет данных.

Далее кодируют промежуточный пакет данных и рассчитывают значение Хэш-функции от исходного пакета, затем включают рассчитанное значение Хэш-функции для пакета, в отведенные для этого 32 бита информации в окончание информационной части пакета и преобразуют его в формат TCP/IP и т.д.

После приема у отправителя уведомляющего пакета согласования из его заголовка выделяют адрес отправителя (ПК взаимодействияА1ск ($A_{трN}$ или $A_{получ}$), выделяют из постоянно-запоминающего устройства ключ Хэш-функции, соответствующую данному адресу и находят ее значение от информационной части пакета, предварительно выделив из него 32 бита информации из конца информационной части пакета, включающих данное значение Хэш-функции, рассчитанной у элемента взаимодействия и сравнивают их (например, побитно) со значением Хэш-функции от уведомляющего пакета. При несовпадении значений Хэш-функции принятый пакет не анализируют, т.к. не принадлежит к числу санкционированных участников информационного обмена. При совпадении значений пакет принимают к обработке, записывают время отправления каждого пакета $t_{отчета}$ в базе данных оперативно-запоминающего устройства. Из принятого пакета сообщений выделяют кодированные данные путем отделения IP-заголовка и декодируют их. Из первых 32ух бит информации уведомляющего пакета выделяют значение обратного IP-адреса элемента взаимодействия А2ск ($A_{обр.трN}$ или $A_{обр.получ}$), и записывают его в постоянно-запоминающее устройство.

Для смены IP-адреса рабочей станции отключают сетевой адаптер от точки доступа к сети связи общего доступа. Изменяют MAC-адрес (адрес физического уровня) сетевого адаптера (или иного физического устройства, осуществляющего подключение к сети). Вновь подключают его к сети связи общего пользования с динамической адресацией. За счет того, что время жизни прежней связки адресов MAC-IP на сервере провайдера (поставщика услуг) не истекло и считается активным, получаем новый IP-адрес рабочей станции, отличный от предыдущего. Записывают в базу данных постоянно-запоминающего устройства значение нового IP-адреса, с пометкой $A_{обр.тр}$, а значение второго IP-адреса с пометкой $A_{тр}$ и т.д.

Затем осуществляется обмен информацией по существующим виртуальным каналам. Для контроля и распределения пакетов по виртуальным каналам на стороне отправителя применяется набор условий, определяющий порядок передачи пакетов, а именно выбор адреса транзита и количество пакетов сессии, через каждый адрес транзита, с этой целью считается количество отправленных пакетов, проверяется соответствие количества пакетов данной сессии выбранному адресу транзита, при превышение ими предельного, рассчитанного числа $\Delta S_{N,}$ изменяют условный номер выбранного виртуального канала N следующее значение, в соответствие с которым и выбирают значение текущего адреса получателя $A_{обр.трN}$. при полной передаче пакетов данной сессии и не прихода отчетов о доставке происходит отсчет контрольного времени и сравнение его с предельным временем ожидания, по истечению которого и не выполнению предыдущего условия

происходит переход на этап определения виртуальных каналов а при выполнении данного условия происходит передача следующей сессии информационных пакетов. При невыполнении ряда условий сформированный информационный пакет преобразуют в формат TCP/IP, при формировании IP-заголовка, поле идентификатора размером 2 байта обозначает условный номер пакета и формируется в зависимости от возрастания номера пакета в сессии. Далее делают запрос на прокси-сервер. В результате чего получают цепочку свободных IP-адресов, состоящую из трех серверов. Исходный пакет полностью инкапсулируется в новый (внешний) IP-пакет и для продвижения пакета по сети используется заголовок нового IP-пакета и т.д.

После приема у отправителя уведомляющего пакета из его постоянно-запоминающего устройства выделяют адреса ПК взаимодействия $A_{трN}$, выделяют ключ Хэш-функции, соответствующий данным адресам и находят ее значение от информационной части пакета, предварительно выделив из него 32 бита информации из конца информационной части пакета, включающих данное значение Хэш-функции, рассчитанной на ПК взаимодействия и сравнивают их (например, побитно) со значением Хэш-функции с ключом, выделенным из постоянно-запоминающего устройства, от информационного пакета. При несовпадении значений Хэш-функции принятый пакет не анализируют, т.к. отправитель не принадлежит к числу санкционированных участников информационного обмена. При совпадении пакет принимают к обработке из принятого пакета сообщений выделяют кодированные данные путем отделения IP-заголовка и декодируют их. Из первых 64-х бит информации уведомляющего пакета выделяют значение обратного IP-адреса транзита $A_{обр.трN}$ и отправителя $A_{обр.получ}$ и записывают их в постоянно-запоминающее устройство. Увеличивают количество принятых отчетов о доставке пакета ΔD на $\Delta D=\Delta D+1$. Изменяют IP-адрес рабочей станции элемента отправителя, для чего отключают сетевой адаптер от точки доступа к сети связи общего доступа. Изменяют MAC-адрес (адрес физического уровня) сетевого адаптера (или иного физического устройства, осуществляющего подключение к сети). Вновь подключают его к сети связи общего пользования с динамической адресацией. Записывают в базу данных постоянно-запоминающего устройства значение нового IP-адреса, с пометкой $A_{обр.тр}$, а значение второго IP-адреса обозначают пометкой $A_{тр}$. Затем формируют новый информационный пакет.

Предложенный вариант изменения логической структуры адресного пространства заключается в расширении адресного пространства элементов сети, тройной инкапсуляции пакетов, организации маскирующего обмена между ложными и реальными сетевыми устройствами элементов сети, а также введении действий по восстановлению связи в маскированной структуре, обеспечивает повышение скрытности за счет маскирования логической структуры адресного пространства, маршрутов передачи сообщений, адресов отправителя и получателя и снижения сложности обеспечения доступности сетевых устройств, в условиях воздействия, путем ведения действий по восстановлению связи в случае нарушения синхронизации выбора адресов при приеме и передаче пакетов сообщений.

СПИСОК ЛИТЕРАТУРЫ

1. *Сухорукова Е.В., Корсунский А.С., Стародубцев Ю.И., Чукариков А.Г.* Принципы безопасного использования инфраструктуры связи применительно к условиям

техносферной войны. Сборник научных трудов (часть вторая) научно-технической конференции «Интегрированные системы управления». 2016 г. - с. 199 – 207.
2. *Стародубцев Ю.И., Евграфов А.А., Сухорукова Е.В.* Проблема формирования системы показателей для оценки защищенности информационно-телекоммуникационных сетей. / Проблемы экономики и управления в торговле и промышленности. 2014. № 3. С. 80-86.
3. *Стародубцев Ю.И., Сухорукова Е.В., Чукариков А.Г.* Методика выявления критически важных элементов информационно-телекоммуникационных систем. / Проблемы экономики и управления в торговле и промышленности. 2014. № 1. С. 95-101.
4. *Стародубцев П.Ю., Сухорукова Е.В., Закалкин П.В.* Способ управления потоками данных распределенных информационных систем. // Проблемы экономики и управления в торговле и промышленности. 2015. № 3 (11). С. 73-78.
5. *Стародубцев Ю.И., Сухорукова Е.В., Яблоков Д.Ю.* Способ повышения защищенности элементов территориально распределенных информационно-телекоммуникационных систем. // Проблемы экономики и управления в торговле и промышленности. 2015. № 1 (9). С. 95-100.
6. *Панкова Н.В., Стародубцев Г.Ю., Алисевич Е.А., Сухорукова Е.В.* Уменьшение операционных рисков при использовании инфокоммуникационных систем. // Проблемы экономики и управления в торговле и промышленности. 2013. № 2. С. 82-88.
7. *Закалкин П.В., Стародубцев П.Ю., Сухорукова Е.В.* Способ управления потоками данных на основе контроля заданного потребителем маршрута и обнаружения факта деструктивного воздействия. // Проблемы экономики и управления в торговле и промышленности. 2015. № 2 (10). С. 84-89.
8. Компьютерные сети. Принципы, технологии, протоколы. Олифер В.Г. и Олифер Н.А. .Уч. для Вузов, 2-изд.;-СПб.: Питер, 2003г. с. 497.
9. Контроль безопасности информации в информационно-вычислительных сетях. Учеб. пособие / В. С. Киреев, О. К. Савицкий, Ю. И. Стародубцев, М. М. Тараскин; Под ред. Е. А. Карпова. – СПб.: ВУС, 2002г.

А.А. Полков, А.С. Совенко

НЕКОТОРЫЕ АСПЕКТЫ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Академия Федеральной службы охраны Российской Федерации, Орел, Россия

Ключевые слова: электронная цифровая подпись, эллиптическая кривая, криптостойкость, большие числа.

В тезисах рассмотрены практические приемы используемые при реализации электронной цифровой подписи.

A.A. Polkov, A.S. Sovenko

SOME ASPECTS OF PRACTICAL REALIZATION OF DIGITAL SIGNATURE.

Academy of Federal Guarding Service of Russian Federation, Orel, Russia

Key words: digital signature, elliptic curve, cryptographic security, large numbers.

The article considers practical ways, which are used in realization of digital signature.

При реализации средств электронной цифровой подписи, согласно требованиям руководящих документов, возникают трудности. Решению некоторых из них посвящены данные тезисы.

Цель работы – рассмотрение особенностей реализации цифровой подписи.

Основными задачами являются:

1. Представить методы нахождения количества точек эллиптической кривой.
2. Рассмотреть способы представления длинных чисел.

Электронная цифровая подпись – реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи, позволяющий определить владельца сертификата ключа подписи и отсутствие искажений информации в электронном документе. Алгоритмы формирования и проверки электронной цифровой подписи, реализуемой с использованием операций в группе точек эллиптической кривой, описаны в российском стандарте ГОСТ Р 34.10–2012 [1].

Тезисы посвящены рассмотрению некоторых алгоритмических решений реализации этапов генерации электронной цифровой подписи. Первым этапом в процессе формирования является выбор эллиптической кривой. Основной особенностью подобных кривых является конечность числа точек. Порядком кривой называется общее число точек, которые ей принадлежат. Криптостойкость всей системы зависит от этого параметра. Процедура выбора кривой состоит из нижеперечисленных этапов:

1. Определение параметров a и b, задающих уравнение эллиптической кривой.
2. Определение порядка эллиптической кривой.
3. Проверка выполнения ряда условий, которым должна удовлетворять рассматриваемая кривая.

На практике для подсчета количества точек чаще всего используется алгоритм Шуфа. Вычислительная сложность данного алгоритма составляет $O(\log^6 q)$. Он трудно реализуем ввиду использования ресурсоемких математических преобразований. Для решения обратной задачи, нахождения кривых с определенным числом точек может использоваться метод комплексного умножения. Для работы данного метода необходимо выполнение ряда условий.

Для описания эллиптической кривой используется следующий набор параметров:

1. Модуль эллиптической кривой $p>3$ – простое число;
2. Коэффициенты a и b;
3. Целое число m – порядок группы точек эллиптической кривой;

4. Простое число q – порядок циклической подгруппы группы точек эллиптической кривой.

Одним из способов представления числа p является запись суммой степеней цифры 2. Например:

$$p = 6277101735386680763835789423207666416083908700390324961279,$$

тогда $p=2^{187}-2^{53}-1$. Описание чисел в данной форме позволяет увеличить скорость выполнения процедур умножения по модулю большого числа. Для получения результата произведения используется объединение машинных слов, полученных в результате умножения.

В данной работе число разрядность которого превышает разрядность процессора называется большим. Например, 64-х разрядный процессор производит обработку целых чисел от 0 до $2^{64}-1$. Но рассматриваемая криптографическая система предполагает обработку чисел порядка 2^{512}. Так как 512-ти разрядных процессоров на данный момент не существует, обработка подобных чисел требует применения специальных способов их представления. Любое число можно представить следующим образом:

$$C = c_{k-1}\beta^{k-1} + c_{k-2}\beta^{k-2} + \ldots + c_1\beta + c_0,$$

где β – основание системы счисления, в которой представляется число, коэффициент c_i должен удовлетворять неравенству $0 \leq c_i < \beta$. Исходя из этого представления, число удобно описывать с помощью массива, хранящего коэффициенты c_i, где i отображает степень β. Не менее важной задачей является определение основания β.

Любое число можно представить в десятитысячной системе счисления. В качестве основания ($\beta = 10^8$). Пример:

$$76895042908718237465_{10} = 7689*(10^8)^2 + 50429087*(10^8)^1 + 18237465*(10^8)^0.$$

Данное представление числа 76895042908718237465, обладает определенными достоинствами:

1. Сокращение количества используемой памяти;
2. В значительной степени уменьшается время необходимое для выполнения стандартных операций над длинными числами.

Первый пункт объясняется тем, что массив из 20 чисел заменен массивом из 3 чисел (7689, 50429087, 18237465). Причина второго достоинства вытекает из того что обработка числа производится не поразрядно, за один шаг происходит преобразование 8 разрядов. Под стандартными операциями подразумеваются операции сложения, умножения, вычитания и возведения в степень. Скорость выполнения операций с 1 - разрядными и 64-разрядными числами одинакова (при использовании 64 - разрядного процессора), эту особенность необходимо использовать. Существует зависимость основания системы счисления β от максимально возможного размера типа данных процессора. Выбор максимально большого основания, равного размеру типа данных, приведет к уменьшению размера представления длинного числа и увеличению скорости операций, производимых с ними. Для обеспечения удобства вывода и отладки можно выбрать β как степень 10, β – степень 2 позволит выполнять быстрые операции на низком уровне [2].

Важно, что массив содержит модуль числа в обратном порядке следования. Для хранения знака числа необходимо использовать другую переменную. Такой способ хранения удобен: все элементы массива имеют одинаковую структуру. Для определения

знака числа производится обработка отдельной переменной. Кроме того выполнение всех операций производится в обычном порядке, т.е. от младшего разряда к старшему.

В заключении необходимо отметить, что программные решения алгоритмов связанных с произведением операций над большими числами представлены в различных библиотеках, применяющихся при решении задач реализации процессов электронной цифровой подписи. Широкое распространение получила библиотека NTL, ее использование возможно как в операционных системах семейства Windows, так и Linux. Наибольшей производительности можно добиться благодаря подключению библиотеки GMP на операционных системах семейства Linux.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 34.10–2012. Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи. – Введ. 2012–08–07. Москва : Стандартинформ, 2012. – 29 с.
2. Wikipedia / Wikipedia community [Электронный ресурс] : Электрон. дан. – 2017. Режим доступа: https://en.wikipedia.org/wiki/Schoof's_algorithm. – Дата обращения: 13.03.2017.

А.А. Полков, Д.С. Совенко

ОБЗОР СПОСОБОВ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ

Академия Федеральной службы охраны Российской Федерации, Орел, Россия

Ключевые слова: линейное преобразование, регистр, линейные комбинации, байт исходного состояния.

В тезисах рассмотрены методы пригодные для программной реализации линейного преобразования.

A.A. Polkov, D.S. Sovenko

OVERVIEW OF WAYS FOR THE SOFTWARE IMPLEMENTATION OF LINEAR TRANSFORMATION.

Academy of Federal Guarding Service of Russian Federation, Orel, Russia

Key words: linear transformation, register, linear combinations, byte of initial state.

The article considers methods and ways, which are qualified for the software implementation of linear transformation.

Цель данной работы – обзор способов реализации линейного преобразования.

Основными задачами являются:

1. Представить способы реализации линейного преобразования.

Рассматриваются некоторые методы пригодные для программной реализации линейного преобразования. Увеличение его размерности используется для обеспечения криптографической стойкости блочного шифра. Однако увеличение размерности линейного узла связано с увеличением сложности его программной реализации. Причем линейное преобразование становится самым медленным компонентом в алгоритме блочного шифра. Следовательно, необходимо искать эффективные способы реализации линейного преобразования. Рассмотрим несколько общих методов реализации линейных отображений.

1.Табличный метод.

При построении отображения $L : V_{128} \mapsto V_{128}$ программными средствами основная проблема − умножение в поле $GF(2^8)$ Для ускорения используется заранее построенная таблица умножения, которая может представлять собой двумерный массив 256 на 16 байт, либо участок памяти заданного размера (4096 байт) [1].

Коэффициенты при степенях примитивного полинома будут записаны в ячейки памяти 1 и 2 по 64 бит каждая. В ячейках памяти 3 и 4 записывается начальное состояние $\left(q_{m-1}^0\ q_{m-2}^0 \cdots q_2^0\ q_1^0\ q_0^0\right)$, где $q_i^0 \in GF(2^8)\ i = 0,1,\ldots 15$.

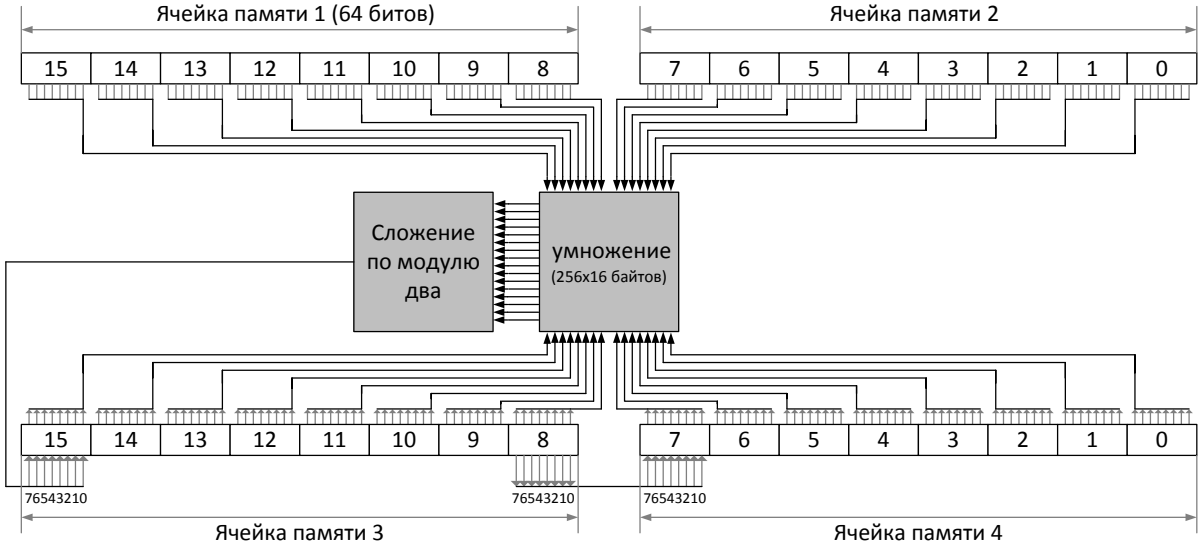


Рисунок 11–Табличный метод в виде схемы

При каждом такте работы регистра происходит сдвиг ячеек памяти 3 и 4 на один байт влево, при этом информация со старшего байта ячейки памяти 3 поступает в таблицу умножения, где выступает в роли адреса для определения результата умножения. Информация со старшего байта ячейки памяти 4 переходит в младший байт ячейки памяти 3, при этом младший байт ячейки памяти 4 становится нулевым. Второй частью адреса поочередно будут выступать байты ячеек памяти 1 или 2. Таким образом, старший байт с выхода ячейки памяти 3 умножится на байты ячеек памяти 1 и 2, а результаты

данных умножений сложатся по модулю два с соответствующими байтами ячеек памяти 3 и 4.

В нашем случае число умножений равно 7, так как только 7 из 16 коэффициентов $h(y)$ имеют нетривиальные различные значения, а число выполнения операции XOR равно 16. За счет того, что внешний полином обратной связи фиксирован, то для ускорения выполнения операции умножения можно составить таблицу для умножения на 7 коэффициентов $h(y)$. Размерность данной таблицы равна 256x7. Поэтому требуются только 1792 байта памяти для хранения данной таблицы. При этом, операции умножения требуют 13 обращений к таблице.

2.Использование таблиц логарифмов Зеча.

Данный метод предполагает использование таблиц логарифмов Зеча [2], суть которых можно описать следующим образом, $\alpha^z = \alpha^x + \alpha^y, где\ z = (x+y) mod\ 255,\ \alpha \in GF(2^8)$ – образующий элемент. Результат умножения получается за счет использования двух таблиц. Первая таблица представляет собой массив данных размером 256 байт, в котором по адресу α^i находится степень i (длиной 8 бит) элемента, при этом $i = 0,1 \ldots 255$. Вторая таблица это также массив данных 256 байт, в котором по адресу i находится элемент α^i (длиной 8 бит).

3.Умножение текущего состояния на матрицу T16.

Данный метод подходит для любой схемы регистра. При построении матрицы T^{16} исходным состоянием регистра выступают коэффициенты при степенях примитивного полинома $h(y)$, без старшей единицы. Это состояние и есть нижняя строка матрицы. Далее производится 15 тактов, при этом после каждого такта состояние регистра записывается в следующую строку матрицы. Регистр сдвигается влево. В результате матрица будет иметь такой вид (hex):

$$T^{16}=\begin{pmatrix}
4b & d2 & 26 & e3 & 73 & 6c & 48 & 7a & b8 & 5d & 27 & bd & 10 & dd & 84 & 94\\
41 & b9 & e4 & 13 & f3 & 77 & d5 & e6 & 49 & d4 & 9f & 95 & e9 & 99 & 2d & 20\\
b7 & a3 & f3 & 94 & 6b & ed & 63 & 4e & 87 & b8 & be & 5e & d0 & 75 & 74 & 85\\
bc & 86 & f6 & 1c & cb & 0c & 16 & 1b & 14 & 2f & 68 & 30 & d9 & ca & 96 & 10\\
7b & cd & a3 & ce & 20 & c4 & 06 & ba & ca & 8d & 1a & e9 & f3 & 97 & 5d & c2\\
ea & d5 & fe & 47 & fb & bc & 2c & 2e & 8c & 13 & 7c & 60 & 94 & 44 & 77 & c0\\
a6 & e3 & aa & 1d & 94 & bf & c4 & f0 & aa & ef & ac & bf & 3d & 5a & 6f & 01\\
88 & 14 & c5 & 48 & 6e & f8 & f7 & be & 48 & f6 & c8 & 11 & af & e0 & de & fb\\
64 & de & 9d & 97 & 54 & 69 & 43 & c4 & 09 & 09 & 84 & ee & 7a & 30 & 54 & 01\\
9a & d6 & f8 & f7 & e4 & 38 & 21 & 39 & 7c & 54 & 2e & 39 & fe & a7 & b4 & c0\\
47 & 93 & a9 & 1b & ac & a0 & 40 & fd & bc & 1f & eb & ed & 64 & 30 & 8c & c2\\
24 & e9 & a0 & 4d & 2e & 30 & 48 & 68 & cb & 65 & ee & 91 & 90 & d3 & d0 & 11\\
f7 & 55 & cc & 99 & 71 & 21 & 3a & e4 & b9 & 52 & 50 & 6f & 52 & de & 44 & 84\\
4a & c6 & 00 & 22 & c6 & 16 & da & 42 & be & 11 & 82 & de & e8 & 48 & 3d & 20\\
22 & a8 & 8c & 70 & 5a & d8 & 02 & 41 & 23 & 4f & 7b & 43 & 9b & 74 & 5a & 95\\
34 & d0 & fe & b8 & 60 & 5e & 61 & ac & 72 & 4f & 8d & c9 & 17 & 12 & 84 & 01
\end{pmatrix}$$

Линейное отображение $L:V_{128}\to V_{128}$ можно выразить так: $Q_{16}=Q_0\times T^{16}$. Обратное отображение $L^{-1}:V_{128}\to V_{128}$ будет задаваться формулой: $Q_0=Q_{16}\times T^{16^{-1}}$.

Для получения обратной матрицы $T^{16^{-1}}$ необходимо принять все коэффициенты при степенях исходного полинома $h(y)$ без старшей единицы) за элемент поля GF((2^n)^m) и найти для него обратный элемент по модулю $h(y)$ (например, с помощью алгоритма Евклида). Далее записать результат, как исходное состояние регистра и так же как получили матрицу T^{16} построить матрицу $T^{16^{-1}}$. Каждая из матриц $T^{16},T^{16^{-1}}$ занимает по 256 байт.

4.Способ одновременного применения коэффициентов внутреннего и внешнего полиномов.

Построим 16 таблиц, 8×8 бит. Первая строка в каждой таблице это соответствующее значение коэффициента внешнего полинома $H=(h_{15},h_{14}\ldots,h_0)$, где $h_i\in GF(2^8)$, $i=0,1,\ldots 15$. Для верхнего блока памяти $i=15,14,\ldots 8$ и первыми строками каждой будут коэффициенты $h_{15},h_{14}\ldots,h_8$ соответственно. Далее 7 раз сдвинуть регистр, и после каждого сдвига его текущее состояние копировать в следующую строку заполняемой матрицы.

Заполнив таким способом, все восемь матриц получим блок памяти, который будет использован для замены операции умножения.

Аналогично строится и второй блок памяти, отличие лишь в том, что i принимает значения от 7 до 0.

Организованные таким образом оба блока памяти, применим для реализации линейного отображения $L: V_{128} \to V_{128}$, .

При каждом такте работы регистра старший байт с выхода ячейки памяти поступает на вход блоков памяти. При этом биты данного байта будут определять, какие строки блоков памяти необходимо прибавить по модулю два к содержимому ячеек памяти. Как и ранее значением ячеек памяти 1 и 2 является исходное состояние $\left(q_{m-1}^0\ q_{m-2}^0 \cdots q_2^0\ q_1^0\ q_0^0\right)$ где $q_i^0 \in GF(2^8)$, $i = 0,1,\ldots 15$ (общей длиной 128 бит). Все отображение $L: V_{128} \to V_{128}$, требует 16 операций сдвига 16-ти байтового массива, 128 логических операций проверки "правда – лож", в среднем 128 обращений к памяти и столько же операций сложения 64-битных слов. Расход памяти 144 байта.

5.Способ "готовых линейных комбинаций".

В данном случае для каждой матрицы блока памяти просчитаны все линейные комбинации строк и записаны в массив. Причем массив организован так, что по адресу 0x01 расположены первые строки всех 16 матриц, а по адресу 0xff – 255-е строки всех матриц. Поэтому все отображение $L: V_{128} \to V_{128}$, требует 16 операций сдвига 16-ти байтового массива, 32 обращения к памяти и 32 сложения 64-битных слов. Расход памяти 4096 байт.

6.Метод "готовых произведений" при умножении текущего состояния на матрицу T16.

При умножении каждого байта исходного состояния регистра на байты столбца матрицы T16, возможно всего 256 различных вариантов, т.к. результат принадлежит $GF(2^8)$. Заранее просчитываются все варианты умножения и записываются в массив, при этом размер такого массива будет 64 кбайт. А далее, по значению байта состояния, выбираются нужные строки из массива данных, и складываться по модулю два. Следующее рассмотрим более подробно данный метод.

Для $a = a_{\square} \square \ldots \square a_{\square} \in V_{\square}, a_{\square} \in V_{\square}, i = 0,\ldots,15,$ линейное преобразование определяется следующим образом:

$$L(a) = aT^{16} = (a_{15}, a_{14}, \ldots, a_0) \cdot \begin{pmatrix} T_{15,15} & T_{15,14} & \cdots & T_{15,0} \\ T_{14,15} & T_{14,14} & \cdots & T_{14,0} \\ \vdots & \vdots & \ddots & \vdots \\ T_{0,15} & T_{0,14} & \cdots & T_{0,0} \end{pmatrix},$$

Таким образом, линейное преобразование L может быть реализовано с помощью отображений $L_0 \ldots L_{15}$. Для каждого i мы создаем таблицу , составляющую 256 строк по 128 бит:

$$\begin{pmatrix} T_{i,15}(0\times 00) & T_{i,14}(0\times 00) & \cdots & T_{15,0}(0\times 00) \\ T_{i,15}(b) & T_{i,14}(b) & \cdots & T_{14,0}(b) \\ \vdots & \vdots & \ddots & \vdots \\ T_{i,15}(0\times ff) & T_{i,14}(0\times ff) & \cdots & T_{i,0}(0\times ff) \end{pmatrix}$$

Обратное преобразование L–1 может быть осуществлено таким же образом, с использованием элементов обратной матрицы $T^{16^{-1}}$ для вычисления справочных таблиц.

Применение методов реализации линейных отображений являются эффективными способами реализации линейного преобразования. Наиболее универсальным методом с точки зрения построения схем регистров является метод умножения текущего состояния на матрицу T16.

СПИСОК ЛИТЕРАТУРЫ

1. *Слепов Н.О.* Квантовая криптография: передача квантового ключа. Проблемы и решения.
2. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии – МЦНМО 2003 .

Н.В. Путилин[1], В.А. Головской[2], В.А. Крутов[1]

КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ И МОДЕРНИЗАЦИИ СЕТЕЙ РАДИОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

[1]Научно-технический отдел (дислокация г. Ростов-на-Дону) Федерального казенного учреждения «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, Ростов-на-Дону, Россия

[2]Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: государственный контракт, комплексный подход, сеть радиосвязи.

В статье приведены результаты проведенного анализа проблемных вопросов, возникающих на этапах построения и модернизации сетей радиосвязи специального назначения из-за несовершенства конкурсной документации. Предложены научно обоснованные рекомендации, направленные на профилактику проблемных вопросов за счет реализации комплексного подхода к формированию конкурсной документации.

N.V. Putilin[1], **V.A. Golovskoy**[2], **Krutov V.A.**[1]

COMPREHENSIVE APPROACH TO BUILDING AND MODERNIZATION OF SPECIAL RADIO NETWORKS

[1]Scientific and Technical Department (dislocation, Rostov-on-Don) of 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

[2]North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: the state contract, a comprehensive approach, radio network.

The article presents the results of a analysis of problems arising at stages of construction and modernization of special radio networks due to the imperfection of the tender documentation. Offered scientific advice aimed at preventing problematic issues through the implementation of an integrated approach to the formation of tender documentation.

В рамках реализации государственной политики [1] в области развития информационно-телекоммуникационных технологий и их внедрения в деятельность органов исполнительной власти в настоящее время осуществляется модернизация единой сети электросвязи РФ, имеющей в своем составе сети радиосвязи специального назначения (СР СН), функционирующие в интересах служб обеспечения правопорядка (СОП). В рамках модернизации выполняется переход СР СН на высокотехнологичные стандарты радиосвязи [2].

Вышеизложенное ставит в прямую зависимость обеспеченность СОП надежной радиосвязью и эффективность выполнения ими поставленных задач и осуществления возложенных функций. Требование же высокой эффективности деятельности ОВД определяет актуальность рассматриваемых в настоящей статье вопросов разработки проекта государственного контракта (госконтракт) на поставку оборудования и построение СР СН. Данные вопросы оказывают существенное влияние на качество функционирование современных СР СН [3, 4].

Вопросы разработки обязательного элемента конкурсной документации – проекта госконтракта на поставку оборудования и построение СРС СН, а также размещения антенных систем в процессе деятельности по построению и модернизации СР СН затрагивают различные области знаний: юридические, организационные, экономические и технические. Целью данной статьи является выработка научно обоснованных рекомендаций по использованию комплексного подхода к формированию госконтракта и планирующей документации, определяющих сроки, порядок и состав мероприятий по построению и модернизации СР СН. Требуемые рекомендации должны основываться на результатах проведенного анализа вопросов, рассматриваемых в настоящей статье.

Объект исследования – комплекты конкурсной документации на право заключения госконтрактов на поставку оборудования и построение СР СН для некоторых регионов РФ

[5–8] и результат реализации одного из госконтрактов [5] – СР СН стандарта APCO 25, развернутая в столице Южного федерального округа − г. Ростове-на-Дону.

Сразу после построения рассматриваемой СР СН были осуществлены натурные испытания. Результаты испытаний показали следующее:

1. Для обеспечения требуемой зоны покрытия СР СН, охватывающей, в том числе, расположенные в городах-спутниках объекты СОП, необходима установка дополнительных базовых станций.
2. При установке дополнительных и в аппаратуре уже установленных базовых станций необходимо реализовать важные функции, предусмотренные стандартом APCO 25, но не реализованные при построении исследуемой СР СН. Такими функциями являются фиксация идентификаторов абонентов радиосети, ведущих радиопереговоры, а также дистанционное прослушивание диспетчером аудиообстановки в зоне конкретной абонентской радиостанции.

В целях оценивания функциональной эффективности и надежности СР СН, выявления проблемных вопросов и выработки методических рекомендаций по их решению была проведена научно-исследовательская работа «Анализ эффективности внедрения в интересах ГУ МВД России по Ростовской области и УМВД России по г. Ростову-на-Дону системы цифровой транкинговой радиосвязи стандарта APCO 25».

В результате проведенного анализа [9], в том числе, были выявлены следующие факторы, влияющие на функциональную эффективность и надежность СР СН:

1. Отсутствие в открытом доступе легальных спецификаций стандарта APCO 25 [10].
2. Наличие угроз информационной безопасности, обусловленное следующими причинами:
   - разработка стандарта APCO 25 осуществлена иностранными специалистами (в основном из стран Северной Америки) [11];
   - использование для производства оборудования компонентной базы в основном зарубежного производства;
   - наличие уязвимостей серверной версии операционной системы аппаратно-программного комплекса контроля и управления оборудованием СР СН [12].
3. Высокая вероятность нарушения требуемых показателей оперативности и доступности связи [13, 14].
4. Несоответствие эксплуатационной документации, предоставленной поставщиками оборудования, требованиям нормативных документов [15].
5. Неопределенность периода проведения гарантийного и послегарантийного обслуживания и ремонта оборудования СР СН [3].
6. Частичное использование эргономических принципов при монтаже оборудования рабочих мест операторов СР СН [9].
7. Существование юридических, экономических и организационных ограничений по размещению антенных систем и объектов связи СОП на наиболее выгодных высотных площадках [9].

Наличие указанных факторов обуславливает необходимость более детального рассмотрения вопросов разработки госконтракта на начальном этапе создания СР СН в рамках деятельности по созданию конкурсной документации. И если для снижения потенциального негативного влияния факторов 1–3 необходимо осуществлять организационно-технические мероприятия, то для исключения возможности повторения

недостатков, обусловленных факторами 4–7, будет достаточно изложить все требования в тексте госконтракта.

В результате проведенных исследований [3, 9] с целью актуализации технической части проекта госконтракта и устранения влияния выявленных негативных факторов выработаны следующие рекомендации:

1. На стадии подготовки к проведению конкурсных мероприятий и разработки проекта госконтракта на поставку высокотехнологичной продукции рекомендуется вносить в конкурсную документацию требования:
   - об обязательном проведении метрологической экспертизы всего комплекта эксплуатационной документации;
   - о предоставлении удовлетворяющей требованиям [15] эксплуатационной документации на бумажном носителе с подписями ответственных должностных лиц и оттиском печати поставщика, а также в электронном виде на любом носителе информации.
2. При формировании конкурсной документации на поставку высокотехнологичной продукции с целью достижения организационно-технического единства, определяющего порядок управления, взаимодействия и использования цифровых технологий, стандартов, протоколов, средств и сетей связи СОП в соответствии с [16] необходимо:
   - развертывать СР СН по плану, учитывающему интересы всех подразделений СОП;
   - соблюдать единую техническую политику, обеспечивающую построение СР СН с учетом перехода на современные технологии;
   - применять оборудование, функционирующее на основе единых стандартов и протоколов связи и отвечающее установленным техническим требованиям;
   - использовать единый подход к техническому обслуживанию оборудования СР СН.

Использование данных рекомендаций позволит заложить прочную базу для эффективного функционирования и дальнейшего развития СР СН.

Таким образом, по результатам исследования проблемных вопросов разработки проекта госконтракта предлагается на начальных этапах построения и модернизации СР СН применять комплексный подход, который подразумевает:

1. Создание рабочей группы по построению СРС, с включением в ее состав соответствующих специалистов: юристов, технических специалистов, специалистов контрактной службы, психологов, сотрудников подразделений-пользователей, специалистов иных подразделений СОП, дислоцированных на территории построения СР СН.
2. Проведение работ по разработке проекта госконтракта необходимо проводить одновременно с определением мест размещения антенных систем и объектов связи СОП.
3. Выработку предложений по резервированию наиболее важных элементов СР СН, с учетом уже имеющихся и планируемых к построению систем передачи информации и управления.
4. Прогнозирование дальнейшего развития территории обслуживания СОП и потребности в обеспечении радиосвязью, реализуемое в форме совместных региональных и муниципальных программ и иных планирующих документов.

В результате исследования вопросов, рассмотренных в статье, сформированы научно обоснованные рекомендации по разработке конкурсной документации, которые нашли свое отражение в соответствующем разделе «Методических рекомендаций по повышению эффективности функционирования цифровой транкинговой системы радиосвязи» [17].

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»: постановление Правительства РФ от 15 апреля 2014 г. № 313 // Сайт Правительства России [Электронный ресурс]. – Режим доступа: http://government.ru/media/files/azI8tHyUZSY.pdf (дата обращения: 03.08.2015).
2. *Ляшенко С.Н.* Совершенствование системы связи МВД России // Информационные технологии, связь и защита информации МВД России. – 2012, № 2, с.18–19.
3. *Путилин Н.В., Головской В.А.* Проект государственного контракта на построение цифровой системы радиосвязи: особенности и этапы разработки // Вопросы тылового обеспечения. – 2014, №7(52), с.24–27.
4. *Головской В.А.* Экспериментальное обнаружение угрозы сети радиосвязи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ. – 2016, с. 280-283.
5. Сведения заказа / Официальный сайт Российской Федерации в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг [Электронный ресурс]. – Режим доступа: http://zakupki.gov.ru/pgz/public/action/orders/info/order_document_list_info/show?source=epz&notificationId=1749614 (дата обращения 03.08.2015).
6. Сведения заказа / Официальный сайт Российской Федерации в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг [Электронный ресурс]. – Режим доступа: http://zakupki.gov.ru/epz/order/notice/ea44/view/documents.html?regNumber=0111100008314000097 (дата обращения 03.08.2015).
7. Сведения заказа / Официальный сайт Российской Федерации в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг [Электронный ресурс]. – Режим доступа: http://zakupki.gov.ru/pgz/public/action/orders/info/order_document_list_info/show?notificationId=1240624 (дата обращения 03.08.2015).
8. Сведения заказа / Официальный сайт Российской Федерации в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг [Электронный ресурс]. – Режим доступа: http://zakupki.gov.ru/epz/order/notice/ea44/view/documents.html?regNumber=0119100010114000108 (дата обращения 03.08.2015).
9. Анализ эффективности внедрения в интересах ГУ МВД России по Ростовской области и У МВД России по г. Ростову-на-Дону системы цифровой транкинговой радиосвязи стандарта APCO 25 : отчет о НИР «Система-Р» (промежуточный) / рук. Крутов В.А.; исполн.: Головской В.А. [и др.]. – ФКУ НПО «СТиС» МВД России, – 2013. – 172 с. – Библиогр.: с. 162. – Гос. рег. № 05133824.

10. Standards Store // Официальный сайт «The Telecommunications Industry Association» [Электронный ресурс]. – Режим доступа: http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-102 / (дата обращения 11.05.2015).
11. *Ketterling Hans-Peter A.* Introduction to digital professional mobile radio. – Norwood, MA: ARTECH HOUSE, INC., –2004. – 358 p.
12. Список уязвимостей // Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: http://www.bdu.fstec.ru/ubi/vul (дата обращения 04.08.2015).
13. *Головской В.А., Крутов В.А.* Недостатки и перспективы развития транкинговых систем радиосвязи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, 2014, Часть I, с. 37-40.
14. *Головской В.А.* К вопросу учета трафика при планировании сетей подвижной радиосвязи // Материалы международной научно-практической конференции «Охрана, безопасность, связь – 2015», часть 3. Воронеж: Воронежский институт МВД России. – 2016, с. 7-13.
15. ГОСТ 2.601–2006 Единая система конструкторской документации. Эксплуатационные документы. Введ. – 2006 – 09 – 01. – М.: Стандартинформ, 2006.
16. Концепция развития информационно-телекоммуникационных технологий и связи органов внутренних дел РФ на период до 2020 года.
17. *Крутов В.А., Головской В.А., Мозоль А.А., Путилин Н.В., Хорольский Е.М., Титов В.Ю*. Методические рекомендации по повышению эффективности функционирования цифровой транкинговой системы радиосвязи. М. : ФКУ НПО «СТиС» МВД России, 2014, – 22 с.

Н.И. Сидняев, С.А. Говор
sidnyaev@yandex.ru, govor_sa@mail.ru

ИССЛЕДОВАНИЕ ПЛАНИРОВАНИЯ ЭКСПЕРИМЕНТА ПРИ ПОСТРОЕНИИ МОДЕЛЕЙ СО СЛУЧАЙНЫМ ДРЕЙФОМ ПАРАМЕТРОВ РЕГРЕССИОННОЙ МОДЕЛИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана), г. Москва, Россия

Ключевые слова: теория планирования эксперимента, регрессионная модель, планы, информационная матрица, коэффициент регрессии.

В статье рассмотрена задача нахождения оценок параметров математической модели исследуемого объекта в предположении, что значения этих параметров не изменяются в течение эксперимента.

N.I. Sydnyaev, S.A. Govor
sidnyaev@yandex.ru, govor_sa@mail.ru

STUDY OF EXPERIMENT PLANNING WHEN BUILDING MODELS WITH RANDOM DRIFT PARAMETERS OF THE REGRESSION MODEL

BMSTU, Moscow, Russia

Key words: theory of planning of experiment, regression model, plans, information matrix, regression coefficient.

The article considers the problem of finding estimates of the parameters of the mathematical model of the object under the assumption that the values of these parameters do not change during the experiment.

Во многих практических ситуациях, возникающих при экспериментальных исследованиях, предположение о неизменности параметров не может быть принято. Приведем несколько примеров таких задач. Пусть данные, полученные в результате наблюдения за входами и выходами некоторого химико-технологического процесса, используются для уточнения параметров модели этого процесса, причем в группе уточняемых параметров находится параметр, характеризующий активность катализатора. Если эксперимент проводится в течение относительно небольшого промежутка времени, то активность катализатора можно принять неизменной. Если период сбора данных значительный, то предположение о неизменности активности катализатора неприемлемо. В этом случае экспериментатора интересует оценка значения показателя активности катализатора либо к моменту завершения эксперимента, либо в какой-то определенный момент времени в будущем. Отметим, что изменение свойств катализатора не всегда может быть описано детерминированной функцией времени, так как возможно существование факторов, влияющих на этот процесс и изменяющихся случайным образом, которые в промышленных условиях не поддаются оперативному контролю.

Другой пример. Пусть управление технологическим процессом осуществляется на основе уточняемой экспериментальным путем модели, причем часть случайно изменяющихся характеристик входного сырья, существенно влияющих на входные переменные процесса, не контролируется. При этом все или некоторые параметры модели будут случайным образом изменяться во времени.

Общим для рассмотренных примеров является наличие неконтролируемого случайно изменяющегося фактора (или факторов), влияющего на значения параметров модели, а также требование знать значения параметров модели в момент завершения или в определенный момент времени после завершения эксперимента. Модели подобного типа будем называть моделями со случайным дрейфом параметров.

Естественно, что подобное усложнение модели требует наличия дополнительной информации о характере изменения дрейфа оцениваемых параметров. От этого характера зависит способ вычисления оценок и выбор наилучшего плана эксперимента.

Отметим, что рассматриваемая здесь задача по существу является задачей фильтрации многомерного случайного процесса, когда наблюдаются не непосредственно составляющие этого процесса, а лишь их некоторая линейная комбинация. Существующая теория фильтрации дает возможность найти оптимальные в определенном смысле способы вычисления оценок в этой задаче. Так, в случае, когда процесс изменения параметров модели является стационарным в широком смысле и определяется корреляционной функцией, наилучшие линейные оценки параметров (минимизирующие сумму квадратов дисперсий оценок) могут быть найдены с помощью алгоритма, описанного в работе [3]. Если процесс изменения параметров нормальный и Марковский, то для вычисления оценок, удовлетворяющих критерию максимума апостериорной плотности вероятностей, можно воспользоваться дискретным алгоритмом фильтрации Калмана [4].

В данной работе сформулирована задача планирования эксперимента при построении моделей со случайным дрейфом параметров. Рассмотрен случай, когда процесс изменения параметров — нормальный и марковский, а для вычисления оценок используется дискретный алгоритм Калмана. В качестве критерия оптимальности планов использован *D*-критерий [2]. Рассмотрены некоторые особенности планирования в условиях, случайного дрейфа параметров модели, проиллюстрированные двумя расчетными примерами. Показано, что последовательная процедура построения планов не приводит в общем случае к получению *D*-оптимальных планов, однако при определенных условиях отличия от оптимальных: планов оказываются несущественными.

Постановка задачи планирования эксперимента

Пусть модель исследуемого объекта имеет вид:

$$\eta(x,\beta(\mathrm{t})) = \beta^T(t)\, f(x). \qquad (1)$$

Здесь $f(x)$ $n-$ мерный вектор-столбец заданных функций от $k-$ мерного вектора входных переменных x;

$\beta(t)$ $n-$ мерный вектор неизвестных коэффициентов, случайным образом изменяющихся во времени.

Положим, что через равные интервалы времени проводится измерение выходной переменной объекта, причем результат измерения в момент t есть

$$y(t) = \eta(x(t),\beta(t)) + \varepsilon(\mathrm{t})\,. \qquad (2)$$

Время t при этом принимает дискретные значения $t = 1,2,\ldots$

Примем, что $\varepsilon(t)$ - случайная ошибка, причем

$$\mathrm{M}\varepsilon(t) = 0,$$

$$\mathrm{M}[\varepsilon(t)\varepsilon(t+\mu)] = \begin{cases} 0, \text{при } \mu \neq 0 \\ \sigma_\varepsilon^2, \text{при } \mu = 0. \end{cases} \qquad (3)$$

Кроме того, положим, что процесс $\beta(t)$ определяется следующим реккурентным соотношением:

$$\beta(t) = F_1\beta(t-1) + F_2\omega(\mathrm{t}),$$

где F_1 и - F_2 известные матрица размера $k \times k$;

$\beta(t-1)$ - значение вектора коэффициентов в момент времени $t-1$;

$\omega(t)$ - случайный вектор размерности k, распределенный по нормальному закону с нулевым математическим ожиданием и известной ковариационной матрицей Q.

Полагаем, что последовательные значения $\omega(1), \omega(2), \ldots$ независимы, т.е. $\mathrm{M}\omega(i)\omega(j) = 0$ при $i \neq j$.

F_2 - известная матрица размера $k \times k$.

Выражение (3) описывает дискретный линейный фильтр первого порядка, на вход которого поступает нормальный белый шум.

$$\max_{1 \le k \le k} \sum_{\mu=1}^{k} |\varphi_{i\mu}| < 1. \tag{4}$$

Нетрудно убедиться, что при указанных условиях процесс $\beta(t)$ является нормальной ковариационной матрицей, равной при $t \to \infty$:

$$C_0 = \operatorname{cov} \beta(t) = \lim_{t \to \infty} \sum_{j=1} F_1^{t-j} F_2 Q F_2^{T} (F_1^{T})^{t-j}. \tag{5}$$

В частном случае, когда $F_1 = \alpha I_k$, имеем

$$\operatorname{cov} \beta(\mathrm{t}) = \frac{1}{1-\alpha^2} F_2 Q F_2^{T}. \tag{6}$$

Свойство марковости нормального процесса непосредственно следует из выражения (3). Приведем еще выражение для корреляционной функции процесса $\beta(t)$:

$$R_\beta(\tau) = F_2 [\lim_{t \to \infty} \sum_{j=1}^{t} F_1^{t-j} (F_1^{T})^{t-j+\tau}] F_2^{T}. \tag{7}$$

В частном случае при $F_1 = \alpha I_k$ имеем

$$R_\beta(\tau) = F_2 Q F_2^{T} \frac{\alpha^{|\tau|}}{1-\alpha^2}. \tag{8}$$

Таким образом рекуррентное выражение (3) полностью определяет все свойства процесса $\beta(t)$.

Пусть измерения выходной переменной проводятся в моменты $t = 1, 2, \ldots, \mathrm{N}$. Значения входных переменных в соответствующие моменты времени образуют план эксперимента $x(1), x(2), \ldots, x(N)$. Результаты эксперимента используются для нахождения наилучших в определенном смысле оценок вектора коэффициентов для $t = N + \gamma$ при $\gamma = 0, 1, 2, \ldots$

Задача определения оценок $\hat{\beta}(\mathrm{N}+\gamma)$ при $\gamma = 0$ является задачей фильтрации, а при $\gamma > 0$ - задачей прогнозирования значений коэффициентов. Алгоритм вычисления оценок $\hat{\beta}(\mathrm{N}+\gamma)$ обеспечивающий получение оценок, соответствующих максимуму апостериорной плотности вероятности коэффициентов, определяется следующими рекуррентными соотношениями [4]:

$$\hat{\beta}(\mathrm{i}+1) = F_1\hat{\beta}(\mathrm{i}) + \frac{C_{(i+1)/i} f(x(i+1))}{f^T(x(i+1))C_{(i+1)/i} f(x(i+1)) + \sigma_\varepsilon^2}(y(i+1) - f^T(x(i+1))F_1\hat{\beta}(\mathrm{i})), \quad (9)$$

Обозначим через $\varphi_{i\mu}$ элемент матрицы F_1. Положим, что

$$C_{(i+1)/i} = F_1 C_i F_1^T + F_2 Q F_2^T, \quad (10)$$

$$C_{i+1} = C_{(i+1)/i} - \frac{C_{(i+1)/i} f(x(i+1)) f^T(x(i+1)) C_{(i+1)/i}}{f^T(x(i+1))C_{(i+1)/i} f(x(i+1)) + \sigma_\varepsilon^2}. \quad (11)$$

Здесь C_{i+1} - ковариационная матрица вектора оценок $\hat{\beta}(i+1)$. В качестве начальных значений для коэффициентов и ковариационной матрицы (при $t=0$) следует использовать параметра априорного распределения коэффициентов, т.е. $\hat{\beta}(0)=0$ и $C_0 = \mathrm{cov}\,\beta(t)$ из выражения (5).

Расчеты по формулам (9) – (11) проводим при $t = 0,1,2,...,N-1$. В результате находим оценку $\hat{\beta}(\mathrm{N})$ вектора коэффициентов для момента $t=N$ и ковариационную матрицу оценки C_N.

Наилучший прогноз для момента $N+\gamma$ определяется выражением:

$$\hat{\beta}(N+\gamma) = F_1^\gamma \hat{\beta}(N), \quad (12)$$

$$\mathrm{C}_{(\mathrm{N}+\gamma)/\mathrm{N}} = F_1^\gamma C_N (F_1^T)^\gamma + \sum_{j=0}^{\gamma-1} F_1^j F_2 Q F_2^T (F_1^T)^j. \quad (13)$$

Здесь $\mathrm{C}_{(\mathrm{N}+\gamma)/\mathrm{N}}$ - ковариационная матрица оценки вектора коэффициентов при прогнозировании на интервал γ, а $\hat{\beta}(\mathrm{N})$ и C_N - соответственно оценки коэффициентов для момента $t=N$ и их ковариационная матрица.

Обозначим через C_i ковариационную матрицу вектора оценок $\hat{\beta}(\mathrm{i})$ в некоторый момент времени $t=i$. Пусть область возможных значений входных переменных есть Ω_x. В момент времени $t=i$ требуется найти план проведения m последующих опытов из условия получения оценок для момента $t=i+m$ с минимальной величиной определителя ковариационной матрицы (D-критерий). Обозначим через X_m матрицу размера $m\times k$, каждая строка которой определяет значения переменных x в последовательных опытах. Тогда оптимальный в вышеуказанном смысле план X_m^* в случае фильтрации находится из условия:

$$\min_{x_m\in\Omega_x} |\,\mathrm{C}_{i+m}(\mathrm{X}_m, \mathrm{C}_i)\,|, \quad (14)$$

где $\mathrm{C}_{i+m}(\mathrm{X}_m, \mathrm{C}_i)$ рассчитывается по рекуррентным формулам (10), (11).

При прогнозировании значений коэффициентов на интервал γ (после момента времени $i+m$) оптимальный в смысле D-критерия план, состоящий из m опытов, находится из условия

$$\min_{x_m\in\Omega_x} |\,\mathrm{C}_{(i+m+\gamma)/(i+m)}(\mathrm{X}_m, \mathrm{C}_i)\,| \quad (15)$$

где матрица $\mathrm{C}_{(i+m+\gamma)/(i+m)}$ рассчитывается согласно выражению (13).

$$\max_{x_m \in \Omega_x} d(x(j)) = \max_{x(j) \in \Omega_x} f^T(x(\mathrm{j}))(F_1 C_{j-1} F_1^T + F_2 Q F_2^T) f(x(\mathrm{j})).$$

План, получаемый на основе критериев (14) и (15), в общем случае зависит от ковариационной матрицы C_i, дисперсии σ_ε^2, а также матриц F_1, F_2, Q, характеризующих процесс изменения коэффициентов. Отметим, что в частном случае, когда $Q = 0$, имеет место детерминированный дрейф. Проблемы планирования эксперимента для этого случая совпадают с задачами, рассмотренными, например, в работе [5]. Если же F_1 - единичная матрица, а $Q = 0$, то задача сводится к обычной задаче последовательного планирования эксперимента [2, 6].

Свойства планов и процедуры вычисления

В общем случае поиск плана X_m^*, оптимального с точки зрения критериев (14) или (15), может проводиться с помощью методов численной оптимизации (при этом размерность пространства переменных, в котором осуществляется поиск, оказывается равной $m \times k$). В ряде случаев оказывается возможным упростить задачу поиска плана, опираясь на особенности задачи оценивания параметров, изменяющихся случайным образом во времени.

Теорема 1. Пусть C_i и $F_2 Q F_2^T$ - положительно определенные матрицы, а $x(i+1), x(i+2), ..., x(i+m)$ - последовательность значений входных переменных в моменты измерения выходной переменной. Положим, что матрица C_{i+m} рассчитана согласно рекуррентным выражениям (10), (11). Тогда:

1) Матрица C_{i+m} положительно определенная;

2) Определитель матрицы C_{i+m} при $m \to \infty$ ограничен снизу положительной величиной $\lambda > 0$.

Из теоремы 1 следует, что с увеличением числа наблюдений в плане m точность оценок параметров модели остается ограниченной. Это значит, что влияние условий $x(i+j)$ наблюдений в момент $(i+j)$ на величину определителя матрицы C_{i+m} уменьшается с ростом m. При этом для достижения предельно возможной (или несущественно отличающейся от нее) точности оценок может в общем случае потребоваться число наблюдений m^*, меньшее m. Очевидно, начинать наблюдения следует в такой ситуации с момента времени $i + m - m^*$.

Интересно попытаться найти оптимальный план (т.е. наилучшую последовательность $x(i+1), x(i+2), ..., \mathrm{x(i+m)}$ с помощью процедуры последовательного планирования, аналогично тому, как это делается при построении непрерывных D-оптимальных планов [2,6]. Приведем теорему 2, относящуюся к свойствам последовательностей $x^*(j), |C_j|, j = i+1, i+2, ...,$ получаемых при последовательном планировании (т.е. для последовательности решений задачи (14) при $m = 1$).

Теорема 2. Точки $x^*(j)$ постановки последовательных опытов при $m = 1$ определяются из условия

$$\max_{(x(j)) \in \Omega_x} d(x(j)) = \max_{(x(j)) \in \Omega_x} f^T(x(j))(F_1 \mathrm{C}_{j-1} F_1^T + F_2 Q F_2^T) f(x(j)).$$

3) С помощью процедуры последовательного планирования при $m=1$ всегда можно найти план X_r, для которого $|C_r| \le |C_0|$, где $|C_0|$ - определитель ковариационной матрицы априорного закона распределения параметров модели.

Отметим, что выражение (16) непосредственно следует из формулы (23) при условии положительной определенности матрицы $F_1 \mathrm{C}_i F_1^T + F_2 Q F_2^T$.

Величину $d(x(j))$ будем называть дисперсией ошибки прогнозирования $\eta(j) = \eta(x(j), \beta(j))$.

Второе утверждение теоремы 2 также является достаточно очевидным. Действительно, получив последовательность $x^*(1), x^*(2)$ и соответствующую ей последовательность $|C_1|, |C_2|, ...,$ всегда можно найти такой номер r, для которого $|C_r| \le |C_0|$. Планы, получаемые с помощью последовательной процедуры, в данном случае, видимо, не будут – оптимальными, однако при определенных условиях могут оказаться близкими к ним. Кроме того, получаемый план можно использовать (в случае необходимости) как начальный при поиске D - оптимального плана.

Для упрощения поиска оптимального плана с помощью последовательной процедуры при $m=1$ было бы полезно указать множество точек, из которых может состоять последовательность $x^*(j)$. Иногда это возможно. Так, если модель линейна по переменным x, процессы изменения параметров модели независимы (при этом матрицы F_1 и $F_2 Q F_2^T$ диагональные), а область планирования – гиперкуб, координатами вершин ± 1, то последовательность $x^*(j)$ содержит только вершины гиперкуба. Этот вывод непосредственно следует из выражения (16).

Отметим еще, что планы, удовлетворяющие критериям (14) (задача фильтрации) и (15) (задача прогнозирования), в общем случае не совпадают. Лишь при детерминированном процессе изменения параметров, когда $F_2 \equiv 0$, один и тот же план X_m^* является оптимальным как для задач фильтрации, так и для задач прогнозирования. Действительно, при этом в силу выражения (13) имеем:

$$\min_{X_m \in \Omega_x} \left| \mathrm{C}_{(i+m+\gamma)/(i+m)}(\mathrm{X}_m, \mathrm{C}_i) \right| = \min_{X_m \in \Omega_x} \left| F_1^{\upsilon} \mathrm{C}_{i+m}(\mathrm{X}_m, \mathrm{C}_i)(F_1^T)^{\upsilon} \right| = |(F_1^{\upsilon})^2| \min_{X_m \in \Omega_x} |\mathrm{C}_{i+m}(\mathrm{X}_m, \mathrm{C}_i)|. \quad (17)$$

Для иллюстрации полученных выше результатов рассмотрим два примера вычисления планов.

Пример 1. Пусть модель объекта имеет вид

$$\eta(i) = \beta_0(i) + \beta_1(i)\,\mathrm{x}_1(\mathrm{i}) + \beta_2(i)\,\mathrm{x}_2(\mathrm{i}) \quad (18)$$

где $\beta(i) = F_1 \beta(i-1) + F_2 \omega(\mathrm{i})$, причем $F_1 = 0.9 I_3, F_2 = I_3, \mathrm{M}\,\omega(\mathrm{i}) = 0, \mathrm{cov}\,\omega(\mathrm{i}) = Q = 0.5$

Здесь I_3 - единичная матрица размера 3×3. Кроме того, положим, что наблюдаемые значения выходной переменной $y(i) = \eta(i) + \varepsilon(i)$, где $\sigma_\varepsilon^2 = 0.5$

Пользуясь выражением (6), находим ковариационную матрицу априорного закона распределения $\beta(i)$:

$$C_0 = \frac{1}{1-0.81} 0.2 I_3 = 1.052 I_3.$$

Положим, что область Ω_x определена неравенствами

$$-1 \le x_1 \le 1, -1 \le x_2 \le 1.$$

Пользуясь критерием (14) при $m = 1$, найдем координаты точек $x_1^*(i), x_2^*(i), \mathrm{i} = 1, 2, \ldots$ Результаты расчетов приведены ниже (в последнем столбце указаны значения определителя ковариационной матрицы оценок параметров модели после $i-$ го опыта).

Таблица 1. Определитель ковариационной матрицы

F_1 i	$x_1^*(i)$	$x_2^*(i)$	$\lvert C_i \rvert$
1	-	+	0.1593
2	+	+	0.0514
3	-	-	0.0261
4	+	-	0.0200
5	-	+	0.0193
6	+	+	0.0190
7	-	-	0.0189
8	+	-	0.0189
9	-	-	0.0189
10	+	+	0.0189
11	-	-	0.0188
12	+	+	0.0188
13	-	-	0.0188
14	+	+	0.0188
15	-	-	0.0188

Начиная с $i = 11$ величина определителя ковариационной матрицы оценок коэффициентов практически не изменяется. Кроме того, точки постановки опытов – вершины квадрата, повторяемые в одной и той же последовательности (сравни точки 1, 2, 3, 4 и 5, 6, 7, 8 и.т.д.). Последовательность повторения опытов определяется порядком перебора вершины в экспериментах при $i = 1, 2, 3, 4.$ Действительно, при $i = 1$ дисперсия ошибки прогнозирования во всех вершинах одна и та же и равна 3.16, поэтому при $i = 1$ может быть выбрана любая вершина, при $i = 2$ в трех оставшихся вершинах имеет место одна и та же величина дисперсии ошибки прогнозирования и.т.д. Однако в дальнейшем изменение порядка перебора вершин квадрата приводит к изменению величины определителя ковариационной матрицы. Если, например, после 11-го эксперимента поменять порядок последующих четырех опытов, то получим

Таблица 2. Определитель ковариационной матрицы

i	$x_1^*(i)$	$x_2^*(i)$	$\lvert C_i \rvert$
12	-	-	0.037
13	+	+	0.044
14	-	+	0.0595
15	+	-	0.0306

Пример 2. Пусть модель объекта имеет вид:

$$\eta(i) = \beta_0(i) + \beta_1(i)\,\mathrm{x}_1(i) + \beta_2(i)\,\mathrm{x}_2(i) + \beta_{12}(i)\,\mathrm{x}_1(i)\,\mathrm{x}_2(i) + \beta_{11}(i)\,\mathrm{x}_1^2(i) + \beta_{22}(i)\,\mathrm{x}_2^2(i), \quad (21)$$

где $\beta(\mathrm{i}) = F_1\beta(i-1) + F_2\omega(i).$

Положим $F_1 = \alpha I_6 = 0{,}8; F_2 = I_6; \mathrm{M}\omega(i) = 0; \mathrm{cov}\,\omega(i) = Q = qI_6 = I_6; \sigma_\varepsilon^2 = 1.$

При этом имеем

$$C_0 = \frac{1}{1-\alpha^2} F_2 Q F_2^T = 2{,}78 I_6.$$

Пусть область Ω_∞ определяется неравенствами (20). Ниже определена последовательность $x_1^*(i), x_2^*(i),$ полученная с помощью последовательного алгоритма, и соответствующие значения определителя ковариационной матрицы оценок параметров модели:

Таблица 3. Определитель ковариационной матрицы

F_1 i	$x_1^*(i)$	$x_2^*(i)$	$\lvert C_i \rvert$	$\lvert C_i \rvert_{опт}$
1	-	-	26.07	-
2	-	+	11.01	-
3	+	-	7.12	7.12
4	+	+	5.56	-
5	-	-	5.39	5.034
6	-	+	5.36	-
7	+	-	5.35	-
8	+	+	5.34	4.753
9	-	-	5.34	-
10	-	+	5.34	-
11	+	-	5.34	-
12	+	+	5.34	4.753

В последнем столбце даны величины определителей $D-$ оптимальных планов, найденные численно с помощью непоследовательной поисковой процедуры, для ряда значений m. В данном случае $m^* \approx 7$ (это справедливо как для оптимального плана от приближенного, найденного с помощью последовательной процедуры). Кроме того, отличие оптимального плана от приближенного по величине определителя ковариационной матрицы оценок не превышает 15 % величины определителя оптимального плана. Такими различиями часто можно пренебречь.

На этом примере был проведен небольшой численный эксперимент с целью выяснения влияния изменения параметров задачи на число m^* точек в плане и соотношение показателей оптимального плана и плана приближенного, построенного на основе последовательной процедуры. В эксперименте варьировались: дисперсия параметров $\beta: \sigma_\varepsilon^2 = q/(1-\alpha^2),$ параметр α корреляционной функции параметров β, дисперсия σ_ε^2 ошибок наблюдения. Проведенное исследование позволило сделать следующие выводы:

1. Оптимальный план содержит конечное число точек m^*, причем m^* уменьшается с уменьшением α (т.е. с увеличением скорости затухания корреляционной функции β) и σ_ε^2, и с увеличением σ_β^2.
2. Имеет место различия в характеристиках оптимальных и приближенных (последовательных) планов, причем относительные величины различий уменьшаются с ростом σ_ε^2 и уменьшением σ_β^2 и α.

Приложение.

Доказательство теоремы 1.

1. Если преобразование F_1 неособенное (т.е. $|F_1| \neq 0$) и не все компоненты вектора x равны нулю, то

$$x^T F_1 C_i F_1^T x = (F_1^T x)^T C_i F_1^T x > 0.$$

Таким образом, матрица $F_1 C_i F_1^T$ - положительна определенная. Так как

$$x^T (F_1 C_i F_1^T + F_2 Q F_2^T) x = x^T F_1 C_i F_1^T x + x^T F_2 Q F_2^T x > 0,$$

то матрица $F_1 C_i F_1^T + F_2 Q F_2^T$ - положительно определенная. Положительная определенность прямой матрицы приводит к положительной определенности обратной. Кроме того, матрица $f(x(i+1)) f^T(x(i+1))$ всегда положительно полуопределенная. Поэтому матрица

$$C_{i+1} = [(F_1 C_i F_1^T + F_2 Q F_2^T)^{-1} + f(x(i+1)) f^T(x(i+1))]^{-1}$$

Является положительно определенной. Рассуждая аналогичным образом, убеждаемся в положительной определенности матриц $C_{i+2}, ..., C_{i+m}$.

2. Так как матрица $F_2 Q F_2^T$ - положительно определенная, то для любого i можно записать

$$\left|C_{(i+1)/i}\right| = |F_1 C_i F_1^T + F_2 Q F_2^T| = |F_1|^2 |C_i| + \delta_i, \delta_i > 0. \tag{22}$$

Из (11) получаем

$$\left|C_{i+1}\right| = |F_1 C_i F_1^T + F_2 Q F_2^T| \left(1 - \frac{f^T(x(i+1))(F_1 C_i F_1^T + F_2 Q F_2^T) f(x(i+1))}{f^T(x(i+1))(F_1 C_i F_1^T + F_2 Q F_2^T) f(x(i+1)) + \sigma_\varepsilon^2}\right). \tag{23}$$

Обозначим

$$s(i+1) = \frac{f^T(x(i+1))(F_1 C_i F_1^T + F_2 Q F_2^T) f(x(i+1))}{f^T(x(i+1))(F_1 C_i F_1^T + F_2 Q F_2^T) f(x(i+1)) + \sigma_\varepsilon^2}. \tag{24}$$

В силу положительной определенности матрицы $F_1 C_i F_1^T + F_2 Q F_2^T$ имеем $0 < s(i+1) < 1$.

Подставим выражение (22) в формулу (23) и учтем (24):

$$\left|C_{i+1}\right| = (|F_1|^2 |C_i| + \delta_i)(1 - s(i+1)). \tag{25}$$

Для $\left|C_{i+m}\right|$ имеем

$$\left|C_{i+m}\right| = |C_i| |F_1|^{2m} \prod_{j=1}^{m} (1 - s(i+j)) + \sum_{\nu=1}^{m} |F_1|^{2(m-\nu)} \delta_{i-1+\nu} \prod_{\mu=\nu}^{m} (1 - s(i+\mu)). \tag{26}$$

$$\lim_{m\to\infty}|C_{i+m}| \geq \lim_{m\to\infty}\sum_{\nu=1}^{m}|F_1|^{2(m-\nu)}\,\delta_{i-1+\nu}\prod_{\mu=\nu}^{m}(1-s(i+\mu)). \qquad (27)$$

Обозначим через $\delta_{\min} > 0$ минимальную из величин $\delta_{i-1+\nu}, i = 1,2,\ldots$, а через $\delta_{\max} < 1$ - максимальную из величин $s(i+\mu), \mu = 1,2,\ldots$

Тогда

$$\lim_{m\to\infty}|C_{i+m}| \geq \lim_{m\to\infty}\delta_{\min}\sum_{\nu=1}^{m}|F_1|^2\,(1-s_{\max})^{m-\nu+1} = \delta_{\min}\sum_{j=0}^{\infty}|F_1|^{2j}\,(1-s_{\max})^{j+1} = \frac{\delta_{\min}(1-s_{\max})}{1-|F_1|^2\,(1-s_{\max})} = \lambda > 0.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Сидняев Н.И., Говор С.А.* Построение факторных планов с использованием циркулянтных матриц Адамара типа H/ Вестник Северо-Восточного федерального университета им. М.К. Аммосова, 2016. № 1(51). С.68-78.
2. *Сидняев Н.И., Говор С.А.* Проверка гипотезы адекватности статистической модели при ротатабельном планировании эксперимента/Вестник МГТУ. Серия «Естественные науки». 2016. №1 (64). С. 3-16.
3. *Сидняев Н.И.* Введение в теорию планирования эксперимента. Учебное пособие/Н.И.Сидняев, Н.Т. Вилисова. –М.: Изд-во МГТУ им. Н. Э. Баумана, 2011. 463с.
4. *Сидняев Н.И.* Теория планирования эксперимента и анализ статистических данных:учебное пособие/Н.И. Сидняев. –М.: Издательство Юрайт, ИД Юрайт, 2011. - 399 с.
5. *Налимов В.В., Чернова Н.А.* Статистические методы планирования экстремальных экспериментов. - М.: Наука, 1965.
6. *Ермаков С.М., Жиглявский И.И.* Математическая теория оптимального эксперимента: Учеб. пособие. – М.: Наука. Гл. ред. физ.-мат. лит., 1987. – 320 с.
7. *Федоров В.В.* Теория оптимального эксперимента. – М.: Наука, 1971.

В.Н. Смоляков, Р.М. Кильдишов

МОДЕРНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОФИСА КОНТАКТНОГО ЦЕНТРА ТЕЛЕ2-РОСТОВ ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: локальная вычислительная сеть, система передачи данных, информационная безопасность, персональный компьютер, комплексная система защиты информации, операционная система, коммутатор, программное обеспечение, межсетевой экран.

Проанализированы методы и средства защиты информации (рассмотрены требования к защищенности информации в информационной системе контактного центра, организационные и инженерно-технические меры защиты информации, структура и модель систем информационной безопасности) предложен вариант усиления информационной безопасности офиса контактного центра Теле2-Ростов аппаратными средствами с применением управляющих элементов ЛВС - маршрутизаторов компании Cisco, рассмотрены вопросы усиления ИБ офиса контактного центра программными средствами - установкой на серверах сетевой ОС Windows Server 2012, а дополнительная защита информации в ПК ЛВС реализована средствами ОС Windows 10**.**

V.N. Smolyakov, R.M. Kildishev

MODERNIZATION OF THE SYSTEM OF INFORMATION SECURITY OFFICE CONTACT CENTER TELE2-ROSTOV SOFTWARE AND HARDWARE

North-Caucasus branch of Moscow technical University of communication and Informatics, Rostov-on-don, Russia

Key words: local area network, data transmission system, information security, personal computer, integrated security system, the operating system, switch, software, firewall.

The methods and means of information protection (requirements are considered protected information in the information system of the contact center, organizational and engineering-technical protection of information, structure, and model systems) with the enhance information security office contact center Tele2-Rostov hardware with the use of control elements LAN - Cisco routers discussed the issues of strengthening information security office contact center software installation on network servers running Windows Server 2012, and the additional protection of information in the PC LAN is implemented by means Windows 10.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности. Национальная безопасность существенным образом зависит от обеспечения информационной безопасности (ИБ), и в ходе технического прогресса эта зависимость будет возрастать. Обеспечение ИБ является одной из приоритетных задач.

Под информационной безопасностью понимают состояние защищенности собственно информации и её носителей (человека, органов управления, систем и средств, обеспечивающих получение, обработку, хранение, передачу и использование информации) от различного вида угроз. Источники этих угроз могут быть преднамеренными (то есть имеющими цель незаконного получения информации) и непреднамеренными (такую цель не преследующими). Обеспечить ИБ можно различными методами и средствами, как организационного, так и инженерного характера. Комплекс

организационных мер, программных, технических и других методов и средств обеспечения ИБ образует систему защиты информации (СЗИ). Проблема защиты информации (ЗИ), стоящая перед современным бизнесом, сводится к задаче рассмотрения всего спектра имеющихся решений и выбора правильной их комбинации. Сегодня предлагается немало технологий и соответствующих средств защиты. Трудность реализации ЗИ в информационной системе (ИС) предприятия заключается не в отсутствии подходящей технологии защиты, а в выборе из множества решений такого, которое лучше всего подойдет для конкретной фирмы и требований бизнеса и при котором затраты на поддержку и сопровождение СЗИ окажутся минимальными.

Проблемы ЗИ в локальных вычислительных сетях (ЛВС), являющихся основой всех современных ИС предприятий, постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Широкое распространение и повсеместное применение вычислительной техники (ВТ) резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации.

ИБ – сравнительно молодая и 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.

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.

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 СЗИ (КСЗИ), так как ЗИ – это комплекс мероприятий направленных на обеспечение ИБ.

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. ЗИ 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.

Сказанное выше подтверждает актуальность разработки эффективной КСЗИ для усиления ИБ офиса контактного центра (КЦ) Теле2-Ростов посредством программно-аппаратных средств защиты

Организационно-штатная структура КЦ Теле2-Ростов показана на рис. 1.

Рисунок 1 – Организационно-штатная структура КЦ Теле2-Ростов

Группа Экспертной поддержки занимается настройкой оборудования (телефонов, модемов, роутеров) для входа в интернет, обслуживает все онлайн-каналы (чат, Mail, телеграмм, Viber, Google Play), дилеров салонов.

Группа по настройке клиентского оборудования обслуживает остатки абонентов CDMA-Скайлинк, MNP, и новую сеть Скайлинк LTE-450 (В. Новгород, Москва, Тверь и С. Петербург).

Группы Абонентского обслуживания (11 групп) приемом звонков обычных абонентов - физических лиц по линии 611.

В контактном центре Теле2-Ростов используется ЛВС, построенная по топологии «Иерархическая звезда» с клиент-серверной архитектурой. В состав ЛВС входят около 70 ПК по управлением ОС Windows 7 (как правило, в зависимости от отдела, ПК установлены у руководителей, менеджеров и некоторых старших специалистов), а также около 250 терминалов (рабочих мест операторов – клиентов ЛВС). В серверной на 3-ем этаже установлено активное сетевое оборудование и 12 серверов (с ОС Microsoft Server

2008). Для передачи данных по этажам используется витая пара, а между этажами - оптоволокно.

Клиентом является рабочее место оператора,которое включает:

- термирнал («тонкий» клиент);
- монитор;
- манипулятор мышь и клавиатура;
- цифровая станция Avaya, модель 2420 или 1408.

Подключение «тонкого» клиента происходит через систему Avaya, которая соединяется с общей сетью.

ИБ – одна из актуальных проблем, стоящих не только перед коммерческими предприятиями, но и перед каждым человеком, живущим в современном обществе. В наше время повсеместного использования ПК и ЛВС, доступ злоумышленников к информации в этих объектах может привести к катастрофическим последствиям. Поэтому защите информации должно уделяться постоянное внимание. К сожалению абсолютной ЗИ не существует. Обход тех или иных средств защиты вопрос только времени, денег и желания. Поэтому при разработке СЗИ необходимо учитывать ценность защищаемого объекта. Нельзя останавливаться на достигнутом. Совершенная сегодня СЗИ завтра может превратиться лишь в небольшую помеху на пути злоумышленников.

В данном проекте предложен вариант усиления ИБ офиса КЦ Теле2 - Ростов. Были проанализированы методы и средства ЗИ (рассмотрены общая характеристика структуры КЦ Теле2-Ростов и его ИС, требования к защищенности информации в ИС КЦ, организационные и инженерно-технические меры ЗИ, оценка вероятного противника и условий решения задачи ЗИ, основные принципы построения систем ИБ, угрозы НСД и особенности защиты компьютерной информации).

На этой основе был предложен вариант усиления ИБ офиса КЦ Теле2-Ростов аппаратными средствами, для чего проведен анализ офиса КЦ Теле2-Ростов как объекта защиты, рассмотрены возможные каналы утечки информации, предложены варианты силения защиты помещения для проведения совещаний, кабинетов руководителей подразделений, серверной, усиления ИБ ЛВС и коммуникаций. Были выбраны аппаратные средства защиты данных для усиления ИБ - произведена подборка сетевого оборудования для создания защищенной СПД с применением управляющих элементов ЛВС - маршрутизаторов компании Cisco.

Для реализации сетевых аспектов ИБ в роли ключевых управляющих элементов сети предлагается использовать маршрутизаторы компании Cisco серии 2800 и 7200

Компания Cisco Systems предлагает концепцию архитектуры ИБ для сетевых решений и позволяет осуществлять внедрение в систему управления ИБ наряду с собственными средствами и управляющими элементами, аппаратных средств сторонних производителей. Помимо повышения производительности, применение специализированной встроенной ОС реального времени также обеспечивает повышение уровня ИБ. В отличие от ОС семейства UNIX, исходный текст которых широко доступен, Cisco PIX - собственная разработка компании, созданная специально для решения задач обеспечения ИБ. Для повышения надежности МЭ PIX Firewall предусматривает возможность установки в сдвоенной конфигурации в режиме «горячего резервирования», за счет чего в сети исключается наличие единой точки возможного сбоя. Если два PIX-

экрана будут работать в параллельном режиме, и один из них выйдет из строя, то второй в прозрачном режиме «подхватит» исполнение всех функций.

Маршрутизаторы с интегрированными сервисами Cisco 2800 Series предоставляют широкий спектр функций:

- встроенная система ИБ: МЭ, шифрование и защита от взломщиков;
- встроенный резервный разъем питания на большинстве моделей для повышения защиты;
- интеграция с приложением Cisco Unified Communications Manager Express
- для поддержки обработки вызовов до 96 пользователей;
- интеграция с Cisco Survivable Remote Site Telephony (SRST) для обслуживания локальных голосовых сервисов в случае потери соединения;
- повышенная надежность и гибкость, что позволяет выставлять приоритеты для передачи голоса и обмена данными, согласовывая предоставление информации с потребностями бизнеса.

Управление маршрутизаторами может осуществляться через WEB-интерфейс или на базе Cisco IOS Software-интерфейса командной строки, в том числе удаленно. Имеется набор предустановленных сценариев настройки, облегчающий администрирование. Архитектура маршрутизаторов с интегрированными услугами семейства **Cisco 2800** базируется на архитектуре мощных мультисервисных маршрутизаторов доступа серии **Cisco 2600**, предлагая дополнительно встроенные функции ИБ, существенно улучшенную производительность и расширенный объем новые интерфейсы высокой плотности. Благодаря достигнутым показателям производительности, доступности и надежности, маршрутизаторы серии Cisc**o 2800** оказываются незаменимыми для критически важных бизнес-приложений.

Работая под управлением ПО Cisco IOS, маршрутизаторы серии **Cisco 2800** поддерживают концепцию сети с возможностями самозащиты Cisco Self-Defending Network – благодаря улучшенным функциям безопасности и возможностям управления, таким как аппаратная акселерация шифрования, поддержка IPSec VPN (с использованием алгоритмов шифрования AES, 3DES, DES), МЭ, система предотвращения вторжений, контроль за доступом к сети и фильтрация по URL. Предустановленная на всех маршрутизаторах серии **Cisco 2800,** интуитивно-понятная система управления с Web-интерфейсом Cisco Router and Security Device Manager существенно упрощает управление и конфигурирование маршрутизатора.

Внедрение в систему ИБ таких элементов как маршрутизаторы компании Cisco сери 2800, позволят обеспечить максимальный уровень аппаратной ЗИ.

В завершение рассмотрены вопросы усиления ИБ офиса КЦ программными средствами. Предложено усилить защиту данных в ЛВС средствами сетевой ОС Windows Server 2012, а дополнительную ЗИ рабочих станций ЛВС реализовать средствами ОС Windows 10: усиление ИБ посредством сервиса Device Guard и с помощью Защитника ОС Windows 10, а также усиление ИБ браузеров Microsoft Edge и Internet Explorer 11**.**

ОС Windows Server 2012 и Windows 10 - результат многолетних усилий корпорации Майкрософт. Эти ОС стали важным достижением корпорации с точки зрения ИБ. Майкрософт создала эти ОС, чтобы устранить современные угрозы и обезвредить тактику самых изощренных злоумышленников. Благодаря существующим решениями по

обеспечению ИБ, ЛВС и ее ПК с ОС Windows Server 2012 и Windows 10 будут надежно защищены.

СПИСОК ЛИТЕРАТУРЫ:

1. *Бугров Ю.Г.* Системные основы оценивания и защиты информации: Учеб. пособие / Воронеж: Воронеж. гос. техн. ун-т, 2012. 354 с.
2. *Домарев В. В.* Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО «ТИД «ДС». 2011. – 688 с.
3. *Малюк А.А., Пазизин С.В., Погожин Н.С.* Введение в защиту информации в автоматизированных системах. – М.: Горяч. линия-Телеком, 2011. – 148 с.: ил.
4. *Олифер В.Г., Олифер Н.А.* Сетевые операционные системы. – СПб.: Питер, 2012. – 544 с.: ил..
5. *Торокин А.А.* Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2011. – 960 с.: ил.
6. *Хорев А.А.* Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Уч. пособие. М.: Гостехкомиссия России, 2012. - 320 с.

В.Н. Смоляков, В.В. Сильченко

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЛВС РУДНЯНСКОГО ЛТЦ ВОЛГОГРАДСКОГО ФИЛИАЛА МРФ «ЮГ» ПАО «РОСТЕЛЕКОМ»

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: локальная вычислительная сеть, система защиты информации, информационная система, персональный компьютер, информационная безопасность, несанкционированный доступ.

Разработать систему защиты информации (ЗИ) ЛВС Рудянского ЛТЦ Волгоградского филиала МРФ «Юг» ПАО «Ростелеком». Для этого на основе проведенного обзора путей и методов ЗИ в информационной системы (ИС), включающего анализ структуры и основных видов деятельности Руднянского ЛТЦ, путей НСД и классификацию способов и средств ЗИ, каналов утечки информации и технических мер ЗИ в ИС, рассмотрены особенности ЗИ в ЛВС Руднянского ЛТЦ (проведен анализ рисков в ИС ЛВС, приведена модель нарушителя и основные понятия ИБ ЛВС, проанализирована защищенность узлов ЛВС Руднянского ЛТЦ). Проведена разработка системы ЗИ ЛВС Руднянского ЛТЦ (рассмотрены средства и способы ЗИ в ПК ЛВС Руднянского ЛТЦ, рекомендованы технические и программные средства ЗИ для установки в помещениях ЛТЦ и на ПК).

V.N. Smolyakov, V.V. Silchenko

DEVELOPMENT OF THE INFORMATION PROTECTION SYSTEM FOR LANTS OF RUDNYANSKY LETTER OF VOLGOGRAD BRANCH OF MYFF "SOUTH" PJSC "ROSTELECOM"

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

Key words: local computer network, information security system, information system, personal computer, information security, unauthorized access.

To develop the information security system of the LVS of Rudyansky LTC of the Volgograd branch of the MYFF "South" of PJSC "Rostelecom". To this end, based on the review of the ways and methods of the IP in the information system (IS), including the analysis of the structure and main activities of Rudnyanskiy LTC , The ways of the NSD, and the classification of methods and means of ZI, information leakage channels and technical measures of IP in the IS. The features of the ZI in the LAN of Rudnyanskiy LTC (the analysis of risks in the IS LAN, the model of the intruder and the basic concepts of the IS LAN, the security of the LAN nodes of Rudnyansky LTC) are analyzed. The development of the ZI LAN system of Rudnyanskiy LTC was carried out (the means and methods of ZI in the LAN of Rudnya LTC were considered, and the technical and software ZI tools were recommended for installation in the premises of LTC and PCs).

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 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) 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 защиты информации, 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 ИБ 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 комплексной системе ЗИ, 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, система ЗИ предназначена обеспечивать, с одной стороны, функционирование надежных механизмов ЗИ, а с другой - управление механизмами ЗИ. В связи с этим должна предусматриваться организация четкой и отлаженной системы управления ЗИ.

Все сказанное выше подтверждает актуальность разработки эффективной СЗИ для обеспечения ИБ в ЛВС. Решению этой проблемы и посвящен данный доклад. В качестве объекта для обеспечения ИБ выбрана ЛВС Руднянского ЛТЦ Волгоградского филиала МРФ «Юг» ПАО «Ростелеком», предоставляющая услуги цифровой связи, широкополосного доступа и Интернет и предоставляющее прочие персональные услуги населению Руднянского района Волгоградской области.

В Руднянском ЛТЦ развернута ЛВС по топологии «звезда» и технологии Fast Ethernet – см. рис. 1.

В настоящее время ИБ – 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 ЗИ в ЛВС должно уделяться постоянное внимание. К сожалению, абсолютной защиты не существует. Обход тех или иных средств ЗИ только вопрос времени, денег и желания. Поэтому при разработке системы ЗИ 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 разработанный программно-аппаратный комплекс для обеспечения ИБ ЛВС Руднянского ЛТЦ имеет возможность достаточно простой дальнейшей модернизации с учетом вновь возникающих угроз.

Для этого был проведен обзор путей и методов ЗИ в ИС, включающий анализ структуры и основных видов деятельности Руднянского ЛТЦ, путей НСД и классификацию способов и средств ЗИ, каналов утечки информации и технических мер ЗИ в ИС, основных направлений и мер ЗИ в ПК и ЛВС, выявление угроз информации в ИС.

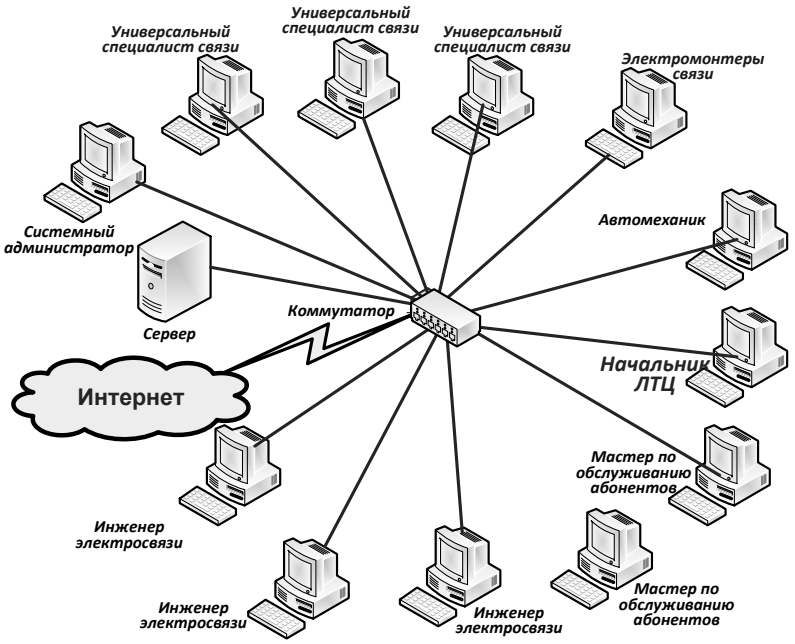


Рисунок 1 – Техническая структура ЛВС Руднянского ЛТЦ

Рассмотрены особенности ЗИ в ЛВС Руднянского ЛТЦ: проведен анализ рисков в ИС ЛВС; приведена модель нарушителя и основные понятия ИБ ЛВС; проанализирована защищенность узлов ЛВС Руднянского ЛТЦ и особенности идентификации и аутентификации пользователей ЛВС ЛТЦ; рассмотрены шифрование данных и организационные меры по обеспечению ИБ.

Проведена разработка системы ЗИ ЛВС Руднянского ЛТЦ. Для этого были рассмотрены средства и способы ЗИ в ПК ЛВС Руднянского ЛТЦ, рекомендованы технические средства ЗИ для установки в помещениях ЛТЦ, разработана СЗИ ЛВС Руднянского ЛТЦ аппаратно-программными средствами вплоть до структурной схемы ЛВС Руднянского ЛТЦ с установленными элементами предложенной системы ЗИ.

В качестве аппаратно-программных средств ЗИ ЛВС ЛТЦ предложено установить на все ПК аппаратный модуль системы ЗИ Secret Net, программный комплекс криптографической защиты File-PRO и антивирусную программу ESET NOD32 Antivirus. В серверной канал связи ЛВС ЛТЦ с Интернет дополнительно защищается межсетевым экраном Symantec Enterprise Firewall и программно-аппаратным комплексом Symantec Network Security 7100. Кроме того предлагается установить комплекс контроля и выявления средств НСД «ТОР» и комплекс виброакустической защиты «БАРОН». На универсальном техническом участке в зале, где располагается ЦАТС, предлагается установить модуль для защиты телефонных линий ПРОКРУСТ-2000, а также анализатор проводных коммуникаций LBD-50.

Была разработана структурная схема предложенной системы ЗИ ЛВС Руднянского ЛТЦ, реализация которой позволит значительно повысить защищенность ИС исследуемой ЛВС от влияния большинства негативных факторов, угроз, хищения информации или НСД к ней при сравнительно небольших затратах.

Таким образом, с учетом выбранных программно-аппаратных средств ЗИ, структурная схема разработанной системы ЗИ Руднянского ЛТЦ примет вид, приведенный на рис. 2.

На все 12 ПК ЛВС устанавливаются:

– антивирус ESET NOD32;
– аппаратный модуль системы ЗИ Secret Net;
– комплекс криптозащиты File-PRO.

В серверной канал связи ЛВС ЛТЦ с Интернет дополнительно защищается межсетевым экраном Symantec Enterprise Firewall и программно-аппаратным комплексом Symantec Network Security 7100. Кроме того будут установлены комплекс контроля и выявления средств НСД «ТОР» и комплекс виброакустической защиты «БАРОН». На универсальном техническом участке в зале, где располагается ЦАТС, предлагается установить модуль для защиты телефонных линий ПРОКРУСТ-2000, а также анализатор проводных коммуникаций LBD-50 (см. рис. 2).

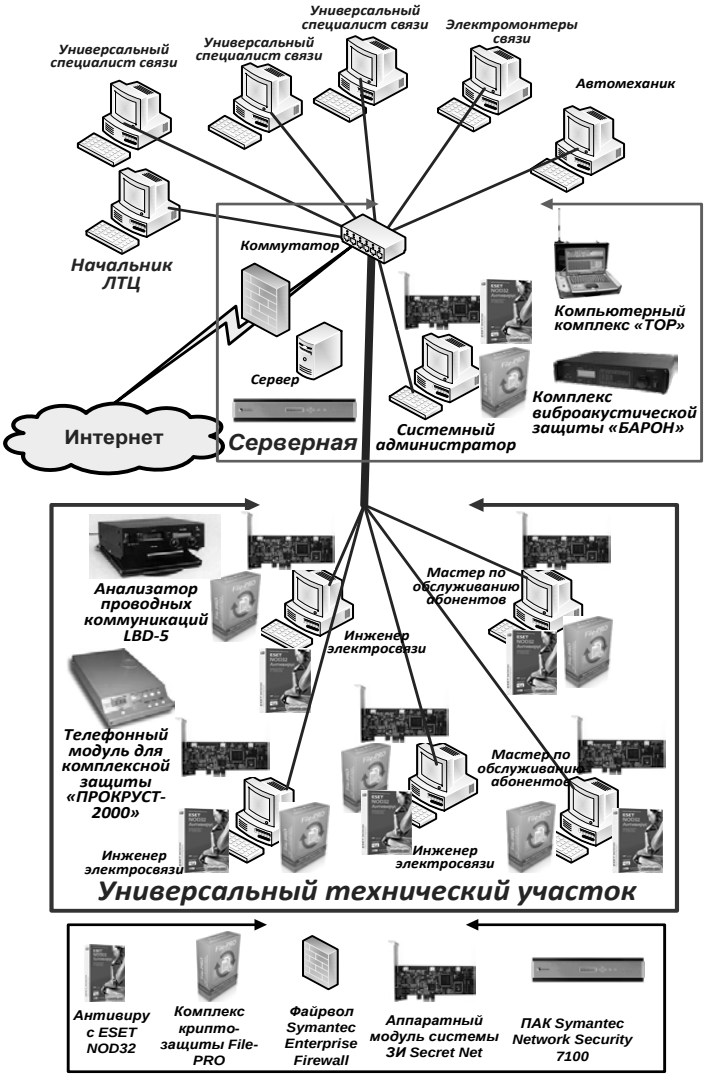


Рисунок 2 - Структурная схема разработанной системы ЗИ ЛВС ЛТЦ

СПИСОК ЛИТЕРАТУРЫ

1. Администратор безопасности сети, часть 2. «Научно-информационный центр проблем безопасности» - СПб., 2014. - 264 с.
2. Гостехкомиссия России. Сборник руководящих документов по защите информации от несанкционированного доступа. СИП РИА. – Москва, 2010 г.

3. *Боккер П.* Цифровая сеть с интеграцией служб. Понятия, методы, системы: Пер. с нем. М.: Радио и связь, 2010. – 212 с.
4. *Грибунин В.Г.* Комплексная система защиты информации на предприятии: учеб. пособие для вузов / - М.: Издательский центр «Академия», 2011. - 416 с.
5. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. – 458 с.

М.Г. Усынин, А.Ю. Опарин

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия.

Ключевые слова: защита информации, информационная безопасность, обеспечение безопасности от вредоносного ПО, криптографическая защита информации, цифровая подпись

В статье рассмотрены проблемы защиты информации и актуальные способы технической защиты информации в Российской Федерации.

M.G. Usynin, A.Yu. Oparin

INFORMATION PROTECTION AND INFORMATION SECURITY

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

Keywords: information security, information security, security against malicious software, cryptographic protection of information, digital signature

In the article are considered problems of information protection and actual ways of information protection in the Russian Federation

There is a wide range of information storage and processing systems nowadays, where in the process of their design, the factor of the information security of the Russian Federation storing confidential information is of particular importance. The threat of information protection has made the means of ensuring information security one of the mandatory characteristics of the information system. Such information systems include, for example, banking or legal systems of

safe workflow and other information systems for which the provision of information security is vital for the protection of information in information systems.

What is "protection of information from unauthorized access" or information security of the Russian Federation? Information security in the Russian Federation means the technique of protecting information from premeditated or accidental unauthorized access and thereby damaging the normal process of document turnover and data exchange in the system, as well as theft, modification and destruction of information.

The phrase "threats to the security of information systems" means real or potentially possible actions or events that are capable of distorting data stored in the information system, destroying them or using them for any purposes not provided for by the rules in advance.

The first division of the security threat of information systems into species

If we take a model describing any managed information system, we can assume that the disturbing effect on it can be random. That is why, considering threats to the security of information systems, it is necessary to immediately identify deliberate and accidental disturbances.

The complex of information protection can be disabled, for example, due to defects in hardware. Also, issues of information security are on edge due to incorrect actions of personnel who have direct access to databases, which entails a decrease in the effectiveness of information protection under any other favorable conditions for the implementation of the information protection measure. In addition, unintentional errors and other information system failures may occur in the software. All this negatively affects the effectiveness of protecting information of any kind of information security that exists and is used in information systems.

Protection of information from computer viruses involves information protection tools on the network, or more specifically software-but hardware information protection that prevents the unauthorized execution of malicious programs that attempt to seize data and send them to an attacker, or to destroy database information, but to protect information from computer Viruses is unable to fully reflect the attack of a hacker or a person called a computer pirate.

The task of protecting information and protecting information from computer viruses is to make it difficult or impossible to penetrate, both viruses and hackers, to sensitive data, for which the burglars in their counter-legal actions are searching for the most reliable source of secret data. And since hackers are trying to get the most reliable secret data with minimal costs, the task of protecting information is the attempt to confuse the attacker: the information security service provides him with incorrect data, the protection of computer information tries to maximally isolate the database from external unauthorized interference.

Protecting computer information from an attacker is the information security measures that need to be circumvented to gain access to information. The computer information security architecture is designed in such a way that an attacker faces many levels of information security: protecting the server by distinguishing between the access and the user authentication system and protecting the computer of the user who is working with sensitive data. Protecting the computer and protecting the server simultaneously allow you to organize a scheme for protecting computer information in such a way that it is impossible for the intruder to penetrate the system using such an unreliable means of protecting information on the network as a human factor. That is, even bypassing the protection of the database user's computer and moving to another level of information security, the hacker should correctly use this privilege, otherwise the server

protection will reject any of his requests for data and an attempt to bypass the protection of computer information will be futile.

Publications of recent years indicate that the technology of information protection does not have time to develop behind the number of abuse of authority, and the technology of information protection always lags behind in its development from the technologies that crackers use to take possession of someone else's secrets.

There are documents on information security describing the information circulating in the information system and transmitted through communication channels, but documents for the protection of information are continuously supplemented and improved, although even after the cybercriminals make more and more technological breakthroughs in the information protection model, It would not be difficult.

Today, to implement an effective information protection measure, it is required not only to develop a means of protecting information in the network and developing mechanisms for an information protection model, but implementing a system approach or an information security complex is a set of interrelated measures described by the definition of "information protection." This complex of information protection, as a rule, uses special technical and software tools to organize measures to protect economic information.

Types of information security, or rather the types of threats to information protection in the enterprise are divided into passive and active.

Passive information security risk is aimed at the illegal use of information resources and is not aimed at breaking the functioning of the information system. Passive information security risks include, for example, access to the database or listening to data transmission channels.

The active information security risk is aimed at disrupting the functioning of the operating information system through a targeted attack on its components.

Active types of computer security threats include, for example, physical inactivity of a computer or a violation of its operability at the software level.

The need for information security tools. Organization of information protection against unauthorized access.

Methods and means of information protection include organizational, technical and legal measures of information protection and information protection measures (legal protection of information, technical protection of information, protection of economic information, etc.).

Organizational methods of information protection and information protection in Russia have the following properties:

- Methods and means of information protection provide partial or complete overlapping of leakage channels in accordance with information security standards (theft and copying of information protection objects);
- The information security system is a unified, integrated information protection body that provides multi-faceted information protection;
- Methods and means of protecting information and the basics of information security include:
- Information technology security, based on the restriction of physical access to objects of information security by means of security measures and methods of information security;
- Information security of the organization and management of information security relies on the delimitation of access to objects of information security - the setting of rules for the delineation of access by information security authorities, encryption of information for its

storage and transmission (cryptographic methods of information protection, software for information protection and information security in networks);

- Information protection must ensure regular backup of the most important data and proper storage;
- Information security authorities should ensure the prevention of infection by computer viruses of the information protection object.

Unauthorized access is the unlawful deliberate acquisition of sensitive data by persons who do not have the right to access data. In this case, the protection of information lies on the shoulders of the law on the protection of information.

Protection of information from leakage through the most common ways of unauthorized access

Any complex system of information protection after an information security audit of an object is started starts to rely on the most common ways of intercepting confidential data, so it is important to know them in order to understand how a complex information security system is being developed.

Problems of information security in the field of technical protection of information:

- Interception of electronic emissions. The problem is solved by ensuring the protection of information transmitted via radio communication channels and data exchange of the information system;
- Forced electromagnetic irradiation (illumination) of communication lines to obtain parasitic carrier modulation. The problem is solved with the help of engineering protection of information or the physical protection of information transmitted through communication cable data lines. This also includes the protection of information in local networks, the protection of information on the Internet and technical means of information security;
  - the use of eavesdropping devices;
  - remote photography;
  - interception of acoustic emissions and restoration of the printer's text;
  - copying of media with overcoming of protection measures;
  - masking for a registered user;
  - masking for system requests;
  - use of software traps;
  - use of shortcomings in programming languages and operating systems;
  - Illegal connection to the equipment and communication lines of specially designed hardware that provides access to information;
  - malicious disabling of protection mechanisms;
  - Decryption of encrypted information by special programs;

Means of ensuring information security from malicious software

Ensuring the security of information systems from virus attacks is traditionally the use of such information protection services as anti-virus software and firewalls. These software solutions can partially solve the problems of information protection, but knowing the history of information protection, it is easy to understand that the installation of a system for protecting commercial information and information protection systems at the enterprise based on anti-virus

software does not yet solve the problem of information security of the society tomorrow. To increase the level of system reliability and ensure the security of information systems, it is also necessary to use other means of information security, for example, organizational protection of information, software hardware protection of information, hardware information protection.

Viruses are characterized by the fact that they are able to independently multiply and interfere with the computational process, gaining the ability to control this process.

It is important to understand that the majority of data thefts are not due to ingenious methods, but because of negligence and inattention, therefore the concept of information security includes: information security (lectures), information security audit, information security assessment, state information security, economic Information security and any traditional and innovative means of protecting information.

The protection of information and information security is based on the following principles:

- The construction of an information security system in Russia, as well as the information security of an organization, requires a systematic approach that presupposes an optimal proportion between the organizational, program, legal and physical properties of the information security of the Russian Federation, confirmed by the practice of creating information protection means by methods of protection Information applicable at any stage of the information processing cycle of the system.
- Continuous development of the information security management system. For any information security concept, especially if methods of protecting information in local networks and computer systems are used, the principle of continuous development is fundamental, because the information security of information is constantly exposed to new and new more sophisticated attacks, therefore Ensuring the information security of an organization can not be a one-time act, and the once-established technology for protecting information will be constantly improved following the growth of the level of breaking in payers.
- The principle of ensuring the reliability of the information security system and information security is the impossibility of reducing the level of system reliability during failures, failures, errors and break-ins (Information security - course work).
- It is imperative to ensure control and management of information security, to monitor and regulate protection mechanisms (download information protection).
- Providing a means to combat malicious software. For example, all kinds of programs for the protection of information and information security system against viruses.
- The economic feasibility of the use of information security system and state secret. The purpose of the system of protection of economic information is to exceed the amount of damage when hacking the information protection system at the enterprise over the cost of developing a means of protecting computer information, protecting banking information and comprehensive information protection.

Methods and means of information security, information security in computer networks. One of the methods of protecting information is to create a physical barrier to the attackers of the protected information (if it is stored on any media).

Access control is an effective method of protecting information that regulates the use of information system resources for which the concept of information security was developed.

Methods and systems of information protection, based on access control, include the following functions of information protection in local networks of information systems:

- Identification of users, resources, and personnel information security network;
- Recognition and authentication of the user on the input of credentials (this principle is the work of most models of information security);
- Admission to certain working conditions in accordance with the regulations prescribed for each individual user, which is determined by means of information protection and is the basis of information security of most typical models of information systems;
- Logging of users' access to resources, information security (rf) of which protects resources from unauthorized access and monitors the incorrect behavior of users of the system;
- Information security of banks and economic information security and other systems should ensure timely response to attempts to unauthorized access to data through signaling, failures and delay in work.

Cryptography is a science that studies and describes the information security model of data. Cryptography opens solutions to many problems of information security of the network: authentication, confidentiality, integrity and control of interacting participants.

The term "Encryption" means the transformation of data into a form that is not readable by humans and software complexes without the encryption-decryption key. Cryptographic methods of information protection provide means of information security, therefore it is part of the concept of information security.

The goals of information protection ultimately amount to ensuring the confidentiality of information and the protection of information in computer systems in the process of transferring information across the network between users of the system.

The protection of confidential information, based on cryptographic protection of information, encrypts data using a family of reversible transformations, each of which is described by a parameter called the "key" and the order that determines the order of application of each transformation.

The key component of the cryptographic method of information protection is the key, which is responsible for choosing the transformation and the order of its execution. A key is a sequence of characters that configures the encryption and decryption algorithm of a cryptographic information security system. Each such transformation is uniquely determined by a key that defines a cryptographic algorithm that ensures the protection of information and the information security of the information system.

One and the same cryptographic information protection algorithm can work in different modes, each of which has certain advantages and disadvantages that affect the reliability of Russia's information security and information security tools.

Protection of information in local networks and information security technologies, along with confidentiality, are also required to ensure the integrity of information storage. That is, the protection of information in local networks must transmit data in such a way that the data remains unchanged during the transmission and storage. To ensure that the information security of information ensures the integrity of data storage and transmission, it is necessary to develop tools that detect any distortions in the original data, for which redundancy is attached to the original information.

Information security in Russia with cryptography solves the issue of integrity by adding a certain control amount or a verification combination to calculate the integrity of the data. Thus,

again the information security model is cryptographic - dependent on the key. According to the information security assessment based on cryptography, the dependence of the ability to read data from a secret key is the most reliable tool and is even used in the information security systems of the state.

Sometimes users of the information system want to abandon their previous obligations and try to change previously created data or documents. The Doctrine of Information Security of the Russian Federation takes this into account and suppresses such attempts. Protection of confidential information using a single key is impossible in a situation when one user does not trust the other, because the sender can then refuse that the message was transmitted at all. Further, despite the protection of confidential information, the second user can modify the data and assign authorship to another user of the system. Naturally, whatever the software protection of information or the engineering protection of information, the truth can not be established in this dispute. The digital signature in such a system of information protection in computer systems is a panacea for the problem of authorship. The protection of information in computer systems with a digital signature contains 2 algorithms: to calculate the signature and to verify it. The first algorithm can be performed only by the author, and the second - is in the public access so that everyone can check the validity of the digital signature at any time.

Cryptographic protection and information security or cryptosystem operates according to a certain algorithm and consists of one or more encryption algorithms using special mathematical formulas. Also, the cryptosystem information protection system includes keys used by a set of data encryption algorithms, a key management algorithm, plaintext and a ciphertext.

The work of the program to protect information using cryptography, according to the RF information security doctrine, first applies an encryption algorithm to the text and generates a key for decryption. After that, the ciphertext is transferred to the addressee, where the same algorithm decrypts the received data into the original format. In addition, in the means of protecting computer information, cryptography includes procedures for generating keys and distributing them.

Symmetric or secret methodology of cryptography Protection of information in Russia

In this methodology, the technical means of information protection, encryption and decryption by the recipient and the sender use the same key, stipulated earlier even before the use of cryptographic engineering information protection.

In the case when the key was not compromised, in the decryption process the authentication of the author of the message will be automatically performed, since only he has the key to decrypt the message.

Thus, programs to protect information by cryptography assume that the sender and the addressee of the message are the only persons who can know the key and its compromise will affect the interaction of only these two users of the information system.

The problem of organizational protection of information in this case will be relevant for any cryptosystem that is trying to achieve the goal of protecting information or protecting information on the Internet, because symmetric keys need to be distributed between users safely, that is, it is necessary that the protection of information in computer networks where keys are transmitted, Was at a high level.

Any symmetric cryptosystem encryption algorithm of a software-based hardware security tool uses short keys and encrypts very quickly, despite the large amounts of data that meet the purpose of protecting information.

Means of protecting computer information based on the cryptosystem should use symmetric key management systems in the following order:

- The work of information security begins with the fact that first the protection of banking information creates, distributes and stores a symmetric key for organizational information protection;
- Further, an information security specialist or a sender of an information security system in computer networks creates an electronic signature by using the hash function of the text and adding the received hash string to the text that must be safely transferred to the information protection organization;
- According to the information security doctrine, the sender uses a fast symmetric encryption algorithm in the cryptographic information security tool along with a symmetric key to the message packet and an electronic signature that authenticates the cryptographic data encryption system user;
- The encrypted message can be safely transmitted even over unprotected communication channels, although it is better to do it as part of the work of information security. But the symmetric key must necessarily be transmitted through the communication channels within the software hardware protection of information;
- In the information security system, during the history of information security, according to the information security doctrine, the recipient also uses a symmetric algorithm to decrypt the packet and the same symmetric key that allows you to restore the text of the original message and decrypt the subscriber's electronic signature in the system Protection of information;
- In the information protection system, the recipient must now separate the electronic signature from the message text;
- Next, the recipient generates another signature using the same hash function calculation for the received text, and this does not end the information security work;
- Now the recipient compares received electronic signatures in order to check the integrity of the message and the absence of corrupted data in it, which in the information security area is called data integrity.

All asymmetric cryptographic means of information protection are the target object of attacks by a cracker operating in the field of information security through direct key enumeration. Therefore, in such an information security of the person or information psychological safety, long keys are used to make the process of searching keys so long that the hacking of the information security system will lose any sense.

It is absolutely not a secret even for someone who is making information protection of information that in order to avoid the slowness of asymmetric encryption algorithms, a temporary symmetric key is created for each message, and then only one is encrypted with asymmetric algorithms.

Systems of information psychological security and information security of the individual use the following procedure for using asymmetric keys:

- In the area of information security, asymmetric public keys are created and distributed openly. In the information security system of a person, a secret asymmetric key is sent to its owner, and an open asymmetric key is stored in the database and administered by the issuance center for certificates of the information protection system that is monitored by the information security specialist. Then, information security, which can not be downloaded free of charge anywhere, implies that both users must believe that such an information security system is

responsible for the safe creation, administration and distribution of keys that are used by the entire information security organization. Even more, if at each stage of information protection, according to the basics of information protection, each step is performed by different persons, then the recipient of the confidential message must believe that the key maker destroyed their copy and no longer provided these keys to anyone Still could download protection of the information transferred in system of means of protection of the information. This is how any information security specialist acts.

- Further, the basics of information protection provide that an electronic signature of the text is created, and the resulting value is encrypted by an asymmetric algorithm. Then, all the same information security fundamentals assume that the secret key from the ruler is stored in a string of characters and it is added to the text that will be transmitted in the information security and information security system because the electronic signature in the protection of information and information security can create an electronic signature.
- Then systems and information security solutions solve the problem of transferring the session key to the recipient.
- Further, in the system of information security means, the sender should receive an asymmetric public key of the issuer of certificates of organization and technology of information protection. In this organization and information security technology, interception of unencrypted requests for obtaining a public key is the most common attack of crackers. That is why in the organization and technology of information security can be implemented a system that confirms the authenticity of the public key certificates.

Thus, encryption algorithms assume the use of keys, which allows 100% protection of data from those users who do not know the key.

СПИСОК ЛИТЕРАТУРЫ

1. *Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.* Технические средства и методы защиты информации // Учебник для вузов. Под ред. А.П. Зайцева и А.А. Шелупанова

А.Н. Чикалов, А.И. Янкина

ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. МЕТОДЫ ОБНАРУЖЕНИЯ И БОРЬБЫ С ДАННЫМ ВИДОМ ЭКСПЛОЙТА.

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: стек, буфер, эксплойт, защита информации, стековый кадр, компьютерная память, переполнение буфера, шеллкод.

В статье рассмотрена проблема такого программного эксплойта, как переполнение буфера в стеке, представлены примеры реализации переполнения буфера в стеке, а также метод обнаружения и предотвращения данного вида угроз информационной безопасности.

A.N. Chikalov, A.I. Yankina

BUFFER OVERFLOW ON THE STACK. METHODS OF DETECTION AND FIGHT AGAINST THIS TYPE OF EXPLOIT.

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

Keywords: stack, buffer, exploit, data protection, stack frame, computer memory, buffer overflow, shellcode.

The article considers a problem of such program exploit as buffer overflow on the stack and bring examples of buffer overflows on the stack as well as methods of detecting and preventing this type of information security threats.

Currently, software exploits (a clever way to make the computer do what you need, even if the program that is currently running does not provide such operations) form the basis for hacking. One such exploit frequently used by attackers is a buffer overflow in the stack. To explain this concept, we introduce several definitions:

1) Computer memory is a part of a computer, a physical device or a medium for data storage used in calculations for a certain time.
2) Stack is a method of organizing memory according to the principle: "last in-first one". Most often, the stack is implemented in RAM from the last of its cells (with the maximum address). The stack stores addresses and presents the mechanism without which subroutines do not work.
3) A buffer is a memory area used to temporarily store data on input or output. Data exchange (input and output) can occur with both external devices and with processes within the computer.
4) Stack frame is placing data in the process stack, mixing program data with control data (including the address of the stack frame start and the return address of the executable function).

So what is this buffer overflow in the stack? Attacks related to such type of exploit as buffer overflow in the stack were the first type of buffer overflow attacks that gained great popularity in the "hacking world". There are thousands of vulnerabilities for attacks to buffer overflow in the stack in commercial software running on almost all platforms. Buffer overflows in the stack are mainly due to the vulnerability of the string processing routines that are present in standard C libraries. The most important concept is the location of a cell in memory. All individual memory bytes have a corresponding numeric address. When the processor reads or writes data to the main memory (RAM), it uses the memory address of the place from which the reading occurs or where the recording is made. System memory is used not only for storing data

but also the executable code, which presents the program itself, i.e. each of the functions used by the program also has an address.

It should be assumed that this results in some damage of the program data or complete loss of it, but the problem with the buffer overflow is much more serious: it causes an execution of the [arbitrary] code, so that an attacker can absolutely calmly get the user's rights. This is because the overflowed buffer will overwrite not only the data, but also some more important information stored on the stack, such as return addresses. The return address controls the choice of instruction the processor will execute, and time period it will take to execute the function. It is obvious that this would be some address inside the calling function itself, but if this value is overwritten by buffer overflow, it can point anywhere. If the attackers can control the buffer overflow, they can also control the return address. If they control the return address, they can tell the processor what to do next, or just perform whatever action they want.

The processor, for sure, does not have a convenient function to "compromise the machine", which an attacker could use, but it does not really matter. After all, even the buffer used to replace the return address can be also used to store a small part of the executable code, the so-called shellcode, which can download the threatening executable file, open the network connection, or fulfill any other wishes of the attacker.

In most cases, each program will use the same addresses in memory every time it runs, even if you reboot the machine, i.e. every time the position of the buffer on the stack will remain the same, and hence the value used to distort the return address will be the same. It is enough for an attacker to learn this address once, and then the attack will work on any computer executing the vulnerable code.

This is done because the program and its libraries are located in the same memory area every time they are started, even after rebooting and even on different computers. A curious thing in this process is that the library itself, from which the springboard takes place, does not require the call esp operator. It is only necessary for it to have 2 suitable bytes (in this case, with the values 0xff and 0xd4) following each other. They could be a part of some other function, or even just a number. For example, X86 instructions can be very long (up to 15 bytes!) and can have a location at any address. If the processor reads the instruction from the middle, then starting from the second byte of the four-byte instruction, for example, the result would be interpreted as a completely extraneous, but still valid, instruction, which makes the finding of useful trampolines simple enough.

But in rare cases, the attack can not set the return address exactly where it is required. Despite the fact that the location of objects in memory is very similar, it may slightly differ from machine to machine or from start to start. For example, the exact location of the attacked buffer can vary up and down in a few bytes, depending on the system name or its IP address, or because of some change made by the minor update of the program. To cope with this, it is useful to be able to specify a return address that is approximately correct, and high accuracy is not necessary.

This can be easily done using a technique called a "landing strip". Instead of writing a shellcode directly into the buffer, an attacker writes a large number of NOP instructions (meaning "no-op", ie, no operation -tells the processor to do nothing), sometimes hundreds, before an actual shellcode. To run the shellcode, the attacker needs to set the return address somewhere in between these NOPs. And if one hits the NOP area, the processor will quickly process them and start the actual shellcode.

The idea is to generate a command line that calls the notesearch program, passing an argument to it in single quotes. To do this, the string functions are used: strlen () to get the length of the string (to set the pointer to the buffer) and strcat () to add a single quote to the end of the string. Finally, the command line is executed using the system function. The buffer placed between the quotes is the main part of the exploit, the rest serves only as a means to deliver this harmful data.

How can we detect and prevent this kind of threat?

The answer is simple - only with the help of intrusion detection systems (IDS) you can detect and prevent attempts to use buffer overflow remotely, because in most cases the data intended to overflow buffer contains long arrays of No Operation (NOP or NOOP) instructions, and the IDS simply blocks all incoming packets with numerous consecutive NOPs. But nothing gives a 100% guarantee. This method of protection does not prevent a damage of the stack. However, in most cases it prevents the execution of the "payload" of the exploit. The program will not be able to insert a shell code into a write-protected memory, such as existing segments of an active shellcode, as it becomes unrealistic to execute instructions in non-executable memory, such as a stack or heap.

The problem of buffer overflows is typical for programming languages such as C and C ++, because they do not hide the details of low-level representation of buffers as containers for data types; therefore, in order to avoid buffer overflow, it is necessary to provide a high level of controlling writing and changing the program code, which manages the buffers. A use of libraries of abstract data types is one of the engineering approaches to preventing buffer overflow.

There are two basic types of data that enable a buffer overflow in these languages:

1) strings;
2) arrays.

It follows that the use of libraries for strings and list data structures that were designed to prevent and / or detect buffer overflows avoids many vulnerabilities.

In addition to the malicious threats mentioned above, a buffer overflow on the stack can also cause the program crash or hang, resulting in a denial of service. Some kinds of overflows, such as overflow in a stack frame, allow an attacker to load and execute an arbitrary machine code on behalf of the program and with the rights of the account from which it is executed.

Based on the article, we can conclude that the purpose of introducing a malicious error such as a buffer overflow on the stack is to control the execution of the attacked program in order to let an attacker execute a malicious code fragment that could be located in memory. In other words, perform actions that will allow executing an arbitrary code. There are many ways to prevent hacker attacks to a machine, but none of them protects the system completely, because new technologies are constantly being developed, which do not respond to these methods of protection. Despite the wide discussion of attacks to buffer overflow and a sufficiently large choice of technical information for attacks to various platforms, there are still many questions on this topic that should be studied. This paper discusses a number of methods that can be easily applied to hack software. In general, we found out that distortion of data in memory is a favorite method of hackers.

Perhaps the problem with such a kind of exploit as a buffer overflow on the stack will someday cease to be relevant if programmers stop using vulnerable string function calls from the libc library. However, currently there is no means to find an absolute solution for this problem.

REFERENCES

1. *Джеймс Фостер, Майк Прайс*. Защита от взлома: сокеты, эксплойты, shell-код = Sockets, Shellcode, Porting, & Coding. — М.: Издательский Дом ДМК-пресс, 2006. — С. 35, 532. — 784 с. — ISBN 5-9706-0019-9.
2. *Джон Эриксон*. 0x320 Переполнение буфера // Хакинг: искусство эксплойта = Hacking: The Art of Exploitation. — 2-е издание. — СПб.: Символ-Плюс, 2010. — С. 139. — 512 с. — ISBN 978-5-93286-158-5.
3. *David A. Wheeler*. Chapter 6. Avoid Buffer Overflow // [www.dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf Secure Programming for Linux and Unix HOWTO]. — 2004. — P. 71. — 188 p.
4. *Enrico Perla, Massimiliano Oldani*. CHAPTER 6 Windows // A Guide to Kernel Exploitation: Attacking the Core. — 2011. — P. 334. — 442 p. — ISBN 978-1-59749-486-1.

О.В. Швачко, И.С. Деркачев

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, информационная безопасность, угрозы безопасности, информационные системы персональных данных, информационное общество.

В статье рассмотрены основные меры обеспечения безопасности персональных данных в информационных системах, описаны основные этапы построения системы защиты информации при внедрении и эксплуатации информационных систем персональных данных.

O.V. Shvachko, I.S. Derkachev

THE ISSUES ON THE PROTECTION OF PERSONAL DATA IN INFORMATION SYSTEMS

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: information technology, information security, security threats, personal data information systems, information society.

The article considers basic measures to ensure the protection of personal data in information systems, described the main stages of development the information security system of personal data information systems.

Информационные технологии, внедряемые в повседневную деятельность человека, способствуют росту производительности труда. Однако, наряду с неоспоримым достоинством – возможностью автоматизации рутинной работы, технологии информатизации и автоматизации несут в себе угрозу утечки и неправомерного использования информации, циркулирующей в информационных системах. Следствием таких действий в отношении персональных данных могут быть финансовые потери и ущемление прав и свобод граждан, а когда речь идет о сведениях, составляющих государственную тайну – это угроза национальной безопасности.

Необходимость обеспечения безопасности персональных данных на современном этапе развития информационного общества – неоспоримый факт. Возросшие технические возможности по сбору и обработке персональной информации и развитие телекоммуникационных технологий выявляют новые угрозы, с точки зрения неправомерного использования персональных данных, например, когда речь идет о банковских вкладах или кредитных картах.

Обеспечение информационной безопасности является не тривиальной задачей, решение которой требует комплексного подхода. Рассмотрим основные аспекты.

Основа для решения задач обеспечения информационной безопасности задается на законодательном уровне. В Российской Федерации, как и в других развитых странах, приняты законодательные акты в области защиты персональных данных [1-4], которые определяют базовые понятия, общие правила и ответственность за их нарушение. В целях обеспечения прав граждан на личную тайну, законодательством регулируются правоотношения, связанные с обработкой персональных данных, как государственными и муниципальными органами, так и коммерческими организациями.

Закон [2] определяет следующие основные понятия:

– персональные данные (ПД) - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). Персональные данные относятся к категории конфиденциальной информации, а значит, подлежат защите от утечки и несанкционированного доступа;

– информационная система персональных данных (ИСПД) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

В соответствии с Законом [2] регулирующие и контрольные функции выполняют:

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - по выполнению требований законодательства и защиты прав граждан;
– Федеральная служба безопасности (ФСБ) - по организации и обеспечению криптографических средств при их использовании;
– Федеральная служба по техническому и экспортному контролю (ФСТЭК) - по обеспечению безопасности персональных данных не криптографическими методами.

Как известно [3], безопасность информации в информационной системе обеспечивается способностью этой системы сохранять конфиденциальность, целостность и доступность информации при её вводе, выводе, передаче, обработке и хранении, что в свою очередь достигается организационными и техническими мерами, направленными на исключение несанкционированного доступа, утечки информации по техническим каналам и программно-технических воздействий на технические средства. Для выработки конкретных мер по защите персональных данных необходимо понимать что, как и от кого защищать. С целью определения актуальных угроз для информационной системы персональных данных [4] разрабатывается частная модель угроз, учитывающая конкретные условия эксплуатации информационной системы. С этой целью ФСТЭК России разработаны нормативные документы [5-6], определяющие единый методический подход к определению угроз и разработке частных моделей угроз безопасности информации. При разработке частной модели необходимо учитывать как прямые угрозы, при осуществлении которых нарушается безопасность информации, так и косвенные, т.е. угрозы создающие предпосылки к возникновению прямых угроз. Основой для разработки частной модели служит базовая модель угроз, разработанная ФСТЭК России [5]. Далее необходимо оценить вероятность реализации выявленных угроз в конкретной информационной системе при исходном уровне защищенности этой системы. Подробный алгоритм определения актуальных угроз безопасности персональных данных описан в методике, разработанной ФСТЭК России [6]. Необходимо отметить, что в случаях внесения каких либо изменений в информационную систему персональных данных или выявления ранее неизвестных уязвимостей, частная модель угроз информационной безопасности должна быть пересмотрена.

После построения частной модели актуальных угроз безопасности информации проводятся мероприятия организационного, технического и контролирующего характера [7], направленные на исключение возможности реализации выявленных угроз или, по крайней мере, затруднения реализации на столько, чтобы затраты на реализацию угрозы превышали ценность информации.

К основным мерам организационного характера, направленным на повышение эффективности защиты информационной системы относятся:

- ограничение доступа посторонних лиц в помещения с размещенными техническими средствами информационной системы, в том числе исключение возможности просмотра через окна;
- обеспечение охраны технических средств и носителей информации от хищения и уничтожения;
- организация контроля доступа к автоматизированным рабочим местам и инфраструктуре информационной системы;
- разработка и утверждение организационно-распорядительной документации по разграничению, предоставлению и прекращению доступа к ресурсам информационной системы, правил действий пользователей и администраторов информационной системы, в том числе при возникновении нештатных ситуаций, правил регистрации событий безопасности, порядка резервного копирования и восстановления, порядка контроля работоспособности и эффективности системы защиты информации;
- исключение возможности доступа к информации при проведении ремонта или технического обслуживания технических средств обработки персональных данных, а также несанкционированного внесения изменений в аппаратную и программную часть информационной системы;

Внедрение вышеописанных административных мер позволяет заложить надежный фундамент для построения эффективной системы защиты персональных данных. Однако, применения организационных мер не всегда бывает достаточно. В целях нейтрализации угроз утечки персональных данных по техническим каналам применяется комплекс технических мер. В качестве первоочередного мероприятия необходимо провести проверку помещений и технических средств на предмет отсутствия аппаратных закладок, предназначенных для негласного съема информации. Во-вторых, необходимо уделить внимание обновлению программного обеспечения (ПО), в том числе антивирусного. Ведь устаревшее ПО может иметь много уязвимостей, которые помогут подготовленному злоумышленнику обойти любую систему защиты, какой бы совершенной она не была. В случае если для функционирования информационной системы используются телекоммуникационные сети общего пользования необходимо позаботиться о применении межсетевых экранов и средств криптографической защиты информации передаваемой по каналам (линиям) связи. Здесь необходимо отметить, что все применяемые технические средства, в том числе программные, должны быть сертифицированы ФСТЭК России. В случае применения средств криптографической защиты, такие средства должны иметь сертификат ФСБ России.

В заключение отметим, что применение организационных и технических мер защиты должно быть обосновано исходя из актуальных угроз в соответствии с эксплуатационными характеристиками информационной системы. Применение необоснованных мер защиты для нейтрализации неактуальных угроз усложняет работу пользователей информационной системы и ведет к увеличению стоимости её внедрения и эксплуатации. Недооценка актуальных угроз, в том числе косвенных, ведет к снижению эффективности системы защиты информации и как следствие к появлению каналов утечки персональных данных, последствия которой могут представлять большую опасность.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 27 июля 2006 года №149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798.
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ (ред. от 22.02.2017) «О персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_61801.
3. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения». Введ. 27.12.2006. – М.: Федеральное агентство по техническому регулированию и метрологии, 2006. – 8с.
4. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". URL: http://www.consultant.ru/document/cons_doc_LAW_137356/
5. ФСТЭК России. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». URL: http://fstec.ru/component/attachments/download/289.
6. ФСТЭК России. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». URL: http://fstec.ru/component/attachments/download/290.
7. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_146520/

Д.А. Яковлев, И.С. Синева

ЧАСТО ВСТРЕЧАЕМЫЕ ОШИБКИ ПРИ ПРОЕКТИРОВАНИИ И РЕАЛИЗАЦИИ СЕТЕВЫХ ПРОТОКОЛОВ ДЛЯ ОБМЕНА ДАННЫМИ

ФГОБУ ВПО Московский технический университет связи и информатики, Москва

Ключевые слова: сетевые протоколы, передача данных, сетевые атаки, сетевая безопасность.

В статье рассмотрены некоторые ошибки, которые часто допускаются на этапе проектирования или программной реализации сетевого протокола, позволяющие эксплуатировать их злоумышленниками с целью проведения различного рода атак.

D.A. Yakovlev, I.S. Sineva

COMMON MISTAKES IN DESIGN AND IMPLEMENTATION OF THE NETWORK PROTOCOLS FOR DATA EXCHANGE

Moscow Technical University of Communications and Informatics, Moscow

Keywords: network protocols, data transfer, network attacks, network security.

The article considers common mistakes in design and implementation of the network protocols, which can be used by attackers to make a machine or network application unavailable to its intended users.

Создавая современные приложения, разработчик так или иначе сталкивается с вопросом передачи данных по сетям связи. Возникает задача, либо спроектировать сетевой протокол прикладного уровня под собственные нужды, либо найти и воспользоваться наиболее подходящим вариантом с уже готовой реализацией.

В данной статье рассмотрены наиболее часто встречаемые ошибки, которые допускаются при проектировании и реализации сетевых протоколов для передачи данных в пакетных сетях связи, позволяющих провести атаки различного рода на конечное приложение. Список составлен на основе анализа и разбора протоколов взаимодействия различных проприетарных приложений. В целях безопасности названия приложений не приводятся, по возможности приведены примеры с обнаруженными ранее обществом аналогичными проблемами в других известных протоколах и приложениях.

Возраст и популярность протокола не дает гарантии на отсутствие уязвимостей в его архитектуре или в его конкретной программной реализации. При этом наличие недоработок характерно, как для приложений, где передача данных требуется только для выполнения небольшой функции, так и для приложений, в которых работа с сетью является строгой необходимостью и лежит в основе его предназначения.

Занимаясь внедрением протокола общения в свою программу, разработчик зачастую решает вопрос удобства и быстроты его интеграции, при этом не задумываясь над возможными проблемами, которые создает такая простота. Рано или поздно, совершенными допущениями начинают пользоваться злоумышленники. С течением времени это привело к тому, что безопасность стала одной из самых больших проблем существующего Интернета [1].

На транспортном уровне для передачи данных в основном применяются протоколы UDP и TCP. При реализации протокола для прикладного уровня необходимо учитывать особенности работы нижестоящих протоколов.

UDP не требует явной установки соединения, как следствие не гарантирует достоверность адреса источника запроса. TCP же наоборот, гарантирует достоверность источника запроса после установки соединения.

1. Размер ответа превышает размер первого запроса. Нередко встречается задача в сфере связи, когда клиенту необходимо получить единоразово информацию от сервера и на этом завершить общение. Например, клиент запрашивает состояние о каком-

нибудь объекте, а сервер в ответ отправляет всю информацию о нем.

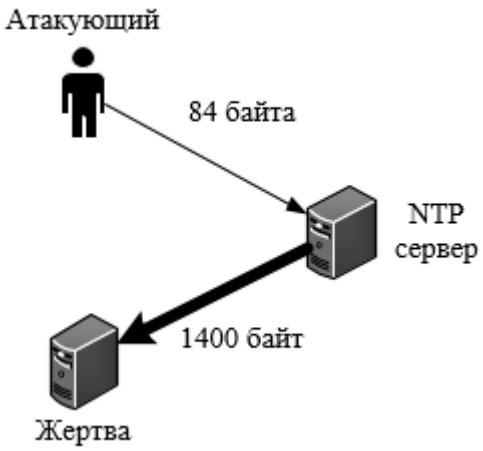


Рис. 1. Амплификация с помощью NTP сервера.

Общение происходит по схеме «вопрос-ответ» и она очень удобна для применения поверх UDP протокола, но в случаях, когда ответ от сервера превышает размер запроса, данную особенность начинают эксплуатировать злоумышленники.

Атакующий в качестве источника запроса использует IP-адрес жертвы и отправляет запрос небольшого размера на сервер. Сервер генерирует ответ, превышающий в несколько раз размер запроса и отправляет его на адрес жертвы (Рис. 1). Данный вид атак относится к классу амплификаций или иначе говоря, к атакам через отражение. Злоумышленник с помощью уязвимых приложений преумножает объем трафика, заполняя канал и ресурсы жертвы.

Одной из самых крупных атак данного вида на текущее время является атака, проведенная в 2014 году с помощью уязвимых NTP серверов. Скорость атаки в пике составляла 400 Гбит/с [2].

На текущий момент присутствует широкий список популярных протоколов, которые подвержены данной атаке. Среди них: DNS, NTP, RIPv1, SSDP, NetBIOS, Quake и др. Сдерживает усугубление ситуации тот факт, что атаки с помощью амплификаторов достаточно просто фильтруются за счет заранее известных сигнатур и номеров портов, на которых работают такие приложения, а также за счет выявления запросов с поддельным IP-адресом на стороне источника амплификации с помощью дополнительных инструментов [3]. Со временем некоторые из протоколов теряют свою популярность, но появляются новые приложения с протоколами, которые подвержены данной атаке.

2. Недостоверная проверка легитимности пользователя. Проверка достоверности источника запроса вытекает, как часть решения предыдущей проблемы, когда транспортный протокол не предоставляет гарантии легитимности запроса. В таких случаях либо прибегают к использованию TCP протокола, либо применяют принцип рукопожатия на прикладном уровне. Первым запросом клиент получает секретный ключ и в последующих пакетах он должен всегда передавать его. На основе сверки ключей сервер делает вывод о том, что клиент легитимный.

При использовании рукопожатия нередко встречаются случаи, когда сервер генерирует ключ по недостаточно устойчивому алгоритму для взлома. Попадаются самые разнообразные варианты:

- сервер для всех клиентов генерирует одинаковый ключ, создаваемый при запуске случайным образом или на основе адреса сервера (в худшем случае, ключ статично зашит в исходном коде);
- ключ генерируется на основе данных, полученных от клиента, например, на основе его порта или IP-адреса без добавления дополнительных случайных параметров;
- ключ генерируется на основе адреса клиента с добавлением дополнительных случайных параметров, но результативный размер ключа достаточно короткий;

– прикладной протокол требует проверку ключа, но в программной реализации проверка не добавлена.

Данные упущения либо сравнимы с тем, что проверка достоверности клиента фактически отсутствует, либо взлом алгоритма генерации ключа достаточно прост, что позволяет злоумышленнику самостоятельно генерировать ключ для любого адреса источника.

В 2016 году группа исследователей рассказала о том, как можно вычислить информацию о номере последовательности, идентифицирующей поток в TCP-соединении, что позволяло отправлять пакеты со стороны. Были наглядно продемонстрированы варианты эксплуатации данной уязвимости на примере внедрения стороннего содержимого в веб-страницу и для принудительного обрыва TCP-сессий. После обнародования информации проблема была устранена, она существовала в Linux с 2012 года [4]. Т.е. при условии того, что злоумышленник не обладает доступом к прослушиванию трафика, даже использование TCP протокола в некоторых случаях не сможет защитить от уязвимостей подобного рода.

3. Резервирование ресурсов по первому пакету со стороны пользователя. Протокол должен быть спроектирован так, чтобы в первом пакете от пользователя не передавались данные, необходимые для дальнейшего общения. Данная проблема, например, характерна для ранее упомянутого TCP протокола. При рукопожатии в первом пакете с флагом SYN передаются TCP опции, которые важны для последующего использования. В следствии чего сервер вынужден, как минимум, сохранять список данных опций.

Первые упоминания об атаках SYN-пакетами для исчерпания ресурсов конечного сервера были в 1996 году [5]. В настоящее время можно встретить новые приложения с протоколами прикладного уровня, работающими поверх UDP, подверженным атакам данного класса.

4. Журналирование информации о запросе. Иногда возникает потребность сохранять некоторую информацию о поступающих запросах в журнал. Например, для отладки и проверки работоспособности приложения, для ведения статистики и т.д. Данный пункт не имеет конкретного отношения к протоколам, но нередко встречаются ошибки, связанные с этим, в программной реализации.

В проанализированных приложениях в самых худших случаях журналирование происходило по первому пакету со стороны клиента, что делает приложение уязвимым перед любыми атаками с большим количеством запросов. Некоторые из приложений сохраняли отладочную информацию при получении некорректных данных.

Журналирование необходимо использовать только в самых важных случаях и только для запросов от легитимных пользователей. Необходимо не забывать отключать отладочные сообщения для публичных приложений, т.к. вывод сообщений и последующее сохранение их на диск считаются достаточно дорогостоящими операциями. Злоумышленник специально сформированными запросами может занять все процессорное время атакуемой системы, что затруднит доступ для легитимных пользователей.

Если ситуация сложилась таким образом, что в сети уже функционирует приложение с такой проблемой, то частично избежать эксплуатации данной уязвимости

можно путем построения лимитов на сетевом оборудовании совместно с системой детектирования DoS-атак [6].

5. Отсутствие шифрования. Важность присутствия шифрования зависит от цели использования приложения. В некоторых случаях необходимо хотя бы обезопасить процесс авторизации, чтобы уменьшить шансы для злоумышленника получить доступ к чужой учетной записи и представиться другим пользователем. В других случаях есть потребность в шифровании абсолютно всего трафика.

Данный тип атак относится к классу man-in-the-middle (MITM). Круг применения достаточно широк и многообразен. Самым распространенным протоколом прикладного уровня, уязвимым перед атаками данного класса, является HTTP.

К особо критичным случаям можно отнести процедуру обновления программного обеспечения, когда разработчик позволяет производить загрузку по нешифрованному каналу без дальнейшей проверки цифровой подписи загруженных файлов. Допущенные ошибки подобного рода позволяют злоумышленнику подменить ПО на вредоносное. На практике известно, что такие проблемы встречались в антивирусах [7], мобильных приложениях, сетевом оборудовании и др. не менее важных продуктах.

6. Доверие данным от пользователя. Все данные поступающие со стороны пользователя необходимо тщательно проверять на соответствие протоколу и быть внимательным при их обработке.

Наивным вариантом является доверие, основанное на логике, что если клиент и сервер являются проприетарными с закрытым исходным кодом, то можно более лояльно относиться к проверке передаваемых данных.

Ошибки, допущенные на этапе разбора сетевого трафика, зачастую сложно поддаются диагностике. При наиболее благоприятном развитии событий приложение завершит свою работу с ошибкой без каких-либо дальнейших последствий. В наихудшем варианте с помощью специально сформированного запроса можно получить доступ к целевой системе.

За последние годы одной из широко известных уязвимостей была ошибка, допущенная в популярной библиотеке OpenSSL с открытым исходным кодом, используемой для шифрования данных. Из-за недостающих проверок в коде одной из процедур расширения Heartbeat для протокола TLS/DTLS была доступна возможность чтения данных из оперативной памяти конечного сервера с помощью специально сформированного запроса [8].

7. Отсутствие кэширования ответов на ресурсоемкие запросы. Если построение ответа на запрос занимает значительную часть времени и вычислительных ресурсов, в таком случае необходимо предусмотреть возможность, как со стороны протокола, так и со стороны программной реализации, возможность кэширования ответов.

Кэширование должно быть обязательно со стороны сервера и опционально на стороне клиента. В ином случае, даже при атаках с небольшим количеством запросов со стороны злоумышленника, сервер будет затрачивать все ресурсы на построение ответов, что затруднит доступ для легитимных пользователей.

Каждый год появляется большое число новых приложений, работающих с сетями

передачи данных. Кто-то использует готовые протоколы высокого уровня, другие же предпочитают разрабатывать протокол под свои нужды. В обоих случаях допускаются ошибки, либо на этапе проектирования, либо на этапе программной реализации. Ошибки допускают как индивидуальные разработчики, так и крупные компании.

Важно уметь достигать баланса, чтобы протокол успешно решал задачу передачу данных, его реализация не была избыточно затруднительной, при этом не допуская возможность злоумышленникам использовать приложение для осуществления атак.

СПИСОК ЛИТЕРАТУРЫ

1. *Синева И.С.* Будущий интернет: сетевой подход // Фундаментальные проблемы радиоэлектронного приборостроения. – 2010. – Том 10. – № 1-3. – С. 237-240.
2. DDoS Attack Hits 400 Gbit/s, Breaks Record. // 2014. URL: http://www.darkreading.com/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787. (Дата обращения: 20.03.2017).
3. *Яковлев Д.А., Синева И.С.* Построение виртуализированной системы фильтрации поддельных сетевых пакетов с использованием Intel DPDK // T-Comm: Телекоммуникации и транспорт. – 2016. – Том 10. – № 8. – С. 30-35.
4. CVE-2016-5696. URL: https://security-tracker.debian.org/tracker/CVE-2016-5696. (Дата обращения: 21.02.2017).
5. TCP SYN Flooding and IP Spoofing Attacks. // 1996. URL: https://www.cert.org/historical/advisories/CA-1996-21.cfm. (Дата обращения: 20.03.2017).
6. *Яковлев Д.А., Синева. И.С.* Детектирование DOS-атак с помощью генетического алгоритма и нечеткой логики // Фундаментальные проблемы радиоэлектронного приборостроения. – 2015. – Том 15. – № 5. – С. 288-291.
7. Эксплуатация уязвимости в процедуре обновления DrWeb. // 2014. URL: https://habrahabr.ru/post/220113/. (Дата обращения: 23.02.2012).
8. CVE-2014-0160. // 2014. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160. (Дата обращения: 19.03.2017).

А.С. Артеменкова, А.И. Момот

ПРИМЕНЕНИЕ СИСТЕМЫ БЕРЕЖЛИВОГО ПРОИЗВОДСТВА НА ПРЕДПРИЯТИЯХ ПОЧТОВОЙ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова статьи: система бережливого производства, почтовая связь, эффективность, технологии, конвейер, бизнес, принципы

Рассматриваются вопросы сущности системы бережливого производства, практики ее применения и возможности использования на предприятиях почтовой связи в России. Приведены расчеты эффективности потока создания потребительской ценности продукции

A.S. Artemenkova, A.I. Momot

APPLICATION OF THE LEAN PRODUCTION SYSTEM AT THE ENTERPRISES OF POSTAL COMMUNICATION

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

Keywords: lean manufacturing, postal services, efficiency, technology, pipeline, business, principles

Discusses the nature of the lean production system, the practice of its application and the possibility of using the postal enterprises in Russia. The calculations of the efficiency of the flow of creation of consumer value products

Актуальность темы. В настоящее время большое значение приобретают новые управленческие системы, которые становятся важным резервом повышения эффективности и качества деятельности любого предприятия. Особенно актуальным это становится в условиях постоянной конкуренции. Одним из способов укрепления своих

позиций на рынке за счет сокращения затрат на осуществление производства является трансферт современных прогрессивных технологий управления.

В обществе сформировалось мнение о том, что важным фактором в повышении эффективности организации труда, привлечение разрозненных и малоэффективных отдельно взятых работников в высокопроизводительные группы становится постоянное совершенствование форм организации производства через применение известных технологий и систем менеджмента. Одной из таких современных управленческих технологий является система бережливого производства.

Актуальность внедрения концепции бережливого производства на предприятиях высокая, мировое сообщество давно обратило свой взгляд на японскую идею и ее реализации. Бережливое производство - это такая организация финансовой, хозяйственной системы разработки, проектирования, планирования, производства и реализации продукции или услуги, которая позволяет выпускать продукцию высокого качества с наименьшими затратами, в нужном количестве и на заданный срок. Причем создание системы бережливого производства позволяет избавиться от 80% расходов.

Целью исследования данной статьи описание опыта внедрения системы бережливого производства на предприятиях отрасли связи в целях повышения эффективности деятельности предприятий.

Проблемы выбора нужной методики внедрения новых технологий управления стоят особенно остро, поскольку от их решения зависит повышение способности предприятий стать более конкурентоустойчивыми к различного рода потрясениям.

Известная в настоящее время система управления производством под названием система Бережливого производства вышла из одной из самых эффективных управленческих технологий – Производственной системы Тойоты, которая получила распространение в мире во второй половине прошлого столетия. Под этой системой понимается такая организация финансовой, хозяйственной системы разработки, проектирования, планирования, производства и реализации продукции или услуги, которая позволяет выпускать продукцию высокого качества с наименьшими затратами, в нужном количестве и на заданный срок. Причем создание данной системы позволяет сократить до 80% расходов.

До середины прошлого века в мире господствовала идеология массового производства, получившая развитие на основе концепции Форда-Тейлора, заключавшаяся в том, что процессы производства на 3/4 представляют собой механизм, в соответствии с которым, люди должны были работать в производственной системе как элементы хорошо отлаженного механизма [1]. На этой основе получили развитие идеи заводов-автоматов и «безлюдных технологий», в которых участие персонала и, соответственно, человеческого труда, сводилось к минимуму.

Создавшееся в начале прошлого века массовое производство на тот момент на основе использования конвейерного производства позволило выпускать продукции в значительно большем количестве, и более дешевой по цене, что соответствовало существовавшим на тот период потребностям. Однако по мере развития общества, повышения его благосостояния и расширения потребностей массовое производство перестало удовлетворять потребителя, ставшего более разборчивым и привередливым.

По сравнению с теорией массового спроса Форда-Тейлора, опиравшейся на концепцию «поточно-конвейерное производство» Производственная система Тойоты стала революционным подходом в сложившихся условиях.

На подавляющем большинстве промышленных предприятий России в основе производственных систем лежат принципы, общие с принципами Производственной системы Форда-Тейлора, построенной еще в начале прошлого века.

Более глубокий анализ свидетельствует о том, что, происходящая трансформация не сводится лишь к вышеперечисленным изменения, а обязывает переосмыслить логику и технологию производства и ведет к переменам не только в ментальности, но и к изменению культуры организации [4, с.52]. Принципиальный путь решения этих задач состоит в увеличении эффективности бизнеса путем непрерывной оптимизации производственной системы предприятия и снижения всех видов затрат.

Сегодня в мире приобрели распространение следующие основные подходы относительно повышения бизнес эффективности предприятия: Производственная система Тойоты; система (технология) бережливого производства; Теория ограничений; Всеобщее обслуживание оборудования и др.

В табл. 1 представлена сравнительная характеристика ремесленного, массового и бережливого производства. При сопоставлении типов производства можно наблюдать, прежде всего, изменения в степени разделения труда, квалификации рабочей силы, организационной структуре, отношению к потребителю и во взаимоотношениях в организации.

Таблица 1-Сравнительная характеристика ремесленного, массового и бережливого производства [Составлено на основе 2; 3]

Типы производства			
Параметры	Ремесленное	Массовое	Бережливое
Степень разделения труда	Владелец, менеджер, производитель являются одним и тем же лицом	Владелец, менеджер, изготовитель являются разными лицами. Менеджер и изготовитель находятся на разных уровнях организации	Владелец, менеджер, изготовитель являются разными лицами. Менеджер и изготовитель - одна команда
Квалификация персонала	Высокая	Низкая	Высокая
Организационная структура	Плоскостная, децентрализованная, гибкая	Вертикальная, централизованная, жесткая	Горизонтальная, командная, гибкая
Адаптивная способность	Высокая	Низкая	Высокая
Использование ресурсов	Рациональное	Нерациональное	Рациональное

Продолжение таблицы 1

Оборудование	Низко производительное общего назначения для всех операций	Высокопроизводительное, узкоспециализированное, сложное для переналадки	Высокопроизводительное широко специализированное, легкое для переналадки
Отношение к потребителю	Изготавливает именно то, что нужно потребителю	Изготавливает то, что может, и уговаривает потребителя, что это именно то, что ему нужно	Изготавливает именно то, что нужно потребителю
Производительность	Низкая	Высокая	Высокая
Стоимость	Высокая	Низкая	Низкая
Степень творчества	Высокая	Низкая	Высокая
Взаимоотношения в организации	Сотрудничество	Подчинение	Сотрудничество

Наиболее известной из них является Производственная система Тойоты, основная задача которой заключалась в том, чтобы связать воедино и обеспечить выравнивание, синхронизацию и производство в потоке единичных изделий на начальных процессах.

В ее основе находится философия. Причины успеха этой системы заключаются в обеспечении стабильного выпуска высококачественной продукции при неизменной операционной эффективности компании на основе последовательного применения систем и технологий **(**Just in time («Точно вовремя»); Kanban (Система «канбан»); Jidoka («Дзидока - интеллектуальная автоматизация»); Andon (Андон) - сигнальная система для остановки линии. Сравнительная характеристика принципиальных подходов к построению системы Бережливого производства представлена в таблице 2.

Таблица 2

Сравнительная характеристика принципиальных подходов к построению системы Бережливого производства

Установки	Основные факторы				
	Японский подход	Американский подход	Европейский подход	Россий подход	
Базовая ориентация	Тойота Production System (TPS)	Lean Production	Lean Production	Массовое производство	Бережливое производство

Продолжение таблицы 2

Цель	При медленном внедрении получение более высоких, устойчивых и надежных результатов	Получение быстрых бизнес-результатов	На основе синтеза управленческих технологий многих стран получение устойчивых бизнес-результатов	Получение быстрых результатов	На основе синтеза создание оптимального комплекса управленческих технологий для получения устойчивых бизнес-результатов
Порядок внедрения	Снизу -вверх	Сверху- вниз	Сверху- вниз	Сверху- вниз	Сверху- вниз Снизу -вверх
Основные разработчики	Весь персонал предприятия	Команда менеджеров	Команда менеджеров совместно с мотивированным персоналом	Команда менеджеров	Команда менеджеров совместно с мотивированным персоналом
Подготовка персонала	Вовлечение в процесс всего персонала, включение интеллекта каждого работника в рациональную организацию его рабочего пространства, а затем и производственного процесса	Использование рабочей силы с более низкой квалификацией, осуществление ускоренной их подготовки и переподготовки с темпами, соответствующими темпам роста производства	Обеспечение мотивированного участия персонала в организации оптимальных форм работы	Использование рабочей силы с более низкой квалификацией, осуществление ускоренной их подготовки и переподготовки с темпами, аналогичными росту производства	Повсеместное обучение и внедрение новой философии для обеспечения мотивированного участия персонала в осуществлении всех видов деятельности.

Другим важным направлением является стремления к стабильному изменению (совершенствованию) на основе незначительных по стоимости, но непрерывных улучшений. Данный метод получил название Кайдзен. Теперь технология бережливого

производства распространяется не только на само предприятие, но и на всех окружающих ее заинтересованных лиц (потребителей, поставщиков, партнеров, и в целом общество).

Наиболее подробно и наглядно суть идеи бережливого производства была изложена труде Д. Вумека и Д.Джонса «Бережливое производство» [5], в котором предлагается определять «бережливое производство» как процесс, состоящий из пяти этапов (принципов):

1. Определение ценности продукта для клиента (покупателя);
2. Составление потока создания потребительской ценности;
3. Создание процесса непрерывности потока;
4. Осуществление принципа «вытягивания» от клиента;
5. Обеспечен6ие постоянного стремления к совершенству

До настоящего времени не существует общепризнанных универсальных методик расчета эффективности внедрения новых технологий управления. Однако уже разработаны методики расчета эффективности отдельных составных частей таких технологий. Но и они имеют достаточно много недостатков. Например, методики расчета, связанные с затратами на качество [6 с.6-7]. Следует учесть, что эти методики разрабатывались для оценки эффективности внедрения систем управления качеством. В настоящее время расширяется практика разработки и уже разработаны методики расчета эффективности, например, технологии Бережливого производства для отдельных предприятий различных отраслей: методика оценки эффективности внедрения Бережливого производства ОАО «КАМАЗ» [7]; методика оценки экономической эффективности внедрения технологий Бережливого производства ОАО «Российские железные дороги» [8]. Также заслуживают внимания качественные методы оценки эффективности инноваций [9]. Однако такие методики также достаточно сложны для применения, так как предусматривают большую подготовительную работу.

Для практического использования целесообразней использовать расчет отдельных составляющих новых технологий управления, в т.ч. отдельных процессов на основе приведенной ниже формулы (1).

$$Э_п = \frac{T_1 + T_2 + T_3 + \ldots T_n}{T} \times 100\% \qquad (1)$$

Где:

$Э_п$ – эффективность потока создания ценностей;

T_1; T_2; T_3; T_n – время проведения каждой операции;

T - полное время прохождения изделия по всему потоку

Таким образом, эффективность потока создания потребительской ценности продукции можно рассчитать, как суммарное время операций, прибавляющих ценность, деленное на полное время прохождения продукта по всему потоку.

Сделанные расчеты на примере движения почтовой корреспонденции с момента выемки писем из почтового ящика до доставки его непосредственному потребителю в сортировочный центр Ростовского-на-Дону почтамта показывают, что в среднем эффективность потока создания ценности может составить 69,8%. Данный показатель выше критерия, установленного для процесса, характеризующегося как бережливое

производство. В соответствии с общепринятой практикой бережливым считается такой процесс, у которого эффективность процесса превышает 25% [10]. Однако эффективность каждого отдельного этапа прохождения может существенно отличаться друг от друга.

В Российской Федерации технологии бережливого производства достаточно широко используются и доказали свою эффективность как в промышленности так и в сфере услуг. В сфере инфокоммуникаций данная технология пока не получила широкого распространения, но динамика в заинтересованности в современных технологиях уже наблюдается.

Особенно важным является внедрение бережливого производства в сфере почтовых услуг, где сроки доставки корреспонденции до сих пор являются самым болевым моментом всей ФГУП «Почта России» [11].

Приведенный в главе анализ движения почтовых отправлений с момента выемки писем из почтового ящика до доставки его получателю свидетельствует о значительных резервах по сокращению времени доставки. Особенно важным это будет не только для крупных автоматизированных сортировочных центров (АСЦ), но и для относительно небольших сортировочных центров региональных и городских масштабов.

СПИСОК ЛИТЕРАТУРЫ

1. *Лайкер Дж.* Дао Тойота: 14 принципов менеджмента ведущей компании мира [пер. с англ.] // Дж. Лайкер. - М.: Альпина Бизнес Букс, 2008. - 402 с.;
2. *Адлер Ю.П.* Бережливое производство: прошлое, настоящее, будущее// Ю.П. Адлер, В.Л.Шпер / МИСиС, Москва, 2004;
3. *Голяков С.М.* Современные производственные системы предприятий [Електронний ресурс]/ С.М.Голяков.– Режим доступу: http://www.ibl.ru/konf/151211/proizvodstvennie-sistemy-predprijatiy.html
4. *Адлер Ю.П.* Что век грядущий нам готовит? (Менеджмент 21 века - краткий обзор основных тенденций) // Ю.П. Адлер, И.З.Аронов, В.Л.Шпер / Надежность и контроль качества (Методы менеджмента качества), 1999, №1, с.26-46. Перепечатано в: Стандарты и качество, 1999. - № 3. — С. 52-60
5. *Вумек Дж.* Бережливое производство: как избавится от потерь и добиться процветания вашей компании //[пер. с англ.]/ Дж.Вумек, Д.Джонс. – М.: Альпина Бизнес Букс, 2004 – 473 с.
6. *Шоттмиллер Дж.* Затраты на качество стимулируют процессы //Дж. Шоттмиллер // Методы менеджмента качества. – 2003. – № 2. – С. 4-9.
7. *Адлер Ю. П.* Бережливость не роскошь, а средство выживания [Електронний ресурс] / Ю.П. Адлер, В.Л.Шпер. – Режим доступу: http://www.markus.spb.ru/biblioteka/shper-berezh.shtml.
8. Об утверждении методики оценки экономической эффективности

внедрения технологий Бережливого производства [Електронний ресурс] / Распоряжение от 29 декабря 2012 г. N 2768р ОАО «РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ». – Режим доступу: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=551113.

9. *Кузовкова Т.А.* Качественные методы оценки эффективности инноваций и развития инфокоммуникаций: Монография// Т.А Кузовкова, Д.В. Кузовков, А.Д. Кузовков/ – М.: ООО «ИД Медиа Паблишер», 2016. – 163 с.
10. *Ефимычев Ю.И.* Реализация резервов развития промышленного предприятия на основе концепции бережливого производства// Ю.И. Ефимычев, Ю.О. Плехова //Экономика и финансы/Вестник Нижегородского университета им. Н.И. Лобачевского, 2007, № 1, С. 223–227/
11. Кузовкова Т.А., Тимошенко Л.С. Анализ и прогнозирование развития инфокоммуникаций. – 2-е изд, перераб. и доп. - М.: Горячая линия – Телеком, 2016. – 174с.

А.Х. Бабаян, П.В. Лобзенко

ИНТЕРАКТИВНОЕ ОБУЧАЮЩЕЕ ПРИЛОЖЕНИЕ ПО ДИСЦИПЛИНЕ «ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ»

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: обучающая программа, интерактивность, информационные технологии, дистанционное обучение.

Представлено разрешение проблемы формирования полноценного интерактивного пособия в среде объектно-ориентированного языка Delphi. Характерной, отличительной чертой исследования считается полноцикловый образ подачи материала вида «тест – теория-практика-тест», что позволило обеспечить полностью самостоятельное изучение дисциплины.

A.H. Babayan, P.V. Lobzenko

AN INTERACTIVE TUTORIAL ON THE SUBJECT "TECHNOLOGY OF PROGRAMMING"

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

Key words: training program, interactivity, information technologies, distance learning.

The resolution of the problems of forming a full-fledged interactive manual in the environment of the object-oriented language Delphi is presented. A characteristic distinctive

feature of the study is the full-cycle image of the material of the "test-theory-practice-test" kind of material, which made it possible to provide a completely independent study of the discipline.

В наше время количество систем, предназначенных для обучения с использованием электронных форм передачи материала, неизменно увеличивается. Таким образом, в силу вступает новая тенденция обучения, основанная на развитии открытого, дистанционного образования, технологической основой которого являются информационные и телекоммуникационные технологии [1, 2]. Дистанционное обучение позволяет обучаться в своем темпе, исходя из личных потребностей в образовании. Поэтому, представленная разработка интерактивной обучающей программы по дисциплине «Технология программирования» является актуальной и востребованной.

В качестве языка программирования был выбран универсальный язык высокого уровня (ЯВУ) Delphi [3]. Он имеет возможность решения широкого класса задач, возможность работы с базами данных, простоту изучения.

Приложение построено на основе Delphi-Forms, или их еще называют «Windows-Forms». При создании графического интерфейса пользователя (ГИП) происходит наследование класса TForm с обширным набором шаблонов создания ГИП. Далее, основная форма приложения наполняется необходимыми средствами управления и отображения материала (листинг 1).

Листинг 1- Фрагмент заполнения основной формы приложения

```
TForm1 = class(TForm)
   GroupBox1: TGroupBox;
   TreeView1: TTreeView;
   WebBrowser1: TWebBrowser;
   MainMenu1: TMainMenu;
   N1: TMenuItem;
   N2: TMenuItem;
   N3: TMenuItem;
   Splitter1: TSplitter;
```

Контент, наполняющий приложение, представляет файлы в формате html, в которых организовано ссылочное связывания блоков изучаемого материала. Это является очень удобным, т.к. материалы для изучения хранятся в отдельной директории и могут быть легко модифицированы, при необходимости.

Одним из главных достоинств обучающей программы является большое количество гиперссылок, которые позволяют после изучения теоретических основ перейти к практическим работам и при необходимости вернуться в необходимую часть лекции (рис. 1).

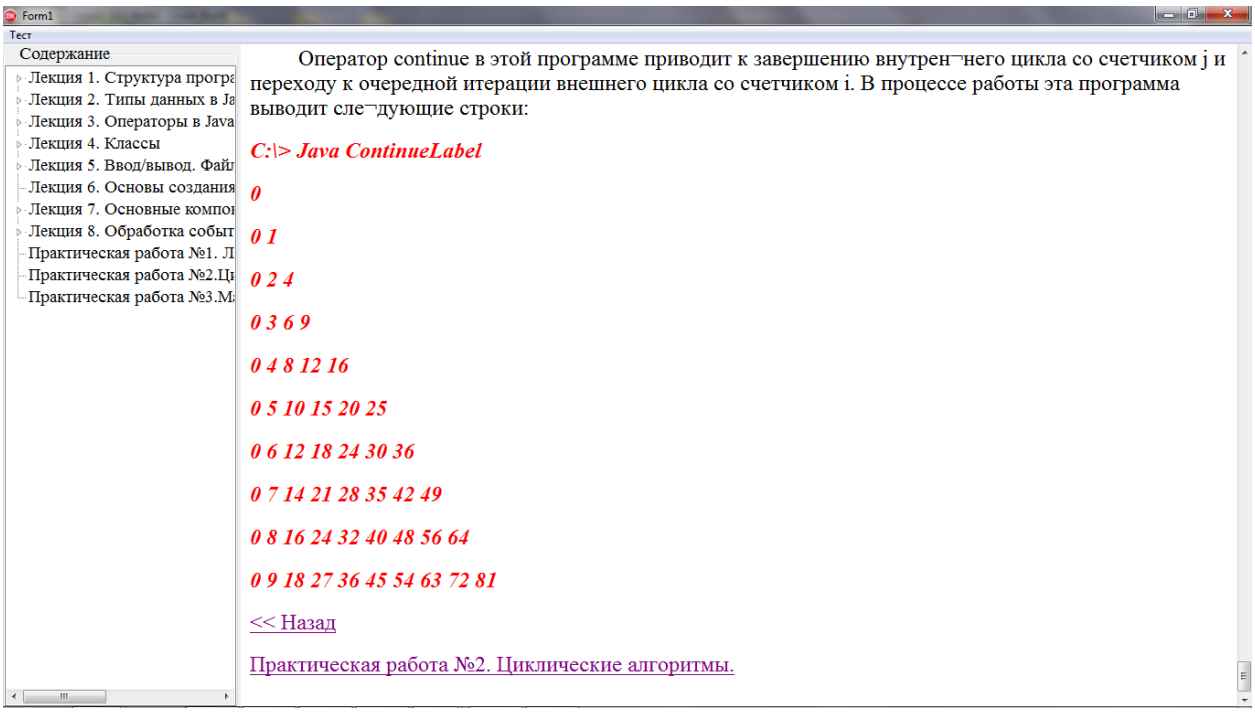


Рисунок 1- Пример перехода по гиперссылкам

В практической части приложения имеются тестовые варианты выполнения заданий. Они снабжены текстом программы, блок-схемой ее алгоритма и действующим ресурсом, куда можно ввести данные и получить результат решения задачи (рис.2).

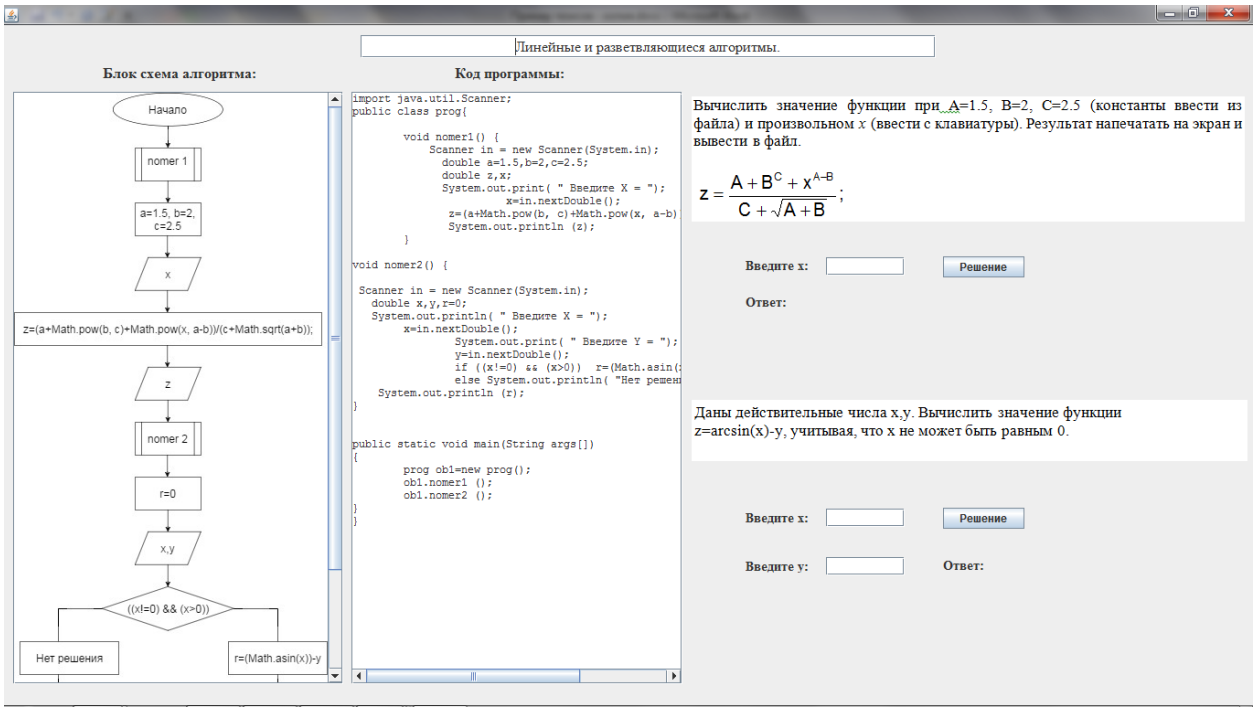


Рисунок 2- Интерфейс расчетного окна практической части приложения

В дополнение ко всему, имеется модуль тестирования, позволяющий проверить остаточные знания, а результаты проверки хранятся в базе данных и ими можно воспользоваться для определения материалов, требующих углубленной проработки.

Таким образом, разработанная обучающая программа имеет следующие преимущества:

1. Является интерактивной, что дает возможность обучающимся контролировать скорость прохождения учебного материала.
2. Имеет понятный, информативный, удобный интерфейс, не требующий отдельного обучения использованию.
3. Есть встроенная система тестирования обеспечивает возможность обучающимся проверить уровень своих знаний и тем самым следить за изучением материала.
4. Является простой в использовании и сопровождении (не требует затрат на ее создание и сопровождение).

СПИСОК ЛИТЕРАТУРЫ

1. Grand Class. Дистанционное обучение. [Электронный ресурс] URL: http://grandclass.net/
2. Дистанционные образовательные технологии. Филиал ВГУЮ. [Электронный ресурс] URL: https://rostov.rpa-mu.ru/distancionnoe-obuchenie.
3. Фаронов В., Delphi 7. Учебный курс – С.-Пб.: Питер, 2012.

***Д.А. Безуглов, **А.П. Кузин, **С.А. Швидченко**

ОБНАРУЖЕНИЕ КОНТУРОВ ИЗОБРАЖЕНИЙ В МУЛЬТИМЕДИЙНЫХ ПРИЛОЖЕНИЯХ НА ОСНОВЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

*Ростовский филиал российской таможенной академии,
**Донской государственный технический университет, Ростов-на-Дону, Россия

Ключевые слова: обработка изображений, вейвлет-дифференцирование, среднеквадратическое отклонение, пиковый сигнал, шум, прямое и обратное вейвлет-дифференцирование.

Известные методы выделения контуров изображений, основанные на эвристических подходах и методах последовательного численного дифференцирования локальных областей изображения с помощью различных масок, как правило, не работоспособны в условиях сильных шумов. Для решения проблемы влияния шумов на результат выделения контуров в данной работе рассматривается метод прямого и обратного вейвлет-дифференцирования. Предлагаемый подход заключается в аналитическом дифференцировании элементов изображения предложенным способом. В работе показано преимущество представленного метода по сравнению с известными на примере анализа серии различных изображений.

***D.A. Bezuglov, **A.P. Kuzin, **S.A. Shvidchenko**

CONTOUR DETECTION OF IMAGES FOR MULTIMEDIA APPLICATIONS BASED ON THE DISCRETE WAVELET TRANSFORM

* Rostov branch of Russian customs Academy, Rostov-on-Don, Russia
**Don State Technical University, Rostov-on-Don, Russia

Key words: image processing, wavelet differentiation, standard deviation, peak signal-to-noise, direct and inverse wavelet differentiation.

Known methods of detecting contours of images based on heuristic approaches and methods of numerical differentiation of successive local image areas with different masks, as a rule, does not work in the conditions of strong noise. To solve the influence of noise on the result of contour extraction in this paper we consider the direct and inverse wavelet differentiation. The proposed approach is the analytical derivation of the elements of the image by the proposed method. The paper shows the advantage of the presented method in comparison with known for example, analyzing a series of different images.

ВВЕДЕНИЕ

Решение задачи выделения контуров используется в промышленности при создании автономных роботов, а также систем анализа изображений в сложных условиях наблюдения, при воздействии различных мешающих факторов, усложняющих процесс регистрации изображения и при отсутствии априорных сведений о виде фоновых шумов. Это значит, что методы и алгоритмы обработки информации с датчиков изображения должны учитывать наличие шумов различной природы, связанных с регистрацией изображений и сигналов в реальных системах [1,2,3,4,5,6,7].

При этом известные в настоящее время алгоритмы решения таких задач предполагают предварительную фильтрацию изображений, а затем решение задачи выделения контуров. При построении методов и алгоритмов фильтрации изображений требуется априорное знание характеристик искажающих помех. На практике, в большинстве случаев такая информация отсутствует или является приближенной.

Смысл операции подчеркивания контуров состоит в том, чтобы усилить резкие перепады яркости, сформировав в соответствующих точках кадра импульсные отклики на фоне сравнительно слабых флюктуаций в других областях картины, не содержащих крутых яркостных перепадов.

По своему характеру все операторы подчеркивания контуров являются различными модификациями дифференцирования двумерного поля по различным направлениям области определения. Как известно, при дифференцировании, в самом деле, в окрестности перепада функции яркости образуется пик, способствующий регистрации этой области. Однако также хорошо известно, что при дифференцировании сигналов с помехами происходит существенное усиление последних, что снижает отношение сигнал/шум и негативно отражается на получаемых результатах.

Обычно оператор подчеркивания контуров представляют в форме масочного линейного фильтра. В процессе обработки маска, которая является просто матрицей

коэффициентов, скользит по полю изображения, занимая поочередно все возможные положения. В каждом положении маска играет роль окна, при помощи которого отбираются отсчеты обрабатываемого изображения, и выполняется их поэлементное умножение на соответствующий элемент маски с последующим суммированием всех произведений

Формирование изображений, улучшение качества и автоматизация обработки изображений, включая изображения, создаваемые рентгеновскими аппаратами, томографами и т.д., являются предметом исследования и разработки. Сегодня в технике широко применяются системы формирования изображения, его преобразования в цифровую форму, визуализация и документирование путем введения в компьютер изображений с помощью специализированных устройств захвата видео. Автоматический анализ в системах дистанционного наблюдения широко применяется при анализе местности, в лесном хозяйстве, например, для автоматического подсчета площади вырубок, в сельском хозяйстве для наблюдения за созреванием урожая, при разведке, в системах противопожарной безопасности. Контроль качества производимой продукции выполняется благодаря автоматическим методам анализа сцен [5,6].

Таким образом, научная задача разработки алгоритмов вейвлет-анализа для мультимедийных приложений в настоящее время не решена в достаточной мере, и является актуальной.

1. ВЕЙВЛЕТ-ДИФФЕРЕНЦИРОВАНИЕ МУЛЬТИМЕДИЙНЫХ ИЗОБРАЖЕНИЙ

В качестве критериев качества в работе использованы следующие.

1. Среднеквадратическое отклонение e_{cko}:

$$e_{ско} = \sqrt{\frac{1}{MN}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(MT_{ij} - \hat{MK}_{ij}\right)^2} \qquad (1)$$

При этом в качестве тестового изображения *MT* использовалось изображение контуров, полученное из незашумленного исследуемого изображения *S* детектором границ *Canny*. В дальнейшем на исходное изображение*S* накладывался аддитивный гауссовский шум и проводилось определение контуров предложенным методом вейвлет-дифференцирования и известным методом *Собеля*. При этом были получены изображения $\hat{MK}$.

2. Отношение пиковый сигнал/шум *SNR1:*

$$\mu = \frac{1}{MN}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(\hat{MK}_{ij}\right)^2;$$

$$SNR1 = \frac{255-\mu}{\sqrt{\frac{1}{MN}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(\hat{MK}_{ij}-\mu\right)^2}}; \qquad (2)$$

где μ - среднее значение $\hat{MK}_{ij}$.

3.Отношение пиковый сигнал/шум *SNR2* (с использованием в расчетах СКО фона):

$$\sigma_{фон} = \sqrt{\frac{1}{\left(N_{фон}\right)^2} \sum_{i=n_1}^{n_1+N_{фон}} \sum_{j=m_1}^{m_1+N_{фон}} \left(M\hat{K}_{ij} - \mu_{фон} \right)^2} \; ; \qquad (3)$$

где: $\sigma_{фон}$ - СКО фона; $\mu_{фон} = \frac{1}{\left(N_{фон}\right)^2} \sum_{i=n_1}^{n_1+N_{фон}} \sum_{j=m_1}^{m_1+N_{фон}} \left(\hat{MK}_{ij} \right)$ - среднее значение фона; n_1, m_1- координаты выбранной площадки фона размером $N_{фон} \times N_{фон}$ на исследуемом изображении $\hat{MK}$,

$$SNR2 = \frac{255 - \mu}{\sigma_{фон}}. \qquad (4)$$

Используя три критерия, в дальнейшем можно будет более адекватно оценить эффективность предложенных алгоритмов по сравнению с известными.

2. ИССЛЕДОВАНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК АЛГОРИТМОВ ВЕЙВЛЕТ-ДИФФЕРЕНЦИРОВАНИЯ

Для качественной и количественной характеристики разработанных алгоритмов проведем проверку их функционирования на тестовых изображениях. При этом будем исследовать тестовые изображения, не подвергшиеся воздействию шума [8,9,10]. Для исследования качественных характеристик предложенного подхода, авторами была разработана компьютерная программа MAC2014v1.2, реализующая предложенные методы вейвлет-анализа [11,12,13]. Скриншот панели ввода исходных данных приведен на рисунке 1.

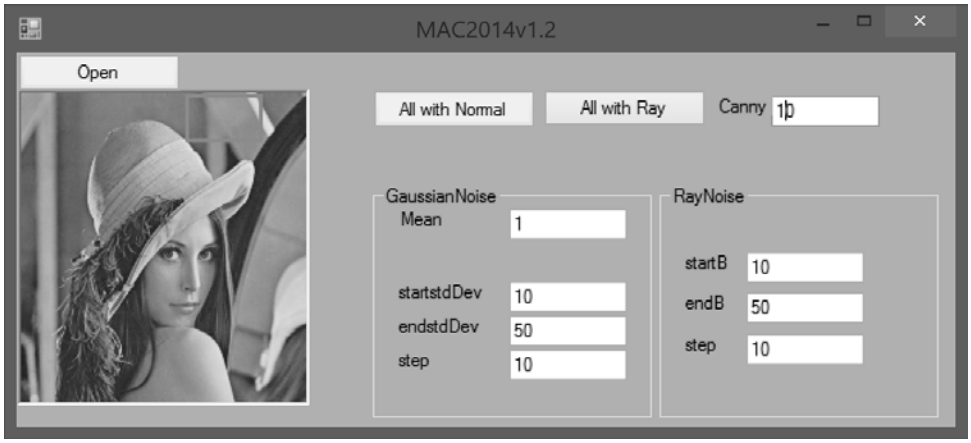
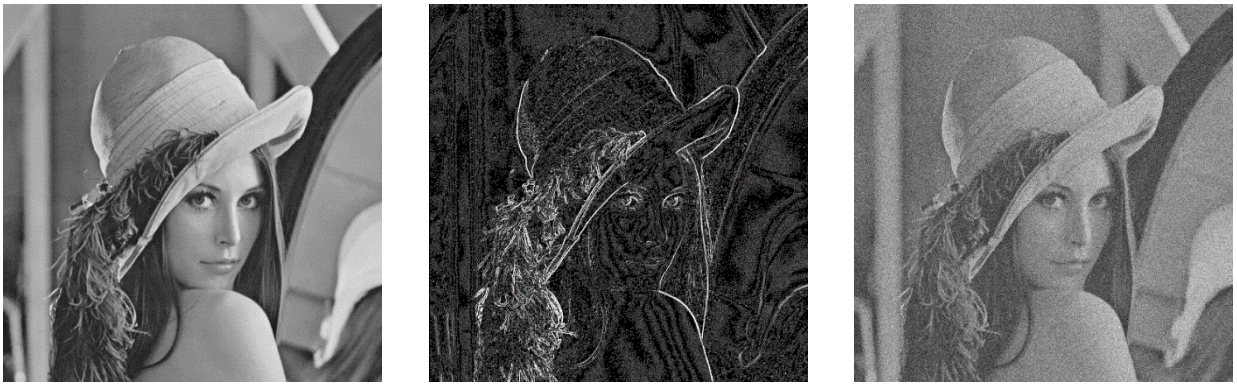


Рисунок 1 - Скриншот панели ввода исходных данных

Рассмотрим эффективность предложенных методов на примере выделения контуров в популярном стандартном тестовом изображении Lena [14]. На рисунке 2

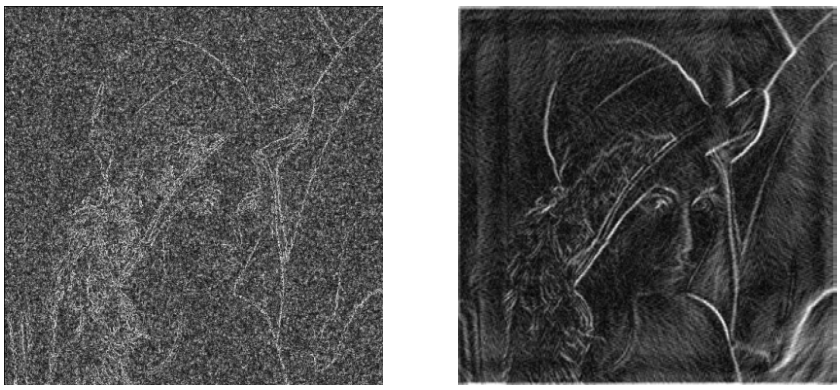
представлены этапы подготовки исходное тестового изображения (рисунок 2а), обработанное оператором выделения границ Canny (рисунок 2б) и результат наложения на исходное тестовое изображение формирующего гауссовского шума с СКО σ =30 (рисунок 2в).



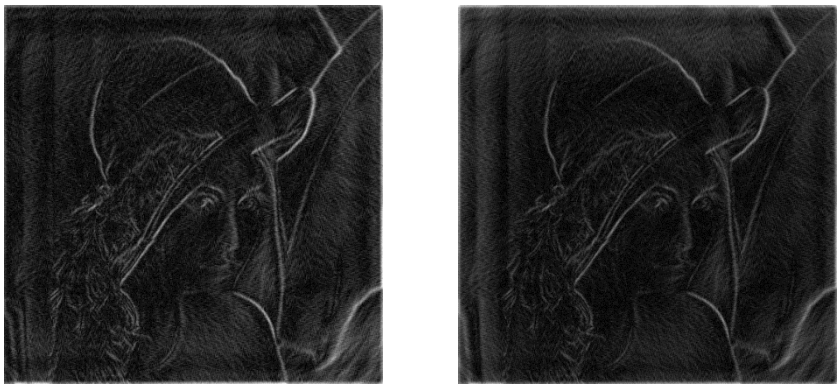
а) б) в)

Рисунок 2 - а) исходное изображение, б) результат выделение контуров изображений с помощью оператора выделения границ Canny, в) исходное тестовое изображениепосле наложения формирующего гауссовского шума с СКО σ =30

После чего к изображению (рисунок 2в) были применены методы вейвлет-дифференцирования на базе вейвлетовMhat, DOG и WAVE. Результаты обработки изображения Lena методами вейвлет-дифференцирования в сравнении с методом Собеля представлены на рисунке 3.



а) б)



в) г)

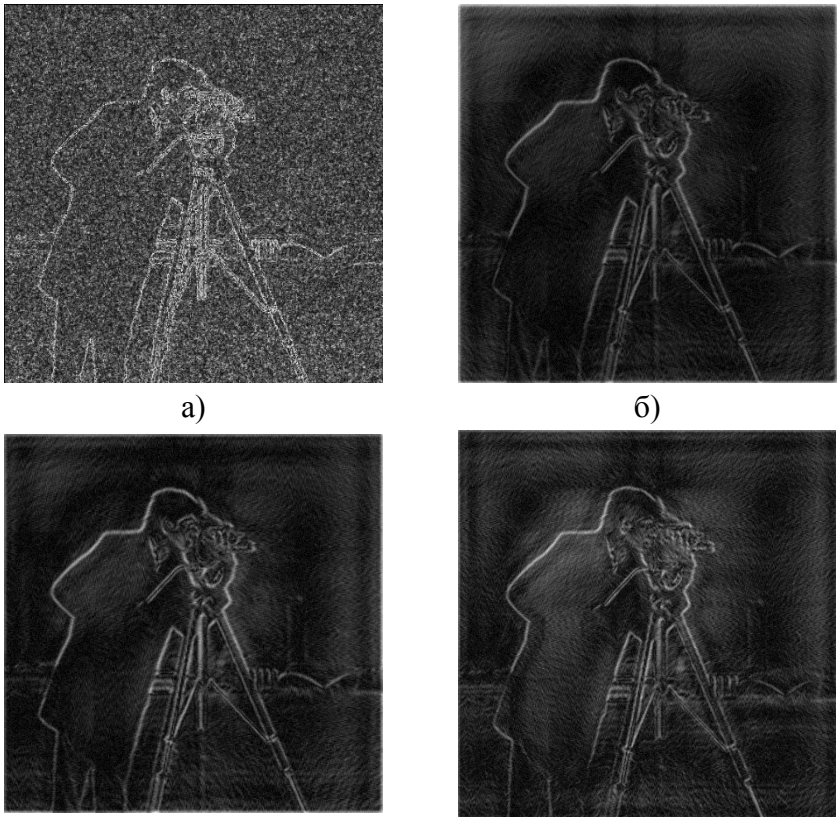
Рисунок 3 - а) Результат обработки изображения Lena оператором Собеля, б) результат обработки изображения вейвлетом Mhat,в) результат обработки изображения Lena вейвлетом DOG, г) Результат обработки изображения Lenавейвлетом WAVE

Рассмотрим эффективность предложенных методов выделения контуров объектов на местности на фоне случайного фона на примере выделения контура тестового изображения Cameramen [15]. Порядок проведения вычислительного эксперимента был аналогичен предыдущему. На рисунке 4 представлены этапы подготовки исходное тестового изображения (рисунок 4а), обработанное оператором выделения границ Canny (рисунок 4б) и результат наложения на исходное тестовое изображение формирующего гауссовского шума с СКО σ =30 (рисунок 4в).

а) б) в)

Рисунок 4 - а) исходное изображениеCameramen, б) результат выделение контуров изображений с помощью оператора выделения границ Canny, в) исходное тестовое изображение после наложения формирующего гауссовского шума с СКО σ =30.

Результаты обработки изображения Cameraman (рисунок 4а) методами вейвлет-дифференцирования в сравнении с методом Собеля представлены на рисунке 5.



а) б)

в) г)

Рисунок 5 - а) Результат обработки изображения Cameramenоператором Собеля, б) результат обработки изображения вейвлетом Mhat, в) результат обработки изображения Cameramenвейвлетом DOG, г) Результат обработки изображения Cameramenвейвлетом WAVE

В таблице 1 приведены результаты выполненных вычислительных экспериментов.

Таблица 1 - Результаты вычислительных экспериментов

	СКО формирующего шума				
	5,00	**20,00**	**30,00**	**40,00**	**50,00**
Критерий 1					
СКО исходного изображения, $e_{ско}$	10,33	31,37	39,98	46,22	50,77
Алгоритмы	**Выигрыш по СКО** $e_{ско}$ **в децибелах**				
Вейвлет DOG	3,14	3,49	3,70	4,22	3,96
Вейвлет WAVE	2,81	3,16	3,39	3,96	3,70
Вейвлет MHAT	2,99	3,21	3,37	4,00	3,57
Критерий 2					
Отношение пиковый сигнал/шум, SNR1 исходного изображения	1,92	2,63	3,05	3,37	3,63

Продолжение таблицы 1

Алгоритмы	**Выигрыш по отношению пиковый сигнал/шум, *SNR1***				
Вейвлет DOG	5,16	4,83	4,89	5,01	5,11
Вейвлет WAVE	5,20	4,80	4,80	4,89	4,97
Вейвлет MHAT	5,34	4,91	4,93	5,00	5,06
Критерий 3					
Отношение пиковый сигнал/шум, по СКО фона исходного изображения, SNR2	8,11	5,94	5,40	5,07	4,89
Алгоритмы	**Выигрыш по отношению пиковый сигнал/шум, по СКО фона, *SNR2***				
Вейвлет DOG	9,64	7,51	7,10	6,91	6,81
Вейвлет WAVE	8,86	7,63	7,32	7,20	7,14
Вейвлет MHAT	9,59	7,16	6,66	6,43	6,30

Полученные количественные результаты и экспертные оценки качества выделения контуров изображений позволяют сделать вывод о преимуществах предложенных алгоритмов по сравнению с известными. Программная реализация предложенных методов и алгоритмов позволяет автоматизировать процессы обработки сигналов и изображений и расширить возможности проведения исследований для создания перспективных информационных систем обработки изображений.

ВЫВОДЫ

Анализ результатов математического моделирования позволяет сделать следующие выводы. Предложенный метод обработки изображений позволяет эффективно выделять контуры изображений, искаженных шумом. Разработанные новый метод и алгоритмы вейвлет-дифференцирования изображений на фоне шума с использованием дискретного вейвлет- преобразования, позволяют повысить отношение пиковый сигнал-шум на 4,8÷9,6 дБ и на 3÷4 раза уменьшить среднеквадратическое отклонение ошибки.

В данном случае свойства вейвлет-преобразования позволяют отказаться от применения различных масок, то есть, по сути, отказаться от малоэффективных методов численного дифференцирования. На базе предложенного метода могут быть реализованы и другие алгоритмы выделения контуров на базе вейвлет-дифференцирования с использованием других вейвлетных базисов.

Таким образом, научная задача разработки методов автоматизированного анализа результатов измерений для выделения контуров фрагментов объектов в изображениях при наличии фонового шума в работе решена. Предложенные методы и алгоритмы могут быть использованы при создании систем обработки сигналов цифровых изображений в промышленности при создании автономных роботов, в условиях наблюдения, усложняющих процесс регистрации и при отсутствии априорных сведений о виде фоновых шумов.

СПИСОК ЛИТЕРАТУРЫ

1. *Прет У.,* Цифровая обработка изображений. М.: Мир,1982.
2. *Гонсалес Р., Вудс Р,* Цифровая обработка изображений. // М.: Техносфера, 2005.
3. *Гольденберг Л.М., Матюшкин Б.Д., Поляк М.Н.* Цифровая обработка сигналов: Справочник. – М.: Радио и связь 1985 г. 312 с.
4. *Дьяконов В., Абраменкова И.* MATLAB. Обработка сигналов и изображений. // Специальный справочник. – СПб.: Питер, 2002, 608 с.
5. *Лукьяница А.А., Шишкин А.Г.* «Цифровая обработка видеоизображений» / М.: – «Ай-Эс-Эс Пресс», 2009. – 518с.
6. *Мартышевский Ю.В., Шакиров И.В., Шаропин Ю.Б.* Применение вейвлет-преобразования при обработке изображений. // Третий международный симпозиум. Р11-97-347. Дубна, 1997.
7. Новейшие методы обработки изображений / Под ред. А.А. Потапова – М.: ФИзматлит, - 2008, 496 с.
8. *Безуглов Д.А., Швидченко С.А.* Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума (статья). // Вестник компьютерных и информационных технологий. №6 (84) 2011г. с.42-45.
9. Безугл*ов Д.А., Рытиков С.Ю., Швидченко С.А., Гаврин М.С., Гаврин Д.С.* Выделение контуров изображений в информационных и управляющих системах с использованием метода вейвлет-преобразования (статья). // Нелинейный мир. № 11 2012г., с.846-852.
10. *Безуглов Д.А., Рытиков С.Ю., Швидченко С.А.* Метод вейвлет-дифференцирования в задаче выделения контуров. /Успехи современной радиоэлектроники. 2012. № 6. С. 52-57.
11. *Швидченко С.А., Безуглов Д.А.,Рытиков С.Ю., Решетникова И.В.* Выделение контуров изображений с использованием метода вейвлет-дифференцирования. Часть 1. /Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2012. № 1. С. 33-36.
12. *Швидченко С.А., Безуглов Д.А., Рытиков С.Ю., Решетникова И.В.,* Выделение контуров изображений с использованием метода вейвлет-дифференцирования. Часть 2. /Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2012. № 1. С. 37-40.
13. *Безуглов Д.А., Кузин А.П., Решетникова И.В., Юхнов В.И,* Информационная технология идентификации изображений. /Фундаментальные исследования. – 2015. № 2-16. С. 3466-3470.
14. *Безуглов Д.А., Кузин А.П.* Информационная технология выделения контуров изображений на фоне шума. /Современные проблемы науки и образования. – 2015. № 2-2. С. 190.
15. *Безуглов Д.А., Кузин А.П.* Информационная технология выделения контуров изображений. /Академический вестник Ростовского филиала Российской таможенной академии. – 2015. № 1 (18). С. 33-39.

Э.А. Бинеев

ОСОБЕННОСТИ СТРУКТУРЫ ДИСЦИПЛИНЫ БЖД ПО НАПРАВЛЕНИЮ ИТСС

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Аннотация: статья посвящена некоторым аспектам структуры дисциплины БЖД. В частности предлагается переход на изучение классических разделов безопасности.

Ключевые слова: разделы БЖД, структура дисциплины.

E.A. Bineev

FEATURES OF THE STRUCTURE OF THE DISCIPLINE LIFE SAFETY IN THE DIRECTION OF ITCS

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

Abstract: the article deals with some aspects of BC discipline structure. In particular the proposed shift to the study of classical security topics.

Keywords: forums BC, the structure of the discipline.

С момента введения в 1990г. в учебные планы вузов новой дисциплины, получившей название безопасность жизнедеятельности (БЖД), ее структура менялась и продолжает меняться до настоящего времени [1-4]. Если авторы [1], переходя к структуре БЖД как охране труда добавляют такие разделы, как «Экстремальные ситуации», «Чрезвычайные ситуации», то авторы [4] увлекаются разделами, которые, по нашему мнению, должны изучаться в школах. Например, «Автономное выживание человека», «Безопасность на транспорте», «Безопасность в городе, в быту и на отдыхе». В учебнике [2] вопросы безопасности жизнедеятельности рассматриваются с точки зрения взаимодействий человека и техносферы. Структура БЖД кардинально меняется, вводятся лишь четыре основных раздела: человек и техносфера, опасности технических систем и защита от них, чрезвычайные ситуации, управление безопасностью жизнедеятельности. Хотя внутри этих разделов проявляется классическая структура изучения вопросов безопасности: опасные и вредные факторы, инженерные системы, уменьшающие их воздействие на человека, трудовое законодательство. В учебнике [3] структура дисциплины, на наш взгляд, наиболее приближена к традиционной структуре дисциплины «Охрана труда», хотя авторы и вводят такие разделы как «Основы обеспечения безвредных и безопасных условий труда», «Основы обеспечения безопасности в производственной среде».

Наш опыт многолетнего преподавания дисциплины БЖД показал, что для лучшего усвоения основных положений дисциплины необходима ее четкая структура, которая не

размывала бы изучаемые вопросы по разным разделам. При этом, по нашему мнению, особое внимание надо уделять вопросам, связанным с изучением производственной безопасности. Более того мы предлагаем в начале изучения четко изложить предлагаемую структуру дисциплины с кратким описанием основных направлений изучаемых вопросов в каждом разделе. Предлагаемая нами структура соответствует классической структуре дисциплины охраны труда с добавлением чрезвычайных ситуаций и экологической безопасности.

Она состоит из семи разделов. В разделе правовые и организационные основы безопасности выделяются два основных направления. Первое – законодательство в различных областях безопасности, их иерархия, нормативные акты, расследование и учет несчастных случаев на производстве, анализ производственного травматизма, оценка рисков и т.п. Второе направление связано с разработкой эффективных систем управления безопасностью на разных уровнях. В разделе производственная санитария, в котором изучаются вредные производственные факторы, выделяются следующие два основных направления. Во первых это изучение биологического воздействия вредных производственных факторов на организм человека, которая является основой для разработки санитарных норм. Во вторых это изучение инженерных систем, уменьшающих воздействие вредных факторов на организм человека. В следующем разделе, техника безопасности или безопасность труда, изучаются опасные производственные факторы. Внимание уделяется воздействию этих факторов на человека и техническим устройствам и системам безопасности. Особое внимание в этом разделе уделяется вопросам электробезопасности.

В разделе пожарная безопасность выделяются четыре направления изучаемых вопросов. Это фундаментальные исследования процессов, являющихся причиной возникновения пожаров: горения, взрыва, детонации. Второе – изучение пожароопасных свойств и характеристик различных веществ и материалов. Третье – повышение пожаростойкости строительных материалов и конструкций. И четвертое направление - основные средства и аппараты тушения пожаров. В разделе экологическая безопасность или охрана окружающей среды выделяются следующие два основных направления. Первое связано со сбором данных, характеризующих состояние окружающей среды: атмосферы, гидросферы и литосферы. Это так называемый мониторинг окружающей среды. Второе направление – это комплекс международных, государственных, региональных и локальных (местных) административно-хозяйственных, технологических, политических, юридических и общественных мероприятий, направленных на обеспечение социально-экономического, культурно-исторического, физического, химического и биологического комфорта, необходимого для сохранения здоровья человека. В разделе эргономика изучаются различные виды совместимости в системе «человек-машина-среда». Основное внимание уделяется антропометрической, энергетической, информационной, социально-психологической и технико-эстетической совместимости. В разделе чрезвычайные ситуации (ЧС) природного характера (стихийные бедствия) и техногенного характера (производственные аварии и катастрофы) выделяются три основных направления. Первое – изучение методов прогноза чрезвычайных ситуаций и пути повышения их надежности. Второе – изучение эффективных способов и средств эвакуации населения из зон возможных ЧС. И третье – изучение эффективных способов и средств ликвидации последствий ЧС.

Конечно, предлагаемая структура дисциплины БЖД не содержит чего-либо нового, но главное в ней это те акценты, которые предлагаются в каждом из разделов, и четкость структур. Наша практика применения такой структуры дисциплины БЖД, отраженная в учебном пособии [5], показала ее эффективность в учебном процессе.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность и охрана труда: Учебное пособие для вузов/ под редакцией О.Н. Русака. СПб: Изд-во МАНЭБ, 2001. – 279с.
2. Безопасность жизнедеятельности. Учебник для вузов/ С.В.Белов, А.В. Ильинская, А.Ф. Козьяков и др.: Под общей редакцией С.В. Белова: – М: Высшая шк., 1999. – 448с.
3. Безопасность жизнедеятельности. Охрана труда: Учеб. пособие для вузов/ А.В. Фролов, Т.Н. Бакаева: под общ. ред. А.В. Фролова. – Ростов н/Д: Феникс, 2005. – 736с.
4. Основы безопасности жизнедеятельности: учеб. пособие/ Р.И. Айзман, Н.С. Шуленина, В.М. Ширшова: под общ. ред. Р.И. Айзмана, С.В. Петрова. - Новосибирск: АРТА, 2011. – 368с.
5. *Бинеев Э.А., Бородин А.В., Шаповалов А.В.* Безопасность жизнедеятельности. Учебное пособие: под. ред. Э.А. Бинеева. – Ростов н/Д: СКФ МТУСИ, 2012. – 265с.

А.Э. Боярчук, *В.И. Юхнов, *П.С. Шевчук

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМ УПРАВЛЕНИЯ ПРОЕКТАМИ

Ростовский филиал государственного казенного образовательного учреждения высшего образования «Российская таможенная академия», г. Ростов-на-Дону, Россия

* Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: бизнес-пространство, проектный метод, стратегический менеджмент, стратегия компании, информационная система управления проектами.

Рассмотрен вопрос повышения эффективности корпоративной системы управления проектами. Стратегия компании рассматривается как управленческий инструмент. Выделены основные составляющие корпоративной системы управления проектами и рассмотрены вопросы повышения их эффективности.

A.E. Boyarchuk, *V.I. Yukhnov, *P.S. Shevchuk

IMPROVING THE EFFICIENCY OF THE SYSTEM PROJECT MANAGEMENT

Rostov branch of the state higher educational institution of higher education
Russian customs academy, Rostov-on-Don, Russia

* North-Caucasian branch of the Order of the Red Banner of Labor of the federal state budgetary educational institution of higher education "Moscow Technical University of Communication and Informatics", Rostov-on-Don, Russia

Keywords: business space, project method, strategic management, company strategy, information system for project management.

The issue of increasing the efficiency of the corporate project management system is considered. The company's strategy is seen as a management tool. The main components of the corporate project management system are singled out and the issues of increasing their effectiveness are considered.

Современная практика показывает, что использование проектного метода для выполнения целей и задач организации в России является весьма распространенным как в крупных, так и в небольших компаниях. Необходимость проектной деятельности обычно обусловлена возникновением уникальной задачи, например, связанной с диверсификацией производства, внедрением новых технологий и многими другими. Проектный подход используется также и в стратегическом менеджменте организации. Внедрение корпоративной системы управления необходимо для поддержания процессов управления стратегически важными проектами [4].

Актуальность исследования обусловливается тем, что повышение эффективности корпоративной системы управления проектами с учетом стратегического менеджмента является недостаточно разработанной с научной точки зрения. Также необходимо отметить, что как теоретики, так и практики менеджмента всегда уделяли пристальное внимание вопросам повышения эффективности организационной деятельности и стратегического развития предприятия.

Типология управленческой деятельности включает в себя три ключевых элемента: операционная деятельность - постоянно повторяющиеся действия на основе бизнес-процессов; оперативная деятельность - оперативное реагирование на нештатные ситуации; проектная деятельность - целенаправленное качественное изменение элемента или функции организации, в результате которого компания получает новое конкурентное преимущество.

Проектная деятельность, направленная на изменение объекта или процесса, характеризуется наличием фиксированной цели, ограниченностью во времени и ресурсах, новизной и комплексностью. Управление проектом это не только постановка цели и ее достижение, но и оценка результатов проекта с точки зрения влияния на развитие организации.

Проекты становятся средством достижения целей и задач организации в контексте стратегического плана. Проекты, как правило, авторизуются в результате одного или нескольких из следующих стратегических соображений: стратегические возможности; требования рынка; технологический прогресс; требования заказчика; законодательные требования.

Эффективная система управления проектами позволяет грамотно планировать и успешно реализовывать проекты с учетом динамики внешней и внутренней среды организации. Это дает не только повышенные результаты деятельности предприятия, но и позволяет достигать конкурентных преимуществ в бизнес-пространстве. Кроме того, регулярное изменение условий существования организации требует постоянного развития системы управления проектами.

Стратегический менеджмент, родоначальником которого считается И. Ансофф, изучался также и другими учеными. Рассмотрим особенности стратегического управления с точки зрения классического подхода.

Стратегия компании, по мнению И. Ансоффа, - набор правил для принятия решений, которыми организация руководствуется в своей деятельности. Классик выявил, что в периоды изменений, когда необходимо из множества альтернатив выбрать правильное направление, в ситуации, которая трудно поддается оценке, и при этом еще нужно скоординировать усилия коллектива, - стратегия становится управленческим инструментом [1].

Стратегическое управление на предприятии выражается в основных функциях: планирование стратегии, организация выполнения стратегических планов, координация действий по реализации стратегических задач, мотивация на достижение стратегических результатов. Для реализации функций стратегического управления необходим специальный набор инструментов, одним из которых является корпоративная система управления проектами.

Рассмотрев различные научные точки зрения, можно сделать вывод, что принципиальных различий во мнениях по поводу структуры систем управления проектами на данный момент нет. Обычно выделяют четыре основные составляющие корпоративной системы управления проектами:

- ресурсы (высококвалифицированные сотрудники);
- информационная система управления проектами (программный инструментарий);
- организационный компонент (распределение ролей);
- методическая и нормативно-регламентная составляющие (стандарты, регламенты, приказы и т. д.).

Таким образом, корпоративная система управления проектами представляет собой комплекс организационных, методических, технических, программных, информационных средств, направленных на поддержку и повышение эффективности процессов планирования и управления проектами в организации [9]. Данные компоненты были выделены не случайно, так как для того, чтобы управление проектами с учетом стратегии компании было эффективным, необходимо консолидировать высококвалифицированных специалистов и обеспечить их необходимыми технологиями, способствующими быстрому решению оперативных задач в рамках общей стратегической цели. Грамотно выстроенная иерархия подчинения и распределения ролей, закрепленная должностными инструкциями,

подтвержденная различными стандартами, является одним из гарантов успешного достижения проектной цели.

Эффективность корпоративных систем управления проектами во многом определяется критериями оценки достижения поставленных целей, а также уровнем качества выполнения каждой стадии проекта: инициация, планирование, выполнение, контроль и завершение.

Для оценки степени достижения стратегических целей организации в рамках проектной деятельности главным образом учитываются ключевые показатели эффективности. Данный метод заимствован из западной научной литературы и называется KPI - Key Performance Indicator. Например, количественными показателями являются: отклонение от запланированного бюджета, снижение затрат. С качественными показателями дело обстоит несколько сложнее. Они основаны исключительно на субъективном подходе, и в разных компаниях оценка качественных показателей строится с различных позиций: может заключаться в оценке приемной комиссии либо сконцентрировано только на окупаемости вложений и других финансовых показателях.

Рассмотрим способы повышения эффективности в достижении стратегически важных целей посредством декомпозиции элементов системы управления проектами.

С точки зрения методологической составляющей формализация проектной деятельности значительно облегчает процесс оценки эффективности элементов системы проекта. Процедуры и регламенты закрепляются в основных документах проекта: уставе и паспорте. Благодаря существующим стандартам становится возможным осуществлять контролирование проекта на этапе планирования. Эффективным методом является переложение инструкций и регламентов стандартов на стратегию конкретного предприятия, при этом по содержанию стандарт должен носить универсальный характер, чтобы можно было вносить изменения в процессе трудовой деятельности.

Далее нужно рассмотреть организационный компонент системы управления проектами. Согласно мнению практиков, повышение эффективности систем управления обеспечивает матричная организационная структура. Она является наиболее гибкой и позволяет на базе постоянных функциональных подразделений создавать временные коллективы для выполнения определенной стратегически важной цели [7]. Также необходимо учитывать уровень зрелости организации. Каждая компания в своем развитии проходит определенные этапы, которые характеризуются различными миссиями, стратегиями, организационной структурой и другими качественными и количественными характеристиками. Оценка зрелости позволяет определить способность отбирать проекты и управлять ими так, чтобы было обеспечено максимально эффективное достижение стратегических целей компании [9].

Другим способом достижения стратегически важных целей служит корпоративный Форсайт. Форсайт-проекты нацелены на выбор технологических приоритетов, определение основных факторов, способных повлиять на изменение рынков, оценку потенциальных продуктов, которые могут быть востребованы на этих рынках, выявление технологического потенциала корпораций, выбор мер, необходимых для развития существующих и достижения новых конкурентных преимуществ [3].

Эффективно функционирующие корпоративные системы приводят к повышению конкурентоспособности на внутреннем и внешнем рынках на фоне растущей региональной конкуренции [8]

Одной из важнейших функций в деятельности любой организации является управление ресурсами. Грамотный подбор участников проекта и распределение ролей в команде обеспечивают значительную вероятность успешного достижения целей проекта. Создание реально работающей команды проекта предполагает возможность ее построения в составе специалистов компании и внешних консультантов. Активное участие руководства и специалистов заказчика в работе совместной команды проекта, реальные полномочия (власть) руководителя и куратора проекта должны быть обеспечены на самых ранних этапах. Важное значение может иметь запуск с самого начала проекта программы внутреннего маркетинга (с целью вовлечения сотрудников в проект и обеспечения положительного отношения к нему).

В любой организации является важным вопрос мотивации сотрудников. Как уже было отмечено ранее, на каждой ключевой точке проектного процесса происходит анализ выполненных работ и корректировка дальнейших планов, если в этом есть необходимость. Научные деятели утверждают, что одним из самых эффективных методов повышения мотивации персонала является вознаграждение по результатам оценки качественных и количественных показателей на текущей стадии выполнения проекта [6].

Внедрение информационных систем управления проектами требует наличия программных продуктов в соответствии с масштабом проекта, его целями и задачами, а также этапом жизненного цикла организации. Благодаря программному обеспечению появляется возможность контролирования процесса выполнения работ, закрепленных за ответственными сотрудниками, так же осуществляется контроль бюджета и многие другие возможности.

Информационная система управления обеспечивает оценку планируемых и фактических характеристик проектных работ, благодаря чему становится возможной оптимизация нагрузки подразделений и отдельных сотрудников, своевременное реагирование на отклонение от планов и принятие эффективных решений, например сокращение некоторых видов затрат и др. Таким образом обеспечивается повышение эффективности всей системы управления проектами [5].

Комплекс технических средств, системных решений и программных продуктов, обеспечивающих и повышающих эффективность планирования и управления проектами, составляет информационную систему управления проектами. Эта информационная система может быть структурирована по этапам жизненного цикла проекта, по функциям управления и по уровню управляющего регулирования. Специализированные программные продукты (ПП), применяемые для целей планирования и управления проектами, делятся на следующие типы.

1. Системы для бизнес-планирования и финансового моделирования, применяемые, в первую очередь, на стадии инициации. В России наиболее распространены два продукта: «Project Expert» и «Альт-Инвест».
2. ПП для календарного планирования. Среди данного типа можно назвать MS Project, Primavera, Open Plan.
3. ПП по управлению бюджетом проекта (Cobra, CM Pro и т.п.).
4. ПП по управлению рисками (Risk+, Risk Analyser for Excel и другие).
5. ПП, формирующие единое коммуникационное пространство проектов (MS Project Server, MS Share Point, 1С:Битрикс).

С точки зрения функциональных обязанностей менеджеров организации крайне важна постановка цели, которая содержит информацию о конкретных задачах и запланированных показателях. Также необходимо осуществлять функцию осведомления персонала различных уровней на предмет изменения или принятия новых стратегических планов.

Результатами повышения эффективности системы управления проектами с учетом специфики стратегического менеджмента могут быть: повышение качества выпускаемого продукта или оказываемой услуги, снижение себестоимости, экономия бюджетных средств, которые можно использовать для достижения других стратегических целей.

По данным консалтинговой компании «Богданов и партнеры», эффективное применение системы управления проектами позволяет сокращать продолжительность стадии реализации и разработки проекта на 20-30% и экономить расходы на 10-15% [5].

Согласно исследованию В. М. Аньшина и О. М. Ильиной методологии оценки и анализа зрелости управления портфелями проектов в российских компаниях, использование системы управления проектами уменьшает время вывода продукта на 35-75%, снижает содержательные и инжиниринговые изменения на 45-68%, в отдельных случаях повышает рентабельность инвестиций примерно на 20%, а также обеспечивает рост среднего показателя прибыли на 6% [2]. Это позволяет сделать вывод, что эффективное применение методологии проектного менеджмента является стратегическим преимуществом организации в конкурентной борьбе.

Подводя итоги можно сказать, что проектная деятельность является фундаментальной основой осуществления стратегического менеджмента, так как любая деятельность в рамках проекта ориентирована на реализацию главной стратегии компании.

В любой деятельности всегда остается актуальным вопрос о повышении эффективности работы системы. В связи с этим возникает необходимость постоянного контролирования и управления результатами проектной деятельности, которые должны соответствовать стратегии организации. Система управления проектами должна модернизироваться в соответствии с динамикой изменений внешней и внутренней среды фирмы. Внедрение корпоративной системы управления проектами должно рассматриваться непременно как элемент организационного развития. Повышение эффективности корпоративной системы управления проектами с учетом специфики стратегического менеджмента осуществляется посредством использования комплекса работ по развитию системы, испытанию, управлению, оценке соответствия системы управления проектами стратегии компании и передаче в эксплуатацию.

СПИСОК ЛИТЕРАТУРЫ

1. *Ансофф И.* Стратегический менеджмент. Классическое издание / пер. с англ.; под ред. А. Н. Петрова. СПб. : Питер, 2009. - 344 с.
2. *Аньшин В. М., Ильина О. М.* Исследование методологии оценки и анализ зрелости управления портфелями проектов в российских компаниях. М.: ИНФРА-М, 2010. - 200 с.
3. *Балашов А. И., Козырев А. А.* Форсайт как технология стратегического планирования // Управленческое консультирование. 2015. № 7(79). С. 45 - 56.

4. *Балашов А. И.* Управление проектами: учебник / А. И. Балашов, Е. М. Рогова, М. В. Тихонова, Е. А. Ткаченко. М. : Юрайт, 2014. - 383 с.
5. Богданов и партнеры: технологии для эффективного управления [Электронный ресурс]. URL: http://www.bogdanov-associates.com/rubrs.asp?rubr_id=534&art_ id=571 (дата обращения: 19.12.2016).
6. *Васецкий А. А.* Основы менеджмента: учеб. пособие / А. А. Васецкий, А. А. Козырев, Н. А. Тарасов, В. В. Яновский. СПб.: СЗАГС, 2011. - 276 с.
7. *Клочков А.* Как повысить и оценить эффективность проектов? [Электронный ресурс] // HRM.RU : ведущий портал о кадровом менеджменте. URL: http://hrm.ru/kak-povysit-i-ocenit-ehffektivnost-proektov (дата обращения: 19.09.2016).
8. *Козырев А. А.* Конкуренция как экономический феномен: основные направления исследований // Управленческое консультирование. 2014. № 10(70). С. 29-35.
9. *Полковников А. В., Дубовик М. Ф.* Управление проектами. М.: Эксмо, 2011. - 528с.

С.А. Быстров

ЗАДАЧА ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГОЛОСУ: АНАЛИЗ ПОДХОДОВ К РЕШЕНИЮ

Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: биометрия, идентификация по голосу, сингулярный спектральный анализ

В статье рассмотрена проблематика идентификации личности по голосу и актуальные подходы к решению поставленной задачи. Приводятся выкладки из личных и обзор приведенных исследований.

S.A. Bystrov

PERSONAL IDENTITY IDENTIFICATION: ANALYSIS OF APPROACHES TO SOLUTION

Federal Communications Agency Ural Technical Institute of Communications and Informatics (branch) FGBOU VO "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibGUTI), Russia

Keywords: biometrics, voice identification, singular spectral analysis

In the article the problems of personality identification by voice and actual approaches to the solution of the task are considered. The calculations from personal and review of the given researches are resulted.

В современном мире просто необходима аутентификация пользователя. Это обуславливается необходимостью ограничения доступа к помещениям или информации, а также предоставлению пользователю каких-либо услуг. Методов подтверждения личности большое количество, будь то идентификация по лицу, по отпечатку пальца, по венам ладони, по радужной оболочке и т.п. [1]. Не стоит забывать, что любые методы аутентификации могут быть скомбинированы для повышения точности определения «свой-чужой» и повышения степени надежности. Хоть по отдельности такие системы и являются достаточно надежными, алгоритмы их реализации имеют свои пределы и при достаточно большом количестве выборки могут допускать ошибки. В биометрии при расчёте точности метода учитываются ошибки первого и второго рода (FAR и FRR). FAR (False Acceptance Rate) — это вероятность ложного допуска объекта, в то время как FRR (False Rejection Rate) — вероятность ложного отклонения объекта. Эти два понятия тесно связаны, так как уменьшение одной ошибки ведёт к увеличению другой. Поэтому разработчики биометрических систем стараются прийти к некому балансу между FAR и FER [2].

Наиболее интересным способом является аутентификация по голосу. Количество абонентов сотовой связи в России превосходит общую численность населения страны (251 млн. абонентов на 147 млн. населения). Это можно объяснить необходимостью использования одним абонентом по 2-3 сим-карты для различных целей. Даже с такой статистикой становится ясно, что идентификация звонящего, скажем в контактный центр, становится актуальной задачей. Достаточно быстрый алгоритм обработки может позволить аутентифицировать абонента и сопоставить данные с номером звонящего и вывести на экран оператора информацию о совпадении или не совпадении реального пользователя сотового номера и звонящего.

Саму идею идентификации по голосу можно также применить и к домофонам. В этом случае реализовать алгоритм идентификации будет значительно проще, в связи с тем, что будет заранее известен набор слов (номера квартир). Поэтому при допуске определенного человека в подъезд, при озвучивания номера квартиры – система проверяет голос, сверяет его с заранее записанными эталонами и предоставляет или отказывает в предоставлении доступа в дом.

Также стоит понимать, что абсолютно любые системы аутентификации можно использовать как подтверждении присутствия или отсутствия человека в определенном месте, анализ частоты посещения определенных объектов или обращений в контактный центр и т.п.

Для реализации такой задачи, как идентификация личности по голосу, может быть использована система с различной архитектурой (клиент-серверные или локальные), методом выделения частот основного тона (ЧОТ) (преобразование Фурье, кодирование коэффициентами Линейного Предсказания, кепстральный анализ, вейвлет преобразование и т.д.), с разными типами обрабатываемой речи (распознавание изолированных слов или слитной речи), для различных целей (командные системы, системы диктовки, системы преобразования или аутентификации), с различными механизмами функционирования и

прочими признаками. В зависимости от поставленной задачи выбирается соответствующая система.

Вне зависимости от типа системы, для снижения различных ошибок и повышения точности алгоритмов обработки и нахождения ЧОТ, речевой сигнал необходимо предварительно обработать. Нужно исключить из сигнала различные шумы и помехи, не относящиеся к голосу (высокочастотные шумы, различные импульсные шумы и т.п.). Необходимо грамотно сегментировать речь в фонограмме. Выбрать оптимальный алгоритм обработки, как всей фонограммы, так и обработки речи и нахождения ЧОТ.

Большой вклад в данную область биометрии внесла компания «Центр Речевых Технологий», занимающиеся не только аутентификацией по голосу, но и другими технологиями, связанные с обработкой речевых сигналов. В данной компании был представлен концепт аутентификации по голосу VoiceKey. Данная разработка вошла в платформу мультимодальной биометрической аутентификации пользователей в каналах дистанционного обслуживания вместе с другой разработкой ЦРТ - АПК ВИЗИРЬ. Соединение двух технологий верификации личности заметно подняло степень безопасности и уменьшило число ложных решений (меньше пропускает «чужих» и чаще «своих»). [3]

Также свой вклад в данную отрасль биометрии внесли Вольф Д.А. и Тиунов С.Д. из «Томского государственного университета систем управления и радиоэлектроники» (ТУСУР).

В ходе диссертационной работы Вольф Д.А. проанализировал сложность обработки речевого сигнала и нахождения ЧОТ. Вольф Д.А. уделил значительное внимание определению ЧОТ различными моделями анализа спектра речевого сигнала, но, к сожалению, уделил внимание только гласным звукам, записанных при идеальных условиях (нет переходов от одного звука к другому, а также различных помех). [4]

Другой представитель ТУСУР - Тиунов С.Д в ходе своей работы представил численные методы и комплекс программ для акустического анализа голоса, которые и использовал в своей работе Вольф Д.А. Тиунов С.Д. разобрал принцип работ голосых складок и проанализировал саму суть речевого сигнала, а также представил готовые модели. [5]

Данные диссертационные работы расширили область применения алгоритмов нахождения ЧОТ, а также упростили аппаратную часть биометрических систем. А представленные системы используются в комплексе программ реабилитации пациентов после полной или частичной потери звучной речи в результате ларингоэктомии.

Однако, говоря про цифровую обработку речевых сигналов, стоит уделить внимание тому, с какой частотой будут браться отчеты. От частоты дискретизации может зависеть не только точность, но и количество необходимой памяти для обработки сигнала. Таким образом, Вольф Д.А. разбирал гласные звуки длиной в 32мс, что, несомненно, достаточно для определения ЧОТ методом сингулярного разложения, но в реальных сигналах выделить настолько узкий интервал с необходимым звуком достаточно сложно. Поэтому возрастает необходимость в увеличении временного интервала, а, следовательно, приведет к увеличению необходимой памяти для обработки. Также в представленных диссертационных работах, говорится о принадлежности одного звука к одной частоте, однако стоит все же рассматривать звук – как комбинацию из частот, а не единственную частоту. Таким образом, можно выделить точное различие между частотами разных

звуков, а благодаря использованию метода сингулярного спектрального анализа (SSA) в поставленной задаче, можно достигать более точных значений частот, по сравнению с, например, преобразованием Фурье (различие 10-20 Гц, что составляет погрешность в 6,6%). Данное сравнение проводились при анализе идеально записанных звуков: профессиональная звуковая аппаратура, отсутствие шумов и высокая частота дискретизации.

Одной из основных задач анализа речевого сигнала является разложение всего сигнала на дискретные временные отрезки, каждому из которых будет соответствовать определенный звук (буква или часть буквы, переход между буквами и т.п.). Именно разделения речи по звукам кажется на данный момент самой проблемной задачей. Составление такого алгоритма значительно упростило бы задачу идентификации речевых сигналов и их обработку в целом. Однако надо понимать, что сложность возникает не только в проблеме выборки диапазона звука. Существует великое множество всевозможных дефектов речи. Не стоит забывать и об различных акцентах (Даже если родной язык не меняется – манера речи, следовательно, и используемые звуки и их комбинация могут различаться).

Если отбросить все условности и смотреть только на анализ получения ЧОТ, то методом SSA можно достичь максимальную точность. Однако при анализе надо понимать, что частоты получаются путем анализа разносности сингулярных чисел λ_i. Значения сингулярных чисел λ_i траекторной матрицы временного ряда (ВР) $F_{N_i}^{\langle 1 \rangle}$ зависимы от длины окна L. И представляя графики для каждого сингулярного числа $\lambda_i = f(L \cdot \Delta t \cdot f)$ можно увидеть параллельные отрезки, соединяющие соседние сингулярные числа на графике $\lambda_i = f(i)$. Данное условие равности сингулярных чисел можно записать через формулу $L \cdot \Delta t \cdot f = 0.5k, k = 1, 2, \ldots$ [6]

Это означает, что сингулярные числа λ_i и λ_{i+1} оказываются одинаковыми только при определенных длинах окон. Или, при увеличении длины окна меняется и расстояние между нулевыми разностями сингуряных чисел. Все эти моменты приводят к погрешности порядка 5% от найденных частот.

Таким образом, задача идентификации личности по голосу актуальна. Однако ее окончательное решение, несмотря на усилия различных исследователей, не найдено.

СПИСОК ЛИТЕРАТУРЫ

1) *Р.М. Болл, Дж.Х. Коннел, Ш. Панканти, Н.К. Ратха, Э.У. Сеньор.* Руководство по биометрии. — М.: Техносфера, 2007. — 368 с. — ISBN 978-5-94836-109-3.
2) *Anil Jain, Arun Ross and Salil Prabhakar* An Introduction to Biometric Recognition (англ.) // IEEE Transactions on Circuits and Systems for Video Technology. — 2004. — Vol. 14, no. 1. — P. 4 - 20.
3) VoiceKey.PLATFORM - спецификации | Центр Речевых Технологий | ЦРТ: [Электронный ресурс] // URL: http://www.speechpro.ru/product/sistemy-upravleniya-kachestvom-i-avtomatizatsii/voicekey/specification
4) *Вольф Д.А.* Модель, численная и программная реализация оценивания частоты основного тона речевого сигнала с помощью сингулярного спектрального анализа: Автореф… дис. канд. техн. наук. - Томск: ТУСУР, 2015. - 23 с.

5) *Тиунов С.Д.* Модель, численные методы и комплекс программ для акустического анализа голоса в задачах диагностики голосовых расстройств: Автореф… дис. канд. техн. наук. - Томск: ТУСУР, 2014. - 19 с.
6) *Поршнев С.В., Рабайа Ф.* Исследование особенностей применения метода сингулярного спектрального анализа в задаче анализа и прогнозирования временных рядов: монография. – Ульяновск: Зебра, 2016. – 167 с.

Н.А. Вернигорова, И.В. Головина

ПРОБЛЕМА ИМПОРТОЗАМЕЩЕНИЯ В ИНФОКОММУНИКАЦИЯХ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: импортозамещение, экспортоориентированное импортозамещение, инфокоммуникации, программное обеспечение, IT-рынок.

В статье исследуется проблема импортозамещения, начиная с предпосылок ее возникновения и заканчивая поиском оптимальных решений поставленных задач как на уровне отдельной отрасли промышленности, так и государства в целом. Анализируется опыт стран, прошедших политику импортозамещения. Рассматривается уровень зависимости инфокоммуникационной отрасли от импорта. Анализируются шаги, предпринятые для решения сложившейся проблемы.

N.A. Vernigorova, I.V. Golovina

THE PROBLEM OF IMPORT SUBSTITUTION IN INFOCOMMUNICATIONS

North-Caucasian branch of the Order of the Red Banner of Labor of the federal state budgetary educational institution of higher education "Moscow Technical University of Communication and Informatics", Rostov-on-Don, Russia

Keywords: import substitution, export-oriented import substitution, infocommunication, software, IT-market.

This article examines the problem of import substitution, starting with the preconditions of its origin and ending with the search for optimal solutions of the tasks on the level of individual industries and the state as a whole. The experience of countries which have adopted a policy of import substitution. Discusses the level of dependence InfoComm industry from imports. Analyzes the steps taken to solve the current problem.

Защита интересов национального производителя, обеспечение экономической безопасности является актуальной задачей правительства каждой страны. Россия не является исключением, поскольку на сегодняшний день многие отрасли отечественной экономики сильно зависят от иностранного оборудования и технологий производства. В большинстве отраслей доля импорта составляет свыше 50 процентов от общего объема продаж. В качестве главного средства решения этой проблемы в настоящее время рассматривается импортозамещение.

Импортозамещающая стратегия как раз направлена на обеспечение экономической независимости и поддержку внутреннего производителя путем замещения импортных товаров отечественной продукцией. Актуальность этой темы особенно возросла, когда в 2014 году против России западноевропейскими государствами и США был введен ряд торгово-экономических санкций. 4 августа 2015 года были созданы правительственные комиссии по импортозамещению и начат процесс по созданию пакета нормативных актов по поддержке отечественного производителя со стороны государства.

Следует отметить, что проблема обеспечения оптимального баланса отечественной и импортируемой продукции на внутренних рынках не является новой для России. После дефолта 1998 гг., в период кризиса и резкой девальвации рубля Россия столкнулась с потенциальным дефицитом валюты у субъектов хозяйственной деятельности и резким удорожанием импорта, который в 1998 г. сократился на 20 %, в 1999 г. – еще почти на 30%. В то же время рост ВВП и промышленного производства в 1999 г. примерно на четверть был обеспечен за счет увеличения выпуска российской продукции, заместившей импортную. Сегодняшняя ситуация, однако, отличается от того, что наблюдалось в конце 90-х годов. В тот период вытеснение импорта отечественной продукцией происходило за счет увеличения загрузки существующих мощностей, а не в результате создания новых отраслей и производств. В настоящее время задача импортозамещающей политики состоит в формировании системы стимулов для поддержки национального производства продукции, конкурентоспособной не только на внутреннем, но и на внешнем рынке. Речь идет не только о том, чтобы удовлетворить внутренние потребности отечественной продукцией, сократив при этом импортные закупки. Никто не отказывается от участия в международном разделении труда и преимуществ глобального кооперирования производства. Однако инвестиции, которых потребует реализация импортозамещающей стратегии, окупятся лишь в том случае, если продукция национального производства выйдет на внешние рынки. Новизна подхода заключается в дополнении импортозамещения чертами экспортоориентированной модели.

Значительная часть существующих сегодня стран мира на пути своего развития уже проходили процесс ограничения импорта с целью стимулировать спрос на отечественные товары. Так, стратегия импортозамещающего роста экономики использовалась в странах Латинской Америки (Бразилия, Аргентина и Мексика) и Азии (Южная Корея, Тайвань). Следует отметить, что для Аргентины итоги импортозамещающей индустриализации в 1970-1980-х гг. оказались неудачными. Из-за относительно небольшого размера внутреннего рынка и жестких ограничений на импорт размер экспорта оказался крайне незначительным. В результате, создав первоначальные условия для развития промышленности и диверсификации экономики, импортозамещающая политика в Аргентине привела к обострению финансовых проблем, технологической отсталости и впоследствии – к дефолту. В Бразилии и Мексике, а также в

государствах Азии результаты импортозамещающей индустриализации оказались успешнее. Политика импортозамещения в Бразилии в большей степени была нацелена на стимулирование экспорта, а не на ограничение импорта. В стране создавались конкурентоспособные на мировом рынке предприятия обрабатывающей промышленности, наращивали экспорт производители нефти и металлургические предприятия. В странах Азии, прежде всего в Южной Корее, политика импортозамещения рассматривалась как средство укрепления национальной экономики и создания мощного экспортного потенциала. Такая стратегия получила название «экспортоориентированного импортозамещения».

Таким образом, политика импортозамещения в странах Латинской Америки и Азии способствовала быстрому развитию промышленности, снижению зависимости стран от импорта, созданию рабочих мест, росту экспорта. Однако, наблюдались и негативные последствия: нарастание финансовых проблем и технологической отставания, снижение конкуренции, сокращение объема выпускаемой продукции, неэффективное использование ресурсов. Из вышесказанного можно сделать вывод о том, что даже в странах, успешно реализовавших политику импортозамещения, она не являлась самоцелью, а была, скорее, средством защиты отечественных производителей и обеспечения экономической независимости.

Для сферы инфокоммуникаций импортозамещение является критически важным. По экспертным подсчетам, на сегодняшний день доля иностранных продуктов на российском рынке ИТ составляет примерно 75% (2). На рынке корпоративного программного обеспечения вообще нет достаточного задела в виде конкурентоспособных отечественных продуктов. Доля импорта в сегменте пользовательского офисного программного обеспечения – 97% (1). В радиоэлектронной промышленности доля отечественных товаров на внутреннем рынке не превышает 18%. Российский рынок инфокоммуникаций фактически монополизирован иностранными производителями. При этом существует достаточно много российских решений, которые позволяют реализовать широкий спектр задач заказчиков, но, несмотря на это, компании продолжают выбирать иностранные продукты. Срабатывает инерция, а также активный маркетинг зарубежных фирм.

Согласно Приказу Минкомсвязи «Об утверждении плана по импортозамещению программного обеспечения” от 01.02.2015 №96, главной целью на сегодняшний момент является установление конкретных задач по поэтапному сокращению доли импортного программного обеспечения в российских государственных и коммерческих предприятиях. Все продукты, либо их прототипы, импортозамещение которых признается необходимым, разделены в документе на три сегмента, к каждому из которых подобран индивидуальный подход со стороны государства. Учитывая важность решения задачи импортозамещения в инфокоммуникационном секторе, помимо мер нормативно-правового регулирования, ведутся работы по разработке и реализации государственных программ. К их числу относится программа «Развитие электронной и радиоэлектронной промышленности на 2013 - 2025 годы», реализация которой позволит снизить долю импорта в сегменте телекоммуникационного оборудования.

Спектр мер, предпринимаемых для реализации импортозамещения в сфере инфокоммуникаций, очень широк. Среди них можно выделить ряд важных административных решений, например, запрет для госорганов и компаний с

государственным участием закупать иностранное программное обеспечение, если есть одобренные российские аналоги. Учитывая, что одномоментно перейти на отечественное ПО невозможно, предлагается создать реестр отечественных программных продуктов, чтобы госзаказчики по крайней мере не покупали за рубежом то, что есть у нас. В связи с этим было принято постановление Правительства №1236, которое устанавливает правила ведения Реестра отечественного программного обеспечения и вводит приоритет отечественного программного обеспечения при госзакупках. Также был сформирован и запущен Единый реестр российских программ для электронных вычислительных машин и баз данных, который включает в себя исключительно российские разработки и к которому должны обращаться госзаказчики при закупках программного обеспечения.

При проведении политики импортозамещения в инфокоммуникационной отрасли прежде всего необходимо стимулировать развитие отечественного производства, так как жесткий запрет на закупку иностранных программ может пагубно отразиться на состоянии российской IT-отрасли и привести к закрытию иностранного рынка программного обеспечения для отечественных производителей. Поэтому выдвигаются предложения о создании некоммерческих организаций, деятельность которых будет направлена на коллективную разработку программного обеспечения для отраслей с высокой степенью зависимости от иностранных поставок. По инициативе Минкомсвязи создан Российский фонд развития информационных технологий для поддержки разработки и продвижения программного обеспечения по таким направлениям, как мобильные операционные системы, системы управления базами данных, корпоративные операционные системы и т.п. Фонд может также заниматься координацией деятельности институтов развития, софинансировать проекты, нацеленные на глобальные рынки.

Предлагается также ввести различные экономические преференции производителям отечественного телекоммуникационного оборудования, например, снижение налога на прибыль и НДС, снижение импортных пошлин на комплектующие изделия и повышение пошлин на ввоз готового телекоммуникационного оборудования и др.

Следует отметить, что реальное продвижение по пути импортозамещения уже имеется. Так, государственная система «Мир», на базе которой осуществляется выдача документов, удостоверяющих личность, перешла на программное обеспечение российского производства, а также на свободное программное обеспечение. В настоящее время система «Мир» использует 130 серверов, базирующихся на процессорах отечественного производства архитектуры «Эльбрус», а также межсетевые экраны «Рубикон-К», производимые компанией НПО «Эшелон». С 2016 г. начала работу первая в России централизованная система поддержки импортозамещения – «Выбирай Российское». Основная задача системы – создание единой площадки для взаимодействия заказчиков и отечественных производителей и информирования заказчиков о возможностях замещения импортных товаров отечественными аналогами.

Смысл импортозамещения в сфере инфокоммуникаций заключается не в отказе или сокращении импорта аппаратных и программных средств, а в создании условий для модернизации российской экономики и обеспечении информационной безопасности. Хотя первоначальным импульсом к разработке программ импортозамещения послужили западные санкции, было бы неправильно утверждать, что это вынужденная мера. Для России это стратегическая задача, имеющая долговременный характер и требующая

серьезных инвестиций в создание и развитие конкурентного внутреннего IT-рынка с экспортными перспективами. Формула «конкурентное импортозамещение» должна получить практическое воплощение.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения» 01.04.2015. – minsvyaz/ru/ru/documents/4548.
2. zimport.ru.
3. www.arppsoft.ru.

И.В. Водовозов, Д.А. Васинев

РАЗРАБОТКА УЗЛА ДОСТУПА К ТРАНСПОРТНОЙ СЕТИ С КОММУТАЦИЕЙ ПАКЕТОВ ДЛЯ ПРИМЕНЕНИЯ В УЧЕБНОМ ПРОЦЕССЕ

Академия ФСО России, Орел, Россия

Ключевые слова: Распределенные компьютерные сети, маршрутизация, туннелирование, GRE, L2/L3VPN.

В статье рассмотрен узел доступа к сети с коммутацией пакетов, позволяющий организовать взаимодействие между территориально распределенными сегментами, благодаря применению технологий GRE и L2/L3 VPN . Предложена схема подключения коммуникационного оборудования применительно к существующей сети учебного заведения.

I.V. Vodovozov, D.A. Vasinev

DEVELOPING OF THE ACCESS NODE TO THE PACKET SWITCHING NETWORK FOR USING IN AN EDUCATION PROCESS

FSO Academy, Orel, Russia

Key words: distributed computer networks, routing, tunneling, GRE, L2/L3 VPN.

The work it is described the access node to the packet switching network, that allows to organize interaction between territorial-distributed segments via implementation of GRE and L2/L3 VPN technologies. Proposed scheme of communication hardware is optimal, according to existing network of the educational institution.

При решении учебных задач в существующей сети учебного заведения возникает проблема, связанная с невозможностью распространения маршрутов ЛВС аудиторий через сеть учебного заведения. Решение данной проблемы возможно с помощью применения технологий GRE и L3VPN, позволяющих организовать статические туннели между учебными аудиториями. Схема подключения коммуникационного оборудования применительно к существующей сети с коммутацией пакетов, реализованная в данном узле доступа является оптимальной.

В работе рассматривается узел доступа к сети с коммутацией пакетов, предназначенный для формирования умений и навыков работы с коммуникационным оборудованием, проведения практических, лабораторных занятий, учебно-производственной практики по дисциплинам сетевой тематики.

Данный узел доступа позволяет организовать взаимодействие территориально-распределенных сегментов внутренней локальной сети через сеть учебного заведения, выступающую в роли сети оператора связи, что позволяет применять его для организации процесса обучения дисциплинам сетевой тематики.

Узел доступа состоит из разработанных телекоммуникационных стоек, коммуникационного оборудования и набора соединительных кабелей, представляющих собой фрагмент сети с коммутацией пакетов. Разработаны типовые задания по настройке коммутации и маршрутизации в коммуникационном оборудовании. Таким образом, на разработанном узле представлены уровни доступа и распределения телекоммуникационной сети. Полученное техническое решение может применяться для формирования у обучающихся умений и навыков построения и администрирования сетей с коммутаций пакетов, функционирующих на основе стека TCP/IP.

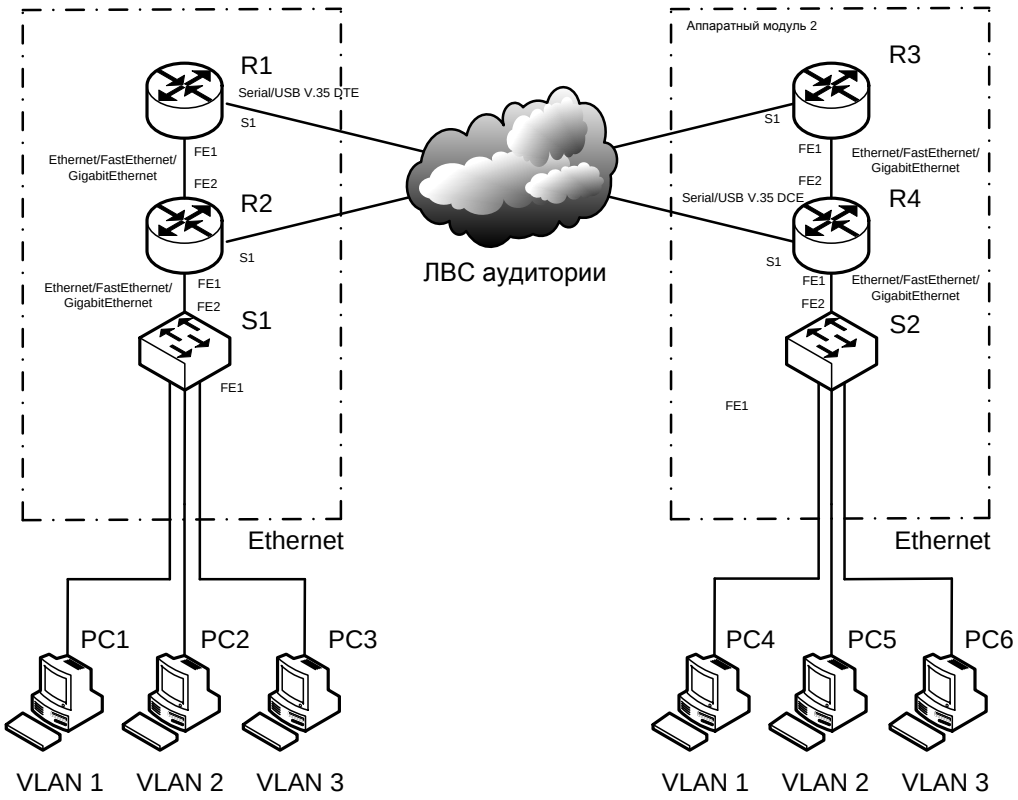


Рис. 1. Структурная схема узла доступа

Узел доступа (рис. 1) состоит из двух аппаратных модулей, каждый из которых включает:

- телекоммуникационную стойку;
- маршрутизаторы (Cisco 2511, Cisco 2800 и Cisco 4500);
- коммутаторы (D-Link DES-1210-52-ME, D-Link DGS-3620-28SC, D-Link DGS-1224T и D-Link DES-1226G);
- сетевые фильтры.

В состав узла доступа входят телекоммуникационные стойки с установленными на них коммутаторами D-Link DES-1210-52-ME, D-Link DGS-3620-28SC, D-Link DGS-1224T и D-Link DES-1226G маршрутизаторами Cisco 2800, Cisco 2511 и Cisco 4500, а также стоечными сетевыми фильтрами.

Данный узел доступа применяется в учебном процессе кафедры. В рамках занятий обучаемые настраивают коммуникационное оборудование различных уровней, формируют умения и навыки в администрировании сетей, построенных на основе стека протоколов TCP/IP. Также разработанный узел доступа позволяет изучать особенности технологической реализации существующих схем связи и исследовать перспективные технологии и отдельные технологические решения.

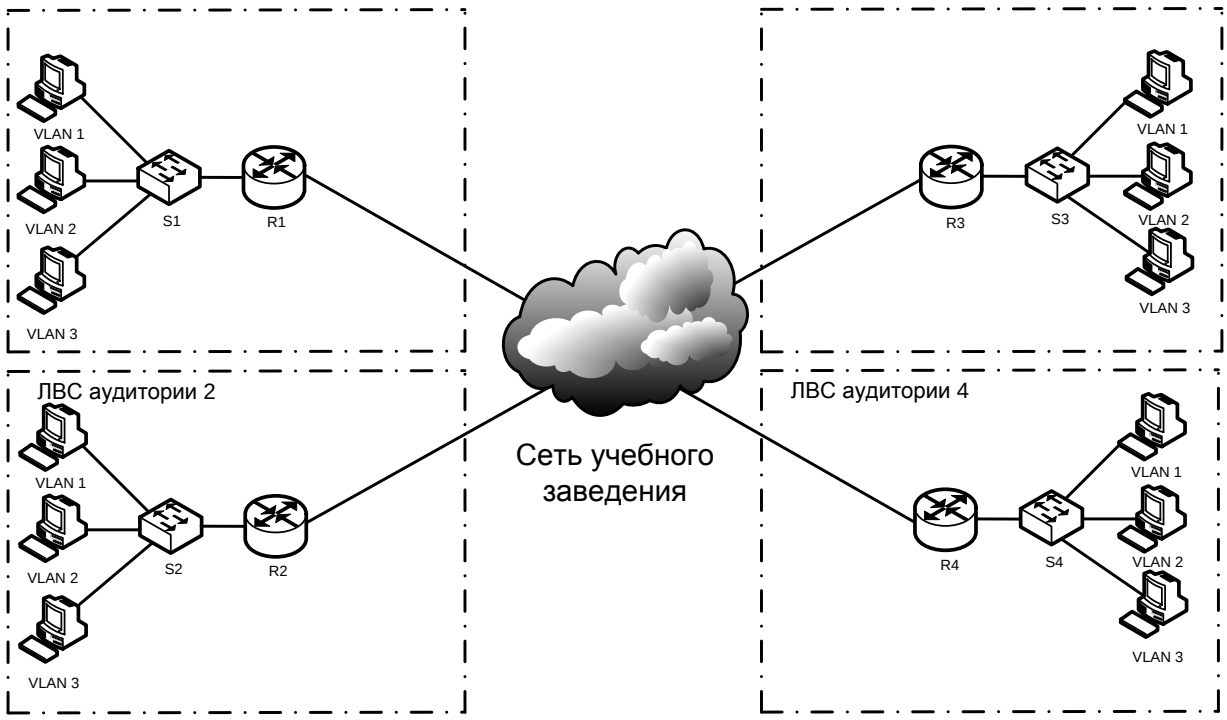


Рис.2. Пример возможной топологии, организуемой на узле доступа

Организуя топологию на основе коммутатора, с помощью коммутации VLAN можно достичь большого количества разнообразных вариантов логической топологии, вносить изменения в которые при помощи предлагаемого способа управления можно будет оперативно, точно и удаленно. Кроме того, данный стенд позволяет исследовать варианты применения отечественного мультипротокольного оборудования в мультисервисном узле связи.

СПИСОК ЛИТЕРАТУРЫ

1. *Олифер В.Г., Олифер Н.А*. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПБ.: Питер, 2010. – 944 с.
2. *Таненбаум Э*. Компьютерные сети, 4-е изд./ Э. Таненбаум. – СПБ.: Питер, 2003. – 992 с.
3. *Кучерявый Е.А*. Управление трафиком и качество обслуживания в сети Интернет. – СПБ.: Наука и Техника, 2004 – 336 с.

М.Г. Гизатуллин, Ф.И. Тураев

НЕКОТОРЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ МЕДИАОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ В РАМКАХ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ»

Уральский юридический институт МВД России, Екатеринбург, Россия

Ключевые слова: образовательная организация высшего образования, основная образовательная программа высшего образования, образовательный процесс, медиаобразовательные технологии, учебная дисциплина, программное обеспечение, криптографическое преобразование, компетенции, обучающиеся.

В статье рассматривается реализация медиаобразовательных технологий на базе программного обеспечения SecurEngine Professional для осуществления обучающимися образовательной организации высшего образования процессов, связанных с криптографическими средствами защиты информации.

M.G. Gizatullin, F.I. Turaev

SOME ASPECTS OF REALIZATION OF MEDIA EDUCATIONAL TECHNOLOGIES WITHIN ORGANIZATION OF EDUCATIONAL PROCESS FOR THE SUBJECT MATTER «BASIS OF INFORMATION SECURITY IN INTERIOR»

Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg, Russia

Keywords: the educational organization of the higher education, the main educational program of the higher education, educational process, media educational technologies, a subject matter, the software, cryptography conversion, competences studying.

In article implementation of media educational technologies on the basis of the software of SecurEngine Professional for implementation by students of the educational organization of the higher education of the processes connected to cryptography means of information protection

is considered.

В соответствии с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года [1], стратегической целью государственной политики в области образования является повышение доступности качественного образования, соответствующего требованиям инновационного развития экономики, современным потребностям общества и каждого гражданина.

В соответствии с федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» [2], экспериментальная и инновационная деятельность в сфере образования осуществляется в целях обеспечения модернизации и развития системы образования. Экспериментальная деятельность направлена на разработку, апробацию и внедрение новых образовательных технологий, образовательных ресурсов. Инновационная деятельность, в частности ориентирована на совершенствование материально-технического обеспечения системы образования.

Во многих образовательных организациях высшего образования различных Федеральных министерств и подведомственных им агентств (Министерство внутренних дел Российской Федерации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерство образования и науки Российской Федерации (Федеральная служба по надзору в сфере образования и науки), Министерство связи и массовых коммуникаций Российской Федерации (Федеральное агентство связи), Министерство транспорта Российской Федерации (Федеральное агентство железнодорожного транспорта) и т.д.) осуществляется внедрение и развитие медиаобразовательных технологий в рамках организации образовательного процесса по реализуемым основным образовательным программам высшего образования.

Внедрение медиаобразовательных технологий в образовательный процесс образовательных организаций высшего образования обусловлено требованиями к характеристике профессиональной деятельности обучающихся, результатам освоения основных образовательных программ высшего образования подготовки обучающихся, структуре основных образовательных программ высшего образования подготовки обучающихся, условиям реализации основных образовательных программ высшего образования подготовки обучающихся, оценке качества освоения основных образовательных программ высшего образования подготовки обучающихся [2].

В образовательных организациях высшего образования, реализующих основные образовательные программы высшего образования по специальностям «Правоохранительная деятельность», «Правовое обеспечение национальной безопасности», «Экономическая безопасность», «Психология служебной деятельности» в соответствии с федеральными государственными образовательными стандартами высшего образования по указанным специальностям [3]-[6], обучающиеся осваивают учебную дисциплину «Основы информационной безопасности в органах внутренних дел».

В рамках осуществления образовательного процесса в образовательной организации высшего образования при организации практических занятий, лабораторного практикума в соответствии с рабочей программой учебной дисциплины [7] «Основы информационной безопасности в органах внутренних дел» для осуществления обучающимися процессов, связанных с криптографическими и стеганографическими

средствами защиты информации рассматривается реализация медиаобразовательных технологий.

Рассмотрим реализацию медиаобразовательных технологий на базе программного обеспечения SecurEngine Professional 1.0 [8] в рамках организации образовательного процесса (практическое занятие, лабораторный практикум) по учебной дисциплине «Основы информационной безопасности в органах внутренних дел» по специальностям «Правоохранительная деятельность», «Правовое обеспечение национальной безопасности», «Экономическая безопасность», «Психология служебной деятельности».

Программное обеспечение SecurEngine Professional 1.0 – это прикладное программное обеспечение, позволяющее обучающимся образовательной организации высшего образования, в общем виде, реализовать процессы, связанные с криптографическими и стеганографическими средствами защиты информации, т.е. получить знания, умения, навыки и (или) опыт деятельности (компетенции) в области реализации программных средств защиты информации. Таким образом, можно отметить, что SecurEngine Professional 1.0 – это своего рода инструмент для осуществления обучения обучающихся образовательной организации высшего образования программным средствам защиты информации.

В работе представлена реализация некоторых возможностей осуществления криптографического преобразования информации на базе программного обеспечения SecurEngine Professional 1.0 в рамках организации образовательного процесса (практическое занятие, лабораторный практикум) по учебной дисциплине «Основы информационной безопасности в органах внутренних дел» по специальностям «Правоохранительная деятельность», «Правовое обеспечение национальной безопасности», «Экономическая безопасность», «Психология служебной деятельности».

На рисунке 1 представлено главное диалоговое окно программного обеспечения SecurEngine Professional 1.0.

Рисунок 1 – Главное диалоговое окно
программного обеспечения SecurEngine Professional 1.0

Главное диалоговое окно программного обеспечения SecurEngine Professional 1.0 содержит следующие элементы:

– «Encrypt Files» («Зашифровать файлы») – элемент, предназначенный для осуществления прямого криптографического преобразования (шифрование исходного файла – прямое преобразование);
– «Decrypt Files» («Дешифровать файлы») – элемент, предназначенный для осуществления обратного криптографического преобразования (дешифрование файла, полученного в результате шифрования исходного файла – обратное преобразование);
– «Hide Files» («Скрыть файлы») – элемент, предназначенный для осуществления прямого стеганографического преобразования (сокрытие исходного файла – прямое преобразование);
– «UnHide Files» («Показать файлы») – элемент, предназначенный для осуществления обратного стеганографического преобразования (представление файла, полученного в результате сокрытия исходного файла в исходном виде – обратное преобразование);
– «Self Decrypt Archive» («Само-дешифровывающийся архив») – элемент, предназначенный для формирования само- дешифровывающегося архива;
– «Wipe Files» («Стирание файлов») – элемент, предназначенный для стирания (уничтожения файлов);
– «Black Board» – элемент, предназначенный для удобства перехода ко всем операциям, реализуемым в SecurEngine Professional 1.0 в рамках одного окна;
– «About» («Информация о программном обеспечении») – элемент, предназначенный для отображения общей информации о программном обеспечении SecurEngine Professional 1.0;
– «Exit» («Выход из программного обеспечения») – элемент, предназначенный для осуществления выхода из программного обеспечения SecurEngine Professional 1.0.

При переходе по элементу «Encrypt Files» («Зашифровать файлы») открывается диалоговое окно, приглашающее пользователя (обучающегося) приступить к процедуре выбора исходных данных для осуществления прямого криптографического преобразования – шифрования исходного файла (рисунок 2).

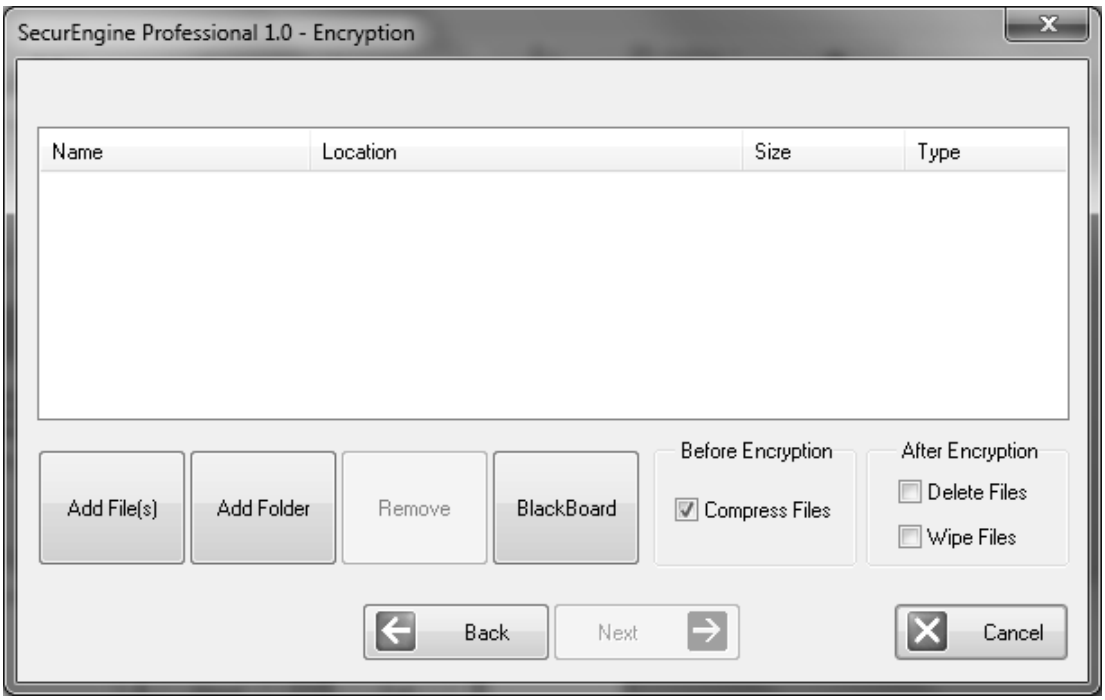


Рисунок 2 – Диалоговое окно прямого криптографического преобразования (выбор исходных данных для осуществления прямого криптографического преобразования)

Диалоговое окно (рисунок 2) содержит следующие элементы:

- «Add File(s)» («Добавить файл (файлы)») – элемент, предназначенный для осуществления выбора файла (файлов), который будет использоваться в качестве исходного компонента в рамках прямого криптографического преобразования (шифрования);
- «Add Folder» («Добавить папку») – элемент, предназначенный для осуществления выбора папки, которая будет использоваться в качестве исходного компонента в рамках прямого криптографического преобразования (шифрования);
- «Remove»» («Удалить») – элемент, предназначенный для удаления файла (фалов), папки, которые выбраны в качестве исходного компонента в рамках прямого криптографического преобразования (шифрования);
- «Black Board» – элемент, предназначенный для удобства перехода ко всем операциям, реализуемым в SecurEngine Professional 1.0 в рамках одного окна;
- «Compress Files» – («Сжать файлы») – элемент, предназначенный для сжатия размера файла (фалов), папки, которые выбраны в качестве исходного компонента в рамках прямого криптографического преобразования (шифрования);
- «Delete Files» («Удалить файлы») – элемент, предназначенный для удаления файла (фалов), папки, которые выбраны в качестве исходного компонента по завершению процедуры прямого криптографического преобразования (шифрования);
- «Wipe Files» («Стирание файлов») – элемент, предназначенный для стирания (уничтожения файлов);
- «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;

– «Next» («Далее») – элемент, предназначенный для перехода к последующему диалоговому окну программного обеспечения SecurEngine Professional 1.0 по окончании выбора определенных элементов текущего диалогового окна;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

По окончании выбора определенных элементов диалогового окна (рисунок 2) необходимо перейти к элементу «Next» («Далее»). При переходе по элементу «Next» («Далее») открывается диалоговое окно, приглашающее пользователя (обучающегося) приступить к процедуре выбора личного (индивидуального) пароля (его подтверждения), алгоритма шифрования, а также пути для сохранения создаваемого файла по завершению процедуры прямого криптографического преобразования (шифрования исходного файла) (рисунок 3).

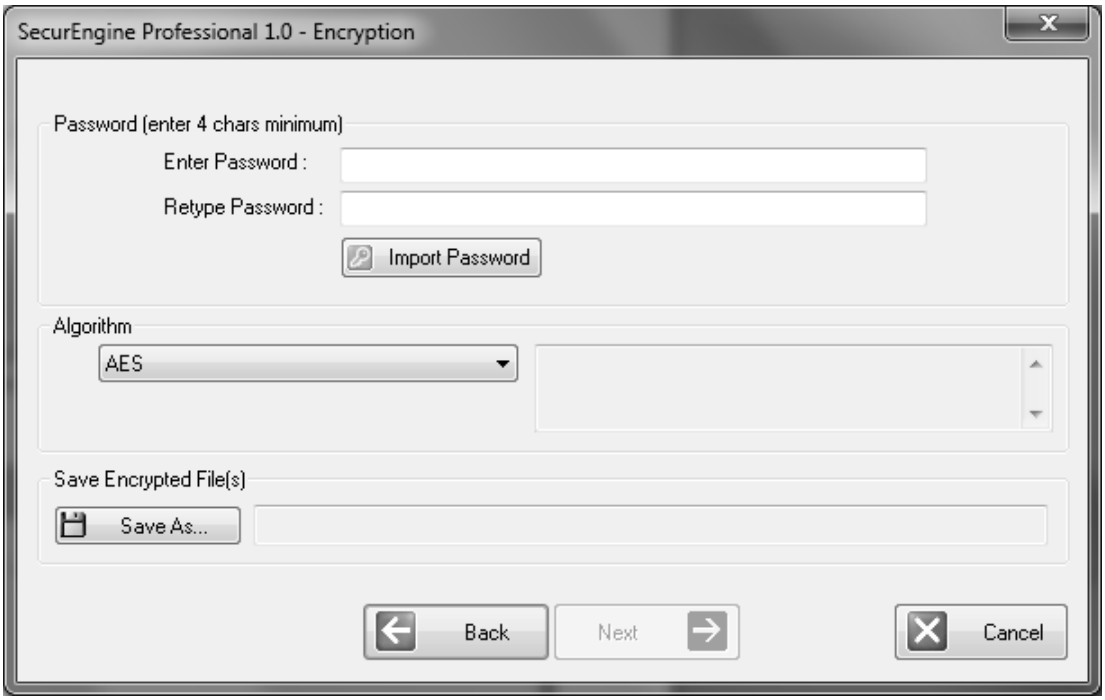


Рисунок 3 – Диалоговое окно прямого криптографического преобразования (выбор личного пароля (его подтверждение), алгоритма шифрования, пути для сохранения создаваемого файла)

Диалоговое окно (рисунок 3) содержит следующие элементы:
– «Enter Password» («Ввести пароль») – элемент, предназначенный для ввода личного (индивидуального) пароля пользователя (обучающегося);
– «Retype Password» («Повторить пароль») – элемент, предназначенный для повторения ввода личного (индивидуального) пароля (подтверждения пароля) пользователя (обучающегося);
– «Algorithm» («Алгоритм») – элемент, предназначенный для выбора алгоритма шифрования пользователем (обучающимся). В программном обеспечении SecurEngine Professional 1.0 представлен ограниченный перечень алгоритмов шифрования, а именно: AES, BlowFish, Gost, ThreeDes;

– «Save As…» («Сохранить как…») – элемент, предназначенный для осуществления процедуры выбора пути для сохранения создаваемого файла в результате прямого криптографического преобразования (шифрования исходного файла). При переходе по элементу «Save As…» («Сохранить как…») открывается диалоговое окно, приглашающее пользователя (обучающегося) приступить к процедуре выбора пути для сохранения создаваемого файла в результате прямого криптографического преобразования (шифрования исходного файла) (рисунок 4);
– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Next» («Далее») – элемент, предназначенный для перехода к последующему диалоговому окну программного обеспечения SecurEngine Professional 1.0 по окончании ввода и выбора определенных элементов текущего диалогового окна;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

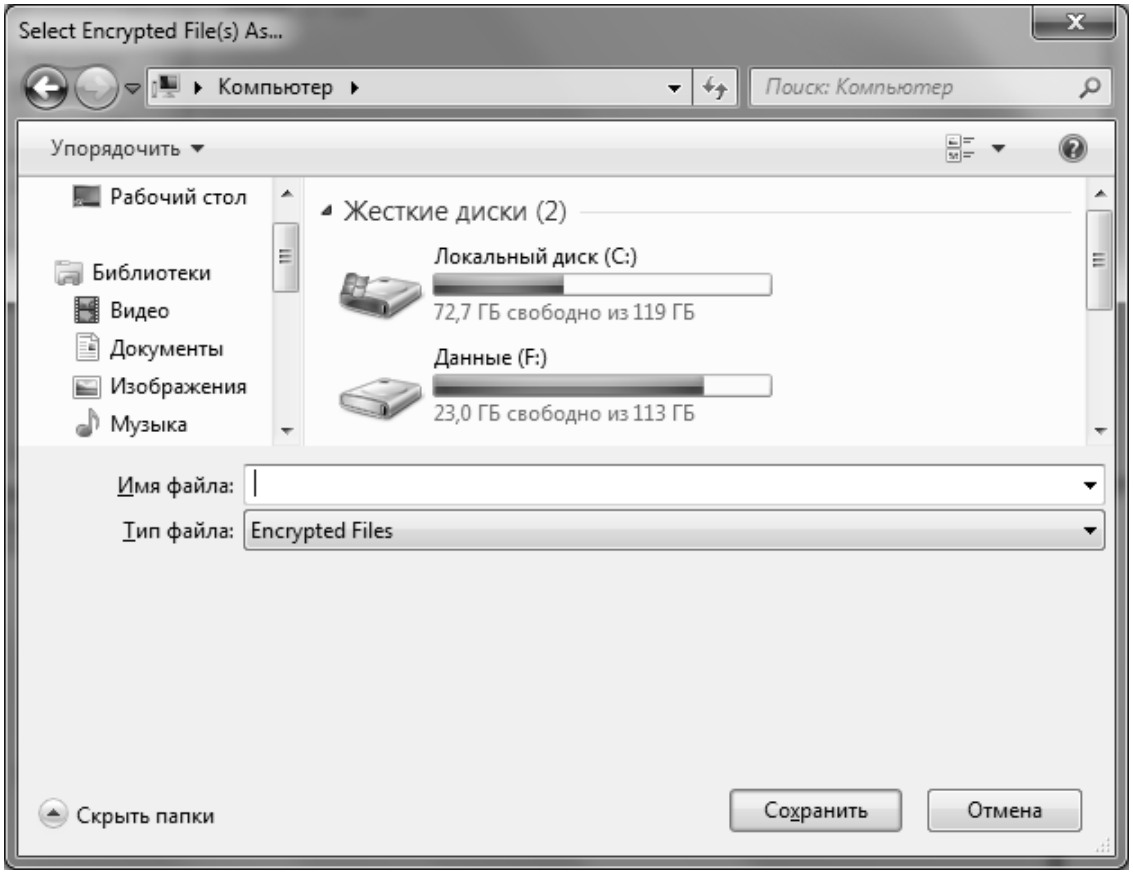


Рисунок 4 – Диалоговое окно выбора пути для сохранения создаваемого файла в результате прямого криптографического преобразования (шифрования исходного файла)

По окончании выбора определенных элементов диалогового окна (рисунок 3) необходимо перейти к элементу «Next» («Далее»). При переходе по элементу «Next» («Далее») открывается диалоговое окно, позволяющее пользователю (обучающемуся)

приступить к процедуре прямого криптографического преобразования (шифрования исходного файла) с учетом выбора ранее определенных элементов (рисунок 5).

Диалоговое окно (рисунок 5) содержит следующие элементы:

– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Encrypt» («Зашифровать») – элемент, предназначенный для осуществления запуска процедуры прямого криптографического преобразования (шифрования исходного файла);
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

При переходе по элементу «Encrypt» («Зашифровать») открывается диалоговое окно, информирующее пользователя (обучающегося) о том, что процедура прямого криптографического преобразования (шифрования исходного файла) завершена (рисунок 6).

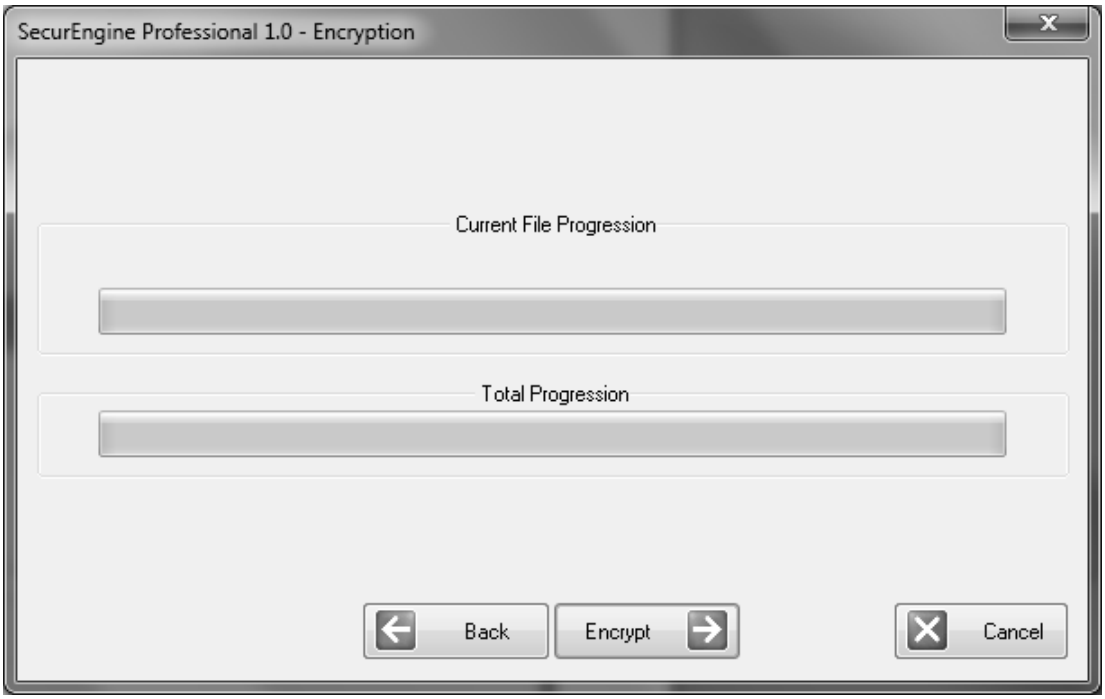


Рисунок 5 – Диалоговое окно, позволяющее пользователю (обучающемуся) приступить к процедуре прямого криптографического преобразования (шифрования исходного файла) с учетом выбора ранее определенных элементов

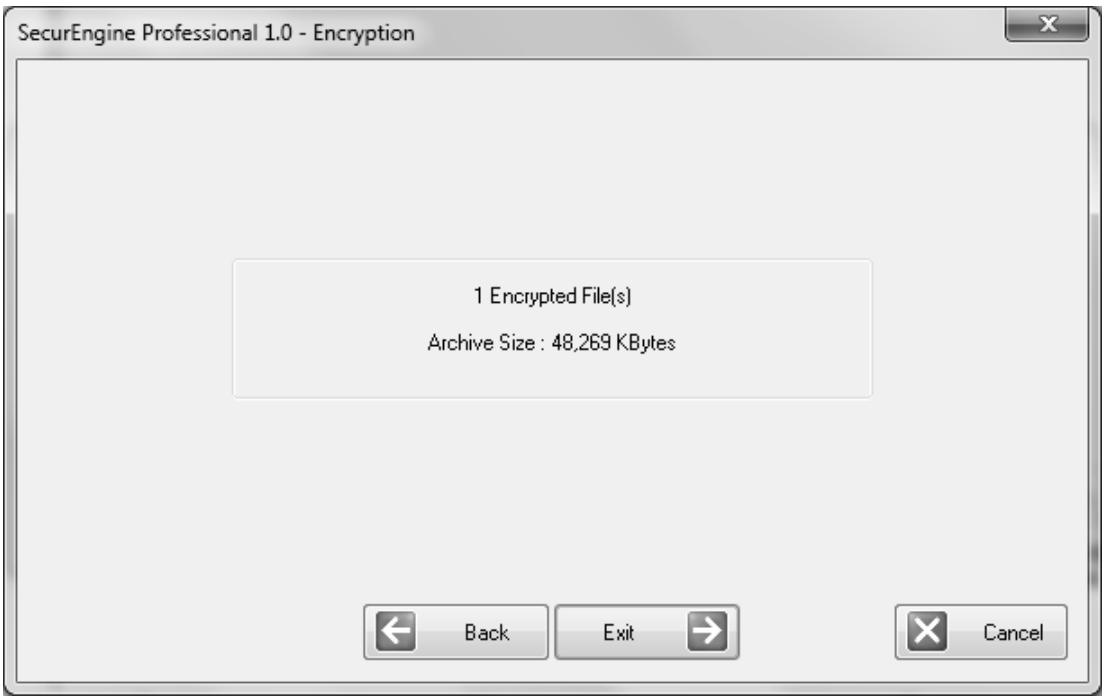


Рисунок 6 – Диалоговое окно, информирующее пользователя (обучающегося) о том, что процедура прямого криптографического преобразования (шифрования исходного файла) завершена

Диалоговое окно (рисунок 6) содержит следующие элементы:

– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Exit» («Выход») – элемент, предназначенный для завершения действий текущего диалогового окна и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

При переходе по элементу «Decrypt Files» («Дешифровать файлы») (рисунок 1) открывается диалоговое окно, приглашающее пользователя (обучающегося) приступить к процедуре осуществления обратного криптографического преобразования – дешифрования файла, полученного в результате осуществления прямого криптографического преобразования (рисунок 7).

Рисунок 7 – Диалоговое окно обратного криптографического преобразования

Диалоговое окно (рисунок 7) содержит следующие элементы:

– «Open…» («Открыть…») – элемент, предназначенный для осуществления выбора файла, полученного в результате осуществления прямого криптографического преобразования.

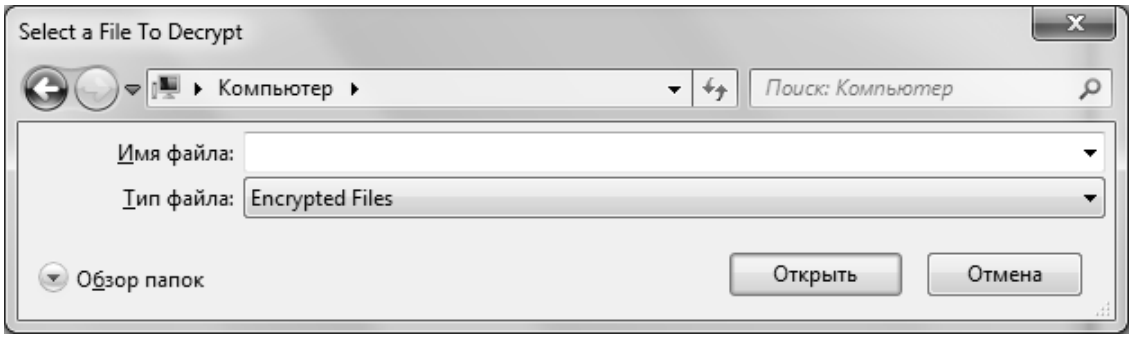


Рисунок 8 – Диалоговое окно выбора файла, полученного в результате осуществления прямого криптографического преобразования

– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Next» («Далее») – элемент, предназначенный для перехода к последующему диалоговому окну программного обеспечения SecurEngine Professional 1.0 по окончании выбора определенных элементов текущего диалогового окна;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

По окончании выбора файла, полученного в результате осуществления прямого криптографического преобразования необходимо перейти к элементу «Next» («Далее») (рисунок 7). При переходе по элементу «Next» («Далее») открывается диалоговое окно,

приглашающее пользователя (обучающегося) приступить к процедуре ввода личного (индивидуального) пароля, алгоритма шифрования (реализуемых в рамках процедуры прямого криптографического преобразования), а также выбора пути для сохранения файла, полученного в результате осуществления обратного криптографического преобразования (рисунок 9).

Рисунок 9 – Диалоговое окно обратного криптографического преобразования (ввод личного (индивидуального) пароля, алгоритма шифрования, а также выбора пути для сохранения файла, полученного в результате осуществления обратного криптографического преобразования)

Диалоговое окно (рисунок 9) содержит следующие элементы:

– «Enter Password» («Ввести пароль») – элемент, предназначенный для ввода личного (индивидуального) пароля пользователя (обучающегося) для осуществления дешифрования;
– «Select the Algorithm» («Выбрать алгоритм») – элемент, предназначенный для выбора алгоритма, использующегося для осуществления дешифрования пользователем (обучающимся);
– «Save As…» («Сохранить как…») – элемент, предназначенный для осуществления процедуры выбора пути для сохранения файла, полученного в результате осуществления обратного криптографического преобразования. При переходе по элементу «Save As…» («Сохранить как…») открывается диалоговое окно, приглашающее пользователя (обучающегося) приступить к процедуре выбора пути для сохранения файла, полученного в результате осуществления обратного криптографического преобразования;
– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;

– «Next» («Далее») – элемент, предназначенный для перехода к последующему диалоговому окну программного обеспечения SecurEngine Professional 1.0 по окончании ввода и выбора определенных элементов текущего диалогового окна;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

По окончании ввода и выбора определенных элементов диалогового окна (рисунок 9) необходимо перейти к элементу «Next» («Далее»). При переходе по элементу «Next» («Далее») открывается диалоговое окно, позволяющее пользователю (обучающемуся) приступить к процедуре обратного криптографического преобразования (дешифрования) (рисунок 10).

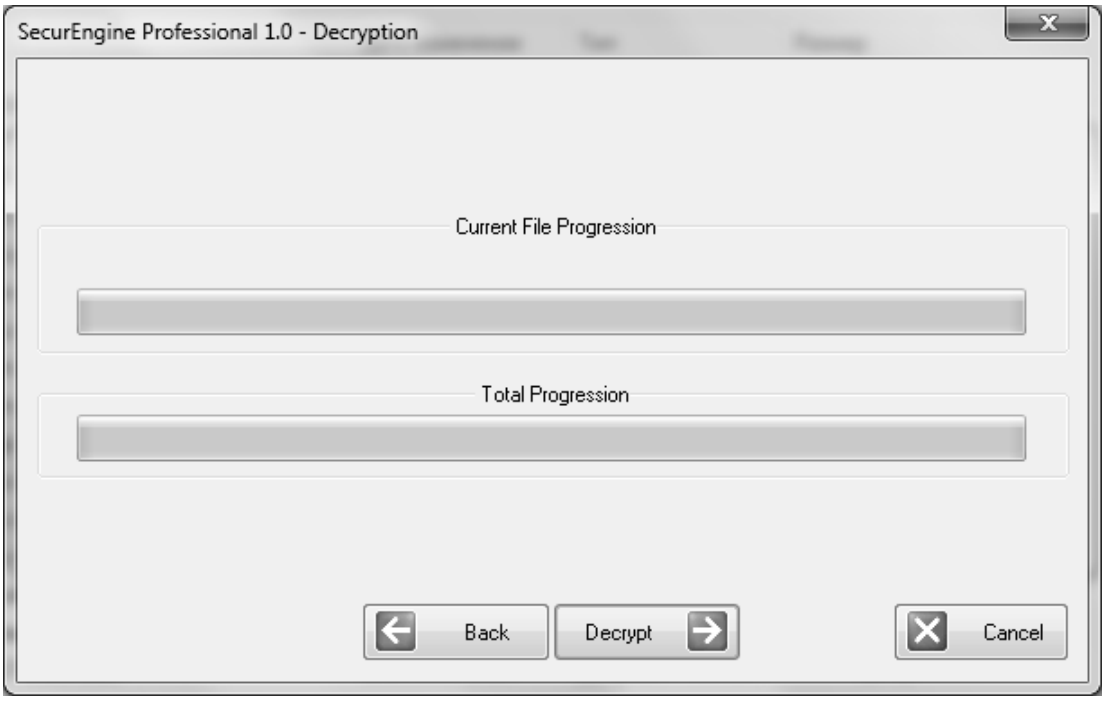


Рисунок 10 – Диалоговое окно, позволяющее пользователю (обучающемуся) приступить к процедуре обратного криптографического преобразования (дешифрования файла, полученного в результате осуществления прямого криптографического преобразования)

Диалоговое окно (рисунок 10) содержит следующие элементы:
– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Decrypt» («Дешифровать») – элемент, предназначенный для осуществления обратного криптографического преобразования (дешифрование файла, полученного в результате шифрования исходного файла – обратное преобразование);
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

При переходе по элементу «Decrypt» («Дешифровать») открывается диалоговое окно, информирующее пользователя (обучающегося) о том, что процедура обратного криптографического преобразования (дешифрования файла, полученного в результате осуществления прямого криптографического преобразования) завершена (рисунок 11).

Диалоговое окно (рисунок 11) содержит следующие элементы:

– «Back» («Назад») – элемент, предназначенный для возврата к предыдущему диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Exit» («Выход») – элемент, предназначенный для завершения действий текущего диалогового окна и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0;
– «Cancel» («Отмена») – элемент, предназначенный для отмены действий пользователя (обучающегося) и перехода к главному диалоговому окну программного обеспечения SecurEngine Professional 1.0.

Рисунок 11 – Диалоговое окно, информирующее пользователя (обучающегося) о том, что процедура обратного криптографического преобразования завершена

В заключение необходимо отметить, что не все основополагающие вопросы по реализации некоторых возможностей программного обеспечения SecurEngine Professional 1.0 вошли в статью в связи с большим необходимым объемом представления информации, а именно: реализация стеганографического преобразования информации, создания само-дешифровывающегося архива и т.д.

Реализация медиаобразовательных технологий на базе программного обеспечения SecurEngine Professional 1.0 в рамках организации образовательного процесса (практическое занятие, лабораторный практикум) позволит обучающимся образовательной организации высшего образования получить и (или) закрепить знания, умения, навыки и (или) опыт деятельности (компетенции) в соответствии с осваиваемой учебной дисциплиной «Основы информационной безопасности в органах внутренних дел».

Программное обеспечение SecurEngine Professional 1.0, в полной мере, может быть использовано в образовательном процессе образовательных организаций высшего образования Федеральных министерств и подведомственных им агентств для осуществления программного криптографического и стеганографического

преобразования информации при выполнении обучающимися практических, лабораторных и исследовательских работ по учебным дисциплинам (модулям, курсам), реализации дипломных проектов (работ), выпускных квалификационных работ и т.д., «затрагивающих» область реализации программных средств защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года: распоряжение Правительства Российской Федерации от 17.11.2008 № 1662-р [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
2. Об образовании в Российской Федерации: федеральный закон от 29.12.2012 № 273-ФЗ [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
3. Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.02 Правоохранительная деятельность (уровень специалитета): приказ Минобрнауки России от 16.11.2016 № 1424 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
4. Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.01 Правовое обеспечение национальной безопасности (уровень специалитета): приказ Минобрнауки России от 19.12.2016 № 1614 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
5. Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета): приказ Министерства образования и науки РФ от 16.01.2017 № 20 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
6. Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 37.05.02 Психология служебной деятельности (уровень специалитета): приказ Минобрнауки России от 19.12.2016 № 1613 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
7. Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры: приказ Министерства образования и науки РФ от 19.12.2013 № 1367 [Электронный ресурс]. – URL:http://www.garant.ru/ (дата обращения: 10.03.2017).
8. Информационный портал по безопасности SecurityLab.ru [Электронный ресурс]. – URL:http://www.securitylab.ru/software/233870.php/ (дата обращения: 10.03.2017).

Е.И. Гниломёдов, И.И. Шестаков

ОЦЕНКА ПРИМЕНИМОСТИ КОМПОНЕНТОВ РАЗВЕТВЛЕННЫХ СЕТЕЙ СТАНДАРТА ITU-T G.984 АРХИТЕКТУРЫ FTTX, ДЛЯ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА С ЦЕЛЬЮ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКОВ В СООТВЕТСТВИИ С ФГОС ВО 3+

Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: пассивная оптическая сеть доступа, технология GPON, архитектура FTTx, учебная лаборатория.

В статье рассмотрены оценка возможности применимости компонентов оптический сетей доступа стандарта ITU-T G.984, для организации проведения лабораторно-практических работ, с целью формирования профессиональных компетенций выпускников технических вузов в соответствии с ФГОС ВО 3+.

Y.I. Gnilomyodov, I.I. Shestakov

ESTIMATION OF THE APPLICABILITY OF THE COMPONENTS OF THE ELECTED NETWORKS OF THE ITU-T G.984 STANDARD ARCHITECTURE FTTX, FOR THE ORGANIZATION OF THE TRAINING PROCESS FOR THE FORMATION OF THE PROFESSIONAL COMPETENCIES OF GRADUATES IN ACCORDANCE WITH THE FEDERAL STATE EDUCATIONAL STANDARD OF HIGHER EDUCATION 3+

Federal Communications Agency Ural Technical Institute of Communications and Informatics (branch) FGBOU VO "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibGUTI), Russia

Key words: passive optical access network, GPON technology, FTTx architecture, training laboratory.

The article considers the assessment of the applicability of the components of the optical access network of the ITU-T G.984 standard, for organizing laboratory and practical work, with the aim of forming the professional competencies of graduates of technical universities in accordance with the Federal State Educational Standards for Higher Education 3+.

Введение

Разветвленные оптические сети стандарта ITU-T G.984 – это пассивные, волоконно-оптические сети доступа древовидной (или шинной) топологии, предназначенные для организации мультисервисных услуг связи (передача видео, голоса и данных – сервис Triple Play) в радиусе двадцати километров.

Сегодня можно выделить две разновидности сетей стандарта ITU-T G.98x, применяемых на практике:

1) гигабитная пассивная оптическая сеть GPON, описывается в рекомендации ITU-T G.984.x;
2) пассивная оптическая сеть на базе протокола Ethernet – EPON, описывается в рекомендации ITU-T G.985 и G.986.

На фоне сетей GPON и EPON реализуемых на практике, прослеживаются попытки технической реализации и внедрения новых стандартов, таких как:

1) XG-PON – гигабитная пассивная оптическая сеть с пропускной способностью нисходящего потока 10/100 Гбит/с, данный стандарт описывается в рекомендации ITU-T G.987;
2) NG-PON2 – гигабитная, многоволновая оптическая пассивная сеть с с пропускной способностью нисходящего потока до 40 Гбит/с, данный стандарт описывается в рекомендации ITU-T G.989.

Анализируя ранок связи в области предоставления услуг Triple Play по технологии PON за десять лет, аналитически можно представить диаграмму проникновения стандартов PON на период до 2030 года (рисунок 1). Из диаграммы видно, что технология EPON не получила широкого применения, и в будущем применяться на практике не будет, основной причиной являются частые сбои в работе связки станционного оборудования (OLT - Otical Line Terminal) и оптических сетевых окончаний (ONT - Optical Network Terminal) устанавливаемых у абонентов.

Таким образом, можно выделить три перспективные разновидности технологий PON: GPON, XG-PON и NG-PON2.

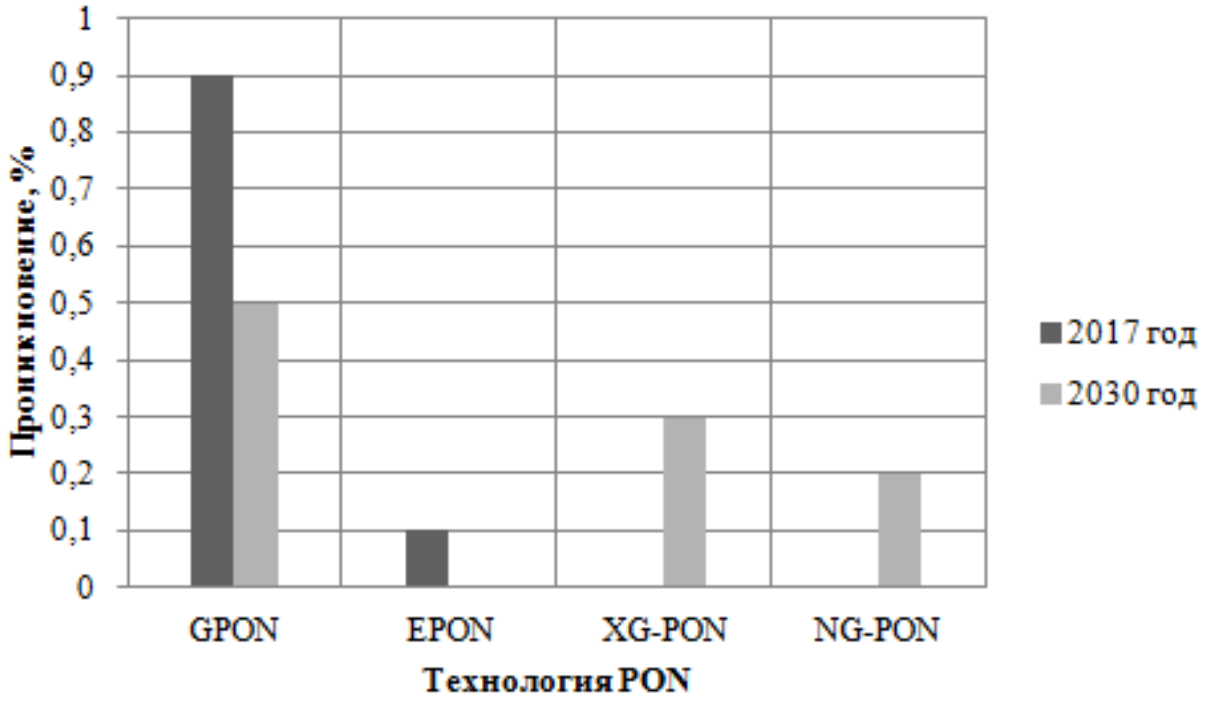


Рисунок 1 - Анализ проникновения стандартов сетей PON на период до 2030 года

Пассивные оптические сети обладают рядом преимуществ и недостатков:

1) преимущества:
   - малая стоимость оптического тракта OLT – ONT;
   - вместо активного оборудования, которое перенаправляет (разветвляет) оптический трафик из «ветви в ветвь» дерева сети PON, применяется пассивное устройство – оптический разветвитель, для которого не требуется организация электропитания; его можно разместить в оптической муфте; стоимость в разы меньше по сравнению с активным оборудованием;
   - быстрая развертываемость;
   - простата масштабируемости;
   - высокая пропускная способность, гигабиты в секунду;
   - для дуплексной связи требуется одно оптоволокно;
   - высокая помехозащищенность, по сравнению с электрическими сетями доступа;
   - технология PON позволяет организовать сервис Triple Play.
2) недостатки:
   - сложность организации СКС в многоэтажных жилых домах;
   - резервирование «ветви» дерева сети PON ведет к увеличению стоимости сети PON в десятки раз;
   - сложность анализа рефлектограмм сети PON, в которой применяются оптические разветвители емкостью более 1×16;
   - дальность связи ограничивается емкостью оптического разветвителя.

Качество связи в сетях PON зависит не только качества монтажных работ, вводного контроля, дальнейшей технической эксплуатации, под которой понимают: настройка и конфигурация оборудования OLT и ONT; метрологические измерения параметров сети PON методом светопропускания и рефлектометрии оптоволокна, но и от выпускников телекоммуникационных ВУЗов, которые будут проектировать, и эксплуатировать сети PON. Для формирования профессиональных компетенций у выпускников, в телекоммуникационных ВУЗах необходимо применять в учебном процессе современную техническую базу в виде лабораторий.

Организация учебной лаборатории

В УрТИСИ СибГУТИ была предложена идея о разработке новой лаборатории «Оптические сети доступа архитектуры FTTx» (Fiber To The x - оптическое волокно до точки «x»). На рисунке 2 представлен план размещения компонентов оптической сети доступа архитектуры FTTx.

Активное станционное оборудование сети PON (оптический линейный терминал OLT) размещается в открытой 19 дюймовой телекоммуникационной стойке. Такое исполнение позволит наглядно продемонстрировать внешний вид OLT, его подключение к оптическому кроссу и системе электропитания (ИБП – источник бесперебойного питания), а также наглядно представить, как выполнено крепление оптического кабеля в стойке и его ввод в оптический кросс.

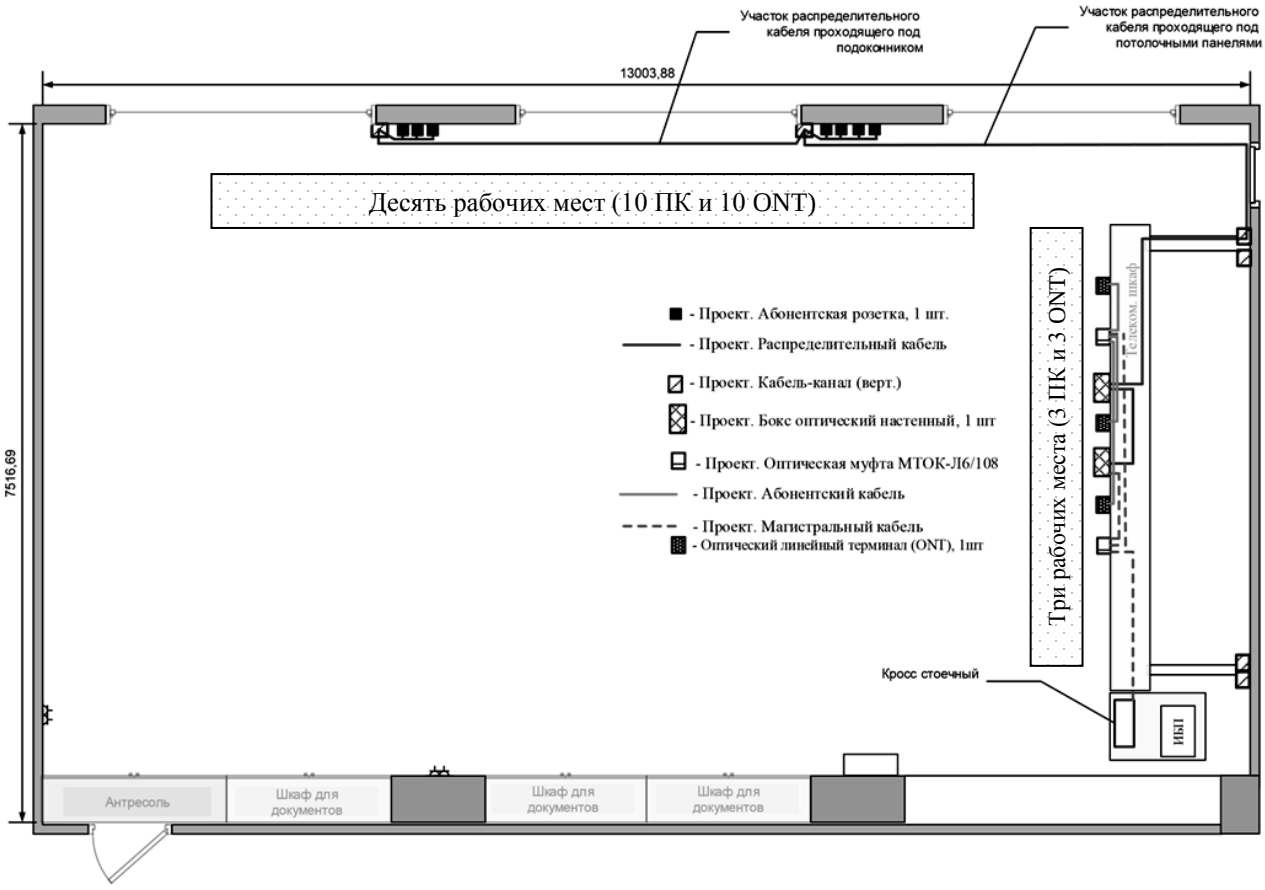


Рисунок 2 – План размещения компонентов оптической сети доступа архитектуры FTTx в лаборатории №101

Активное пользовательское оборудование (оптическое сетевое окончание ONT) размещено на одиннадцати рабочих местах. Подключение сетевого окончания ONT к распределительной волоконно-оптической линии связи выполнено по схеме: оптический порт GPON ONT – патч-корд SC/APC-SC/APC – оптическая абонентская розетка SC/APC, в которой разварено волокно распределительного оптического кабеля типа «Райзер» и пигтейла SC/APC.

На участке от абонентской оптической розетки SC/APC до БОНа №2 (бокс оптический настенный) организован оптический распределительный кабель типа «Райзер». Для наглядного представления, как прокладывается райзер кабель в слаботочном канале, как выведены волокна из кабеля, как выполнена защита места вывода оптоволокна из кабеля, в лаборатории были задействованы межоконные колонны, вдоль которых смонтирован кабель-канал, в котором проложен райзер кабель, и смонтированы распределительные межэтажные коробки. Кроме этого, в лаборатории наглядно представлена инсталляция БОНов, оптических муфт, разварка оптических волокон магистральных и абонентских самонесущих оптических кабелей с оптическими разветвителями, разварка оптических волокон и разветвителей в БОН.

На рисунке 3 представлена схема организации связи сети PON архитектуры FTTx в учебной лаборатории УрТИСИ СибГУТИ. На рисунке 4 представлен внешний вид компонентов сети PON архитектуры FTTx в учебной лаборатории УрТИСИ СибГУТИ. Смонтированная сеть PON архитектуры FTTx наглядно демонстрирует студентам, как по нормам и правилам выполняется инсталляция оптических компонентов сети PON

архитектуры FTTH и FTTB в частном секторе и жилой местности с многоэтажной застройкой.

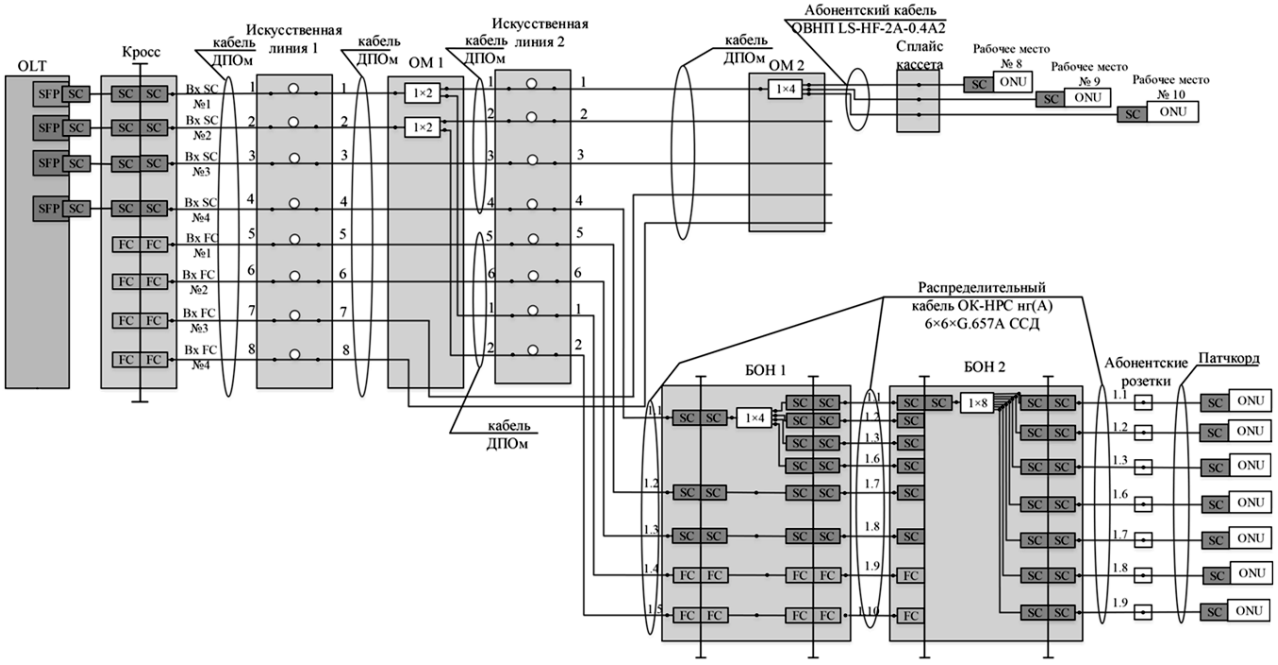


Рисунок 3 – Схема организации связи сети PON архитектуры FTTx в учебной лаборатории УрТИСИ СибГУТИ

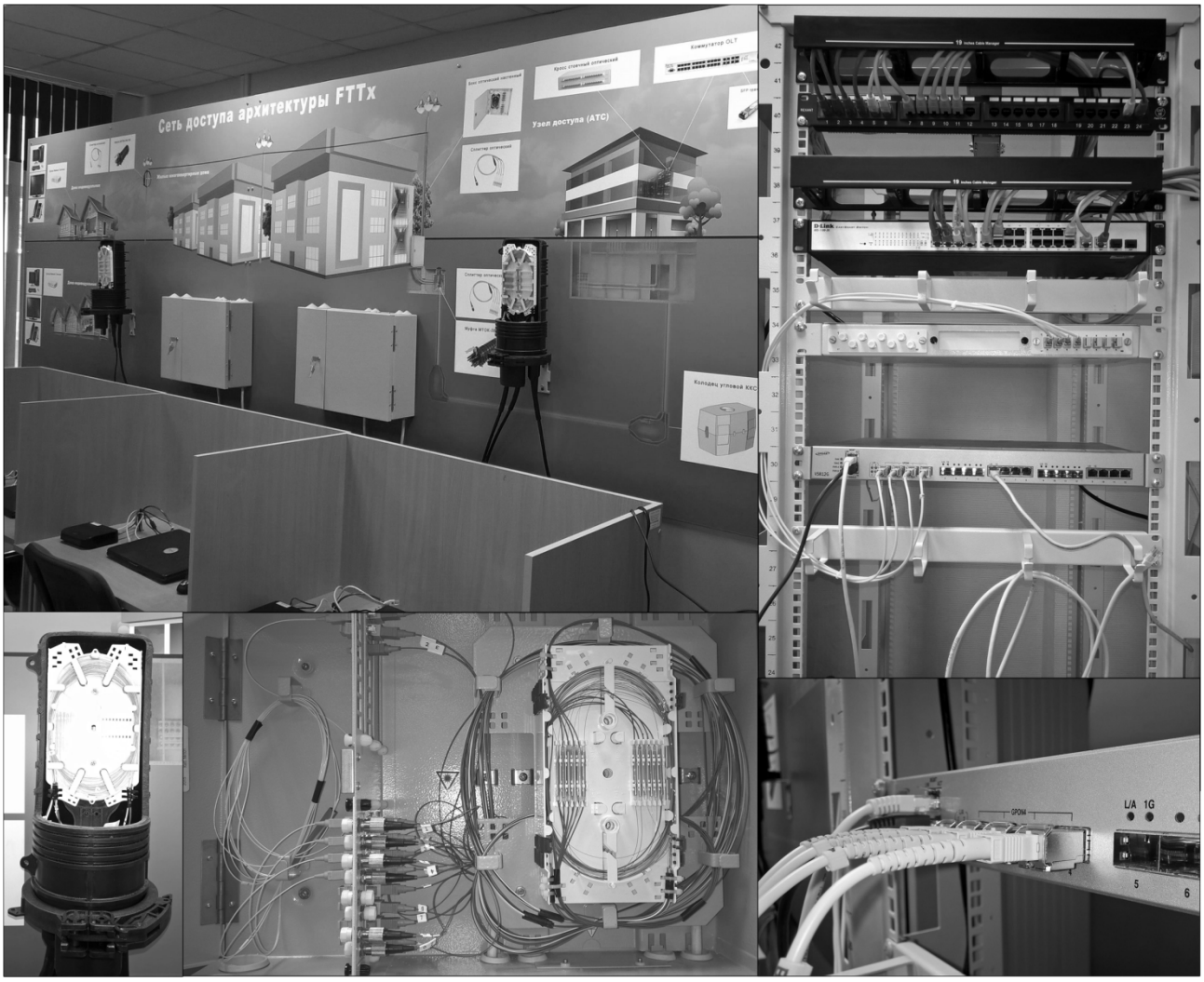


Рисунок 4 – Внешний вид компонентов в учебной лаборатории

Для проведения лабораторных и исследовательских работ, на данном этапе применяется оборудование корейского вендера DASAN, в телекоммуникационной стойке установлено оборудование OLT GPON марки V5812G (4×GPON SFP ports 1:128, 4×EPON), на стороне пользователя установлены ONT GPON марки H640G.

Заключение

Оборудование GPON вендера DASAN, разветвленная волоконно-оптическая линия связи на базе PLC разветвителей 1×2, 1×4 и 1×8, дают возможность организовать лабораторные работы:

1) для бакалавриата:
   - «Конфигурирование оборудования OLT GPON марки V5812G со стороны администратора сети GPON»;
   - «Удаленное конфигурирование оборудования ONT GPON марки H640G со стороны администратора сети GPON»;
   - «Конфигурирование оборудования ONT GPON марки H640G со стороны пользователя сети GPON»;
   - «Конфигурация и проключение оптического маршрута на участке от OLT до ONT»;

– «Рефлектометрия разветвленной сети PON архитектуры FTTx»;
– «Оценка оптических потерь разветвленной сети PON архитектуры FTTx методом светопропускания»;

2) для магистрантов и аспирантов:
– «Исследование влияние коэффициента разветвленности сети PON на качество связи»;
– «Исследование влияние количества подключаемых ONT устройств сети PON на качество связи»;
– «Настройка динамической и статической маршрутизации трафика внутри дерева сети PON, и в сети в целом»;
– «Оценка и анализ возможности организации технологии NG-PON2 поверх существующей архитектуры ВОЛС сети GPON»;
– «Исследование приоритизации трафика на участке OLT – ONU сложной архитектуры».

Учебная лаборатория «Оптические сети доступа архитектуры FTTx» позволит не только сформировать у студентов профессиональные компетенции в соответствии с ФГОС ВО 3+ по дисциплинам «Технология широкополосного абонентского доступа», «Оптические сети», «Сети и системы оптического доступа», «Методы и средства измерений в телекоммуникационных системах», но и организовать проведение курсов повышения квалификации по настройке и конфигурированию оборудования OLT GPON V5812G и ONT GPON H640G компании DASAN; по технической эксплуатации сетей PON архитектуры FTTx.

СПИСОК ЛИТЕРАТУРЫ

1. *Петренко И.И., Убайдуллаев Р.Р.* Пассивные оптические сети PON. Часть 1. Архитектура и стандарты [Электронный ресурс]. Режим доступа: http://t8.ru/wp-content/uploads/2012/01/24.pdf
2. *Гасымов И.* Архитектура оптических сетей доступа FTTH (Fiber-to-the-Home) [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/ downloads/ Cisco_ FTTH_architecture.pdf
3. Рекомендация ITU-T G.984 – Режим доступа: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=G.
4. *Алексеев Е.Б.* Основы технической эксплуатации современных волоконно-оптических систем передачи. Учебное пособие. М.: ИПК при МТУСИ, 1998 г.-224 с.
5. *Богачков И.В., Майстренко В.А., Горлов Н.И.* Новые задачи технической эксплуатации разветвленных волоконно-оптических сетей // Тр. IX Междунар. науч.-техн. конф. «Проблемы техники и технологий телекоммуникаций» ПТиТТ-2008. – Казань: Изд-во КГТУ, 2008. – 514 с. – С. 282–285.

О.В. Гончарова, А.Ю. Опарин

ЗДОРОВЬЕ ПЕДАГОГА – ЗАЛОГ ПРОФЕССИОНАЛЬНОГО ДОЛГОЛЕТИЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: психологическое здоровье преподавателей, квадранты здоровья человека, мотивации здорового образа жизни, стратегии профессионального долголетия.

В статье рассмотрены проблемы психологического, психического и физического здоровья преподавателей. А также определены стратегии профессионального долголетия.

O.V. Goncharova, A.Yu. Oparin

THE HEALTH OF THE TEACHER IS THE KEY TO PROFESSIONAL LONGEVITY

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

Keywords: psychological health of teachers, the quadrants of the health motivation healthy lifestyle, the strategy of professional life.

The article considers the problems of psychological, mental and physical health of teachers. And also identifies the strategy of professional life.

Традиционно можно выделить следующие компоненты здоровья:

- психологическое здоровье;
- психическое здоровье;
- социальное здоровье;
- физическое здоровье.

Психологическое здоровье выступает необходимым компонентом полноценного функционирования и развития человека в ходе его жизнедеятельности.

Психологическое здоровье выступает условием выполнения человеком соразмерных возрастных, социальных и культурных ролей, а также обеспечивает возможность постоянного развития на протяжении всей жизни человека.

Психологическое здоровье акцентирует неразделимость телесного и психологического в человеке, наличие этих элементов необходимо для полного функционирования и жизнеспособности. В связи с этим можно сделать вывод о том, что психологическое здоровье выступает предпосылкой физического.

Здоровье любого человека можно представить в виде круга, поделенного на четыре сектора: физического, эмоционального, интеллектуального и духовного, что представлено на рисунке 1.

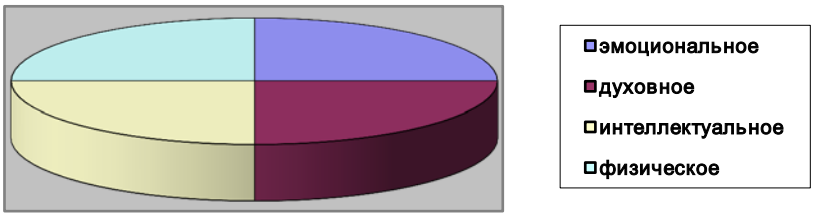


Рисунок 1 – Квадранты здоровья человека

Психологически здоровый человек находится в постоянном развитии и тем самым способствует развитию других людей, адаптируется к быстроменяющимся условиям и требованиям жизни и работы.

Однако если психологическое здоровье – необходимое условие полноценного функционирования, то насколько оно взаимосвязано с физическим здоровьем? Именно психологическое здоровье является предпосылкой здоровья физического.

«Портрет» психологически здорового человека заключается в следующем: творческий, жизнерадостный, открытый и познающий себя и окружающий мир.

Человек может быть здоровым только при наличии всех компонентов здоровья. Добиться этого можно, воспитав в человеке определенную культуру – культуру здорового образа жизни. В формировании культуры здорового образа жизни велика роль педагогов и непосредственного окружения.

При выборе здорового образа жизни можно выделит следующие мотивации:

- самосохранение. Это заключается в том, что человек знает о последствиях совершаемых действий (если это действие угрожает его жизни и здоровью), он это действие не совершает;

- этнокультурные требования общества. Человек живет в обществе, которое на протяжении длительного времени формировало привычки, навыки, вырабатывало систему защиты от неблагоприятных факторов внешней среды;

- возможность для самосовершенствования. Здоровье дает возможность заниматься самосовершенствованием, тем самым можно подняться на более высокую ступень общественной лестницы.

Митина Л.М. выделяет основные показатели профессионального здоровья педагогов, ими являются такие интегральные характеристики личности, как

– педагогическая направленность;
– компетентность (коммуникативная);
– педагогическая гибкость. [1]

Компонентом профессионального здоровья педагога является психологическая культура, которая содержит теоретическую подструктуру – это система сформированных теоретических и эмпирических знаний, и практическую подструктуру – умения и навыки.

В укреплении здоровья педагога необходимо применять стратегии, приемы, способы сохранения профессионального долголетия, к которым можно отнести:

– смыслотворчество – поиск новых смыслов своей трудовой и профессиональной деятельности;
– внутренняя гармония – способность жить в согласии с самим собой;

– понимание себя как индивидуальности, видение самобытности своей личности и осуществление действий не вопреки своей индивидуальности, а в союзе с ней;
– умелое сочетание опыта профессионального сохранения других преподавателей с выработкой своего индивидуального стиля;
– усиление авторства своей профессиональной жизни, поддержание у себя стремления к самовыражению, самоактуализации в личностно значимых и доступных сферах деятельности.

Маслоу А. считал, что люди, достигшие вершин самоактуализации, могут расцениваться как живые эталоны психического здоровья[2].

Каждому педагогу необходимо построить свою индивидуальную программу профессионального самосохранения, результатом которой будет физическое и профессиональное творческое долголетие.

СПИСОК ЛИТЕРАТУРЫ

1. *Митина Л.М.* Психология труда и профессионального развития учителя. М., Академия, 2014
2. Мотивация и личность. 3-е изд. Пер. с англ. Маслоу А. СПб.: Питер, 2015

А.М. Данилова, Ш.А. Турсунов

ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ ИНВЕСТИЦИОННЫМИ ПРОЦЕССАМИ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Ташкентский университет информационных технологий, Ташкент, Узбекистан

Ключевые слова: инвестиции, инвестиционные процессы, информационно-коммуникационные технологии, глобализация, методы оценки инвестиций.

В данной статье рассмотрены вопросы, связанные с управлением инвестиционных процессов в сфере информационно-коммуникационных технологий. Также в статье рассмотрена важность развития информационно-коммуникационных технологий на сегодняшний день. Наглядно представлены виды и принципы инвестирования в сферу информационно-коммуникационных технологий, а также методы оценки инвестиций, применимых для данной сферы.

A.M. Danilova, Sh.A. Tursunov

ORGANIZATION OF INVESTMENT PROCESSES MANAGEMENT IN THE SPHERE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Tashkent university of information technologies, Tashkent, Uzbekistan

Keywords: investments, investment processes, information and communication technologies, globalization, assessment methods of the investments.

In this article the questions connected with investment processes management in the sphere of information and communication technologies are considered. Also in article importance of information and communication technologies development is considered. The types and the principles of investment into the sphere of information and communication technologies, and also assessment methods of the investments applicable for this sphere are visually presented.

В настоящее время информация – основной ресурс в любой сфере деятельности человека. Как гласит, знаменитая фраза Н.М. Ротшильда: “Кто владеет информацией, тот владеет миром”. А с развитием технологий, важность информации увеличивается. Появилось такое понятие, как информационно-коммуникационные технологии.

Развитие современного общества невозможно без информационно-коммуникационных технологий, что позволяет говорить о новой фазе общественного развития, которая получила название «Информационное общество».

Информационное общество – это стадия развития общества, когда использование информационно-коммуникационных технологий (ИКТ) оказывает существенное влияние на основные сферы жизни, как экономика и деловая сфера, государственное управление, образование, социальное обслуживание и медицина, культура и искусство.

А самое главное направление воздействия информационно-коммуникационных технологий *(*ИКТ) на общество – это влияние на структуру народного хозяйства. Как следствие, формируется новая коммуникационная экономика, в которой основным ресурсом развития становятся знания и информация. В связи с этим представляется справедливым характеризовать соответствующий коммуникативной экономике новый тип общества как информационное общество.

Как говорил Первый Президент Республики Узбекистан И.А. Каримов в своем Докладе на расширенном заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2015 году и важнейшим приоритетным направлениям экономической программы на 2016 год: «В современных условиях, в эпоху Интернета и электроники приоритетное значение имеет **широкое внедрение современных информационно-коммуникационных технологий в отраслях экономики, кардинальное ускорение создания системы «Электронное правительство».** Весь мировой опыт показывает, что в настоящее время в глобальной экономике все более возрастающую роль и значение приобретает сектор информационно-коммуникационных технологий, включающий в себя производство компьютерных и телекоммуникационных технологий, разработку программного обеспечения и

предоставление на их основе широкого спектра интерактивных услуг. Не следует забывать, что развитие ИКТ напрямую влияет на уровень конкурентоспособности страны, позволяет собирать и обобщать огромные массивы информации, открывает широкие возможности для управления на стратегическом уровне. Надо сказать, что уже сегодня на ИКТ приходится примерно 5,5 процента мирового ВВП, а по оценкам авторитетных международных экспертов к 2020 году этот показатель превысит 9 процентов». [1]

Поэтому инвестирование в сферу информационно-коммуникационных технологий имеет особое значение.

Узбекистан принимает все меры по совершенствованию процесса управления инвестиционными процессами.

В 2015 году в общем было привлечено и освоено инвестиций за счет всех источников финансирования в эквиваленте 15,8 миллиарда долларов США, или с ростом против 2014 года на 9,5 процента. При этом более 3,3 миллиарда долларов, или свыше 21 процента всех инвестиций – это иностранные инвестиции, из которых 73 процента составляют прямые иностранные инвестиции. [1]

Инвестирование в сферу информационно-коммуникационных технологий отличается своей сложностью и рискованностью.

По объектам инвестирования выделяют следующие виды инвестиций в сферу информационно-коммуникационных технологий:

- Инвестиции в оптимизацию деятельности (Support)
- Инвестиции в развитие новых технологий (Brainware)
- Инвестиции в программные комплексы (Software)
- Инвестиции в аппаратные комплексы (Hardware)
- Инвестиции в инфраструктуру (Infrastructure)

Можно сформулировать следующие принципы инвестирования в сферу ИКТ:

- Рассмотрение проекта на протяжении всего его жизненного цикла
- Сопоставимость условий сравнения различных проектов
- Принцип положительности и максимум эффекта
- Учет фактора времени
- Сотрудничество ИТ специалистов и менеджеров других отделов при принятии других решений
- Рассмотрение ИТ проекта как самостоятельного проекта
- Формирование системы показателей критических для данных компании
- Учет всех издержек, касающихся внедрения и эксплуатации
- Выявление экономических выгод
- Соотнесение предполагаемых результатов внедрения со стратегическими целями внедрения

Одним из ключевых моментов реализации инвестиционных решений является оценка их эффективности. В целом, к методам оценки эффективности проектов предъявляются следующие требования:

- Метод анализа должен быть строго обоснован (не должен содержать противоречий).
- Метод должен учитывать случайных характер изменения во времени показателей информационной системы и разновременность показателей затрат и доходов.

- Метод должен позволять с единых позиций подходить к разным классам систем управления в разных отраслях народного хозяйства и на разных этапах внедрения ИТ.

Итак, можно выделить следующие методы оценки информационно-коммуникационных технологий:

1. **Net Present Value (NPV)** - метод чистого приведенного дохода. Стоит отметить, что метод чистого приведенного дохода скорее способен определить наиболее эффективные инвестиции в информационные технологии, то есть осуществить выбор между несколькими возможными вариантами инвестиций, нежели оценить непосредственно экономический эффект. Однако, само обоснование инвестиций также можно произвести на основании данного метода. Итак, на основании сравнения сумм первоначальных вложений, ожидаемого размера входящих денежных потоков в течение определенных периодов времени и определенной финансовой политикой Компании внутренней стоимости собственного либо привлеченного капитала, метод NPV определяет само наличие прибыльности данных вложений. [2]

2. **Internal Rate of Return (IRR)** - внутренняя норма доходности. Метод внутренней нормы доходности определяет процентную ставку, отношение, а не абсолютную величину, а затем, производится сравнение полученной ставки со ставкой окупаемости уже учитывающей риски проекта. Если рассчитанная окупаемость превышает окупаемость с учетом рисков, то в таком случае инвестиции можно считать обоснованными, если же нет, увы, проект подлежит отклонению. Метод внутренней нормы доходности многими признается наиболее удачным из всех финансовых методов, поскольку является не количественным, а качественным показателем, по сути – пропорцией, а потому более точно способен дать представление по предпочтительности того или иного проекта, особенно в условиях, когда проекты сильно (как в примере, указанном выше) отличаются друг от друга. [2]

3. **Payback** - срок возврата инвестиций. Метод определения срока возврата инвестиций является самым простым, но и самым поверхностным из всех рассматриваемых нами финансовых методов. Уже из названия можно понять, что в рамках данного метода производится расчет срока в течении которого должны окупиться первоначальные инвестиции. Таким образом, срок окупаемости инвестиций в информационные технологии ставится во главу угла. При всей своей кажущейся простоте метод не лишен объективности, и вот почему. Как мы видим, в наше время развитие информационных технологи происходит весьма быстрыми темпами, что влечет за собой появление все новых и новых инструментов и методик, направленных на поддержание бизнеса со стороны ИТ. [2]

4. **Information Economics (IE)** - информационная экономика. Данный метод ориентирован на объективную оценку портфеля инвестиционных проектов и предусматривает направление ресурсов туда, где они приносят наибольшую выгоду. Идея заключается в том, чтобы заставить информационную службу и бизнес - менеджеров расставить приоритеты и представить более объективные заключения о стратегической ценности отдельных проектов для бизнеса для дальнейшего направления инвестиций по самым важным для бизнеса направлениям. Руководителям отделов информационных технологий и бизнес - менеджерам в рамках применения данного метода необходимо составить список из десяти (или более в зависимости от специфики деятельности Компании) главных факторов, влияющих на процесс принятия решения, и оценить

относительную значимость и риск каждого из них для бизнеса. Таким образом, получившиеся значимость и риски будут являться, соответственно, плюсами и минусами проектов. В результате получается полный относительный рейтинг каждого инвестиционного проекта в портфеле информационной службы. Один из самых быстрых способов определения приоритетов и сопоставления инвестиций в информационные технологии с бизнес – стратегией компании, что определяет его широкую распространенность.[2]

Проведем сравнительный анализ приведённых выше методов оценки инвестиций в сферу информационно-коммуникационных технологий (Таблица №1).

Таблица №1. Сравнительный анализ методов оценки привлечения инвестиций в сферу ИКТ.

№	Признаки / Метод оценки	Простота	Затратность	Трудоемкость	Рискованность	Стратегический характер	Оперативность	Поверхностность	Удачность при отдельном использовании
1.	NetPresentValue (NPV)	-	+	+	+	-	+	+	-
2.	Internal Rate of Return (IRR)	-	+	+	+	-	-	-	-
3.	Payback - срок возврата инвестиций	+	-	-	+	-	+	+	-
4.	Information Economics (IE) - информационная экономика	+	-	+	+	-	+	-	-

На основании всего вышесказанного можно сделать достаточно простой вывод. Абсолютно все методы определения экономической эффективности имеют определенные недостатки, поэтому использования одного из методов может как не дать результата вовсе, так и, дав какой-либо результат, привести к ошибочным управленческим решениям. Таким образом, очевидна необходимость использования комплекса методов. Чтобы определить какой комплекс методов использовать, необходимо руководствоваться постулатом, что затраты на осуществление какого либо действия не должны превосходить результаты от этого действия.

Можно сделать вывод, что сфера информационно-коммуникационных технологий является перспективно развивающейся, здесь аккумулируется большое количество средств, требующее эффективное управления для будущего развития. Процесс инвестирования имеет свои методы оценки количественных и качественных показателей эффектности вложений. Необходимо тщательно подходить к выбору метода оценки инвестиций, особенно в сфере информационно-коммуникационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. *Каримов И.А.,* Доклад Первого Президента Республики Узбекистан Ислама Каримова на расширенном заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2015 году и важнейшим приоритетным направлениям экономической программы на 2016 год
2. *Крысанова С.П.,* Инвестиции в информационные технологии. ГОУ ВПО ГУУ, Журнал «Общество, государство, право», 2015

Н.В. Данилова

ОЦЕНКА ПАРАМЕТРОВ В МОДЕЛИ СТОХАСТИЧЕСКОЙ ВОЛАТИЛЬНОСТИ

Южный федеральный университет, Ростов-на-Дону, Россия

Ключевые слова: модель стохастической волатильности, фильтр Калмана, оценка параметров

В статье приведена модель стохастической волатильности и рассмотрен способ оценки параметров модели с помощью фильтра Калмана-Бьюси

N.V.Danilova

ESTIMATION OF PARAMETERS IN THE STOCHASTIC VOLATILITY MODEL

South Federal University, Rostov-on-Don, Russia

Keywords: stochastic volatility model, Kalman filter, estimation of parameters

The stochastic volatility model is presented in the paper. The way of estimation of parameters is considered.

Оперируя конкретной моделью, наиболее естественным было бы получение оптимальной в среднеквадратичном смысле оценки волатильности или какой-либо функции от волатильности. Так, оперируя моделью стохастической волатильности первого порядка [1,2,3], естественно попытаться найти оптимальную оценку $\ln\sigma_n^2$, исходя из уравнений:

$$\ln h_n^2 = \ln\sigma_n^2 + \ln\varepsilon_n^2,$$
$$\ln\sigma_n^2 = a_0 + a_1 \ln\sigma_{n-1}^2 + c\delta_n.$$

Введем обозначения: $x_n = \ln h_n^2, y_n = \ln \sigma_n^2$. В этих обозначениях система приобретает вид:

$$x_n = E\ln \varepsilon_n^2 + y_n + \left(\ln \varepsilon_n^2 - E\ln \varepsilon_n^2\right),$$
$$y_n = a_0 + a_1 y_{n-1} + c\delta_n.$$

Рассмотрим случайную величину $\eta_n = \ln \varepsilon_n^2 - E\ln \varepsilon_n^2$. Математическое ожидание и дисперсия $E\eta_n = 0, D\eta_n = D\ln \varepsilon_n^2 = \frac{\pi^2}{2}$. Представим уравнения в виде:

$$x_n = E\ln \varepsilon_n^2 + y_n + \frac{\pi}{\sqrt{2}}\xi_n,$$
$$y_n = a_0 + a_1 y_{n-1} + c\delta_n,$$

где $\xi_n = \frac{\sqrt{2}}{\pi}\eta_n$. Математическое ожидание и дисперсия $E\xi_n = 0, D\xi_n = 1$. Таким образом, полученные уравнения задают линейную стохастическую систему, в которой величины δ_n распределены по нормальному закону $N(0,1)$, а величины ξ_n не являются гауссовскими. Это обстоятельство препятствует непосредственному использованию теории линейной фильтрации Калмана-Бьюси [4,5].

Тем не менее, чтобы получить линейный фильтр, рассмотрим фильтр Калмана-Бьюси, который будет оптимальным при условии гауссовости величин ξ_n. Обозначим через $z_n = Dy_n$, u_n – наилучшая в среднеквадратичном смысле линейная оценка y_n по наблюдаемым $x_1, ..., x_n$. В этих обозначениях фильтр Калмана-Бьюси реализуется в уравнениях [6,7]:

$$u_{n+1} = \left(a_0 + a_1 u_n\right) + \frac{a_1 z_n}{\pi^2/2 + z_n}\left(x_{n+1} - E\ln \varepsilon_n^2 - u_n\right)$$

$$z_{n+1} = \left(a_1^2 + c^2\right) - \frac{\left(a_1 z_n\right)^2}{\pi^2/2 + z_n}.$$

При этом $u_0 = Ey_0, z_0 = Dy_0$.

Если построить график $\ln \sigma^2$ и u, то становится понятно, что прогноз с помощью линейного фильтра Калмана-Бьюси является удовлетворительным прогнозом. Отметим, что прогноз волатильности позволяет найти одношаговый интервальный прогноз цены

Отметим, что в том случае, когда в исходной модели известны априорные распределения вероятностей для параметров, при оценке более эффективным является байесовский подход, в котором используется апостериорное распределение параметров модели.

До сих пор мы использовали в качестве исходного гауссовское распределение. Однако тематика нелинейных моделей далеко не исчерпывается этим. Интерес представляют также и другие распределения, обладающие свойствами устойчивости и безграничной делимости.

СПИСОК ЛИТЕРАТУРЫ

1. *Ширяев А.Н.* Основы стохастической финансовой математики. Т.1.Факты, модели. Т.2. Теория. М.:ФАЗИС, 2004.
2. *Ширяев А.Н.* Вероятность. Изд.2-е, перераб. и доп. М.:Наука, 1989.
3. *Липцер Р.Ш., Ширяев А.Н.* Статистика случайных процессов. М.: Наука, 1974.
4. *Балакришнан А.В.* Теория фильтрации Калмана. М.:Мир, 1988.
5. *Леман Э.* Теория точечного оценивания. М.: Наука,1991.
6. *Белявский Г.И., Данилова Н.В.* Линейные и нелинейные модели финансовых индексов. Ростов-на-Дону, ЮФУ, 2014.
7. *Белявский Г.И., Данилова Н.В.* Модели финансовых рынков с дискретным временем. Ростов-на-Дону, ЮФУ, 2016.

Д.Е. Демидов, Л.Н. Евдакова

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ РАЗВИТИЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ В РОССИИ

Уральский технический институт связи и информатики, Екатеринбург, Россия

Ключевые слова: инфокоммуникационные технологии, информационное общество, сети следующего поколения, интернет вещей, конвергенция, IMS, Softswitch, OTT-провайдер.

В статье рассмотрены проблемы и перспективные направления развития инфокоммуникационных технологий в России до 2030 г, в частности, концепции сетей следующего поколения – IMSи Softswitch, интеллектуальные сети, облачные вычисления, OTT-провайдеры, Интернет вещей (IoT), а также мобильные сети пятого поколения 5G.

D.E. Demidov, L.N. Evdakova

DEVELOPMENT PROSPECTS AND PROBLEMS OF INFOCOMMUNICATION BRANCH IN RUSSIA

Ural Technical Institute of Communication and Computer Sciences (branch) “Siberian State University of Telecommunications and Informatics” in Ekaterinburg.

Key words: infocommunication technologies, information society, Next Generation Networks, Internet of things, convergence, IMS, Softswitch, OTT service provider.

The problems and perspective trends of development of infocommunication technologies in Russia up to 2030, in particular the concept of the Next Generation Networks – IMS and

Softswitch, intelligent network, cloud computing, OTT service providers, the Internet of Things (IoT) and mobile networks of the fifth generation 5G are discussed in this article.

Телекоммуникации, мультимедиа и информационные технологии – сфера, которая всемирно подвержена стремительным, кардинальным и непрерывным изменениям. Каждую секунду во всех странах, в сердце мировых технологических инноваций – Калифорнийской Кремниевой долине, в научно-исследовательских центрах, за стенами корпораций мировых гигантов ведутся маркетинговые войны за оригинальную идею, инновационное решение, нового покупателя,новое предложение. Отрасль инфокоммуникационных технологий (ИКТ) проникает во все сферы деятельности человека и является одной из самых значимых по степени влияния на частную и рабочую жизнь, социальную сферу, экономику, имидж и статус страны в мировом сообществе.

Как показывают международные исследования, существует тесная взаимосвязь между развитием ИКТ и экономическим благополучием страны. Масштабное развертывание технологий интернет-доступа и высокоскоростной связи является катализатором развития ИКТ проектов, способствует ускорению и масштабированию технологического прогресса,создает множественный мультипликативный эффект на другие отрасли национальной экономики, и в итоге обеспечивает рост валового внутреннего продукта (ВВП) как отдельных регионов, так и страны в целом. Кроме того, развивающиеся страны с более совершенной инфокоммуникационной инфраструктурой привлекают больше иностранных инвестиций, а также аутсорсинговых компаний.

Развитие инфокоммуникационных технологий (ИКТ) является одним из стратегических направлений модернизации экономики, афинансированиеразвитияинфокоммуникационной инфраструктуры способствует укреплению стратегического положения каждой страны в перспективе на долгие годы [4].

Актуальность выбранной темы обусловлена тем, что развитие ИКТ является одним из стратегических направлений модернизации экономики, а финансированиеразвитияинфокоммуникационной инфраструктуры способствует укреплению стратегического положения каждой страны в перспективе долгих лет.

Цель работы – определить перспективы и проблемы развития инфокоммуникационной отрасли в России до 2030 года.

На сегодняшний день значительное влияние на требования к ИКТ-услугам оказывает процесс*конвергенции,*который приводит к тому, что данные услуги становятся доступны всем пользователям, независимо от способов доступа.

Классическим примером результата конвергенции являются сети следующего поколения (NextGenerationNetworks, NGN). NGN– концепция построения сетей связи, которые обеспечивают предоставление широкого спектра услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

На базе концепции NGNбыли сформированы такие концепции, как Softswitchи IMS (IP Multimedia Subsystem). На данный момент наблюдается активное внедрение данных технологий в существующие сети связи.

IMS – это ключевая ступень в эволюции операторов на пути создания сети связи новогопоколения, реализующая принцип доступности всего спектра услуг, как для мобильныхабонентов, так и для абонентов фиксированной сети доступа. Платформа IMS представляетсобой экономичное решение, которое позволяет с минимальными издержками внедритьогромный спектр новых услуг для абонентов, в том числе с учетом их индивидуальныхпотребностей. Экономичность решения основана на универсальности компонентов,использовании стандартных интерфейсов и возможности интеграции в существующуюсеть оператора. Платформа IMS – этоважнейший элемент сети связи, обеспечивающий предоставление новых услуг, их роуминг,мобильность абонента и ряд других перспективных возможностей.

Softswitch, согласно словам президента Lucent Technologies Джека Мерфи, представляет собой «систему, предназначенную для того, чтобы отделить функции управления соединениями от функций коммутации, способную обслуживать до 100 тыс. абонентов и поддерживать открытые стандарты, а следовательно - взаимодействовать с серверами приложений», что так же характеризует ее, как сеть NGN[1].

Принципы организации и архитектура инфраструктуры инфокоммуникаций современной экономики определяются специфическими признаками развития ИКТ. Будущая эволюция инфокоммуникационных технологий будет осуществляться в направлениях:

- повышения скорости передачи информации, что обусловлено возрастающими возможностями оптических каналов и широкополосных линий;
- удешевления и миниатюризации оконечных средств;
- интеллектуализации сетей передачи информации;
- развития технологий и стандартов беспроводной связи, освоения более высоких частот радиочастотного ресурса;
- удаленного управления финансами, производством и домом на основе мобильного Интернет;
- виртуализации хранилищ и обработки данных.

Высокие скорости передачи данных требуются для передачи объемных мультимедийных данных. Рост интеллектуальности сетей обеспечивается за чет использования микроэлектроники и применения программного обеспечения во всех сетевых устройствах. Данная интеллектуальность обеспечивает увеличение гибкости, возможностей и надежности сетей, а такжезначительно упрощает управление глобальными сетями,в частности, в неоднородных средах.

Миниатюризация и беспроводные средства приводят к широкому распространению мобильных оконечных устройств и,следовательно, к глобальной мобильности и доступу к ИКТ-услугам, независимо от местоположения. Возрастающее проникновение стандартов,миниатюризация электронных устройств, а также снижение стоимости приводят к созданию и наиболее широкому применениюмобильных устройств.

Интеллектуальная сеть предполагает огромноеколичество служб как для администратора сети, так и для пользователя. К ключевым особенностямданных сетей относятся: простая и динамичная система заказов ИКТ-услуг и конфигурации в соответствии с изменениями потребностей пользователя, быстрая адаптация управления глобальными сетями в неоднородных средах.

Способность к взаимодействию нескольких систем или компонентов для обмена и использования информациипредоставляет возможность создавать инфокоммуникационные системы бизнеса и производства, образования и науки с возможностью удаленного управления ими, доступу к вычислительным ресурсам через сеть Интернет.

Значительные перспективы использования инфокоммуникаций дает информационно-технологическая концепция Cloud Computing, называемая «облачные технологии» или «облачные вычисления», которая позволяет на основе распределенных центров обработки данных (ЦОД) и виртуальных баз данных оказывать услуги.Непостоянство потребления услуг иобъединение ресурсов поставщика услуг для обслуживания большого числа потребителейпозволяют получать экономию на масштабах производства услуг, в перечень которых входят не только услуги вычисления, но и программное обеспечение (ПО), платформа и инфраструктура как услуги. Данная модель бизнеса обеспечивает возможность применения потребителем виртуальной инфраструктуры для самостоятельного управления ресурсами хранения и обработки данных, прикладным ПО исетями, а также для размещения собственного ПО и приложений.[2]

Еще одной тенденцией на рынке инфокоммуникационных услуг является появлениесильных конкурентов для операторов связи в лице OTT-провайдеров (Over-The-Top), предоставляющих услуги с использованием IP-технологий. Отличительным признаком данной услуги является ее специальный субъект – поставщик услуги, а не оператор связи. Характерными примерами OTT-провайдеров являются мессенджеры, позволяющие передавать как текстовую, так и мультимедийную информацию (Skype, Viber, WhatsApp), онлайн-кинотеатры (Ivi, MEGOGO, Zoomby), сервисы потокового видео (YouTube, RuTube) и т.п.

Конкуренция на рынке услуг, предопределившая успех OTT-провайдеров, обусловлена следующим фактором – абоненты все реже используют традиционный услуги связи, предоставляемые сотовыми операторами, предпочитая им бесплатные OTT-сервисы для мобильного широкополосного доступа.

Данная тенденция на телекоммуникационном рынке вполне объяснима. В основе нее находится психология абонентов, которые заинтересованы в том, чтобы получать услуги при наименьших затратах, не задумываются о том, каким образом происходит процесс их предоставления.

Основной объем трафика OTT-услуг формируют услуги, связанные с передачей тяжелого контента, например, потоковое интернет-видео, обмен файлам и online-игры. Постоянный рост IP-трафика формирует потребность в необходимых для пропуска данного трафика сетевых ресурсах, т.е. доступная полоса пропускания сетей операторов должна наращиваться пропорционально росту трафика. В том случае, когда модернизация сети связи, проводимая оператором и направленная на увеличение ее пропускной способности, не успевает за темпами роста трафика, возникает эффект перегрузки данной сети связи.

Прямым следствием перегрузки является снижение качества всех предоставляемых на ее базе услуг: как OTT, формирующих основные объемы трафика, так и базовых услуг, формирующих доходы операторов связи. Только создание операторами альтернативного

продукта способно снизить OTT-трафик посредством того, что аналогичные OTT-сервисам услуги начнет оказывать непосредственно оператор связи.

Реальным решением проблемы для операторов связи в контексте острой конкуренции с OTT-провайдерами является создание телекоммуникационной экосистемы, основанной на RCS-решении (RichCommunicationServices) – Расширенные Мультимедийные Услуги.

Телекоммуникационная экосистема оператора связи предполагает построение RCS-ядра как сетевого элемента, основанного на мультимедийной подсистеме IMS (IP Multimedia Subsystem), что позволит оператору предоставить в пользование абонентам коммуникационный сервис, по своей функциональной составляющей аналогичный OTT-сервисам на современном этапе.[3]

Одним из важнейших направлений в развитии отрасли является Интернет вещей (Internetof Things, IoT).Интернет вещей представляет собой сеть, в которой программируемые объекты (вещи) могут беспрепятственно обмениваться информацией при помощи интернет. Управление осуществляетсяавтоматически и не требует контроля со стороны человека.

IoT все чаще применяется в жизни людей в таких важных сферах, как медицина, экономика, образование, сельское хозяйство, строительство, банковское дело и во многих других.

В сфере медицины IoT помогает в уходе за больными пациентами. Например, разработанный специализированный цифровой приемник собирает информацию о состоянии больного с различных сенсоров, которые находятся на нем. Далее информация анализируется и передается лечащему врачу в любой точке мира. Таким образом, пациент может получать консультации,не выходя из дома.

Набирает темпы производство умных велосипедов с поддержкой GPS-навигации, что позволяет определять местоположение велосипеда. Помимо этого,такие велосипеды оснащены аккумулятором, что позволяетзарядить смартфон, а это, в свою очередь, повышает мобильность пользователя и его независимость от электросети. Проводятся активные разработки повнедрению противоугонной системы для велосипедов, которой пользовательсможет управлять при помощи смартфона.

Интернет вещей дает возможность экономить и в дорожном строительстве. Так, например, при строительстве новой дороги, прежде чем укладывать асфальт, проводится большое количество подготовительных работ. Проводятся такие работы в ручном режиме и требуют от исполнителя высокого уровня подготовки и квалификации.

Однако если дорожная техника обладает специальной системой управления, то ее можно задействовать в автоматическом режиме, загрузить трехмерную цифровую модель проекта и, например, за счет этого сократить количество смен. Подобная автоматизация поможет повысить качество дорожных работ, например, в таком сложном вопросе, как выравнивание полотна дороги с точностью до 1-2 см.

Частным решением IoT является технология«умный дом» (smarthome), благодаря которой пользователь может самостоятельно управлять безопасностью своего дома, а также бытовой техникой, например, при помощи смартфона, находясь вне дома. Для этого на смартфон необходимо установить соответствующее приложение.

Примерами технологий «умного дома» являются:

– Датчики на смесители и на газовые конфорки. При фиксировании утечки с этих датчиков на смартфон владельца квартиры (дома)поступает сообщение. Хозяин отправляет команду, после которой принудительно перекрывается вода и/или газ.
– Умное УЗО (устройство защитного отключения), при помощи которого можно выборочно отключить объект, подключенный к электричеству, например, чайник, утюг, или освещение.
– Смарт-телевизор, холодильник, умный ночник, термостат и т.п. Таким образом, умный холодильник может составить список продуктов, в соответствии с диетойпользователя смартфона. Помимо этого, смарт-холодильник позволяет заказать доставку еды, при ее отсутствии.

Многие производители бытовой техники планируют выпускать в дальнейшем только смарт-вещи (умные вещи) с доступом в интернет и управлением, например, при помощи смартфона или планшета.

Вопросы безопасности квартиры (дома) можно решать при помощи электронных замков, видеокамер, сигнализации и датчиков движения. При этом все перечисленные устройства могут быть подключены к Интернету. А после установки на смартфон соответствующего приложения этими устройствами можно управлять при помощи смартфона. Таким образом реализуется система умной безопасности.

Сегодня популярны гаджеты, которые удобно носить с собой, они имеют небольшие габариты и малый вес. К примерам носимых гаджетов можно отнести ювелирные изделия, умные часы, гибкие экраны, смарт-очки, фитнес-трекеры, освобождающие от необходимости носить с собойсмартфони т.д.

В ближайшее время бизнес, связанный с IoT, будет активно развиваться как в мире, так и в России. В этом сходятсямнения многих экспертов. Инвестиции в индустрию интернета вещей увеличиваются с каждым годом, что свидетельствует о большом интересе к данным технологиям.

Умные дома сегодня становятся уже не только удовольствием, роскошью или престижем, но и образом жизни людей, что подтверждает успехи технологий IoT[5].

Ожидается также появление сетей мобильной связи пятого поколения (5G). На данный момент во всем мире (как и в России) существует четыре поколения мобильной связи. Существует гипотеза, что пятое поколение мобильной связи должно появится к 2020 году. Объясняется это тем, что существует, так называемое, правило десяти лет. Если обратиться к истории развития мобильной связи, можно заметить, что каждое новое поколение появлялось примерно через 10 лет после появления предыдущего: первое поколение появилось в начале 80-х годов, второе в начале 90-х, третье в начале 2000-х, а четвертое в 2009 году. Напрашивается вывод, что первые сети пятого поколения 5G появятся примерно в 2020 году. А поскольку новые поколения сетей в России внедряются весьма долго в следствие большой территории, пользоваться ими абоненты смогут несколько позднее.

На данный моментактивно проводятся программы по разработке основных критериев стандарта пятого поколения. Следовательно, точного определения 5G на сегодняшний день дать нельзя, можно толькопредположить, как изменятся сети мобильной связи после 2020 года.

Безусловно, в будущем к сети мобильной связи будет подключено значительно больше устройств, большинство из которых будут работать в режиме «онлайн». В свою

очередь, довольно важнойхарактеристикой будет являться значительно меньшее энергопотребление по сравнению с предыдущими поколениями.

Известны следующие требования к сетям пятого поколения:

- Пропускная способность сети свыше 10 Гбит/сек.
- Задержка передачи данных на радио интерфейсе не более 1 мс.
- Поддержка одновременного подключения до 100 млн. устройств/км$^{2.}$

К услугам в сетях 5G относятся:

- Массовая межмашинная связь (Massive Machine-Type Communications, mMTC) – поддержка Интернета вещей (ультра узкополосная связь);
- Сверхширокополосная мобильная связь (Extreme Mobile Broadband, xMBB) – реализация ультра широкополосной связи с целью передачи «тяжелого» контента;
- Сверхнадежная межмашинная связь (Ultra-reliable MTC, uMTC) – обеспечение особого класса услуг с очень низкими задержками [6].

Основными проблемами отрасли телекоммуникаций на сегодняшний день являются:

- снижение доходов от сегмента традиционных услуг;
- насыщение рынка сотовой связи;
- недостаточное развитие услуг широкополосного доступа;
- недостаточность финансирования на разработку и внедрение новых технологий, например,IoT;
- трудности с покрытием мобильной сети связи, как следствие большой территории страны;
- большие объемы передачи трафика данных в мобильных сетях, вызванные всплеском пользовательского интереса к OTT-сервисам, негативно влияют на качество передачи данных в сетях операторов связи и создают риски перегрузки сетей;
- вытеснение с рынка сотовой связи таких услуг массового пользования, как передача SMS и MMS-сообщений;
- расширенные функциональные возможности OTT-сервисов, такие как передача голоса и видео, а также текстовых сообщений в неограниченном количестве на бесплатной основе для пользователей, вызывают падение интереса абонентов к операторским услугам, что в перспективе грозит операторам связи стать востребованными только в качестве поставщиков мобильного Интернета;
- условно-бесплатная бизнес-модель предоставления OTT-услуг является более привлекательной для абонентов в сравнении с операторскими услугами;
- потеря доходов операторов связи с развитием OTT-услуг [3].

На сегодняшний день в России отрасль инфокоммуникаций может предоставить широкий спектр современных услуг связи, оказание которых базируется на сформировавшейся законодательной базе. На развитие связи государство выделяет существенные для отрасли средства консолидированного бюджета.С появлением конкуренции на рынке соотношение «цена - качество» становится все более выгодным для абонентов.

Перед связью на данный момент лежат новые задачи и высоты, которые необходимо покорить. Активное, устойчивое и динамичное развитие отрасли позволит повысить уровень и качество жизни населения, раскрыть человеческий потенциал, способствует развитию экономики страны в целом.

СПИСОК ЛИТЕРАТУРЫ

1. *Гольдштейн А.Б.* Устройства управления мультисервисными сетями: Softswitch. –М: «Вестник связи», №4, 2002.
2. *Кузовкова Т.А* Оценка роли инфокоммуникаций в национальной экономике и выявление закономерностей их развития / Системы управления, связи и безопасности. – М, 2015.
3. *Букрина Е.В.* Экосистема телекоммуникационного оператора: Учебное пособие. Е.В. Букрина, Варламов Е.А. – Екатеринбург: УрТИСИ ФГОБУ ВПО «СибГУТИ», 2015.
4. Развитие отрасли Инфокоммуникационных технологий (ИКТ) в России [Электронный ресурс] / CRN ИТ-Бизнес.– Электрон. дан. – М, [2012]. – Режим доступа: https://www.crn.ru/news/detail.php?id=68520. – Загл. с экрана.
5. Интернет вещей: что это такое? [Электронный ресурс] / Интернет-грамотность. – Электрон.дан. – М. [2017]. – Режим доступа:https://www.inetgramotnost.ru/dostup-v-internet/internet-veshhej-chto-eto-takoe-i-primery.html
6. Что такое 5G? [Электронный ресурс] / Портал о современных технологиях мобильной и беспроводной связи. – Электрон. дан. – М. [2017]. – Режим доступа: http://1234g.ru/5g/chto-takoe-5g

Ю.Н. Денисенко, Ю.А. Олейникова

«САРАФАННЫЙ» МАРКЕТИНГ КАК ИНСТРУМЕНТАРИЙ БРЕНДИНГА

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Федеральное государственное бюджетное образовательное учреждение высшего образования Донской государственный технический университет (ДГТУ), Ростов-на-Дону, Россия

Ключевые слова: маркетинг, актуальные проблемы продвижения бренда, WOM-маркетинг, «сарафанный» маркетинг, маркетинговые технологии, продвижение товара.

В статье рассмотрены проблемы и актуальные тенденции современного бренд-менеджмента, представлены основные задачи в области продвижения бренда компании, определено положительное влияние маркетинговых технологий на развитие бизнеса и создание положительного образа компании у клиентов.

Yu.N. Denisenko, Yu.A. Oleinikova

"WORD OF MOUTH" MARKETING AS A TOOL OF BRANDING

North-Caucasian branch of the order of the red banner of Labour of the Federal state budgetary educational institution of higher professional education "Moscow technical University of communications and Informatics", Rostov-on-don, Russia

Federal state budgetary educational institution of higher education
Don state technical University (DSTU), Rostov-on-don, Russia

Key words: marketing problem of brand promotion, WOM marketing, "word of mouth" marketing, marketing techniques, product promotion.

The article considers problems and trends of modern brand management, the main tasks in the field of brand promotion, the company identified a positive impact of marketing technologies on business development and creating a positive image of the company among the customers.

В условиях развития рыночных отношений для хозяйствующих субъектов различных форм собственности, в процессе их деятельности в ряду наиболее актуальных проблем, одним из важных направлений выступает поддержание положительного мнения потребителей о компании на необходимо высоком уровне. Этому во многом способствует такой инструмент бренд-менеджмента как WOM-маркетинг.

Word-of-mouth (WOM) - маркетинг («сарафанный» маркетинг или маркетинг «из-уст-в-уста») представляет собой альтернативную маркетинговую стратегию, которая мотивирует потребителей к диалогу о продуктах и услугах. WOM-маркетинг осуществляется посредством различных инструментов онлайн и оффлайн тактики, часто используя агентов влияния и сообщества.

К разновидностям «сарафанного» маркетинга маркетологи относят вирусный маркетинг, маркетинг разговоров, скрытый маркетинг, маркетинг сообществ, маркетинг влияния, «народный» маркетинг.

Так, Энди Серновиц, давая определение WOM-маркетингу, считает, что есть b2b (consumer-to-consumer — «от потребителя к потребителю»). и b2c рынок, а WOM — это b2c2c (business-to-consumer — «от бизнеса к потребителю») «от бизнеса, через одного потребителя к другому». По его мнению «сарафанный» маркетинг - это маркетинг c2c: consumer-to-consumer - «от потребителя к потребителю», ведь сущность его заключается в передаче информации через обычных людей, которая происходит сама собой [1].

Потребители определенных товаров и услуг обычно ведут обсуждение различных компаний и их товаров - когда интересуются новым телефоном, машиной, квартирой, выбирают салон красоты или ресторан, думают, с каким поставщиком выгоднее работать.

Результаты обсуждений имеют большое влияние на общественное мнение. Согласно статистическому опросу Nielsen, в котором приняли участие 29000

респондентов из 58 стран мира, 84% из них больше всего доверяют мнению о товарах и компаниях, услышанному от своих близких и друзей. Это исследование подтверждает тот факт, что у всех есть психологическая особенность в большей мере доверять мнению знакомых людей.

Следовательно, можно отметить, что «сарафанное» радио существует как естественный процесс, окружающий общество. При этом «сарафанный» маркетинг - это деятельность, целью которой является сделать так, чтобы в процессе обсуждений люди называли определенный бренд как предпочтительный.

Благодаря Интернет-ресурсам, мнение о товарах и компаниях, передаваемое из «уст в уста», приобрело глобальный характер. В социальных сетях и на форумах бренды обсуждают публично и открыто. А главное честно - потребители просто описывают опыт взаимодействия с потребляемым продуктом. Это могут быть негативные и позитивные отзывы, и неизвестно, кто первым напишет отзыв - разъяренный или благодарный потребитель.

Именно поэтому маркетолог, продвигая продукт или бренд, должен быть в курсе обсуждений: регулярно отслеживать порталы с отзывами, вести соответствующий раздел на созданном компанией сайте, читать форумы, комментарии в социальных сетях. И, конечно же, принимать участие в обсуждениях и создавать новые.

Практика показывает, что беседы, которые выгодны бренду, начинают опытные маркетологи или агенты влияния компаний на форумах и в социальных сетях. И уже затем их подхватывают потребители, и обсуждение начинает обретать большие масштабы, вовлекая новых и новых потенциальных клиентов.

Благодаря социальным сетям компании наконец-то могут не просто интегрироваться в процесс обсуждения бренда, но и активно влиять на него, задавая тон. И это приносит весьма ощутимые результаты.

Согласно проведенному анализу исследований, «сарафанный» маркетинг увеличивает эффективность маркетинговой деятельности на 54%, одобрение аудитории - на 10% и обеспечивает подъем продаж на 1,5%.

Первое, на что обращают внимание маркетологи: «сарафанный» маркетинг - это диалог, а не манипуляция. У агентов влияния есть цель - сделать мнение о бренде позитивными. Однако, необходимо контролировать количество и виды информации, потому что пользователи социальных сетей и форумов негативно реагируют на любое вмешательство извне, считая Интернет свободным и честным пространством.

Даже если обнаружены негативные отзывы о бренде или продукте, не следует сразу переубеждать участников такой дискуссии. Необходимо воспринимать это как возможность изменить ситуацию, сделав товар или сервисное обслуживание качественнее. Негативные отзывы и критику можно воспринимать, как возможность начать общение и изменить мнение о бренде, продукте, на позитивное. При вступлении в диалог с неудовлетворенными клиентами необходимо попытаться решить возникшую проблему.

Необходимо всегда помнить, что наибольшую долю рынка завоюет не тот производитель, который пытается манипулировать чьим-то мнением, а тот, кого реально поддерживают потребители. В конечном итоге выбор остается за ними, и они сделают его сами. Клиентов можно подтолкнуть к тому, чтобы они выбрали определенную компанию, если постоянно создавать поводы для ее позитивного обсуждения. В этом и заключается

управление «сарафанным» радио. Хороший word-of-mouth- маркетинг представляет собой сочетание ценности, сторителлинга и общения с клиентами.

Если выпускаемый фирмой продукт клиенты уже предпочитают и предлагаемый сервис их устраивает, компании не следует останавливаться на достигнутом результате. Необходимо регулярно создавать дополнительные ценности, постоянно улучшать сервис, придумывать и внедрять новые инновационные и креативные идеи. Предела совершенству и новым идеям не существует, многие маркетологи советуют не просто соответствовать ожиданиям потребителей, но и быть выше всех ожиданий.

Любое действие, направленное на это и ценное для потребителя - повод для обсуждения и получения положительных отзывов. Западные маркетологи отмечают, что «сарафанный» маркетинг делает бизнес лучше и честнее, так как маркетинговой целью является создание определенного впечатления и мнения у потребителя, и для этого необходимо работать максимально хорошо и добросовестно.

Исходя из этого, можно отметить, что в создании положительного образа историй участвуют и преданные потребители. Следовательно, необходимо использовать их мнение в написанных отзывах на созданном компанией сайте и других сайтах или, удачным моментом будет распространение ими положительной информации о компании. Пусть потребители опишут опыт взаимодействия с компанией и то, почему они выбирают именно этот бренд или продукт. При этом, можно сослаться на удачно завершенные сделки и удовлетворенных потребителей, сделать с ними интервью.

Еще одним хорошим источником распространения информации являются лидеры мнений. В Интернет - пространстве это могут быть блогеры, пользователи форумов с высоким рейтингом, популярные участники социальных сетей с большим количеством друзей. Потребляя продукт или услугу, они расскажут об этом опыте другим, напишут пост, и очень вероятно, что он распространится по всему Интернету и запустит множество обсуждений.

Кроме того, возможно самостоятельно создавать темы для стимулирования обсуждений в социальных медиа. И это не только сообщения о новых акциях и распродажах. Потребители ценят и другие моменты. Узнавая мнение клиентов о том, как улучшить сервисное обслуживание, можно предложить самостоятельно новую идею, поговорить о чем-то важном для потребителя, возможно и о том, что с предприятием и его основной деятельностью вообще не связано. И потребители будут это обсуждать.

Маркетологи считают, что наиболее эффективный «сарафанный» маркетинг обладает следующими качествами:

1. Достоверность - честные и аутентичные сообщения от брендов клиентам и от человека к человеку.
2. Прозрачность и доверительность информации - имеет важное значение в диалоге между брендом и потребителями.
3. Социальная вовлеченность - должно быть постоянное «онлайн» отслеживание всех возможных каналов, т.е. способность слушать, отвечать, разговаривать.
4. Измеряемость - необходимо постоянно отслеживать и измерять собственные успехи. Необходимо знать, сколько новых контактов принесет «сарафанный» маркетинг, количество потребителей, лояльных к бренду.

5. Повторяемость – необходимо постоянно быть на «слуху», как только одна кампания закончилась, необходимо начинать следующую, постоянно стимулировать обсуждения и разговоры вокруг бренда.

Еще одним плюсом «сарафанного» маркетинга является его универсальность. Этот метод продвижения работает для компаний абсолютно любого масштаба. При этом неважно, какой бизнес - транснациональная корпорация, работающая с сотней стран мира, или малое предприятие, открытое недавно. Тип бизнеса также не имеет значения, как и локация.

Эта модель может подходить для всех компаний и действовать будет удачно, если выполняется и определенное условие. Без выполнения этого условия все вышесказанное просто не принесет результатов. Это- необходимый уровень качества продукта и сервисного обслуживания. Если они по-настоящему хороши, и потребители остаются довольными после взаимодействия с компанией, то WOM-маркетинг дает положительный эффект. В противном случае, все усилия могут обернуться против бренда и появится вероятность наступления кризисной ситуации.

Если продукт некачественный, а сервисное обслуживание оставляет желать лучшего, то «сарафанный» маркетинг как метод продвижения бренда и увеличения имиджевых характеристик компании, использовать нежелательно. В результате можно получить не только недовольных потребителей, но и серьезную проблему, провоцирующую настоящий репутационный кризис.

Качество и доверие - самая первая ступень «сарафанного» маркетинга. Многие маркетологи даже утверждают, что в таком случае «сарафан» станет почти бесплатным способом маркетинга. Если компания имеет устойчивое высокое мнение о своем бренде, то в геометрической прогрессии начнут увеличиваться рекомендации, стоит запустить только первый импульс этому в Интернете.

Не следует считать, что «сарафанный» маркетинг является бесплатным. Существуют примеры, когда без каких-либо усилий компании становились популярными и обсуждаемыми, но их единицы. Во многих остальных случаях в WOM-маркетинг нужно вкладывать временные и финансовые затраты. При использовании традиционных маркетинговых каналов, существует линейная зависимость между затратами и окупаемостью. Получая определенное количество обращений по конкретной стоимости, к примеру, каждая единица дополнительных рекламных вложений генерирует определенный процент увеличения продаж. Чтобы увеличить количество обращений, необходимо увеличить финансирование на конкретную сумму.

В случае с word-of-mouth маркетингом все немного иначе. Когда маркетинговая кампания заканчивается, результат продолжает возрастать, при этом вложения уменьшаются. С этого момента начинает работать органический «сарафанный» маркетинг, который получил импульс от оплаченного. Эффект от кампании ощущается еще долгое время после ее окончания - разговоры продолжаются по инерции.

Большинство маркетологов хотели бы попробовать, как работает WOM-маркетинг, чтобы оценить его эффект. Но часто они имеют слишком малый бюджет, короткие сроки и, кроме того, высокие ожидания. И, при таком подходе, они не получают ожидаемых результатов.

Существует множество разных методик WOM-маркетинга, как в онлайне, так и в офлайне. Согласно статистике во всемирной сети происходит лишь 20% всех обсуждений компаний, которые могут повлиять на 80% всех остальных обсуждений в реальности.

Как уже упоминалось, согласно статистическому опросу, проведенному Nielsen, 84% людей доверяют рекомендациям своих знакомых. При этом рекламе на телевидении доверяют 62% опрошенных, 61% - рекламе в газетах, 57% -рекламе на радио, 48% - рекламе в социальных сетях, 42% - баннерной рекламе [3]. Данные опроса свидетельствуют, что доверие к традиционной рекламе и ее влияние ниже, чем у WOM-маркетинга.

«Сарафанный» маркетинг является довольно эффективной формой рекламы, что можно продемонстрировать на примере компаний, работающих на китайском рынке. Около 60% потребителей в КНР постоянно «разносят слухи» о тех или иных товарах и услугах, которыми они уже успели воспользоваться.

Китай - страна потребительских новинок, где с каждым днем появляются новые продукты, многие из которых задерживаются здесь надолго. Модель китайского «сарафанного» маркетинга можно представить следующим образом: чем больше родственников или друзей пользуются каким-либо продуктом, тем быстрее китаец купит именно этот товар, даже несмотря на то, что он может быть недешевым. Используя свой менталитет, жители Китая рассуждают: «Чем больше людей, которых я знаю, пользуются именно этим, тем больше я могу быть уверен в том, что именно этот продукт не имеет никаких дефектов и попросту не развалится, и я «сохраню лицо», если приобрету его»[2] Очень многое, если не все, в этой стране построено на доверии.

Разговоры о товарах и услугах не утихнут никогда: люди всегда будут говорить о бытовой технике, машинах, компьютерах, телепередачах и различного вида услугах. Они могут критиковать их, а могут рекомендовать своим друзьям или оставлять отзыв в Интернете, где его прочитают миллионы потенциальных клиентов.

Сообщества в социальных сетях, интересные события и новости о бренде, агенты влияния, вирусная реклама - с помощью этого можно привлечь внимание, по-хорошему удивлять потребителей и быть узнаваемым и обсуждаемым.

Современное общество редко задумываемся о том, что каждый его член непременно принимает участие в процессе «сарафанного» маркетинга. Советуя друг другу модель автомобиля или марку смартфона, курортный город или новое кафе, детский сад или агентство недвижимости - в центре подобных обсуждений всегда оказываются бренды. Потребители охотно советуют друзьям и знакомым то, что понравилось им самим.

При этом «сарафанный» маркетинг выступает и рекламной формой, которой люди склонны наиболее доверять, так как человек, советующий какой-либо товар или услугу, не извлекает личной выгоды. Такая форма бесплатной рекламы, с помощью которой удовлетворённые пользователи рассказывают другим людям, почему им нравится какой-либо товар или услуга, в большинстве стран очень эффективна. Множество стартапов, имея очень малое количество пользователей, успешно используют этот маркетинговый инструмент.

Подводя итог, можно отметить, что по нашему мнению, «сарафанный» маркетинг - это прежде всего маркетинговая технология, позволяющая спровоцировать позитивные разговоры о бренде в среде потенциальных потребителей.

СПИСОК ЛИТЕРАТУРЫ

1. *Энди Серновиц*, Сарафанный маркетинг. Как умные компании заставляют о себе говорить: Манн, Иванов и Фербер; М.: 2012.-108 с.
2. «Культ лица» в Китае https://laowai.ru/kult-lica-v-kitae/ [электронный ресурс], дата обращения 04.02.2017
3. Доверие потребителей к разным видам рекламы http://www.nielsen.com/ru/ru.html [электронный ресурс], дата обращения 06.03.2017

В.Ю. Денисов, И.С. Синева

ПРИМЕНЕНИЕ И ИНСТРУМЕНТЫ BUSINESS INTELLIGENCE

Московский технический университет связи и информатики, г. Москва, Россия

Ключевые слова: информационные технологии, большие данные, анализ данных, визуализация данных, бизнес-аналитика.

В статье рассмотрены основные задачи Business Intelligence и подходы к их решению. Описаны схемы хранения и обработки информации, варианты визуализации данных, применение статистического анализа данных и методов оптимизации для решения конкретных бизнес-задач.

V.Yu. Denisov, I.S. Sineva

BUSINESS INTELLIGENCE: USAGE AND TOOLS

Moscow Technical University of Communication and Informatics, Moscow, Russia

Keywords: information technology, big data, data analysis, data visualization, business analytics, business intelligence.

The article considers common Business Intelligence’s issues and ways to solve them, describes storage and processing of information, data visualization, usage of statistical data analysis and methods of mathematical optimization for solving specific business cases.

Текущая ситуация в информационных технологиях обязывает руководящих сотрудников принимать data-driven решения, однако для извлечения и обработки информации требуются некоторые знания в области программирования и анализа данных. Цель Business Intelligence – показать пользователям без особой подготовки информативные данные в удобном и осмысленном виде [1].

Область Business Intelligence охватывает практически все этапы работы с данными:

- Эффективное хранение и агрегация данных в дата-центрах.
- Система Extract-Transform-Load (ETL), которая позволяет провести стандартизацию информации.
- Система визуализации данных и отчетности, работающая в режиме реального времени.
- Контроль версий (CVS).
- Статистический анализ и предиктивная аналитика.
- Оптимизация ключевых показателей эффективности (KPI).

Одной из задач аналитика является обеспечение работоспособности системы Business Intelligence и удобного доступа к данным заинтересованным лицам внутри компании.

Зачастую необходимо работать со множеством источников данных. Обычно информацию можно получить при помощи SQL или HTTP API, однако в некоторых случаях данные нужно собрать при помощи Web Scraping или анализа текста. Самый простой способ решить проблему с доступом к подобного рода информации – создание скрипта, который загружает с определенным интервалом данные из источника в базу. В таком случае доступ к базе будет производиться при помощи стандартного SQL.

Хранилища аналитических данных можно грубо классифицировать на три типа:

- Key-value database (или NoSQL) – данные хранятся в виде ключ-значение. База данных такого типа позволяет быстро получить информацию по ключу (в т. ч. и составному).
- Row-oriented DBMS – привычная для многих пользователей реляционная база данных, которая хранит данные по строкам.
- Column-oriented DBMS – база, используемая для больших объемов информации. Способ хранения данных (по столбцам) подразумевает лучшую по сравнению с row-oriented DBMS производительность для получения агрегированных данных.

Система ETL используется для того, чтобы преобразовать данные из одного представления в другое (при этом единое). Таким образом, вся необходимая информация из различных источников будет находиться в одном месте, что в дальнейшем обеспечит большое число параметров для анализа.

Рассматривая реальную задачу проектирования системы ETL в компании Sports.ru, было необходимо получать данные о посещении веб-сайтов (лог-файлы сервера) и мобильных приложений (API), продажах (API), активности пользователей (PostgreSQL и MSSQL), трудозатратах разработчиков (API).

Большинству сотрудников компании интересны цифры о посещаемости разрабатываемых ими продуктов. При помощи системы визуализации данных Redash [2] данные можно изобразить графически (рис. 1).

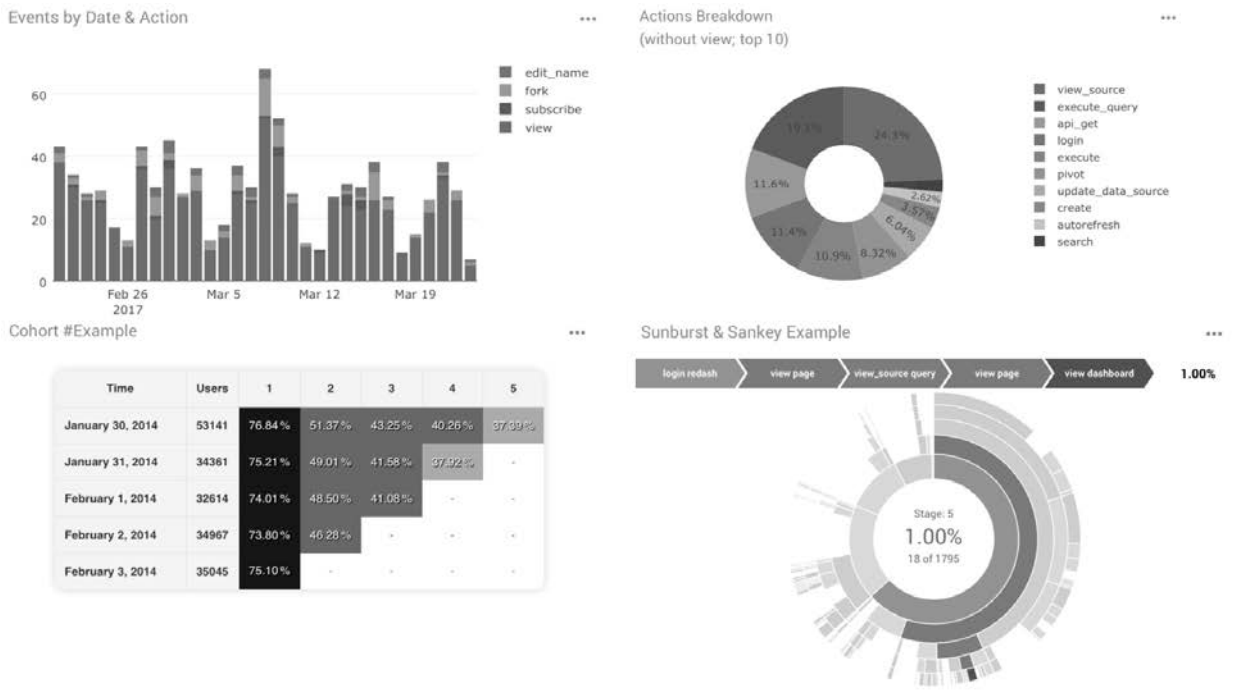


Рис. 1. Варианты отображения данных в Redash

Визуализации в данной системе интерактивны и обновляются автоматически, что позволяет сотрудникам видеть информацию в любое время без участия аналитиков.

Контроль версий осуществляется при помощи инструментов CVS, например, Git или SVN. Данный формат изменения программного кода широко применяется среди классических разработчиков и позволяет в случае неудачных правок быстро откатиться на предыдущую версию. Системы контроля версий базируются на простом правиле: каждое изменение – это разница строк между текущей и предыдущей версией, что позволяет хранить только набор дельт относительно начальной версии кода.

К статистическому анализу относят проверку гипотез, подсчет основных параметров выборки, корреляционный анализ, регрессионный анализ, анализ временных рядов и тому подобное. Проверка гипотез особенно актуальна в области web-технологий и является основным инструментом оценивания качества изменений продукта при помощи A/B-тестирования [3]. Суть такого тестирования заключается в том, что новые функции (например, вид кнопки) показывают не всем пользователям, а лишь некоторой доли, которую равномерно разбивают на несколько частей, каждой из которой, в свою очередь, показывают разный вариант. Во время проверки гипотез оценивается конверсия, которая в данном случае равна отношению числа кликов на кнопку к числу показов кнопки. Предиктивная аналитика позволяет предположить, как будет развиваться тот или иной проект на основе исторических данных. Пример такого графика изображен на рис. 2.

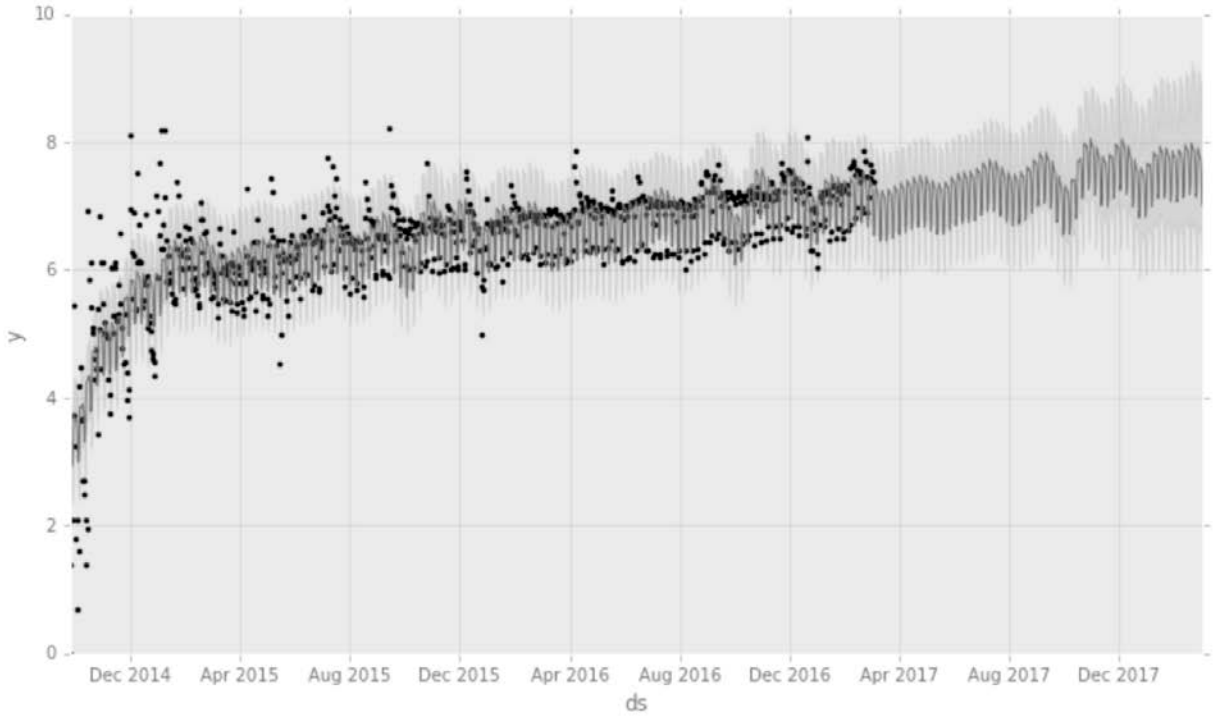


Рис. 2. Прогноз изменения числа страниц за сеанс на веб-сайте

Для того, чтобы понимать успешен ли разрабатываемый продукт, нужно соотносить финансовые затраты на его разработку и продвижение с деньгами, которые он приносит. В случае с digital-средой довольно часто основным заработком является реклама. Нужно понимать, сколько прибыли приносит среднестатистический пользователь за все время пользования продуктом, и этот показатель называется ценность пользователя (lifetime value или LTV [link]). Формулу можно представить следующим образом [4]:

$$LTV = Lifetime * ARPU,$$

где $Lifetime$ – время жизни пользователя, $ARPU = Revenue/AU$ – отношение дохода к уникальным пользователям.

Посчитать время жизни пользователя можно различными способами, однако самый точный основан на анализе возвращаемости (retention), график которого изображен на рис. 3 [5].

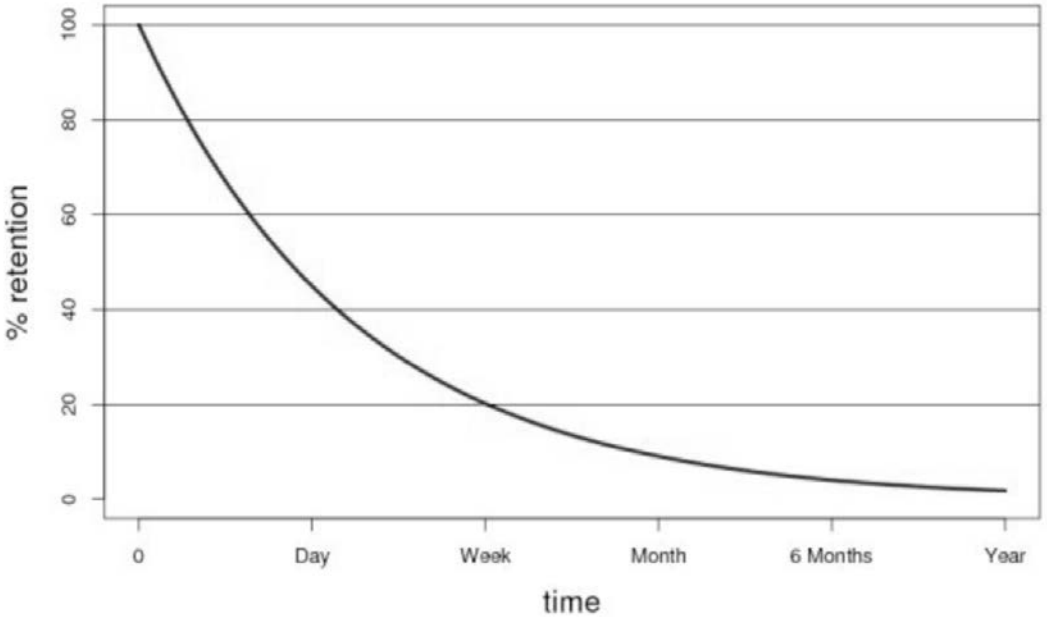


Рис. 3. График возвращаемости пользователей

Следующий этап – найти такую функцию $F\left(time\right)$, которая наилучшим образом описывает полученный график. Для данной задачи подойдет функция вида

$$F\left(time\right) = A + \frac{B}{time + C}$$

где коэффициенты A, B, C вычисляются при помощи метода наименьших квадратов.

Площадь под полученным графиком (или интеграл от функции) – искомая величина времени жизни пользователя, которая вычисляется при помощи суммы или бесконечного ряда:

$$Lifetime = \sum_{i=0}^{N} \frac{F\left(i\right)}{\left(1+d\right)^{i}},$$

где d – ставка дисконтирования WACC, которая применяется для пересчета будущих потоков доходов в единую величину текущей стоимости [6].

Зная доход, количество аудитории и её время жизни, не составит труда посчитать ценность среднестатистического пользователя.

Таким образом, применение инструментов Business Intelligence существенно упрощает работу с данными и позволяет получить более полное представление о разрабатываемом продукте.

СПИСОК ЛИТЕРАТУРЫ

1. *Luhn H. P.* A Business Intelligence System // IBM Journal of Research and Development. – 2010. – № 2. – С. 314-310.
2. Redash. Make Your Company Data Driven. [Электронный ресурс]. 2017. Дата обновления: 12.02.2017. URL: https://redash.io (дата обращения: 21.03.2017).
3. *Mathis L.* Designed for Use. Raleigh: The Pragmatic Bookshelf. 2011. 310 с.

4. Two Methods for Modeling LTV with a Spreadsheet. [Электронный ресурс]. 2015. Дата обновления: 24.03.2014. URL: https://redash.io (дата обращения: 20.03.2017).
5. Как считать lifetime value: обзор методов / Хабрахабр. [Электронный ресурс]. 2015. Дата обновления: 08.07.2015. URL: https://redash.io (дата обращения: 21.03.2017).
6. *Теннент Д.* Управление денежными потоками: как не оказаться на мели. М.:Альпина-Паблишер. 2014. 208 с.

С.А. Докучаев, Г.С. Костецкая, Н.О. Светличная

О ФОРМИРОВАНИИ ОБЩЕПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНЦИИ БАКАЛАВРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ПРИ ИЗУЧЕНИИ ОБЩЕНАУЧНЫХ ДИСЦИПЛИН (НА ПРИМЕРЕ КЕЙС-МЕТОДА)

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: кейс-метод, общепрофессиональные компетенции, информационные технологии

Рассматриваются новые требования, предъявляемые федеральным государственным образовательным стандартом высшего образования к подготовке бакалавров по направлению «Информатика и вычислительная техника». Описывается метод кейсов как одно из наиболее эффективных средств при формировании общепрофессиональных компетенций бакалавров.

S.A. Dokuchaev, G.S Kostetskaya, N.O. Svetlichnaya

TO THE QUESTION OF FORMING GENERAL VOCATIONAL COMPETENCES OF BACHELORS IN THE FIELD OF INFORMATION TECHNOLOGIES AND COMPUTING TECHNIQUES WHEN STUDYING GENERAL SCIENCE GROUP SUBJECTS (ON THE EXAMPLE OF CASE-METHOD)

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

Keywords: case-study, general vocational competences**,** information technologies

The work considers new requirements imposed by the Federal State Educational Standard

for Higher Education to prepare bachelors in the “Informatics and computer engineering” direction. The article describes the use of case-study method as one of the most effective means to form general vocational competences.

Утвержденный в 2016 г. федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), предъявляет принципиально новые требования к подготовке бакалавров в области информационных технологий и вычислительной техники [1]. Эти требования предусматривают формирование у обучающихся трех видов компетенций: общекультурных, общепрофессиональных и профессиональных.

Общекультурные компетенции предполагают формирование гуманитарной эрудированности [5], культурной нормы и социализированности обучающихся. Профессиональные компетенции призваны сформировать производственно-технологическую составляющую готовности выпускника к профессиональной деятельности и отражают одну из целей компетентностного подхода - подготовку компетентностного специалиста. Роль общепрофессиональных компетенций в образовательном процессе заключается в формировании у студентов необходимой базы для развития последующих специальных профессиональных компетенций, отражающих специфику профессиональной деятельности. Уровень сформированности общепрофессиональных компетенций имеет больше значение, поскольку влияет на успешность создания остальных компетенций и профессиональной компетентности студентов в целом. Общепрофессиональные компетенции служат своеобразным трамплином для эффективной подготовки будущего бакалавра к решению стандартных задач в профессиональной деятельности.

Очевидно, что формирование общепрофессиональных компетенций бакалавра по направлению 09.03.01 невозможно без изучения базовых математических дисциплин: «Математический анализ» и «Теория вероятностей и математическая статистика». На лекционных и практических занятиях по данным дисциплинам от преподавателя требуется не только привить студентам знания основных понятий и методов математического анализа, теории вероятностей и математической статистики, навыки решения типовых и нестандартных задач. На первый план выходит формирование общепрофессиональной компетенции ОПК-5, т.е. способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий. Нам представляется, что одним из наиболее эффективных средств для достижения этой цели является кейс-метод **[2].**

Суть кейс–метода состоит в том, что усвоение знаний и формирование умений есть результат активной самостоятельной деятельности обучающихся по разрешению противоречий, в результате чего и происходит творческое овладение профессиональными знаниями, навыками, умениями и развитие мыслительных способностей. Если метод кейсов применяется в учебном процессе многократно, то у студентов вырабатываются навыки решения практических задач, анализа жизненных ситуаций, определения задачи, которая требует решения, оценивать полученный результат, давать оценку своей деятельности в процессе решения **[3]**.

Применение кейс-метода как эффективного метода обучения оправдано не только для естественных, но и гуманитарных наук. Обучение иностранному языку в неязыковом вузе направлено на формирование следующей компетенции в соответствии с ФГОС ВО+: «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия» [1]. Изучение иностранного языка направлено на реализацию данной компетенции в областях социально-бытового и профессионального общения, поэтому основным методами активизации познавательной деятельности студентов является контекстное и проблемно-ориентированное обучение.

Проблемное обучение как развивающее обучение позволяет студентам усвоить новые знания и приобрести навыки и умения творческой деятельности. Настоящая проблема всегда связана с жизненными реалиями / наукой, она содержит явное противоречие, не имеет окончательного ответа на главный вопрос проблемы и, следовательно, требует поисковой, исследовательской работы. Проблемная задача предполагает ряд действий, для ее решения студенту нужно самостоятельно провести частичный поиск. Применение проблемного подхода целесообразно для занятий по темам: Связь и Интернет, Общество и технологии, Тенденции развития телекоммуникаций и ИТ.

Эффективность преподавания дисциплины связана с формой проведения практических занятий. Наиболее актуальной признана интерактивная форма обучения с применением инновационных технологий. Интерактивная деятельность на уроках иностранного языка предполагает организацию и развитие диалогового общения, которое ведёт к взаимодействию, совместному решению общих задач. Для этого на уроках организуются индивидуальная, парная и групповая работа, применяются творческие задания, ролевые игры. Одним из самых популярных методов интерактивного обучения является «кейс-метод (Case study) - метод анализа ситуаций (с англ.яз. case - случай, a case study - обучающий случай) на основе реальных ситуаций» **[7]**. Задачей применения кейс-метода в техническом вузе является совершенствование навыков и получение опыта в следующих областях: выявление, отбор и решение проблем; работа с информацией, анализ и синтез информации и аргументов; работа с предположениями и заключениями; оценка альтернатив и принятие решений **[6].** Применение данного метода при обучении иностранному языку эффективно для студентов неязыковых вузов, поскольку позволяет сочетать игровую форму учебной деятельности и применение разных умений, навыков, знаний смежных дисциплин и, как следствие, активизировать и применить знания английского языка.

Таким образом, практическая составляющая, заключенная в решении кейсов, позволяет формировать общепрофессиональную компетентность будущего бакалавра в области информационных технологий и вычислительной техники. Кейсы позволяют эффективно и грамотно, с опорой на полученные знания, решать стандартные задачи профессиональной деятельности, формируют у студентов опыт использования знаний, умений и навыков в профессиональной деятельности, способствуют их будущей профессиональной состоятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт Высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата) [Электронный ресурс]. / URL: http://fgosvo.ru/uploadfiles/fgosvob/090301.pdf (дата обращения 27.03.2017)
2. *С.А.Докучаев, Г.С. Костецкая* Кейс метод как эффективное средство формирования общепрофессиональной компетенции бакалавров в области инфокоммуникаций при изучении математических дисциплин. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2016.
3. *Седова Н.С.* Использование метода кейсов в процессе развития стохастической компетентности будущего учителя математики. / Письма в Эмиссия.Оффлайн: электронное научное издание 2011. №9 (сентябрь). ART 1645. URL: http://emissia.org/offline/2011/1645.htm (дата обращения 27.03.2017)
4. *Юрьев А.В.* Анализ информационных компетенций бакалавров технических специальностей // Современная педагогика. 2016. № 12 [Электронный ресурс]. URL: http://pedagogika.snauka.ru/2016/12/6527 (дата обращения: 07.01.2017). http://pedagogika.snauka.ru/2016/12/6527
5. *Соловьева Е.С., Федуленкова Т.Н.* Из опыта формирования лингво-культурологических компетенций в обучении английскому языку будущих культурологов // Современные проблемы науки и образования. – 2016. – № 4.; URL: https://science-education.ru/ru/article/view?id=24902 (дата обращения: 10.04.2017).
6. *Докучаев С.А., Костецкая Г.С.* Интерактивные методы обучения бакалавров в области инфокоммуникаций по дисциплине Теория вероятностей и математическая статистика. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2016.
7. *Павленко В.Г.* Применение кейс-метода при обучении английского языка в неязыковом вузе // Научно-методический электронный журнал «Концепт». – 2016. – Т. 17. – С. 534–538. – URL: http://e-koncept.ru/2016/46282.htm.

С.А. Докучаев, Г.С. Костецкая

О МЕЖДИСЦИПЛИНАРНОМ ВЗАИМОДЕЙСТВИИ ПРИ ОБУЧЕНИИ БАКАЛАВРОВ В ОБЛАСТИ ИНФОКОММУНИКАЦИЙ (НА ПРИМЕРЕ ОДНОЙ ЗАДАЧИ МАТЕМАТИЧЕСКОЙ ФИЗИКИ)

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: междисциплинарное обучение, уравнение математической физики, операционный метод

Рассматривается метод проблемно-ориентированного междисциплинарного обучения бакалавров в области инфокоммуникаций. В качестве иллюстрации его эффективности приведена схема решения одной задачи математической физики.

S.A. Dokuchaev, G.S Kostetskaya

TO THE QUESTION OF INTERDISCIPLINARY INTERACTION IN EDUCATING BACHELORS OF INFOCOMMUNICATION INDUSTRY (ON THE EXAMPLE OF A PROBLEM OF MATHEMATICAL PHYSICS)

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

Keywords: interdisciplinary training, operation method, equations of mathematical physics.

The work considers problem-oriented interdisciplinary training of bachelors of the infocommunication industry. The paper offers a scheme to solve a problem of mathematical physics as an illustration of its efficiency.

Федеральный государственный образовательный стандарт высшего образования по направлению 11.03.02 «Инфокоммуникационные технологии и системы связи» предъявляет особые требования к выбору методов обучения бакалавров в области инфокоммуникаций. Одним из эффективных методов при формировании общепрофессиональной компетенции нам представляется проблемно-ориентированное междисциплинарное обучение [1].

Данный метод обучения используется для повышения мотивации к изучению дисциплины и закрепления полученных теоретических и практических знаний. В ходе лекций и практических занятий студенты рассматривают реальные примеры применения математических методов по направлению и профилю обучения, выявляют и подтверждают взаимосвязь изучаемых математических дисциплин с другими дисциплинами [2].

Проиллюстрируем эту взаимосвязь на примере задачи математической физики.

Задача. Найти решение $u(x,t)$ дифференциального уравнения

$$A(x)\frac{\partial^2 u}{\partial x^2} + C(x)\frac{\partial^2 u}{\partial t^2} + D(x)\frac{\partial u}{\partial x} + E(x)\frac{\partial u}{\partial t} + F(x)u + G(x,t) = 0, \quad (1)$$

где $A(x), C(x), D(x), E(x), F(x)$ – непрерывные функции на отрезке $0 \le x \le l$.

Будем считать, что $A(x) > 0$. Тогда: 1) если $C(x) < 0$, то уравнение (1) принадлежит гиперболическому типу; 2) если $C(x) \equiv 0$, то – параболическому.

Будем искать решение $u(x,t)$ уравнения (1) в области $0 < x < l$ (в частности, возможно $l = \infty$) и $t > 0$, удовлетворяющее заданным начальным условиям

$$u(x,t) = \varphi_1(x), \quad \frac{\partial u(x,t)}{\partial t} = \varphi_2(x) \text{ при } t = 0 \qquad (2)$$

(второе условие задается лишь в гиперболическом случае) и краевым условиям

$$\alpha_1 \frac{\partial u(x,t)}{\partial x} + \beta_1 u(x,t) = g_1(t) \quad \text{при } x = 0$$

$$\alpha_2 \frac{\partial u(x,t)}{\partial x} + \beta_2 u(x,t) = g_2(t) \text{ при } x = l \qquad (3)$$

Здесь $\varphi_1(x), \varphi_2(x), g_1(t), g_2(t)$ – заданные функции

$\varphi_1(x), \varphi_2(x)$ – непрерывные для любого $0 \le x \le l$), $\alpha_1, \alpha_2, \beta_1, \beta_2 -$ постоянные, удовлетворяющие условиям ${\alpha_1}^2 + {\beta_1}^2 \neq 0$, ${\alpha_2}^2 + {\beta_2}^2 \neq 0$.

Заметим, что краевые условия могут несколько видоизменяться. Кроме того, при $l = \infty$ второе условие отпадает.

Будем предполагать (физически это оправдано), что функция $u(x,t)$ и ее частные производные, входящие в уравнение (1), рассматриваемые как функции от t, являются оригиналами.

Ход решения уравнения (1) при условиях (2), (3) можно представить в виде следующей схемы, пригодной и для линейных дифференциальных уравнений в частных производных второго порядка более общего вида, и для линейных дифференциальных уравнений в частных производных с двумя независимыми переменными x и t порядка выше второго, если коэффициенты этих уравнений зависят только от x, в частности являются постоянными. Мы ограничились случаем уравнения (1) ради простоты изложения и имея в виду его распространенность при решении прикладных задач (уравнение теплопроводности, телеграфное уравнение).

Схема

Пространство оригиналов	Уравнения в частных производных + начальные условия + граничные условия ↓	Решение ↑
	Преобразование Лапласа ↓	Обратное преобразование Лапласа
Пространство изображений	Обыкновенное дифференциальное уравнение + граничные условия →	↑ Решение →

Заметим, что при решении линейных дифференциальных уравнений в частных производных с постоянными коэффициентами нужно учесть, что в общем решении однородного уравнения, соответствующего изображающему уравнению, некоторым видам корней характеристического уравнения соответствуют слагаемые, равные тождественно нулю. Это, в частности, корни вида $\alpha p + i\beta p$, где $\alpha, \beta -$ действительные числа, $\beta \neq 0$. Это связано с тем, что не всякая функция может быть изображением.

СПИСОК ЛИТЕРАТУРЫ

1. *Докучаев С.А., Костецкая Г.С.* Интерактивные методы обучения бакалавров в области инфокоммуникаций по дисциплине «Теория вероятностей и математическая статистика». – Труды Северо-Кавказского филиала Московского технического университета связи и информатики, 2016

2. *Болотюк Л.А., Сокольникова А.М., Швед Е.А.* Применение интерактивных методов обучения на практических занятиях по теории вероятностей и эконометрике / Интернет журнал «НАУКОВЕДЕНИЕ» №3(16), 2013 URL: http://naukovedenie.ru/PDF/70pvn313.pdf (Дата обращения 27.03.2017 г.)

Л.И. Долинер, Н.Г. Бикбулатова

ЭЛЕКТРОННЫЙ КУРС КАК БАЗОВЫЙ КОМПОНЕНТ ОБУЧЕНИЯ В СОВРЕМЕННОМ ВУЗЕ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: системы дистанционного обучения, электронный курс, смешанное обучение, клиповое мышление.

В статье предлагается точка зрения авторов на технологию создания и использования электронных курсов, используемых в учебном процессе при обучении студентов [технического] вуза.

L.I. Doliner, N.G. Bikbulatova

E-COURSE AS A BASIC COMPONENT OF LEARNING IN MODERN UNIVERSITY

Key words: remote training system, e-course, blended learning, video thinking

The article offers the authors ' point of view on technology creation and use of e-learning used in educational process at training of students of [technical] University.

Введение

Основная причина, которая побудила нас написать эту статью связана с дискуссией, которая велась (и ведется)в Интернете по теме «Что такое идеальный электронный курс?». Смутило то, что, с одной стороны, профессионалы вполне серьезно это обсуждают, а, с другой, ряд авторов вполне разумно (с нашей точки зрения) говорят о бесполезности подобного диспута, поскольку итог – это осознание того, что критерии идеального курса в общем случае, скорей всего, найдены не будут. Но все в этой жизни относительно, ведь у всех есть представление, что такое «идеальный электронный курс», но свое… С нашей точки зрения «идеальный курс» в каждом конкретном случае – это курс, который позволяет научить всех, кто учится. А его структура, видимо, определяется психологическими аспектами категории обучающихся и требованиями к результатам

обучения тех, кто этот процесс организует. Поэтому мы сочли возможным изложить свою точку зрения на процесс создания и использования электронных курсов в [техническом] вузе.

Зачем нужны электронные курсы

Мы до сих пор не использовали термин «дистанционное обучение», поскольку считаем, что электронные курсы давно вышли за рамки специализированных форм обучения. Сегодня имеет смысл рассматривать *смешанное обучение.*

«Смешанное обучение (англ. «BlendedLearning») – это сочетание традиционных форм аудиторного обучения с элементами электронного обучения, в котором используются специальные информационные технологии, такие как компьютерная графика, аудио и видео, интерактивные элементы и т.п.

Электронные курсы

Учебный процесс при смешанном обучении представляет собой последовательность фаз традиционного и электронного обучения, которые чередуются во времени».

Электронный курса сегодня (опять же – с нашей точки зрения) – это просто еще один (или главный?) инструмент обучения, которые обеспечивает студентам выбор своей траектории обучения, сохраняя, с одной стороны, определенные правила регламентации учебной деятельности [в вузе], а с другой, – учитывая интересы студентов и темп жизни, в котором они живут (или пытаются жить).

Электронный курс сегодня выступает (должен выступать, будет выступать) в качестве основного средства обучения на любой ступени образования. Связано это исключительно с требованиями времени и аспектами восприятия обучающихся информации. Этот тезис актуален, поскольку:

сегодня на дворе эпоха *клипового мышления*, во время которой «окружающий мир превращается в мозаику разрозненных, мало связанных между собой фактов, частей, осколков информации. Человек привыкает к тому, что они постоянно, как в калейдоскопе, сменяют друг друга и постоянно требует новых». М. Маклюэн в своей теории этапов развития цивилизации отмечает, что «…общество, находясь на современном этапе развития, трансформируется в «электронное общество» или «глобальную деревню» и задает, посредством электронных средств коммуникации, многомерное восприятие мира. Развитие электронных средств коммуникации возвращает человеческое мышление к дотекстовой эпохе, и линейная последовательность знаков перестаёт быть базой культуры». Как следствие – современная молодежь все меньше воспринимает ценности (в том числе и технологии учения), которые были выработаны в предыдущие эпохи;

как отмечают многие исследователи, «клиповое» мышление – это естественная защита нервной системы от реалий быстроменяющегося и информационно-насыщенного современного мира. Становится важной актуальность знаний в данное время и в данном месте. Классические энциклопедические подходы такой динамике неподвластны. И в образовании тоже. Современные учебники устаревают в момент, когда они выходят из типографии. Мы проанализировали существующую практику и получили следующие результаты: по бумажным учебникам реально (т.е. открывают их, разбираются в том, что там написано, делают краткий конспект и т.п.) работают меньше 10% студентов. Конспекты лекций в тетради (в меньшей степени), материалы в Интернете, видеозаписи

лекций – это основные источники информации. Наверное, это странно, но самыми прилежными учениками, штудирующими традиционные учебники, являются… сами преподаватели;

представляется, что современному образованию требуется учебник, который, с одной стороны, бесплатен для обучающихся, а с другой обладает высочайшей потребительской стоимостью. Если в вузе учебники выдаются, то говорить об их актуальности смысла не имеет, поскольку на практике трудно предположить, что вуз будет реально закупать сотни (или тысячи) новых учебников ежегодно. Да, и учебник должен быть легко модифицирован – даже тот, который в данный момент есть у обучаемых. Пособия, которые выпускаются преподавателями вузов, эту проблему решают лишь частично;

более того, в идеале учебник, скорей всего, должен представлять собой электронный ресурс и быть размещен в информационной образовательной среде (ИОС), обеспечивать доступ с любого устройства, имеющегося у студента;

и, наконец, раз учебник размещается в ИОС, желательно, чтобы он обеспечивал и непосредственно организацию образовательной деятельности, включая консультацию, систему диагностики, ведение журнала со статистикой и диагностикой выполненной деятельности. Причем разделял информацию для преподавателя (полную) и для студента (краткую). Получение такой информации позволит студенту и преподавателю эффективно корректировать результаты обучения.

Современные системы дистанционного обучения (СДО), в рамках которых разрабатываются электронные курсы, практически все перечисленные задачи в состоянии реализовать. Причем, как следует из определения смешенного обучения, электронный курс может взять на себя решение большого количества образовательных задач, но потребность в обычном очном взаимодействии с преподавателям никоим образом не отменяет. Может быть реализована уникальная ситуация, при которой будет реально контролироваться не только деятельность на очных занятиях, но и самостоятельная работа. Причем системность контроля позволит существенно облегчить диагностику результатов обучения, объективность оценки и понимание реального уровня подготовленности студентов.

Требования к электронным курсам

На самом деле требований к электронным курсам достаточно много. Наибольший интерес, с нашей точки зрения, представляют требования, сформулированными теми, кто практически курсы разрабатывает, внедряет и широко использует. Видимо, следует констатировать, что единых требований к электронным курсам не существует. И, надеемся, существовать не будет. Все подобные требования, которые есть в открытой печати, носят рекомендательный характер и их соблюдение является частным делом тех структур, которые подобные курсы создают. Разумеется, у нас тоже есть своя точка зрения на построение подобных решений. Попытаемся их сформулировать, но уже с какими-то вескими (по крайней мере, для нас) обоснованиями.

Размещение большого количества текста в качестве [элемента] электронного курса однозначно недопустимо. С точки зрения результатов обучения разницы между бумажным учебником (пособием, задачником и т.п.) и его электронной версией нет никакой. Если не учатся по бумажным книгам, не будут учиться и по электронным версиям этих же книг.Поэтому просто не имеет смысла создавать подобные электронные

курсы. И, как показал наш опыт, добавление туда тестов ситуацию не меняет. Разумеется, при наличии высокой мотивации и эти курсы могут работать. Но только при наличии такой мотивации, что не является массовым явлением.

Электронный курс состоит из набора занятий. Мы согласны с Еленой Тихомировой, что планируемая продолжительность одного занятия (сеанса) не должна превышать в среднем 15-20 минут. И неважно, что она рассматривает преимущественно корпоративное обучение. Как показала наша практика, в условиях клипового мышления студентов это оптимальное время одноразового сеанса, на который они (студенты) идут без особых проблем. Создание занятия, рассчитанного на существенно большее время, резко снижает эффективность не только этого занятия, но и курса в целом.

Электронный курс должен быть модульным, причем структура курса может (или должна?) быть нелинейной. У студента, который реально учится, должна быть ситуация успеха, причем чем больше занятий/модулей он прошел, тем значимей будут его результаты. Достигается это множеством различных приемом, среди который сегодня наиболее популярна геймификация.

Если не вдаваться в детализацию деятельностного подхода в обучении (Л.С. Выготский, Л.В. Занков, А.Р. Эльконин, В.В. Давыдов и др.), его можно сформулировать так: новое знание не может быть передано учащемуся в готовом виде, т.е. путем сообщения или показа. Усвоение– результат собственной деятельности обучающихся. Привычный термин «научить» означает лишь «помочь обучаемому научиться». Т.е. в основе обучения лежит организованная деятельность обучающихся. Причем эта деятельность должна быть обеспечена высоким уровнем мотивации. Отсюда вытекают требования к аспектам взаимодействия студентов с электронным курсом. Во-первых, подобный курс должен быть преимущественно интерактивным, моделируя (хотя бы в какой-то степени) взаимодействие между обучаемым и обучающим. Во-вторых, курс должен быть мультимедийным, предоставляющим студентам разнообразный спектр информационных ресурсов, влияющих на максимально возможный спектр их восприятия (зрение, слух; пространственное представление; жаль, что пока еще не очень распространены электронные ресурсы, влияющие на обоняние). Т.е. интересным!

Электронный курс должен быть легко модифицирован. Как показывает практика, создание первого варианта курса удачным сразу назвать сложно. Как бы детально он не был сделан, всегда найдутся места, которые плохо понимают студенты, не совсем корректные вопросы, недостаточно продуманные практикумы, не всегда правильно работающие алгоритмы оценки и т.п. Технология создания открытых курсов, которую пытаются внедрять в современных вузах, с нашей точки зрения не оптимальна, поскольку создание сценария преподавателями и последующая разработка на основе этого сценария электронного он-лайн курса обладает существенным недочетом: результаты обучения оцениваются, чаще всего, по конечному результату и «голосованию ногами» (уходят с курса или вообще не приходят).

Заключение

Как всегда, решение о технологии создания модификации курса лежит в промежутке между «курс создается полностью преподавателем» и «курс создается полностью программистами». С нашей точки зрения использование профессиональных инструментов создания видеолекций, специализированных тренажеров, сложных

технических моделей, которые следует использовать при подготовке, например, студентов технических специальностей, конечно же нужно разрабатывать специалистам: инженерам и дизайнерам по видео, программистам и т.п. Но создавать на основе этих материалов (и многих других) электронного курса должен сам преподаватель. И, разумеется, нести ответственность за образовательный результат.

В идеале, создавать электронный курс целесообразно не одному, а группе преподавателей. Причин здесь несколько. Во-первых, не каждый преподаватель является специалистом по каждой из тем курса. Во-вторых, необходима перманентная перекрестная экспертиза разделов курса. В-третьих, существенно ускоряется время разработки курса.

Следующий момент связан с технологией создания электронных курсов. На самом деле есть серьезное противоречие между необходимостью создавать широкий спектр интерактивных материалов и уровнем реальной подготовленности для этой деятельности преподавателей. Вряд ли в вузе можно набрать достаточное количество преподавателей, знающих технологию создания продуктов на основе html5, flash и т.п. Один из путей решения этой проблемы – это обучение преподавателей использованию инструментов создания учебных модулей и электронных курсов. Например, у нас есть опыт обучения работе с такими пакетами, как eAuthoru iSpringSuit. Эти пакеты позволяют существенно ускорить разработку курсов.

И еще один нюанс. Перечисленные пакеты позволяют сохранять учебные модули в формате SCORM, что обеспечивает автоматизацию хранения результатов работы студентов с этими модулями. Это крайне важно, поскольку позволяет, с одной стороны, контролировать работу студентов, а, с другой, оценивать качество созданного продукта. Кроме того, эти пакеты сохраняют учебные модули в форматах html5 и flash, что обеспечивает возможность работы с электронным курсом как с помощью стационарного компьютера или ноутбука, а также с помощью мобильных устройств, включая и смартфоны.

Есть определенная проблема: из электронного курса пытаются сделать некий фетиш, регламентируя его структуру, правила использования, имущественную принадлежность и т.п. Как правило, из этого ничего хорошего не получается. Однако с имущественной принадлежностью в условиях СДО все решается достаточно просто: преподавателю оплачивают создание электронного курса, авторское право остается за ним, а имущественное (если разработка оплачена) – за вузом. Это позволяет использовать разработанный и доработанный курс и другими преподавателями.

СПИСОК ЛИТЕРАТУРЫ

1. *Долинер Л.И.* Информационные и коммуникационные технологии как системообразующий компонент обучения в информационном обществе (статья) // Информационные и коммуникационные технологии в образовании / Материалы VI-ой Международной научно-практической конференции. - Екатеринбург: ГБОУ ДПО СО «ИРО», УрФУ, 2012. – 383 с..– 13-18
2. *Долинер Л.И.* Дистанционное обучение как ключевой тренд современного образования // Информационные и коммуникационные технологии в образовании

/ Материалы VIII-ой Международной научно-практической конференции. - Екатеринбург: ГАОУ ДПО СО «ИРО», УрФУ, 2014. – 296 с.– 121-123 с.
3. *Долинер Л.И. , Бикбулатова Н.Г.* Виртуальная моделькомпьютерного класса как основа синергентического подхода в обучении // РЕШЕНИЕ /Материалы четвертой Всероссийской научно-практической конференции. - Издательство Пермского национального исследовательского политехнического университета: г. Березники, 16 октября 2015 г.

А.С. Доткулова, М.С Мосева.

МЕТОД ИНТЕЛЛЕКТУАЛЬНОЙ ВЕРИФИКАЦИИ ЛОГИЧЕСКИХ СВЯЗЕЙ МОДУЛЕЙ ООП В СООТВЕТСТВИИ С ФГОС ВО

Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: информационные технологии, интеллектуальная верификация, образовательный стандарт, семантический анализ, граф связности.

В статье рассмотрены проблемы автоматизации формирования методической документации, сопровождающей образовательный процесс в условиях постоянного роста информационного поля и различных изменений нормативных документов, регламентирующих деятельность образовательных организаций. Разработан web-интерфейс для автоматизированной разработки учебно-методического комплекса дисциплин и анализа взаимосвязей между ними.

Dotkulova A.S., Moseva M.S.

METHOD OF INTELLECTUAL VERIFICATION OF LOGICAL CONNECTIONS OF MODULES OF EDUCATIONAL PROGRAM IN ACCORDANCE WITH NEW EDUCATIONAL STANDARDS

Moscow Technical University of Communications and Informatics,
Moscow, Russia

Keywords: information technology, intellectual verification, educational standard, semantic analysis, connectivity graph.

The article considers problems of automatization of compilation of methodical documentation that supporting educational process in terms of permanent growth of information field and different changes of normative documents regulating activities of educational

institutions. There was developed web-interface for automated development of the educational-methodical complex of disciplines and analysis of the interrelations between them.

В настоящее время в сфере образования, как и в других сферах деятельности, наблюдается увеличение объемов информации. Это обусловлено переходом к Болонской системе, принятием новых законов и актов в образовательной сфере, разработкой новых стандартов образования. Таким образом, необходимо своевременно актуализировать документы, сопровождающие образовательный процесс. Основным документом в сфере образования является основная образовательная программа (далее - ООП) (рис. 1).

Рис. 1. Структура образовательной программы

В 2003 году Россия присоединилась к Болонской декларации (1999 г.). Цель Болонской декларации – создание единой системы знаний и единого образовательного пространства высшего профессионального образования для обеспечения мобильности людей, возможности быть востребованным и конкурентоспособным специалистом не только на внутреннем рынке, но и на мировом трудовом пространстве.

С 2011-12 образовательного года наша страна полномасштабно вступила в Болонский процесс, введя в действие федеральные государственные образовательные стандарты высшего профессионального образования (ФГОС ВПО) третьего поколения по направлениям подготовки квалифицированных бакалавров и магистров.

Подписание 29 декабря 2012 года Президентом России ФЗ № 273-ФЗ «Об образовании в Российской Федерации» отменило с 1 сентября 2013 года два действующих до этого времени федеральных закона: Закон Российской Федерации «Об образовании» и Федеральный Закон «О высшем и послевузовском профессиональном образовании».

Согласно данному закону утверждаются федеральные государственные образовательные стандарты нового поколения. Эти стандарты находятся в свободном доступе на Портале Федеральных государственных образовательных стандартов высшего образования.

Специальности и профили подготовки, соответствующие ФГОС высшего образования, были утверждены Приказом Министерства образования и науки РФ № 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования» 12 сентября 2013 г.

Принятие нового закона об образовании и утверждение новых образовательных стандартов определили переход к образовательному процессу, в основе которого лежит компетентностно-ориентированный подход. Этот подход заимствован из Болонской декларации и адаптирован для России. Данный подход оперирует двумя основными понятиями – компетенция и компетентность. Компетенция – компонент качества студента, определяющий его способность выполнять определенную совокупность действий в сфере того или иного вида деятельности. Умение применять и актуализировать освоенные компетенции для решения реальных задач означает компетентность. Таким образом, компетентностно-ориентированный подход направлен на развитие способностей человека реализовывать определенные компетенции, научить его действовать в реальных условиях. При таком подходе, в качестве результата образования рассматривается не сумма усвоенной информации, а способность студента найти метод решения проблемы. Применение компетентностного подхода обусловлено постоянным увеличением и обновлением теоретических и профессиональных знаний в условиях социальных, экономических, производственных информационных изменений. Современному обществу необходим специалист, не просто обладающий определенным набором знаний, а специалист, имеющий информационную базу и способность к саморазвитию и самообразованию для постоянного повышения своей профессиональной квалификации.

Для осуществления компетенстностно-ориентированного подхода в соответствии с новыми образовательными стандартами необходимо разрабатывать методическое обеспечение образовательных программ с соблюдением соответствия компетенций и видов деятельности обучающегося, на которые направлен образовательный процесс. В связи с вступлением в силу ФГОС 3+ и в скором времени ФГОС четвертого поколения увеличилась нагрузка по составлению и актуализации документации, способствующей учебному процессу, такой как рабочий учебный план, рабочие программы дисциплин (РПД), фонды оценочных средств (ФОС), средства оценивания результатов освоения дисциплин. Так как они должны постоянно находиться в актуальном состоянии, и ВУЗ должен гарантировать преподавание дисциплины на современном уровне, выпускающие кафедры вузов вынуждены проводить их обновление ежегодно.

Все вышеперечисленные документы взаимосвязаны между собой и имеют сложную структуру. Рассмотрим основные компоненты регулирования образовательного процесса, которые необходимы кафедре для обеспечения качественного образования (рис.2).

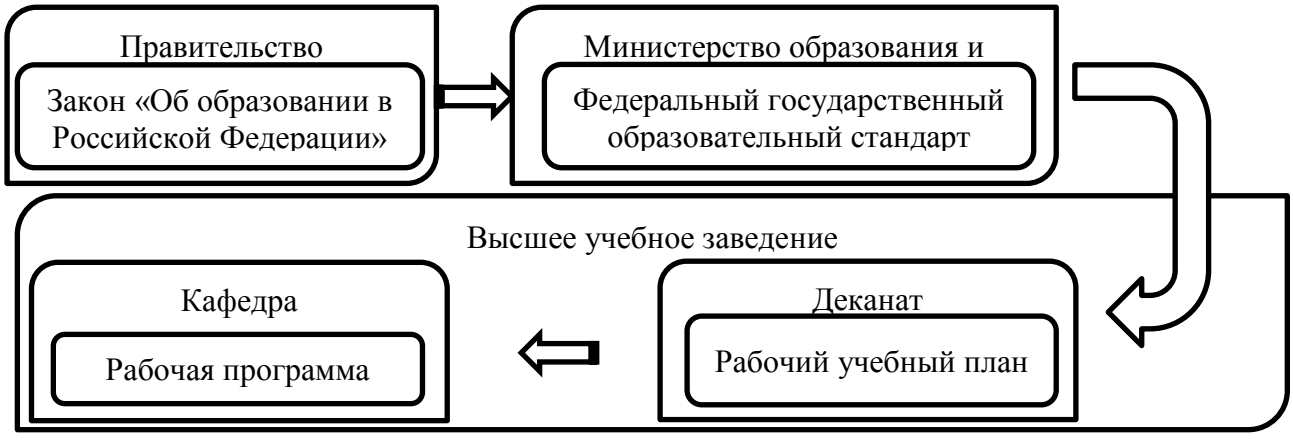


Рис 2. Взаимосвязь основных компонентов, регулирующих образовательный процесс

Основными документами является учебный план и рабочая программа. Учебный план — это документ специальности или направления, определяющий продолжительность учебного года, длительность семестров, каникул, выпускных работ, экзаменов, практик; распределение дисциплин по годам обучения и времени в целом; количество часов по каждой дисциплине за все время обучения и на изучение дисциплины в конкретном семестре; количество часов в неделю на изучение каждой дисциплины; время, отведенное на аудиторные часы и самостоятельную работу студента (СРС), виды итоговых и промежуточных аттестаций, структуру и продолжительность практик, типы занятий и т. д.

В учебном плане (рис. 3) отражаются виды деятельности, распределение компетенций по дисциплинам (список компетенций генерируется из образовательного стандарта). Дисциплины, которые включены в учебный план, делятся на базовые (обязательные) и вариативные (по выбору).

Грамотно структурировать учебный план для эффективного освоения всего курса дисциплин – непростая задача. Необходимо формировать список дисциплин и связи между ними на основе выбранной специальности, образовательного учреждения и направленность выпускающей кафедры.

Рис 3. Структура учебного плана

Учебный план строится постепенно. На каждом уровне прописываются цели и задачи, которые необходимы решить в процессе обучения. Дисциплины логически структурируются и как кирпичики формируют образовательный процесс. Проверяются связи между изучаемыми темами в каждом предмете и выстраивается соответствующий порядок. С помощью образовательного стандарта составляется список конпетенций и закрепляется за каждой дисциплиной свой набор. Составляется примерный план тематик для каждого предмета и рассчитывается исходя из этого время на аудиторные часы и самостоятельную работу студента, после разрабатываются системы оценки знаний и трудоемкость практик. Как только учебный план полностью готов, можно перейти к разработке рабочей программы (РПД) по каждой дисциплине в отдельности.

Разработка РПД является трудоемким процессом и требует значительных временных затрат. При разработке РПД необходимо ориентироваться на РУП и учитывать взаимосвязь между дисциплинами. Для решения задачи был разработан модуль, позволяющий значительно сократить время, затраченное на разработку УМКД, уменьшить количество ошибок, упростить доступ к УМКД и учитывать взаимосвязь между дисциплинами для обеспечения качественного высшего образования.

Рабочая программа имеет сложную структуру и состоит из многих элементов (рис. 4).

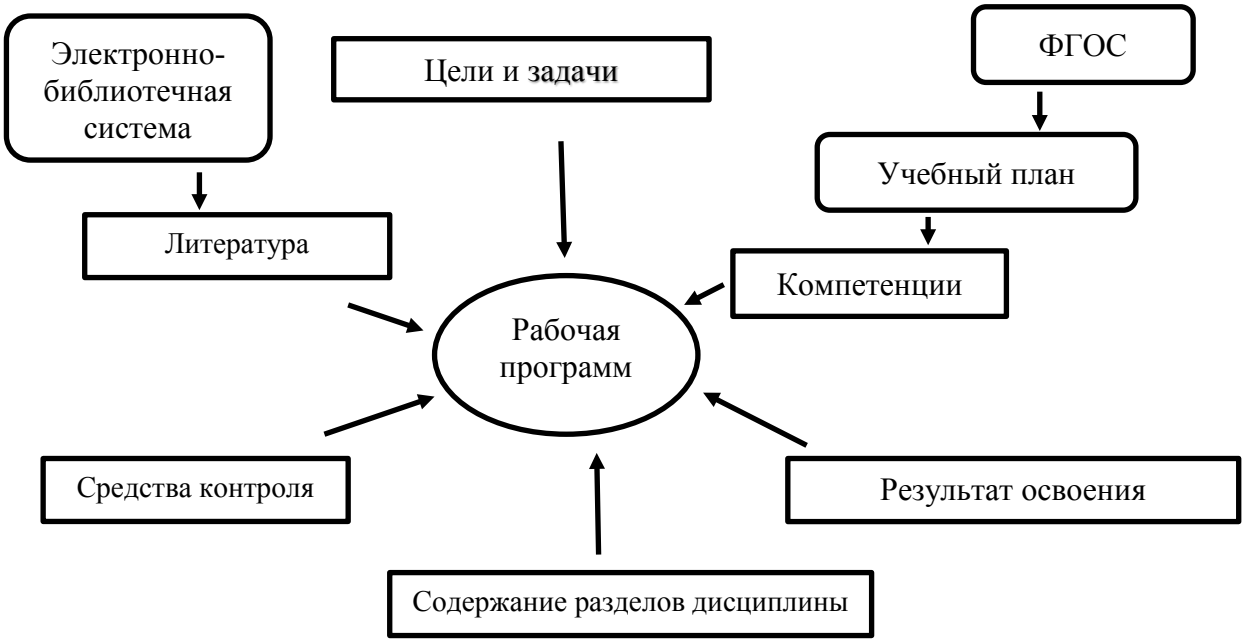


Рис 4. Структура рабочей программы

Рабочая программа (РП) должна быть составлена с учетом Федерального государственного образовательного стандарта (ФГОС) по направлению обучения и рабочего учебного плана (РУП) направления.

В настоящее время существует множество систем по автоматизации учебного процесса вуза. Однако процесс автоматизации разработки и актуализации рабочих программ в этих системах реализован мало. В связи с этим вопрос об автоматизации разработки РПД, а также учебно-методического комплекса учебных дисциплин остается актуальным. Поэтому было принято решение разработать такой модуль.

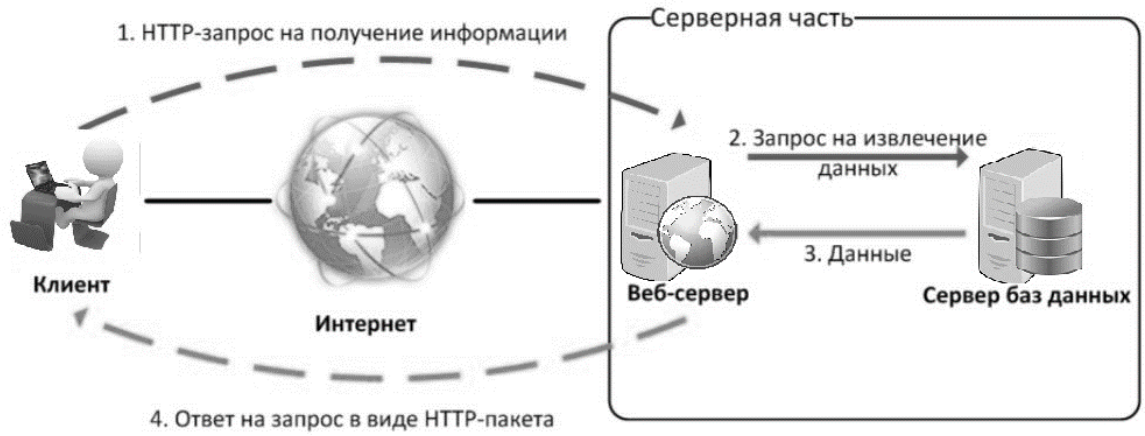


Рис 5. Архитектура разработанного модуля автоматизации генерации рабочих программ

Модуль РПД-МКиИТ взаимодействует с такими документами, как учебный план специальности, образовательный стандарт специальности. Была разработана база данных, в которой содержатся необходимые данные о подразделениях вуза, специальностях, кадровом составе, дисциплинах и др. Таким образом, данные о специальности, расчасовке дисциплины, перечне и описании компетенций по направлению берутся автоматически из соответствующего источника.

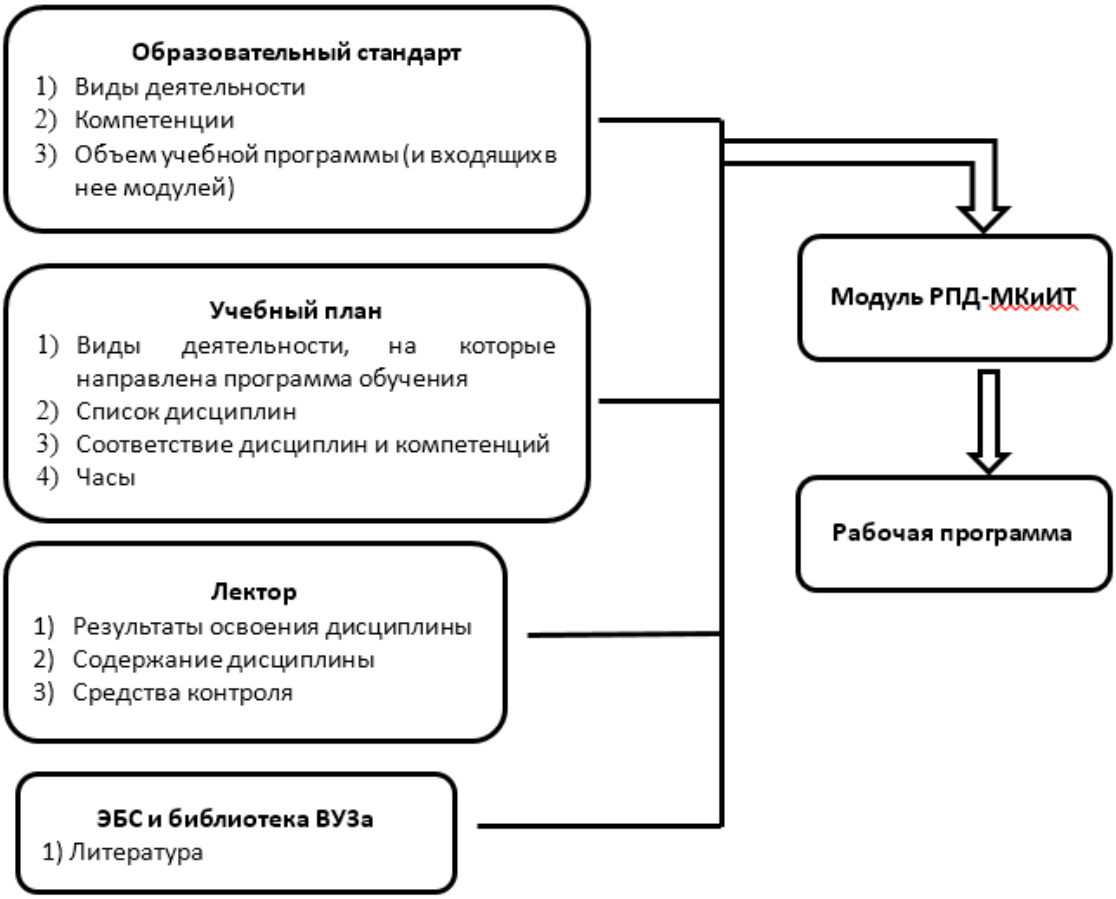


Рис 6. Внедрение модуля РПД-МКиИТ

Достоинства использования разработанного модуля при составлении рабочих программ и фондов оценочных средств дисциплин:

- существенно сокращается время, затрачиваемое преподавателем на разработку рабочей программы дисциплины;
- исключаются ошибки при заполнении расчасовки, перечня компетенций и связанных дисциплин;
- формируется выходной файл, оформленный с учетом требований ФГОС;
- все разработанные программы и фонды оценочных средств сохраняются в системе, что обеспечивает оперативный доступ к ним в любое время;
- поддерживается возможность редактирования уже созданных рабочих программ и фондов оценочных средств.

Таким образом, использование информационно-коммуникационных технологий уже является необходимым атрибутом образовательной деятельности. Поэтому, подготовка студентов высших учебных заведений, составление учебно-методических комплексов невозможна без интеграции вспомогательных полу-автоматизированных и автоматизированных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "Об образовании в Российской Федерации" N 273-ФЗ от 29 декабря 2012 года с изменениями 2017-2016 года;
2. “Joint declaration of the European Ministers of Education convened in Bologna on the 19th of June 1999”, http://ec.europa.eu/education/policies/educ/bologna/bologna.pdf, p. 7-8.
3. “The Bologna Declaration on the European space for higher education: an explanation” http://ec.europa.eu/education/policies/educ/bologna/bologna.pdf, p. 3-4.
4. *Буслаев А.П., Бурикова Т.А., Доткулова А.С., Наконечный И.И., Яшина М.В.* Применение информационно – вычислительных сетей для мониторинга сложных социально-технических процессов на примере системы сопровождения оценивания качества знаний по математике в вузе. Часть 2. Технология аттестации, ФГОБУ ВПО МТУСИ, 2013;
5. *Yashina M.V., Dotkulova A.S., Nakonechniy I.I.* The method of cloud services using for testing in mathematical education, CMMSE 2016;
6. *Подласый И.П.* Педагогика: 100 вопросов - 100 ответов: учеб. пособие для вузов, 2004.

Л.Н. Евдакова

РОЛЬ САМОСТОЯТЕЛЬНОЙ РАБОТЫ В ФОРМИРОВАНИИ КОМПЕТЕНЦИЙ У СТУДЕНТОВ ИНФОКОММУНИКАЦИОННЫХ ВУЗОВ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО "Сибирский государственный университет телекоммуникаций и информатики" в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: самостоятельная работа студентов, компетенции, компетентностный подход, федеральный государственный стандарт высшего образования 3+

В статье рассмотрены формы, функции и задачи самостоятельной работы студентов.

L.N.Evdakova

THE ROLE OF SELF-WORKING IN THE INFOCOMMUNICATION UNIVERSITY STUDENTS COMPETENCES FORMATION

Ural Technical Institute of Communications and Informatics (branch) FGBOU VO "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibGUTI)

Keywords: independent work of students, competences, competence approach, federal state standard of higher education 3+

The article considers the forms, functions and tasks of independent work of students.

Рынок труда предъявляет к работникам требования, которыми должны обладать специалисты отрасли инфокоммуникаций такие как: готовность и умение переучиваться, самостоятельно совершенствовать профессиональные знания, творчески перерабатывать всё возрастающие потоки информации и компетентно использовать их на практике. По оценкам специалистов благосостояние и духовное развитие отдельного человека и всего человечества в целом сегодня, все больше зависит от умения и способности работать с информацией. Нарастание статуса информации приводит к многочисленным переменам, в частности – к изменению роли в подготовке специалиста такой формы обучения как самостоятельной работы студентов (СРС),. Появляется новая цель образовательного процесса – воспитание компетентной личности, способной решать проблемы и задачи исходя из приобретенного учебного опыта и адекватной оценки конкретной ситуации. Необходима новая система обучения, которая содержала бы некую совокупность стимулов, ориентирующих студентов на равномерную и достаточно интенсивную самостоятельную работу.

Решение этих задач вызывает необходимость по новому использовать формы и методы самостоятельной работы в вузе, для обеспечения возможности развития, саморазвития и самореализации личности.

Одной из особенностей Федерального государственного образовательного стандарта (ФГОС) высшего образования (ВО) в настоящее время является его ориентация не столько на ресурсы и содержание образования, сколько на компетенции выпускников. В образовательном стандарте отражается современная мировая практика разработки образовательных программ, основанная на планировании результатов обучения, получившая название «компетентностный подход». В настоящее время в развитых странах отмечается устойчивая тенденция к снижению общего времени на аудиторное занятие и увеличению времени на внеаудиторную, самостоятельную работу студентов. Такой подход усиливает значимость самостоятельной работы и повышает ее роль в улучшении качества подготовки выпускников.

В УрТИСИ ФГОБУ ВО «СибГУТИ» в процессе подготовки кадров для отрасли инфокоммуникаций реализуется компетентностный подход. Обязательное планирование содержания самостоятельной работы студентов, дифференциация ее объема по формам учебных занятий, позволяет варьировать виды самостоятельной работы по учебным дисциплинам в зависимости от применяемой преподавателем методики, регулярный контроль выполнения заданий для самостоятельной работы – все это составляет важную особенность ФГОС ВО 3+.

Рассчитывать на то, что студенты сами, без постороннего квалифицированного руководства смогут организовать свою работу, было бы совершенно нереалистично. Поэтому вся деятельность по разработке новой, эффективно действующей системы СРС должна осуществляться силами профессорско-преподавательского состава. Всю перестройку учебного процесса нужно с самого начала поставить на прочную методологическую базу, в частности, необходима опора на принцип системности и деятельностный подход.

Системность в данном случае означает, что СРС нельзя рассматривать как автономную часть учебного процесса. Она должна быть согласована с другими элементами образовательного процесса в вузе. Формы, виды и содержание СРС должны разрабатываться с учетом таких, например, факторов, как цели и сроки обучения, содержание и специфика учебных дисциплин, образовательный и интеллектуальный уровень обучающихся, их потребности и интересы и т.п.

Деятельный подход, в высшем образовании направлен на формирование определенных компетенций, чтобы выпускник мог выполнять, вполне, определенную деятельность; учить нужно тому, что необходимо для успешного выполнения этой деятельности; обучение нужно строить так, чтобы оно реализовалось в процессе интерактивной деятельности.

В связи с совершенствованием системы образования, расширением перечня изучаемых предметов, углублением их содержания становится как никогда важно внедрение в вузе более совершенной методики обучения, обеспечивающей повышения качества учебной работы, активизацию познавательной деятельности студентов, развитие их умственных способностей. В решении этой проблемы значительная роль отводится формированию у обучающихся навыков самостоятельного мышления и практического применения знаний. Задача преподавателя вуза – научить студента учиться

самостоятельно, приобретать знания из различных источников информации путем самостоятельного поиска.

Возможны два основных направления построения учебного процесса на основе самостоятельной работы студентов. Первый – это увеличение самостоятельной работы в процессе аудиторных занятий. С этой целью преподавателю необходимо разрабатывать методики и форм организации аудиторных занятий, способных обеспечить высокий уровень данного вида работ и улучшение качества подготовки.

Второй – увеличение работы студентов во внеаудиторное время. Это вызывает определенные сложности. В первую очередь это неготовность к нему как большинства студентов, так и преподавателей, причем и в профессиональном и в психологическом аспектах [1].

Необходимо так же, пересмотреть существующее информационное обеспечение учебного процесса для эффективной организации самостоятельной работы. Современное планирование СРС должно быть направлено на то, чтобы исключить элементы стихийности, самотека и беспорядочности в работе студента над учебным материалом. Важную роль в управлении самостоятельной работой студентов являются диалог и обратная связь с преподавателем.

Следовательно, основная задача при организации самостоятельной работы студентов на наш взгляд заключается в создании психолого-педагогических условий развития интеллектуальной инициативы и мышления на занятиях любой формы. Основным принципом организации СРС должен стать перевод всех студентов на индивидуальную работу с переходом от формального выполнения заданий к познавательной активности с формированием собственного мнения при решении поставленных проблемных вопросов и задач [6].

На сегодняшний день в УрТИСИ при изучении каждой дисциплины организация СРС представляет собой единство трех взаимосвязанных форм [4,5]:

1. Внеаудиторная самостоятельная работа (ВСРС);
2. Аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя;
3. Творческая, в том числе научно-исследовательская работа.

Виды внеаудиторной СРС разнообразны: подготовка и написание рефератов, докладов, очерков и других письменных работ на заданные темы. Студенту необходимо предоставить право выбора темы выполнение домашних заданий различного характера. Это – решение задач; перевод и пересказ текстов; подбор и изучение литературных источников; разработка и составление различных схем; выполнение графических работ; проведение расчетов и др.; выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы. Индивидуальное задание может получать как каждый студент, так и часть студентов группы; выполнение курсовых проектов и работ; подготовка к участию в научно-теоретических конференциях, смотрах, олимпиадах и др. [8].

Чтобы развить положительное отношение студентов к внеаудиторной СРС, следует на каждом ее этапе разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий, семинаров, выполнении лабораторного практикума и во время чтения лекций. Необходимость организации со студентами разнообразной самостоятельной деятельности определяется тем, что удается разрешить противоречие между трансляцией знаний и их усвоением во взаимосвязи теории и практики.

Самостоятельная работа выполняет ряд функций, к которым относятся [4,5,7]:

- развивающая (привитие навыков творческого труда, обогащение интеллектуальных способностей);
- информационно-обучающая (постановка познавательной или практической задачи, проблемного вопроса или задачи и особого времени на их выполнение, решение);
- стимулирующая (побуждения и мотивация студента);
- воспитательная (развитие профессиональных качеств у обучающихся);
- исследовательская (формирование и совершенствование творческого мышления).

Данные функции позволяют реализовывать следующие задачи, которые стоят в процессе обучения перед преподавателем:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умения использовать справочную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений [4,5,7].

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рабочей учебной программой и методическими указаниями по организации СРС.

В самостоятельную работу студентов во внеаудиторное время входит проработка лекционного материала, подготовка к практическим и лабораторным занятиям, повторение пройденного материала, а также изучение нового, отведенного на самостоятельное освоение. При составлении методических указаний по СРС преподавателю следует помнить и о трех уровнях формирующих процессов в деятельности студентов: репродуктивном (тренировочном), реконструктивном и творческом (поисковом) уровнях [2].

Репродуктивные самостоятельные работы выполняются по образцу: решение задач, заполнение таблиц, схем и т.д. от простого воспроизведения, выполнения задания по жесткой схеме с целью закрепления изученных алгоритмов, методик. Познавательная деятельность студента проявляется здесь в ознакомлении, осмыслении, запоминании. Цель подобных работ – закрепление знаний, формирование умений, навыков. В ходе реконструктивных самостоятельных работ происходит перестройка решений, составление тезисов, аннотирование. Творческий характер самостоятельной работы проявляется в получении новой информации анализе проблемной ситуации, и ее решении. Студент должен самостоятельно выбрать средства и способ решения. Данный уровень формируется в ходе выполнения научно-исследовательских и курсовых работ (проектов) и написания выпускной квалификационной работы.

Внеаудиторная работа студентов способствует развитию самостоятельности за рамками учебного процесса, что позволяет готовить компетентных работников для отрасли инфокоммуникаций. Регулярные самостоятельные занятия позволяют структурировать знания, укрепляют память, развивают мыслительную способность.

Формирование компетенций предъявляемых к выпускнику в рамках ФГОС ВО 3+ требует усиления межпредметных связей при организации учебного процесса, так как в рамках одной дисциплины этого сделать невозможно. На это направлена работа всего преподавательского коллектива вуза. Для этого необходимо в процессе разработки основной образовательной программы и рабочего плана выпускающей кафедре более внимательно отнестись к составлению матрицы компетенций. Это позволит в дальнейшем преподавателям кафедр вуза более качественно разработать методические рекомендации для самостоятельной работы по конкретной дисциплине.

К сожалению, иногда преподаватели концентрируют внимание на формировании у студентов знаний и умений только по своей дисциплине. Однако формирование этой важной способности одновременного применения комплекса разноплановых знаний позволит студенту уже во время учебы в вузе научиться самостоятельному поиску необходимых знаний различной содержательной направленности при решении в будущем конкретных инженерных задач.

В современном быстротечном мире появляется потребность и в постоянном накоплении и пополнении знаний. Важным условием организации самостоятельной работы студентов и повышения эффективности СРС является наличие и доступность учебно-методического и справочного материала. В последнее время резко возросло освоение учебного материала с использованием Интернета. В УрТИСИ вся учебно-методическая документация (УМД) помимо бумажного носителя в библиотеке размещается в единой научно-образовательной электронной среде института (Е-НОЭС). Несмотря на широкое использование электронных средств для поиска учебной информации, основными источниками знаний остаются лекционные материалы, рекомендуемая литература и методические разработки преподавателей.

На основе вышеизложенного можно сделать следующие выводы:

1. Формирование конкурентоспособного выпускника востребованного на быстроменяющемся рынке труда возможна при эффективной организации образовательного процесса, рациональное планирование и распределение времени на различные виды и формы самостоятельной работы в вузе.
2. Под самостоятельной работой студента понимается деятельность студентов как в учебной аудитории, так и вне её, в контакте с преподавателем и в его отсутствии.
3. Активная самостоятельная работа студентов возможна только при наличии серьезной и устойчивой мотивации. Самый сильный мотивирующий фактор – подготовка к дальнейшей эффективной профессиональной деятельности.

Внутренние факторы, способствующие активизации самостоятельной работы:

- Полезность выполняемой работы.
- Участие студентов в научно-исследовательской, опытно-конструкторской или методической работе.
- Применение интерактивных методов обучения (инновационные и организационно-деятельностные игры и т.д.).

- Участие в олимпиадах по учебным дисциплинам, конкурсах научно-исследовательских или прикладных работ и т.д.
- Использование мотивирующих факторов контроля знаний (накопительные оценки, рейтинг, тесты, нестандартные экзаменационные процедуры).
- Поощрение студентов за успехи в учебе и творческой деятельности (стипендии, премирование, поощрительные баллы) и санкции за плохую учебу.
- Индивидуализация заданий, выполняемых как в аудитории, так и вне её, постоянное их обновление.
- Личность преподавателя (преподаватель может быть примером для студента как профессионал, как творческая личность).
- Наличие и доступность учебно-методического и справочного материала.

Происходящие в России процессы реформирования системы высшего образования требуют новых подходов в организации образовательного процесса. Увеличение времени на самостоятельную работу студентов в вузах России не может быть осуществлено без достаточной подготовки методического обеспечения, серьезного изменения структуры методической работы.

Таким образом, с помощью самостоятельной работы как одной из формы организации учебного процесса можно сформировать у студентов общекультурные, обще профессиональные и профессиональные компетенции, востребованные в отрасли инфокоммуникаций. В существующих рыночных условиях умелая организация учебного труда будущего специалиста, рациональное планирование и распределение времени на самоподготовку к занятиям по различным дисциплинам, несомненно, пригодится в его профессиональной деятельности. Отсюда, в рамках инновационной модели образования самостоятельная работа студентов, безусловно, оказывает полноценное влияние на процесс формирования профессиональных компетенций специалистов при ответственном подходе к ее организации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Арутюнова Г.З.* Методы измерения педагогических процессов. Ростов на Дону, Прометей, 2002. 132 с.
2. *Белогурова В.А.* Научная организация учебного процесса / В.А. Белогурова. – М.: Медицина, 2010. – 296 с.
3. *Беспалько В.П.* Слагаемые педагогической технологии. М.: Педагогика, 2009. – 203с.
4. *Евдакова Л.Н., Кузнецова Н.А.* Исследование роли самостоятельной работы студентов в рамках реализации ФГОС ВПО третьего поколения // Сборник научно-технических и методических трудов. Теория, техника и экономика сетей связи. Выпуск 11. – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2013. с.206 – 211.
5. Образование для инновационного общества/ Встреча глав государств и правительств «Группы восьми»// Официальные документы в образовании. – 2006. – №24. с.4–13.
6. Проектирование основных образовательных программ вуза при реализации уровневой подготовки кадров на основе федеральных государственных образовательных стандартов / Под ред. С.В. Коршунова. М.: МИПК МГТУ им. Н.Э. Баумана, 2010. –212 с.

7. *Трофимова И.А.* Педагогика и психология. Основы самостоятельной работы студентов / И.А. Трофимова. – СПб., 2011. – 222 с.
8. *Шишкин В.П.* Планирование, организация и контроль внеаудиторной самостоятельной работы студентов. Ивановский государственный энергетический университет (ИГЭУ, г. Иваново), 2010. – 91.

И.В. Калиенко, И.С.Абрамов, Н.И.Абрамова

РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ИССЛЕДОВАНИЮ ТИРИСТОРОВ НА ЛАБОРАТОРНОЙ УСТАНОВКЕ «ЭЛЕКТРОННЫЕ ПРИБОРЫ» КАФЕДРЫ «РАДИОЭЛЕКТРОНИКА» ДГТУ

Донской государственный технический университет, ДГТУ, г.Ростов-на-Дону, Россия
Государственное бюджетное образовательное учреждение ростовской области

«Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий» (ГБПОУ РО «РКРИПТ»), г.Ростов-на-Дону, Россия

Ключевые слова: информационные технологии в образовании, коммутационные устройства, экспериментальные измерения параметров.

В статье рассмотрены актуальные вопросы измерения параметров и характеристик полупроводниковых тиристоров, применение тиристоров в системах коммутации, разработаны рекомендации по проведению исследований, определению параметров, представлены результаты проведенных экспериментальных исследований, полученные значения основных параметров тиристоров.

I.V. Kalienko, I.S. Abramov, N.I. Abramova

DEVELOPMENT OF METHODICAL RECOMMENDATIONS STUDY OF THYRISTORS IN A LABORATORY SETTING "ELECTRONIC DEVICES" OF THE DEPARTMENT "ELECTRONICS" DGTU

Don state technical University DSTU, Rostov-on-don, Russia

State budgetary educational institution of Rostov region "Rostov-on-don College of radio electronics, information and industrial technologies" (GOU SPO RO "SCRIPT"), Rostov-on-don, Russia

Key words: information technologies in education, a switching device, experimental measurements of the parameters.

The article considers topical issues of measurement of parameters and characteristics of semiconductor thyristors, the use of thyristors in switching systems, developed recommendations for research, measurement, and presents the results of experimental studies obtained values of the main parameters of the thyristors.

Тиристор - полупроводниковый прибор с двумя устойчивыми состояниями, имеющий три или более *p*-*n*-переходов, который может переключаться из закрытого состояния в открытое и наоборот.

С точки зрения применения тиристор - это полупроводниковый ключ, т.е. прибор, основное назначение которого состоит в замыкании и размыкании цепи нагрузки с помощью внешних сигналов. Аналогично транзисторному ключу, тиристор имеет два статических состояния - закрытое, или состояние низкой проводимости, и открытое, или состояние высокой проводимости. В любом из двух статических состояний тиристор может находиться сколь угодно долго. Переход из одного состояния в другое происходит относительно быстро только под воздействием кратковременного внешнего сигнала.

По этой причине тиристоры находят применение в коммутационных устройствах систем коммутации.

Широкое применение тиристоры находят в блоках вторичного электропитания с синусоидальной широтно-импульсной модуляцией.

Поэтому тиристоры необходимы для изучения студентами ДГТУ специальностей 110301 «Радиотехника» и 110302 «Инфокоммуникационные технологии и системы связи».

Цель работы – разработать методические рекомендации для исследования полупроводниковых тиристоров.

На кафедре «Радиоэлектроника» ДГТУ в составе лабораторного оборудования имеется лабораторная установка «Электронные приборы». Установка предназначена для проведения лабораторно-практических занятий по курсам: "ЭЛЕКТРОННЫЕ ПРИБОРЫ" и "МИКРОЭЛЕКТРОНИКА" и другим курсам подобной тематики со студентами ВУЗов, колледжей, слушателями военных учебных заведений. Конструктивно установка выполнена в настольном исполнении (рисунок.1).

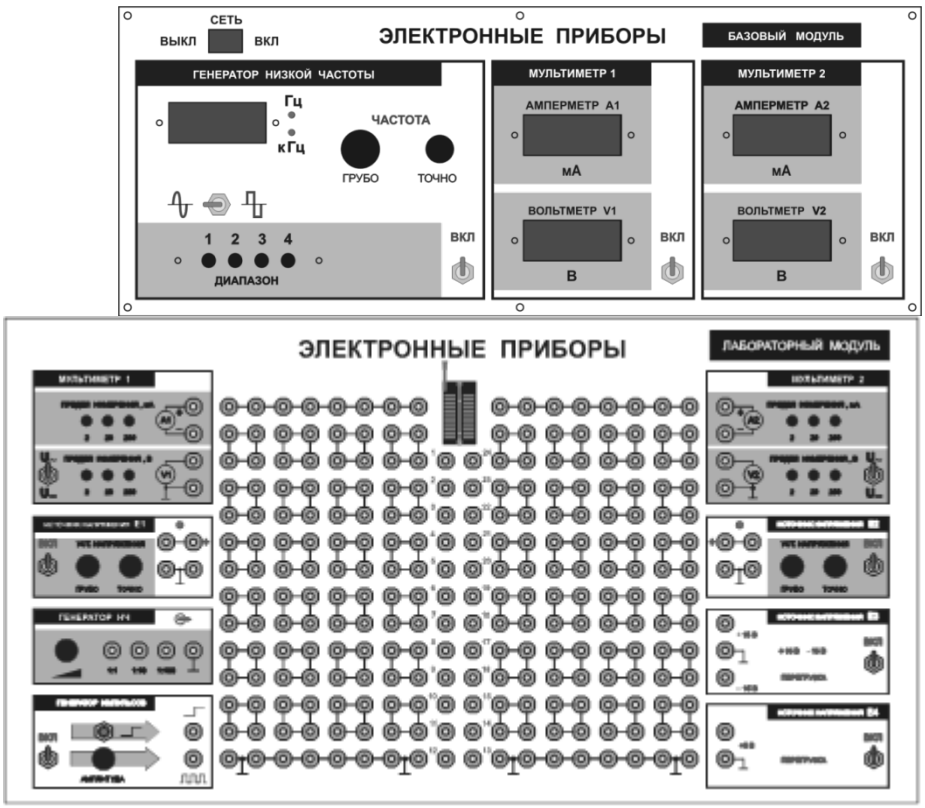


Рисунок 1 - Лабораторная установка «Электронные приборы»

В состав комплектующих элементов для лабораторной установки входит маломощный тиристор КУ102А. Однако, в «Методических рекомендациях для проведения лабораторных работ» отсутствуют какие-либо указания по объему и порядку выполнения лабораторных опытов с тиристорами.

Тиристоры - это название целого класса полупроводниковых приборов. Их классифицируют по следующим признакам: количеству выводов, виду выходной ВАХ, способам выключения и управления и др.. По количеству выводов различают: - диодные тиристоры (динисторы), имеющие только два вывода - анод и катод; - триодные тиристоры (тринисторы), имеющие три вывода - анод, катод и управляющий электрод и другие.

Вольтамперная характеристика динистора представлена на рисунке 2. На прямой ветви характеристики можно отметить две устойчивые области: запирания (ОА) с малыми токами при высоких напряжениях, и отпирания (БВ), с большими токами при малых напряжениях. Между этими областями заключена неустойчивая область отрицательного дифференциального сопротивления (АБ).

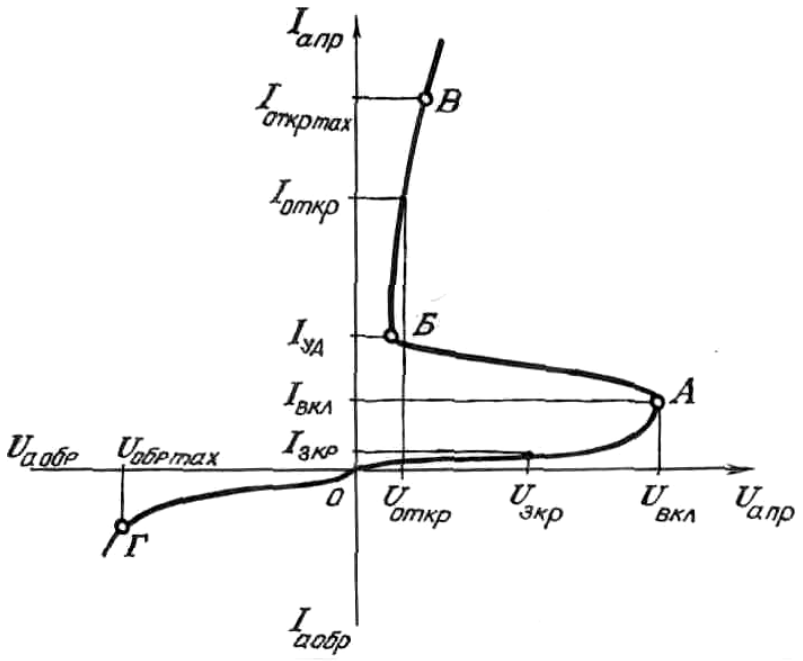


Рисунок 2 – Вольтамперная характеристике динистора

Тринисторы (триодные тиристоры) отличаются от динисторов тем, что кроме анода (А) и катода (К), имеют третий вывод - управляющий электрод (УЭ), который делается от одной из баз. Если управляющий электрод подключен к *p*-базе, ближайшей к *n*-катоду, то такой тринистор называется с управлением по катоду.

Такие структуры имеют гораздо большие управляющие возможности, чем динисторы. Простейшая схема включения триодного тиристора показана на рисунке 3. При отключенном управляющем электроде (*Iуэ=0*) тринистор ведет себя подобно динистору. Подача внешнего прямого смещения на управляющий электродприводит к росту тока через систему и снижение величины напряжения включения $U_{ВКЛ}$.

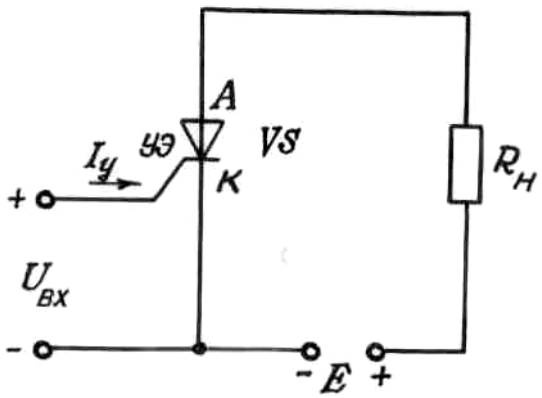


Рисунок 3 – Простейшая схема включения тринистора

Тринистор переводится во включенное состояние при меньшем анодном напряжении. Чем больше управляющий ток *Iуэ*, тем больше инжекция из управляемого *p-n*-перехода. Поэтому при меньшем анодном тиристор включается.

Таким образом, подавая прямое смещение на управляющий электрод, можно регулировать напряжение включения выходной коммутируемой цепи $U_{ВКЛ}$ (рисунок 4). Чем больше ток $Iуэ$, тем ниже $U_{ВКЛ}$.

Вольт-амперная характеристика триодного тиристора (рисунок 4), снятая при нулевом токе управляющего электрода $Iуэ =0$, подобна ВАХ диодного тиристора. Рост тока управляющего электрода (от $Iуэ=0$ до $Iуэ_3$) приводит к смещению вольт-амперной характеристики в сторону меньшего напряжения включения. При достаточно большом токе управляющего электрода $Iу_4$, называемого током спрямления, вольт-амперная характеристика тринистора вырождается в характеристику обычного диода, теряя участок отрицательного сопротивления.

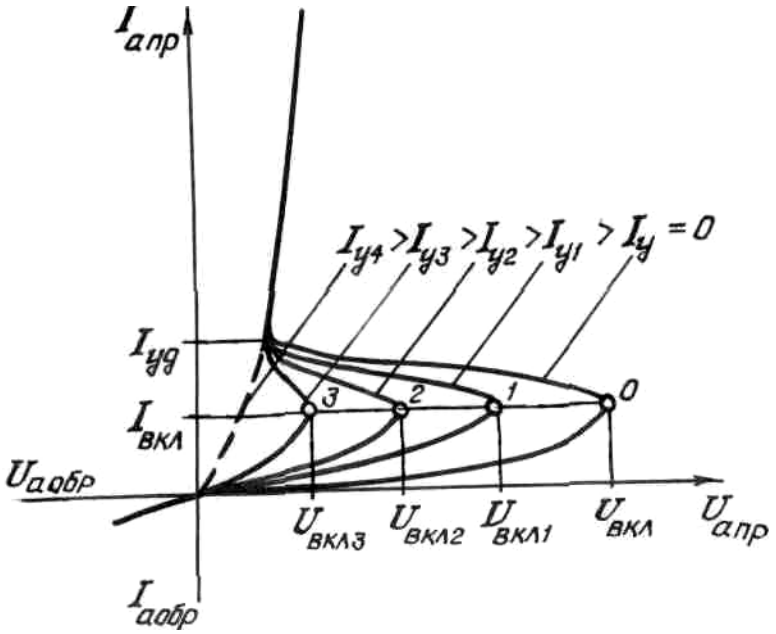


Рисунок 4 - Вольт-амперная характеристика триодного тиристора

Для выключения тринистора необходимо, так же как и для динистора, снижая напряжение, уменьшить на нем ток анода I_a до значения меньшего, чем ток удержания $I_{УД}$, т.е. выключение происходит по анодной цепи.

Наличие на вольтамперной характеристике тиристора двух участков с существенно различными значениями токов и напряжений не позволило проводить лабораторные опыты по непосредственному измерению вольтамперной характеристики. В результате, принято решение о целесообразности проведения лабораторных исследований каждого участка работы тиристора отдельно, независимо друг от друга.

Таким образом, сформировано задание на проведение лабораторных исследований тиристора.

Задание на проведение исследования тиристора.

Задание по лабораторной работе «Исследование тиристора»:

1. Исследовать полупроводниковый тиристор в открытом и закрытом состояниях,
2. Исследовать процессы переключения полупроводникового тиристора в открытое и закрытое состояния.

В лабораторной работе требуется:

Опыт 1. Исследовать полупроводниковый тиристор в закрытом состоянии.

Опыт 2. Исследовать процесс переключения тиристора в открытое состояние.

Опыт 3. Исследовать полупроводниковый тиристор в открытом состоянии.

Опыт 4. Исследовать процесс переключения тиристора в закрытое состояние.

Схема лабораторного опыта представлена на рисунке 5. Внешний вид установки «Электронные приборы» с собранной схемой исследования тиристора показан на рисунке 6.

Схема исследований собрана на универсальном коммуникационном поле с регулярной структурой. В ходе исследований использовались встроенные приборы:

1. Регулируемые источники постоянного напряжения: E1 (0-10 В) и E2 (0-20В);
2. Миллиамперметры – 2 шт., для измерения постоянного тока с пределами измерений 2, 20, 200 мА;
3. Вольтметры – 2 шт., для измерения постоянного и переменного тока с пределами измерений 2, 20, 200 В.

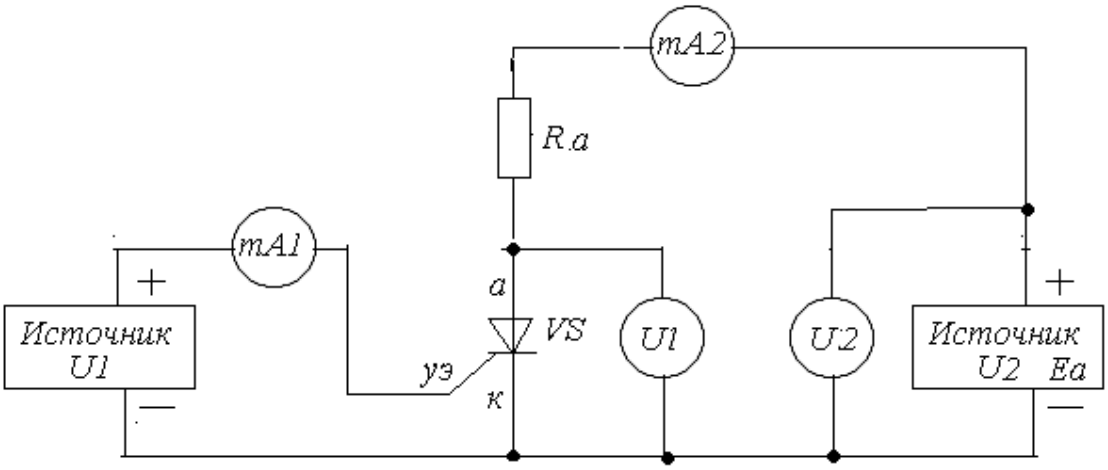


Рисунок 5 – Исследование полупроводникового тиристора

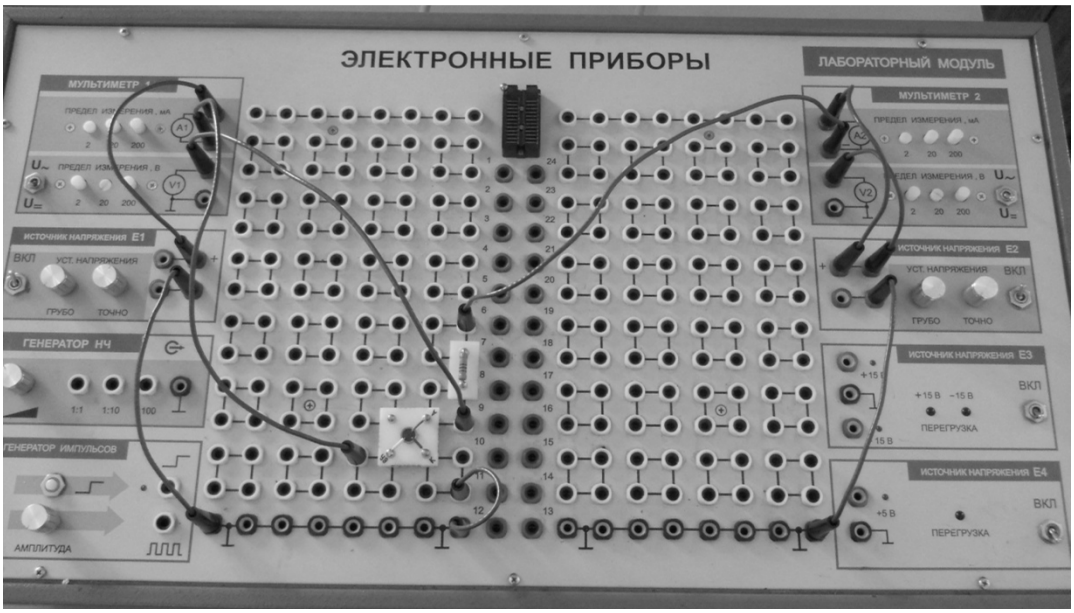


Рисунок 6 – Исследование полупроводникового тиристора на лабораторной установке «Электронные приборы»

В ходе проведенных исследований принято решение использовать в качестве анодных резисторов *Ra* штатные резисторы из состава комплектующих элементов для лабораторной установки номинальными значениями резистор 1 кОм и резистор 3,3 кОм.

Результаты проведенных исследований/

Рассмотрим результаты исследований и проведем их анализ.

Опыт 1. Исследовать полупроводниковый тиристор в закрытом состоянии

Отключить управляющий электрод. Ток управляющего электрода равен Iуэ=0. Изменять напряжение на аноде тиристора Еа. Измерять ток закрытого тиристора Iа и напряжение анод-катод Uак. Убедиться, что тиристор не включился. Результаты занести в таблицу.

По результатам исследований рекомендовано в опыте 1 изменять анодное напряжение источником Е2 от 2В до максимального значения 18В.

Таблица 1 - Исследование тиристора в закрытом состоянии

Iуэ=0	Еа,В	2	5	10	12	14	16	18	Резистор *Ra*=1 кОм
	Uак,В	2	5	10	12	14	16	18	
	Iа, мкА	0	0	0	0	0	0	0	
Iуэ=0	Еа,В	2	5	10	12	14	16	18	Резистор Ra=3,3 кОм
	Uак,В	2	5	10	12	14	16	18	
	Iа, мкА	0	0	0	0	0	0	0	

Вывод по опыту 1.

При отсутствии воздействия на управляющий электрод тиристор не переходит в открытое состояние. Напряжение анодного источника лабораторной установки не достигло напряжения включения $U_{ВКЛ}$. Анодный ток кремниевого закрытого тиристора настолько мал, что точность и чувствительность лабораторных приборов не позволило его определить и измерить.

Опыт 2. Исследовать процесс переключения тиристора в открытое состояние

Исходное состояние – тиристор закрыт. Установить значения напряжение на аноде Еа по указанию преподавателя. Плавно увеличивать ток управляющего электрода Iуэ. Зафиксировать значение Iуэ в момент переключения тиристора в открытое состояние. Результаты занести в таблицу.

По результатам исследований рекомендовано во 2 опыте проводить измерения при анодном напряжении источника Е2 10В и 15В для двух резисторовRa=1кОм и Ra=3,3кОм.

Таблица 2 – Исследование процесса переключения тиристора в открытое состояние

Iуэ, мА	Еа, В	Uак, В	Iа, мА	Резистор Ra
0,15	10	0,8	9,13	1кОм
0,15	15	0,81	14,09	1кОм
0,15	10	0,8	2,79	3,3кОм
0,15	15	0,79	4,31	3,3кОм

Вывод по опыту 2.

При воздействии на управляющий электрод существенно облегчался перевод тиристора в открытое состояние. Открывание тиристора происходило при токе управляющего электрода Iуэ=0,15мА. При включении тиристора скачком через неустойчивый участок резко возрастал анодный ток Ia, а напряжение анод-катод Uак уменьшалось до минимально возможного открытого значения Uакоткр ≈0,8В. Величину тока открытого тиристора можно рассчитать по формуле

$$Ia\ откр = (Ea - Uакоткр)/ Ra.$$

Расчеты удовлетворительно согласуются с результатами эксперимента с учетом погрешности измерений и разброса параметров анодных резисторов Ra.

Опыт 3. Исследовать полупроводниковыйтиристор в открытом состоянии

Перевести тиристор в открытое состояние. Отключить управляющий электрод. Ток управляющего электрода равен Iуэ=0. Изменять (уменьшать) напряжение на аноде тиристора Ea по указанию преподавателя. Измерять ток открытого тиристора Ia и напряжение анод-катод Uак. Убедиться, что тиристор остается в открытом состоянии. Результаты занести в таблицу.

По результатам исследований рекомендовано в 3 опыте проводить измерения для двух резисторов Ra=1кОм и Ra=3,3кОм. При этом анодное напряжение источника E2 изменять (уменьшать) от максимального значения 18В до значения 6В при анодном резистореRa=1кОм и до значения 12В при анодном резисторе Ra=3,3кОм. Выполнение указанных рекомендаций позволяет сохранять тиристор в открытом состоянии.

Таблица 3 - Исследование тиристора в открытом состоянии

Iуэ=0	Ea, В	18	16	14	12	10	8	6	Резистор Ra=1кОм
	Uак, В	0,81	0,81	0,8	0,8	0,8	0,8	0,8	
	Ia, мА	17,08	15,12	13,17	11,19	9,2	7,19	5,18	
Iуэ=0	Ea, В	18	16	14	12				Резистор Ra=3,3кОм
	Uак, В	0,81	0,8	0,8	0,79				
	Ia, мА	5,41	4,62	4,01	3,42				

Вывод по опыту 3.

При сохранении тиристора в открытом состоянии остаточное напряжение на тиристоре остается минимальным

$$Uакоткр \approx 0{,}79\ldots0{,}81В.$$

Остаточное напряжение на тиристоре в открытом состоянии не зависит от напряжения Ea источника анодного питания. Величину тока открытого тиристора можно рассчитать по формуле

$$Ia\ откр = (Ea - Uакоткр)/ Ra.$$

Расчеты удовлетворительно согласуются с результатами эксперимента с учетом погрешности измерений и разброса параметров анодных резисторов Ra.

Опыт 4. Исследовать процесс переключения тиристора в закрытое состояние.

Перевести тиристор в открытое состояние. Отключить управляющий электрод. Ток управляющего электрода равен Iуэ=0. Уменьшать напряжение на аноде тиристора Ea. Убедиться, что тиристор переключился в закрытом состоянии. Зафиксировать процесс выключения. Измерить (фиксировать) ток удержания Iуд, при котором тиристор перейдет в закрытое состояние. Измерить напряжение источника питания, подаваемое на анод тиристора Ea, и напряжение анод-катод Uак после перевода в закрытое состояние.

По результатам исследований рекомендовано в 4 опыте проводить измерения для двух резисторов Ra=1кОм и Ra=3,3кОм. При этом анодное напряжение источника E2 изменять (уменьшать) от максимального значения 18В до значения, при котором произойдет скачкообразное закрывание тиристора.

Таблица 4 – Исследование процесса переключения тиристора в закрытое состояние

Iуд, мА	Ea, В	Uак, В	Резистор Ra
2,88	3,77	3,77	1кОм
2,88	10,37	10,37	3,3кОм

Вывод по опыту 4.

Перевод тиристора в закрытое состояние происходит уменьшением значения тока в анодной цепи до значения тока удержания. При любом значении анодного резистора Ra ток удержания равен

$$I_{уд}=2{,}88 \text{ мА}.$$

Значение тока удержания Iуд можно определить по установившемуся значению анодного напряжения после закрывания по формуле

$$I_{уд} = (E_a - U_{акоткр})/ R_a.$$

Расчеты удовлетворительно согласуются с результатами эксперимента с учетом погрешности измерений и разбросом параметров анодных резисторов Ra.

Заключение

В результате проведенных исследований изучена работа тиристора как в открытом, так и в закрытом состояниях во всех основных участках вольтамперной характеристики его работы. А также исследованы процессы переключения тиристора из закрытого состояния в открытое и наоборот. Измерены параметры тиристора:

- открывание тиристора происходило при токе управляющего электрода Iуэ=0,15мА;
- значение тока удержания Iуд=2,88 мА;
- при сохранении тиристора в открытом состоянии остаточное напряжение на тиристоре остается минимальным Uакоткр ≈0,79…0,81В.

Анодный ток кремниевого закрытого тиристора настолько мал, что точность и чувствительность лабораторных приборов не позволило его определить и измерить.

Разработаны рекомендации для проведения лабораторных занятий по исследованию тиристора.

Результаты проделанной работы внедрены в учебном процессе кафедры «Радиоэлектроника» ДГТУ по дисциплине «Электроника» специальностей 110301 «Радиотехника» и 110302 «Инфокоммуникационные технологии и системы связи».

СПИСОК ЛИТЕРАТУРЫ

1. *Безуглов Д.А., Калиенко И.В.* Цифровые устройства и микропроцессоры. Ростов-н/Д.: Феникс, 2008. 468 с.
2. *Опадчий Ю.Ф., Глудкин О.П., Гуров А.И.* Аналоговая и цифровая электроника (полный курс). Учебник для вузов. –М.: Горячая линия – телеком, 2000.
3. *Булычев А.Л., Галкин В.И., Лямин П.М.* Полупроводниковые приборы: Диоды: Справочник. Мн.: Беларусь, 1994. 346 с.
4. *Калиенко И.В.* Аппроксимация вольтамперных характеристик полевых транзисторов на основе кубических сглаживающих сплайнов // Измерительная техника. Май, 2001. с. 60-63.
5. *Воржев В.Б., Балдин О.В., Рогов И.Е.* Аппроксимация вольт-амперных характеристик полевых транзисторов экспоненциальными кривыми с полиномиальными показателями // Современные проблемы науки и образования [Электронный ресурс]: электрон. науч. журн. – 2015. - №2. Режим доступа: http://www.science-education.ru/129-21621

Е.А. Коломиец, А.М. Коршун

СОВЕРШЕНСТВОВАНИЕ ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ НА БАЗЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: внеаудиторной самостоятельной работы, образовательный процесс, рабочая программа дисциплины, информационные технологии.

В работе рассмотрены некоторые вопросы модернизации самостоятельной работы обучающихся на базе информационных технологий. Показано перераспределение рабочего времени между внеаудиторной самостоятельной работой обучающихся и их аудиторными часами. Приведены виды внеаудиторной самостоятельной работы и рассмотрены её этапы. Предложены информационные ресурсы и формы телекоммуникации, рекомендуемые для самостоятельной работы в учебном процессе. Рассмотрен метод компьютерной презентации как форма представления полученных результатов.

E.A. Kolomiets, A.M. Korshun

IMPROVING OF THE STUDENTS OUT-OF-CLASS INDIVIDUAL WORK BASED ON INFORMATION TECHNOLOGIES

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

Keywords: out-of-class individual work, educational process, work program of discipline, information technologies.

The paper considers a number of issues concerning modernization of students individual work based on the information technologies. The redistribution of training time between the students out-of-class individual work and their class work is shown. The article considers types of out-of-class individual work and its stages. Information resources and forms of telecommunications recommended for independent work in the educational process are offered. The method of computer presentation as a form of demonstrating results obtained is considered.

Преобразования современного российского общества потребовали пересмотра качества профессиональной подготовки, в том числе и подготовки студентов-связистов. Как следствие, в последние годы в вузах осуществлен переход на многоступенчатую подготовку студентов, внедрена модульно-рейтинговая система, происходит регулярное обновление образовательных стандартов.

В Федеральных государственных образовательных стандартах высшего образования (ФГОС ВО) акцентировано внимание на том, что в результате освоения программы бакалавриата у выпускника должны быть сформированы общекультурные, общепрофессиональные и профессиональные компетенции соответствующие выбранному профилю подготовки [1;2].

Рабочие программы дисциплины «Экология» разработаны в нашем ВУЗе в соответствии с требованиями ФГОС ВО нового поколения, а так же на основании учебных планов направлений подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» и 09.03.01 «Информатика и вычислительная техника» и в соответствии с Положением о рабочих программах дисциплин, практик (СМК-П-2.02-01-16), построены на модульной основе, нацелены на формирование у выпускников компетенций и позволяют студентам овладевать необходимыми знаниям, умениями и навыками в области экологии [1;2].

Целями изучения дисциплины «Экология» является

- формирование у студентов экологического мировоззрения;
- обучение основам экономики рационального природопользования, экологического права и профессиональной ответственности.

В рабочих программах определено содержание дисциплины «Экология», которое включает модули, часы аудиторных занятий и внеаудиторной самостоятельной работы студентов (ВСРС) (таблица 1), той работы, которая осуществляется по заданию и при методическом руководстве и контроле преподавателя, но без его непосредственного участия (подготовка к лекциям, лабораторным и практическим занятиям, зачетам и т.п.)

Таблица 1

Модули дисциплины	Направление подготовки 11.03.02		Направление подготовки 09.03.01	
	аудиторные занятия (час.)	внеаудиторная самостоятельная работа студентов (ВСРС) (час.)	аудиторные занятия (час.)	внеаудиторная самостоятельная работа студентов (ВСРС) (час.)
Модуль 1. Основы общей экологии	8	16	8	32
Модуль 2. Биосфера и её антропогенное загрязнение	14	28	16	38
Модуль 3. Рациональное природопользование и система обеспечения экологической безопасности	14	28	12	38

Из таблицы 1 мы видим, что происходит перераспределение рабочего времени между внеаудиторной самостоятельной работой обучающихся и их аудиторными часами в пользу первой, которая составляет 3/4 и 2/3 учебного времени по дисциплине.

В связи с этим можно сказать, что в настоящее время внеаудиторная самостоятельная работа студентов занимает лидирующее место в учебном процессе и выходит на один уровень по значимости с аудиторными занятиями.

Введение в учебный план значительной доли внеаудиторных часов самостоятельных занятий по дисциплине «Экология» в соответствии с новыми образовательными стандартами требует усовершенствования учебного процесса.

В данной статье мы поставили задачу определить возможные пути модернизации самостоятельной работы обучающихся как формы организации обучения, необходимой для формирования компетенций [1;2] в результате освоения дисциплины.

Однако, виды внеаудиторной самостоятельной работы обучающихся могут быть различными, например:

- работа с основной и дополнительной литературой, учебно-методическим обеспечением дисциплины для самостоятельной работы обучающихся, рекомендуемыми источниками для углубленного изучения учебного материала, конспектами лекций, электронными образовательными ресурсами;
- подготовка ответов на контрольные вопросы по теме;
- ознакомление с нормативными и правовыми документами;
- подготовка рефератов, докладов и т.д.;
- выполнение расчётно-графических работ, применяя компьютерную технику;
- самостоятельное изучение научно-технической информации, отечественного и зарубежного опыта в области профессиональной деятельности.

Процесс организации внеаудиторных самостоятельных занятий обучающихся включает в себя следующие этапы:

- составление рабочей программы дисциплины с включением тем и заданий для самостоятельной работы, подготовку учебно-методического обеспечения дисциплины для самостоятельной работы обучающихся;
- проведение индивидуальных и групповых консультаций;
- проверку промежуточных результатов, итоговый контроль.

Для контроля усвоения учебного материала целесообразно проводить групповые собеседования или обсуждение изучаемого материала, контрольные работы в виде короткого письменного ответа на несколько вопросов, тестирование и т.д. Контрольные мероприятия при должной их организации позволяют не только оценить знания материала, но и углубить и закрепить его у обучаемых.

ФГОС ВО предусматривает применение для самостоятельной работы обучающихся информационных технологий, в части использования информационных ресурсов и виртуальной среды для общения и обучения [1;2].

Надо сказать, что сами информационные технологии, по сути, являются совокупностью методов обучения, обеспечивающих оптимальное и эффективное восприятие, усвоение и использование учебной информации в интерактивном режиме. К несомненным достоинствам информационных технологий можно отнести такие как доступность, мобильность, портативность, интерактивность, широкий охват аудитории и т.д. [3].

Информационные технологии так же облегчают усвоение абстрактного материала, позволяют многое из него представить в виде конкретных образов, приучают к точности, аккуратности, последовательности действий и способствуют развитию самостоятельности [5].

К информационным ресурсам, рекомендуемым для самостоятельной работы в учебном процессе по дисциплине «Экология» можно отнести

а) интернет-ресурсы

«Россия в окружающем мире» (ежегодник) http://eco-mnepu.narod.ru/book/

б) Сайты:

Министерства природных ресурсов и экологии Российской Федерации http://www.mnr.gov.ru,

Гринпис России http://www.greenpeace.org/russia/ru/,

WWF (Всемирный фонд дикой природы) http://www.wwf.ru/,

Центр экологической политики России и др. сайты государственных и общественных экологических организаций http://www.ecopolicy.ru,

а так же словари, энциклопедии, виртуальные библиотеки (научная электронная библиотека eLIBRARY.RU, Электронно-библиотечная система Znanium.com и др.),

Справочная система КонсультантПлюс (некоммерческая интернет-версия), информационная система "Единое окно доступа к образовательным ресурсам" и т.д.

Для организации диалога в сети «преподаватель – студент», целесообразно использовать такие формы телекоммуникации, как электронная почта, чат, социальные сети, форум, веб-конференция, видео-телефония и т.д.

Остановимся на некоторых из них:

– электронная почта является альтернативным способом оказания помощи студенту дистанционно. Электронная почта воспринимается преимущественно как средство для передачи инструкций преподавателем студентам, проведения индивидуальных консультаций, выполнения и сдачи письменных работ и переписки студентов между собой;
– социальная сеть сегодня – это, в первую очередь, инструмент для общения on-line, который нам предлагает Интернет. Это интернет-площадка, которая позволяет зарегистрированным на ней пользователям размещать информацию о себе и общаться, устанавливая социальные связи. Контент на такого рода сайтах размещается непосредственно самими пользователями (UGC - user-generated content);
– видео-телефония (Skype и др.)-это возможность видеть друг друга во время телефонного общения. Видеосвязь позволяет более продуктивно общаться т.к. посредством голоса передается лишь 20% информации.

Выше перечисленные информационные технологии повышают активность обучающихся. Из пассивного получателя информации они превращаются в её добытчиков.

Завершающим этапом самостоятельной работы является представление полученных результатов (в виде итоговой компьютерной презентации) на очередном аудиторном занятии с дальнейшим их обсуждением группой. Именно метод компьютерных презентаций позволяет представить объемный теоретический и прикладной материал в виде тезисов, таблиц, рисунков, графиков и т.д., что, безусловно, способствует более лёгкому его усвоению [4].

Важно, чтобы в обсуждении и оценке результатов выполненной работы принимали участие, как преподаватель, так и сами обучающиеся. Открытое оценивание результатов деятельности однокурсников позволяет сформулировать субъективные критерии оценивания, корректно выразить замечания и предложения.

Все это эффективно и полезно не только преподавателю, но в первую очередь для самих студентов. Такой подход развивает необходимые умения и навыки для дальнейшей профессиональной деятельности так, как на современном трудовом рынке, как никогда, стало важным умение грамотно и убедительно презентовать себя и свои результаты деятельности [4].

В заключение отметим, что это лишь ряд возможностей, которые нам предоставляют современные информационные технологии, в части применения различных информационных ресурсов и виртуальной среды для общения и постоянного обучения. Планомерное внедрение информационных технологий, в образовательную сферу послужит эффективным инструментом не только в модернизации организации внеаудиторной самостоятельной работы студентов, но и всего учебного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. ФГОС ВО, Министерство образования и науки РФ, Приказ от 06.03. 2015 г. №174.
2. ФГОС ВО, Министерство образования и науки РФ, Приказ от 12.01. 2016 г. №5.
3. *Коршун А.М., Коршун М.С.* Роль информационных технологий в экологическом образовании////«ИНФОКОМ-2012»/ Материалы международной молодежной

научно-практической конференции СКФ МТУСИ, 22-25 апреля 2012 г. Ростов-на-Дону. – ПЦ «Университет» СКФ МТУСИ, 2012, ч. 1., с. 250-253.
4. *Коршун А.М., Коршун М.С.* Мультимедийные технологии в образовательном процессе//«ИНФОКОМ-2012»/ Материалы международной молодежной научно-практической конференции СКФ МТУСИ, 22-25 апреля 2012 г. Ростов-на-Дону. – ПЦ «Университет» СКФ МТУСИ, 2012, ч. 1., с. 253-256.
5. *Махаматова З.Х., Шарипходжаева Ф.* Информационные технологии в организации самостоятельной работы//«ИНФОКОМ-2015»/ Материалы международной молодежной научно-практической конференции СКФ МТУСИ, 20-25 апреля 2015 г. Ростов-на-Дону. – ПЦ «Университет» СКФ МТУСИ, 2015, ч. 2., с. 174-176.

Б.Б. Конкин

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ

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

Ключевые слова: информационно-коммуникационные технологии, интерактивная среда, контрольно-обучающая программа, многоуровневое обучение, индивидуальное образование, рейтинговая система, тестирование, лекционные, лабораторные и практические занятия.

В работе обсуждается использование информационно-коммуникационных технологий в обучении. Приведены технологии, способствующие развитию навыков самостоятельной работы студента, проявлению заинтересованности в обучении и более глубокому пониманию предмета. Представлены инструменты, способствующие освоению необходимых знаний, навыков и умений студентов.

B.B. Konkin

INFOCOMMUNICATIONS TECHNOLOGIES USED IN EDUCATION

North-Caucasus branch of the Moscow technical university of communications and informatics,
Rostov-on-Don, Russia

Keywords: information and communication technologies, interactive environment, control training program, multilevel training, individual education, rating system, testing, lecture, laboratory and practical training.

The work discusses the use of information and communication technologies in training. The paper provides technologies promoting development of skills of student

independent work, manifestation of interest in training and deeper understanding of a subject. The tools promoting development of necessary knowledge, skills and abilities of students are presented.

В настоящее время каждый человек испытывает на себе мощнейшее влияние медиа технологий. Процессы информатизации, характеризующиеся совершенствованием и массовым распространением современных информационно-коммуникационных технологий (ИКТ), активно используются не только для передачи данных, но и для обеспечения взаимодействия обучающего и обучаемого в современной системе образования [1]. Это требует от преподавателя не только овладения навыками работы с ИКТ, но и умения профессионально применять их в своей деятельности.

Основное средство ИКТ для системы образования – это персональный компьютер, оснащенный необходимым программным обеспечением, к которому можно отнести текстовые представления и презентации, электронные таблицы и графические пакеты, органайзеры и базы данных и т. п. Общая классификация средств ИКТ по областям методического назначения представляется [2] следующим образом:

1. Обучающие. Они сообщают знания, формируют навыки практической или учебной деятельности, обеспечивая требуемый уровень усвоения материала.
2. Тренажеры. Предназначены для отработки различных умений, закрепления или повторения пройденного урока.
3. Справочные и информационно-поисковые. Сообщают сведения по систематизации информации.
4. Демонстрационные. Визуализируют изучаемые явления, процессы, объекты с целью их изучения и исследования.
5. Имитационные. Представляют собой определенный аспект реальности, позволяющий изучать его функциональные и структурные характеристики.
6. Лабораторные. Позволяют проводить эксперименты на действующем оборудовании.
7. Моделирующие. Дают возможность составлять модель объекта, явления с целью его изучения и исследования.
8. Расчетные. Автоматизируют расчеты и разнообразные рутинные операции.
9. Учебно-игровые. Предназначены для создания учебной ситуации, в которой деятельность обучаемых реализована в игровой форме.

Студенты, особенно те, кто изучает естественнонаучные дисциплины, такие как физика, математика, химия и т.п., испытывают потребность не только в получении информации, но и в возможности более разнообразной и детально-конкретной ее проработки и интерпретации, что обеспечивает глубину понимания и усвоения материала. Поэтому представляется, что наряду с информационными модулями должны быть весьма востребованными и интерактивные среды – контрольно-обучающие программы, что соответствует выше представленной классификации [2].

Предлагаемая компьютерная программа является многоуровневым многофункциональным интерактивным комплексом [3] по курсу физики. Весь комплекс содержит около сотни информационно-обучающих блоков, охватывающих практически все темы учебной программы. Каждый блок включает в себя следующие модули:

1. Электронный учебник – это теоретическая информация о рассматриваемом физическом явлении или процессе.

2. Лекционные демонстрации – это динамически развивающиеся на экране монитора картины рассматриваемых явлений.
3. Исследовательские задания – это качественное ознакомление с конкретными процессами.
4. Моделирование процессов – это варьирование элементов виртуальной установки и ее физических параметров, направленное на глубокое усвоение материала.
5. Электронные методические пособия – это примеры решения практических задач.

Представляемый комплекс рассчитан на широкий круг пользователей. Для тех, кто только начинает изучать физику, основной упор можно делать на использование модуля лекционных демонстраций физических явлений. Главным элементом демонстрационного модуля [4] и всего блока является компьютерная модель, которая дает наглядное представление численного эксперимента, достоверно отражающего физические законы. Диапазон регулируемых параметров позволяет получать достаточно большое и разнообразное количество экспериментальных данных. Такие модели помогают пользователю глубже понять и усвоить суть реальных физических явлений.

Модули исследовательских заданий включают в себя соответствующую компьютерную модель [5] и тренажер. Исследовательские задания имеют пять уровней сложности, начиная с программ в игровой форме, но отражающих выполнение законов физики, и заканчивая серьезными качественными вопросами. Их применение нацелено на углубление понимания теории и физических особенностей протекания рассматриваемого процесса или явления и знакомство с интерфейсом.

Моделирование процессов – это основной интерактивный контрольно-обучающий модуль каждого блока программы, включающий в себя десять контрольных заданий [6]. Тренажер этого модуля содержит систему инструментов, задающих исходные параметры; динамические строящиеся графики и таблицы, информирующие о ходе процесса; диалоговое окно, служащее для получения оценки, комментариев и конкретных заданий. Пользователю также предоставляется возможность самостоятельно собирать виртуальную установку или схему, например, электрическую цепь, состоящую из представленных для выбора элементов и рассчитать ее. Контрольные задания, количество и сложность которых выбирается пользователем, определяют степень усвоения материала. Исходные параметры контрольных вопросов задаются генератором случайных чисел. Программа предусматривает возможность получения правильного ответа несколькими способами: аналитическим, графическим и интуитивным, требующим понимания физической сущности рассматриваемого процесса. Оценка производится по рейтинговой системе.

В качестве примера [7] ниже приведены исследовательские и контрольные вопросы контрольно-обучающего модуля по упругому соударению тел (третий уровень сложности).

Исследовательские задания.

1. Исследование влияния начальных условий на результат неупругого соударения (результаты запиши в тетрадь и сравни их с «Ответами на исследовательские задания»):
   а) Исследуй влияние изменения начальной скорости первого шара на начальную скорость и высоту подъема системы шаров после удара. Для этого изменяй только скорость первого шара, оставляя остальные параметры неизменными.
   б) Исследуй влияние начальной высоты первого шара на начальную скорость и высоту подъема шаров после удара. Для этого с помощью левой кнопки мышки

устанавливай первый шар в разные положения, оставляя остальные параметры неизменными.

в) Исследуй влияние изменения массы первого и второго шара на начальную скорость и высоту подъема системы шаров после удара. Для этого создавай различные комбинации масс первого и второго шаров, оставляя остальные параметры неизменными.

г) Исследуй влияние изменения гравитации (ускорения свободного падения) на начальную скорость и высоту подъема шаров после удара. Для этого выбирай различные g, оставляя остальные параметры неизменными.

2. Исследование изменения импульса системы (результаты запиши в тетрадь и сравни их с «Ответами на исследовательские задания»):
   а) Установи в левой части рисунка левой кнопкой мышки первый шар. Задай начальную скорость, массы и ускорение g или используй их значения по умолчанию. Запусти процесс. Используя данные панели, рассчитай начальный импульс системы, импульс 1 и 2 шаров после удара. Сравни полученные значения с ответами. Сделай вывод о выполнении закона сохранения импульса.
3. Исследование изменения механической энергии системы (результаты запиши в тетрадь и сравни их с «Ответами на исследовательские задания»):
   а) Установи в левой части рисунка левой кнопкой мышки первый шар. Задай нулевую начальную скорость, для массы и ускорение g используй их значения по умолчанию. Запусти процесс. Используя данные панели, рассчитай механическую энергию системы до и после удара. Сравни полученные значения с ответами. Сделай вывод о выполнении закона сохранения механической энергии.

   б) Установи в левой части рисунка левой кнопкой мышки первый шар. Задай начальную скорость 30 м/с, для массы и ускорение g используй их значения по умолчанию. Запусти процесс. Используя данные панели, рассчитай кинетическую энергию системы до и после удара. Сравни полученные значения с ответами. Сделай вывод о выполнении закона сохранения механической энергии. Рассчитай максимальную кинетическую энергию системы после удара и сравни ее с максимальной потенциальной энергией. Сделай вывод о выполнении закона сохранения механической энергии. Рассчитай силу натяжения подвеса сразу после удара. Сравни полученные значения с ответами.

Контрольные задания.

1. Определи максимальный импульс первого шара.*
2. Определи импульс первого шара после удара.*
3. Определи импульс второго шара после удара.*
4. Определи начальную механическую энергию системы.*
5. Определи максимальную кинетическую энергию второго шара.*
6. Определи максимальную потенциальную энергию системы после удара.*
7. Определи силу натяжения подвеса сразу после удара.*

* Дополнительную информацию ищи на «Панели выбора параметров», «Панели текущих параметров». Ответ вводи с помощью Scroll Bar и кнопки «Ввод ответа».

Варьируя сложность заданий, представленный комплекс может применяться как на лекционных занятиях, так и для выполнения исследовательских, лабораторных и практических заданий студентами вузов. Возможность диагонального и вертикального

перемещения по всему комплексу и любой его части предоставляют пользователю возможность самостоятельно, как усложнить, так и упростить выполняемое задание, пытаясь понять суть рассматриваемого явления или процесса. Комплекс может быть использован как для работы под руководством преподавателя [8] , так и для самостоятельного обучения.

СПИСОК ЛИТЕРАТУРЫ

1. *Конкин Б.Б., Сафронов В.П.* Интерактивная среда – инструмент современного обучения // Открытое образование: науч.-практ. журнал / Москва. – 2011. – № 4(87), с. 11 – 18.
2. http://fb.ru/article/145313/informatsionno-kommunikatsionnaya-tehnologiya-ikt-tehnologii.
3. *Сафронов В.П., Конкин Б.Б., Ваган В.А.* Интерактивная обучающая среда «Курс физики» // Открытое и дистанционное образование, 2007. №3(27).С.56.
4. *Конкин Б.Б., Сафронов В.П., Ступаков В.Я.* О структуре контрольно-обучающей среды «Курс физики» // Труды Северо-кавказского филиала Московского технического университета связи и информатики «ИНФОКОМ-2013»: материалы междунар. науч.-практ. конф. СКФ МТУСИ 22-26 апр. / Ростов н/Д, 2013, с.416-422.
5. *Конкин Б.Б.* О роли интерактивных методов и современных технологий в обучении // Труды Северо-кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2016, с. 494-497.
6. *В.П. Сафронов, Б.Б. Конкин, В.А. Ваган.* О методике использования интерактивной обучающей среды «Курс физики» // Открытое и дистанционное образование 2008, № 3(31), с.52.
7. *Конкин Б.Б.* Контрольно-обучающая программа по физике // Труды Северо-кавказского филиала Московского технического университета связи и информатики, часть II: материалы междунар. науч.- практ. конф.СКФ МТУСИ «ИНФОКОМ-2015» / Ростов-на-Дону, 2015, 348 с.
8. *Конкин Б.Б., Сафронов И.П.* Рейтинговая система оценки знаний в технических вузах и обучающие среды // Труды Северо-кавказского филиала Московского технического университета связи и информатики. Часть 2 «ИНФОКОМ-2014»: материалы междунар. науч.- практ. конф. СКФ МТУСИ 22-25 апр. / Ростов н/Д, 2014, с. 175-179.

Д.В. Костюченко, П.М. Табунщикова

КУЛЬТУРА РЕЧИ В ЖИЗНИ IT-СПЕЦИАЛИСТОВ И ВСЕГО ЧЕЛОВЕЧЕСТВА

Северо -Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информации» ,
г. Ростов-на-Дону, Россия.

Ключевые слова: культура речи, профессиональное общение, информационное общество, технократия, технический вуз, речевая культура специалиста, техническое образование, грамотная речь.

Описана проблема значения культуры речи технических специалистов в современном информационном обществе с точки зрения моулодежи, руководителей компании и научно-педагогической элиты.

D.V. Kostyuchenko, P.M. Tabunshchikova

CULTURE OF SPEECH IN THE LIFE OF IT-SPECIALISTS AND ALL OF HUMANITY

North-Caucasian Branch of the Order of the Red Banner of Labor of the Federal State Budget Educational Institution of Higher Professional Education "Moscow Technical University of Communications and Informatics" Rostov-on-Don, Russia.

Key words: culture of speech, professional communication, technocracy, technical college, speech culture of a specialist, technical education, literate speech.

The problem of the importance of the speech culture of technical specialists in modern society from the point of view of youth, the company's leaders and the scientific and educational elite is described.

В современном обществе телекоммуникации являются основой развития, а информационные ресурсы становятся основным национальным богатством. Революционные достижения последних десятилетий в области микроэлектроники, вычислительной техники, оптических и квантовых технологий позволили создать принципиально новые устройства обработки, передачи и хранения информации: микросхемы сверхвысокого уровня, процессоры, запоминающие устройства и многое другое. Они послужили толчком к стремительному развитию современных информационных и телекоммуникационных технологий, совершенствованию различных средств связи и обработки, хранения и распределения информации. Уже несколько лет президент и правительство РФ проводят всестороннюю поддержку технического образования, государство осуществляет широкую программу предоставления грантов для студентов технических вузов, на развитие технической базы выделяются средства из

бюджета страны. Вот слова В.В. Путина, сказанные буквально 21.03.2017 года в Новосибирске: «Мир сегодня стоит на пороге больших перемен. И прежде всего это касается информационных технологий. Сегодня идет зарождение новых рынков, новых трендов, таких, как „большие данные“, промышленный интернет и интернет вещей, технологии прогнозной аналитики и когнитивных решений, искусственный интеллект»

Эта политика повышает интерес к техническим вузам и наукам. Кроме того, спрос на специалистов данных сфер продолжает расти. В Ростовской области губернатор В. Голубев и Правительство опубликовали список самых востребованных профессий, в который вошло значительное число технических специальностей. Это гарантирует быстрое трудоустройство и карьерный рост. Таким образом, выбор технической специальности, становится всё более предпочтительным, что и констатировала министр образования и науки Ольга Васильева в сентябре этого года.

Но какую же роль играет культура речи в этом «техническом» мире? Я провела небольшой опрос среди своих друзей старшеклассников и студентов.

Анонимное голосование

Как вы считаете необходимо ли преподавание русского языка и культуры речи в технических вузах?

Да	35	**66%**
Нет	18	**34%**

Проголосовало **53** человека.

Результаты анонимного голосования, проведенного среди молодежи, с одной стороны говорят о понимании важности владения речью техническими специалистами, ведь в современном мире система деятельности «человек-машина» существует скорее как абстракция, а не тип деятельности. Но с другой стороны 34% - это треть опрошенных, которые не принимают или недопонимают изменений, происходящих в современном мире. И это удручает, так как студенты не думают о влиянии культуры речи на общественную жизнь. «Русский язык и культура речи», на мой взгляд, является ключевым звеном, в формировании речевой культуры студента, но в технических вузах в число основных данная дисциплина не входит и изучается вскользь, и из-за этого мы недооцениваем всю ее важность.

Следующим объектом моего исследования стали сайты работодателей. Среди характеристик, необходимых работникам сотовых компаний и Ростелекома присутствует требование грамотной речи. Эта компетенция необходима как рядовому сотруднику, так и руководителю. Ведь именно речь на любом уровне взаимодействия выступает как средство формирования положительного впечатления о сотруднике той или иной фирмы и как следствие о предприятии в целом. Умение работника подать себя, четко сформулировать ответ на интересующего клиента вопрос, разъяснить сложные моменты как минимум всегда оставляет приятный след в памяти, и ,что важнее, помогает определению и решению любой проблемы. Грамотная речь также способствует

карьерному росту и налаживанию межличностных отношений внутри рабочего коллектива.

На сайте межвузовского центра по историческому образованию в технических вузах Российской Федерации, Межвузовского центра по политологическому образованию в рамках II Всероссийской научно-методической конференции профессор Московского государственного университета путей сообщения Воробьева И.В. поднимала проблему обучения культуре речи в техническом вузе.

« В современном мире - как на Западе, так и на Востоке (Япония) - обучению правильной и эффективной речи принадлежит центральное место в системе теоретического гуманитарного знания и в системе учебных предметов. В США риторика считается не просто наукой, но является предметом государственной идеологии в средних и высших учебных заведениях». А преподаватель Уральского федерального университета Ган О.И. пишет, что именно гуманитарные дисциплины должны способствовать формированию не просто конкурентоспособного специалиста (инженера, программиста, экономиста и пр.), а личности яркой, творчески мыслящей, ориентированной на нравственные идеалы.

Если рассматривать эту проблему глобально, то именно эффективность использования различных технологий в государственном и военном управлении, в промышленности, науке и образовании во все большей степени будет определять национальную безопасность страны и ее важнейшую составную часть - обороноспособность государства, а также показывать уровень его развития. Именно благодаря техническому прогрессу у нас появятся новые возможности, перспективы развития. Специалисты, обслуживающие машины станут самым многочисленным социальным слоем. Воцарится технократия. Создание искусственного интеллекта тоже находится в их руках. Важно ,чтобы эти люди имели не только технические знания но и обладали духовным богатством, ведь именно от тех, кто будет давать ход нашему развитию и зависит всеобщая безопасность и благополучие. Не зря говорят « как ты говоришь- так ты и мыслишь».

Таким образом, мы видим, что проблема формирования грамотной речи студентов в технических вузах существует и поднимается на разных уровнях , пренебрегать развитием речи непозволительно. Владение родным языком на высоком уровне – само собой разумеющаяся особенность носителей языка, и тем печальнее рост безграмотности и проблемы, связанные с ограниченным словарным запасом, засильем сленга и заменой слов и целых выражений примитивными символами. Культура речи – не просто средство профессиональной деятельности или компетенция; это – часть общей культуры образованного человека и не важно техническое или гуманитарное образование он получил.

СПИСОК ЛИТЕРАТУРЫ

1. Рабочая встреча Владимира Путина с Министром образования и науки Ольгой Васильевой 29.09.2016
2. Риторика и культура речи. Введенская Л.А., Павлова Л.Г. 12-е изд., стер. - М.: 2012.
3. Правительство Ростовской области. Постановление от 15.02.2016 № 80

4. Современные образовательные технологии и их использование в системе гуманитарной подготовки инженеров. Материалы II Всероссийской научно-методической конференции; Москва. МГТУ им. Н.Э. Баумана. 2010
5. Тематическое приложение к газете «Коммерсантъ» №047 от 21.03.2017г.

В.Г. Лисицин

ПРОБЛЕМЫ ОРГАНИЗАЦИИ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ В МАЛОМ БИЗНЕСЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования Донской государственный технический университет (ДГТУ), Ростов-на-Дону, Россия

Ключевые слова: малый бизнес, маркетинг, маркетинговые коммуникации, маркетинговые технологии, продвижение товара, брендинг.

В статье рассмотрены проблемы и актуальные тенденции современного малого бизнеса, представлены основные задачи в области маркетинговых коммуникаций, определены основные направления формировании маркетинговых коммуникаций в малом бизнесе.

V.G. Lisitsin

PROBLEMS OF ORGANIZATION MARKETING COMMUNICATIONS IN A SMALL BUSINESS

Federal state budgetary educational institution of higher education Don state technical University (DSTU), Rostov-on-don, Russia

Keywords: small business, marketing, marketing communications, technology marketing, sales promotion, branding.

The article considers problems and trends of contemporary small business, presents the main challenges in the field of marketing communications, defines the main directions of the formation of marketing communications in small business.

Развитие бизнеса в современных условиях во многом определяют технологии, позволяющие получить доступ к достоверной, полной и качественной информации. Особенно остро проблема использования передовых достижений в сфере коммуникаций стоит перед малым бизнесом, обладающим ограниченными финансовыми возможностями,

но который оценивается многими специалистами как перспективное и наиболее приоритетное направление формирования инновационной экономики России.

Субъекты малого бизнеса различных направлений деятельности на постоянной основе продвигают свою продукцию, услуги на рынке, стремясь реализовать несколько целей:

1) информировать потенциальных клиентов об условиях продажи, о характеристиках продуктов, услуг, предоставляемых компанией;
2) убедить покупателя в необходимости сделать выбор именно этой торговой марки, продукта или посетить определенное заведение;
3) воздействовать на покупателя таким образом, чтобы тот действовал здесь и сейчас, то есть совершал покупку, а не переносил ее на ближайшее будущее.

Реализация малым бизнесом вышеприведенных целей обычно осуществляется с помощью рекламы, почтовой рассылки, раздачи скидочных купонов, бесплатных образцов и других коммуникационных средств. Однако, стоит при этом заметить, что малые предприятия в современных условиях используют лишь отдельные элементы комплекса маркетинговых коммуникаций, и то не в полной мере. Зачастую это продиктовано недостатком финансовых ресурсов, необходимых для инвестирования в маркетинговые коммуникации. Кроме того, на предприятиях малого бизнеса маркетинговая служба может либо отсутствовать, либо быть представлена одним, двумя сотрудниками, компетентность которых также может вызывать вопросы. Следовательно, малые компании вынуждены планировать и осуществлять комплекс маркетинговых коммуникационных мероприятий не только в условиях ограниченного бюджета, но и в условиях дефицита персонала [1].

Маркетинговые коммуникации являются самым важным средством привлечения целевых потребителей, поскольку конкуренция среди предприятий малого бизнеса по качеству продукции и услуг практически отсутствует, а цена сегодня для потребителя не выступает в роли ориентира при оценке качества продукции или услуги. Реализация дополнительных сервисных услуг тоже не всегда способствует увеличению притока клиентов. В этих условиях руководству малого предприятия для того, чтобы маркетинговые инструменты оказались действенны необходимо сформировать систему эффективных бизнес-коммуникаций с клиентами.

Основным средством связи на настоящий момент у большинства малых компаний в России являются одноканальные городские номера и мобильные телефоны, использование которых для формирования постоянного потока клиентов не совсем практично в современных реалиях. Во-первых, во время общения с клиентом сотрудник не имеет возможности ответить на параллельный звонок или перевести его коллеге, а значит, есть риск потерять клиента, особенно высока такая вероятность, если он звонит впервые в компанию. Во-вторых, у руководителя малого бизнеса отсутствует возможность определить сколько клиентов звонили в организацию, но не получили ответа от ее сотрудников, поскольку те были заняты. В-третьих, представляется затруднительным процесс оценки вежливости, приветливости и компетентности персонала организации в процессе общения с клиентом. Кроме того, использование городских номеров в коммерческих целях согласно ценовой политике ПАО «Ростелеком» для малого бизнеса оказывается достаточно дорогим удовольствием (это касается так

называемых «золотых» и «серебряных» телефонных номеров, впрочем, использование других в бизнесе представляется не совсем целесообразным).

Согласно статистике руководителя филиала «Манго Телеком» в Санкт-Петербурге, Алексея Горбунова, из-за неправильно организованных коммуникаций бизнес теряет в среднем 30% потенциальных покупателей, даже не подозревая об этом. Порядка десяти процентов клиентов обычно не перезванивают, если слышат сигнал «занято» [2].

Многие предприятия малого бизнеса указывают на сайте и других средствах распространения информации о своей деятельности несколько контактных номеров – одноканальных городских и мобильных. Но и это не всегда является решением проблемы потери потенциального клиента, поскольку тот, позвонив в компанию и услышав «занято» обычно не перезванивает по следующему номеру из списка, а набирает номер другой компании.

Одним из выходов является переход на телефонную линию с многоканальным номером, бесплатной внутренней связью, которая не затрагивает внешние линии, записью разговоров и отчетами по звонкам. Но не все малые предприятия в силу ограниченного бюджета способны себе это позволить, особенно в условиях кризиса, даже понимая, что теряют клиентов из-за неправильно организованных коммуникаций. Офисная мини-АТС, в зависимости от функциональности, стоит от нескольких десятков тысяч до сотен тысяч рублей, при этом, не всегда решает все проблемы бизнеса в этой сфере. На просторах всемирной паутины существуют и бесплатные программные решения, но для них необходимо наличие сервера. Следует также заметить, что и аппаратные, и тем более программные АТС нужно настраивать и обслуживать в отличие, например, от виртуальной АТС, которая работает на мощностях оператора и предоставляется как сервис за умеренную абонентскую плату, в рамках которой руководство малого предприятия получает отчеты в режиме онлайн в личном кабинете [2].

Оптимальная настройка коммуникаций с учетом индивидуальных потребностей клиентов особенно важна для решения таких базовых задач маркетинга как формирование спроса и стимулирование сбыта. Целенаправленное воздействие на рынок посредством использования маркетинговых коммуникаций обеспечивает малым предприятиям формирование и поддержку взаимосвязей, взаимопонимания и сотрудничества между организацией и ее целевыми группами.

Среди элементов интегрированных маркетинговых коммуникаций, применяемых малыми предприятиями, следует выделить рекламу, связи с общественностью, брендинг, программы лояльности и стимулирование сбыта.

В качестве рекламных носителей выступают наружные специальные сооружения, рекламные афиши в транспорте, аудио-реклама в крупных торговых центрах. При сообщении рекламной информации (акции, открытие нового кафе, магазина) абсолютно все носители обычно содержат одинаковую информацию, они выполнены в едином стиле с нанесением логотипа и слогана-названия, идентифицирующего субъект малого бизнеса.

Предприятия малого бизнеса обращаются к широкой общественности в основном через публикации в средствах массовой информации (интервью, комментарии к событиям).

Подражая во многом крупным компаниям, руководство малых фирм стремится иметь собственный стиль, логотип, который может использоваться при брендировании одежды персонала, сувенирной продукции и любого другого фирменного носителя.

Для привлечения новых клиентов и повышения лояльности постоянных субъектами малого бизнеса обычно используется бонусная программа, позволяющая клиенту на специальной карте накапливать проценты или бонусы от сделанных заказов.

В области стимулирования сбыта малые предприятия в преддверии праздников (Новый Год, 23 февраля, 8 марта и т. д.) разрабатывают специальные программы, позволяющие получить скидку, памятный подарок, праздничное угощение и т.д.

Отдельно стоит заметить, что в среде российского бизнеса, в том числе и малого, сравнительно недавно произошло осознание того, что социальные сети являются важным средством привлечения целевой аудитории и повышения уровня ее лояльности. Но многие малые компании относятся к продвижению в социальных сетях с осторожностью, упуская отличные возможности для формирования лояльности потребителей. Современный покупатель выработал на традиционную рекламу стойкий «иммунитет»: пока на газетных страницах «пестрят» уже приевшиеся слоганы, а проплаченный эксперт расхваливает компанию с телеэкрана, потребитель ищет о ней живые отзывы среди «своих» – на форумах и в социальных сетях. Нельзя отрицать и тот факт, что социальные сети на данный момент стали настолько коммерциализированы, что зачастую число подписчиков пользователя в Instagram ё1 можно смело делить на два, потому что половину составят специальные профили различных компаний и сайтов, цель которых привлечь клиентов [3]. Для малого бизнеса, имеющего сравнительно небольшой бюджет на рекламу и маркетинг, особенно важно оценить возможность продвижения в социальных медиа в общем, и социальных сетях, в частности. Нельзя отрицать, что процесс продвижения посредством социальных медиа может быть очень финансово затратным, особенно если привлекать таргетированную различную рекламу и создавать широкомасштабные рекламные кампании. Однако, продвижение в данной среде возможно и за счет меньших финансовых затрат, если иметь четкое представление о том, кто является целевой аудиторией и какие у нее потребности.

Таким образом, малый бизнес может получить максимальную отдачу от потраченного рекламного бюджета, поскольку в традиционных видах рекламы очень мало дешевых способов привлечения внимания клиентов по сравнению с социальными сетями. Концепция работы в социальных медиа стала настолько приемлемой в бизнесе, что появились рекламные схемы для привлечения наиболее релевантной аудитории.

Развитие интернет технологий сформировало новые требования к процессу построения бизнес-модели: перенос бизнес-отношений в интернет-среду, развитие интернет-торговли и появление возможности налаживать контакты через прямое общение с клиентом поставило перед руководством малого бизнеса задачу разработки адекватной к меняющейся среде стратегии продвижения.

СПИСОК ЛИТЕРАТУРЫ

1. Третьякова, Т.С. Комплекс маркетинговых коммуникаций субъектов малого предпринимательства на основе малобюджетных технологий // Проблемы современной экономики. - №1, 2011: http://cyberleninka.ru/article/n/kompleks-marketingovyh-kommunikatsiy-subektov-malogo-predprinimatelstv
http://realty.rbc.ru/news/57c6e6449a79471cc44edc52(дата обращения: 17.04.2017)

2. http://spb.rbcplus.ru/partners/5710d5767a8aa96ecf0a7d22 (дата обращения: 16.04.2017)
3. http://earchive.tpu.ru/bitstream/11683/28844/1/TPU197625.pdf (дата обращения: 21.04.2017)

Р.А. Момот

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ПРОЦЕССОВ ВЕНЧУРНОГО ИНВЕСТИРОВАНИЯ В РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)», Ростов-на-Дону, Россия

Ключевые слова: венчурное финансирование, инвестирование, экономические стимулы, инновационное предпринимательство, бизнес

Рассмотрены вопросы особенностей венчурного инвестирования в России. Сделана сравнительная характеристика различных подходов и моделей поддержки венчурного бизнеса отдельных стран, лидирующих в области венчурного инвестирования.

R.A. Momot

PECULIARITIES OF FORMING VENTURE PROCESSES INVESTMENTS IN RUSSIA

Rostov State University of Economics, Rostov-on-Don, Russia

Keywords: venture financing, investment, economic incentives, innovative entrepreneurship, business.

The questions of peculiarities of venture investment in Russia are considered. Comparative characteristics of different approaches and models of venture business support of individual countries leading in the field of venture investment are made.

Процесс интеграции российской экономики в мировое экономическое пространство становится необратимым. Эти вопросы затрагивают и развивающееся в России новое направление финансовой индустрии – развитие венчурного инвестирования. Активное развитие венчурного инвестирования во всем мире является одной из составляющих успеха стран в международной конкуренции. На сегодняшний день можно наблюдать различные подходы и модели поддержки венчурного бизнеса, которые использовали в своей истории разные страны, их достижения и ошибки. Можно привести несколько моделей, которые являются показательными с точки зрения успешности. Характеристика таких стран представлена в таблице 1.

Таблица 1- Сравнительная характеристика различных подходов и моделей поддержки венчурного бизнеса отдельных стран, лидирующих в области венчурного инвестирования (составлено на основе [3; 4; 5])

Страна и используемая модель	Основные особенности	Результат
США SBIC (The Small Business Investment Company)	Разработана Программа компании по инвестициям в малый бизнес, учрежденная и управляемая частными лицами, лицензируемая Администрацией малого бизнеса	Сыграл важную роль в процессе восстановления американской экономики после последней рецессии. Только за один 2005 г. трудоустроил более 218 тыс. работников
Израиль (Yozma)	Модель предполагала создание государственного венчурного «фонда фондов» и последующее развитие 10 частных фондов с участием государства, каждый с капиталом 20 млн. долл. или более	Обеспечил резкий рост инновационной активности и расширение экспорта высокотехнологичной продукции с 2,2 млрд долл. в 1991 году до 11 млрд в 2000-м.
Финляндия: (SITRA)	Создание одной из самых эффективных систем венчурного финансирования на основе оптимального взаимодействия государства (Национального фонда исследований и развития (SITRA), науки и частного бизнеса в результате координации общих правил и согласования интересов.	Поддержка инновационных компаний посредством прямых инвестиций и инвестиций через венчурные фонды позволила стать одним из лидеров мирового рынка венчурных инвестиций
Китай (Программа «Четырех модернизаций»)	На основе государственной программы «Четырех модернизаций», легализации иностранной инвестиционной деятельности, открытия специальных экономических зон, принятия законов, облегчающих создание коммерческих и иностранных венчурных фондов	Создано более 86 тысяч высокотехнологических предприятий с более чем 6 млн работников, совокупная выручка которых составила около только за один 202 г. Составила 180 млрд долл.

Продолжение таблицы 1

Россия (Фонд содействия развитию малых форм предприятий в научно-технической сфере)	Особенность российского венчурного инвестирования заключается в значительной роли государства в его функционировании и развитии на основе Программы поддержки малых и средних компаний научно-технической сферы, организованной Министерством экономического развития в 2005 г. В рамках программы было создано 20 региональных государственно-частных венчурных фондов, перешедших под управление созданной министерством Российской венчурной компании.	Обеспечивает рост инновационной активности в сфере инфокоммуникационных технологий и продуктов

Однако в России становление национальной венчурной индустрии идет не столь быстро, как хотелось бы. К числу основных проблем, препятствующих развитию венчурной индустрии в России, можно отнести [1, с.55].

- незначительные объемы российского капитала в венчурной индустрии России;
- недостаток экономических стимулов для привлечения прямых инвестиций в предприятия высокотехнологичного сектора, обеспечивающих приемлемый риск для венчурных инвесторов;
- отсутствие развитой инфраструктуры, которая могла бы обеспечить появление новых и развитие существующих малых и средних быстрорастущих технологических инновационных предприятий,
- невысокий авторитет предпринимательской деятельности в области малого и среднего бизнеса.

В России пока не получили достаточного развития элементы сложной инфраструктуры поддержки деятельности в области венчурного финансирования.

Для стимулирования инновационной деятельности малых и средних предприятий создана Российская венчурная компания (РВК), которая должна обеспечить ускоренное формирование эффективной и конкурентоспособной национальной инновационной системы, в результате образования эффективной саморазвивающейся венчурной отрасли. Однако, следует учесть, что фонды, которые образовывались на базе Российской венчурной компании, в большинстве случаев своей целью имеют поддержку уже существующих и действующих бизнес-проектов. В тоже время, недостаточно внимания оказывается инвестициям в «стартапы» небольших и средних компаний.

Проведенный Центром экономической конъюнктуры при Правительстве Российской Федерации [1, с.76] анализ показал, что к числу основных факторов, сдерживающих инновационную деятельность в России, относятся:

- в финансовой сфере: недостаток собственных финансовых средств (41%), а также недостаток инвестиций (12%), ограниченность централизованных источников

финансирования, заемных и привлеченных средств, неприемлемые условия кредитования (16%);

– в сфере потребностей в инновациях: недостаточно высокое внедрение и реализация определенных инновационных проектов в результате невысокого спроса на научно-техническую продукцию.

Сложившийся до настоящего времени в России частно-государственный механизм венчурного финансирования пока не способен активно устранять сложности финансирования инновационного предпринимательства в области малого и среднего бизнеса. Это объясняется, прежде всего, тем, что российские венчурные компании имеют форму закрытого паевого фонда (ЗПИФ) [2, с.49]. Это накладывает ограничение на сам смысл работы венчурного инвестирования как рискованного вложения денежных средств.

Кроме того, существует и такая проблема как закрытость информации о проектах венчурных фондов. Это связано с тем, что по инвестиционному законодательству раскрывать информацию о деятельности венчурных фондов запрещено. Подобная информация может быть доступна лишь квалифицированным инвесторам. Хотя это касается государственных финансовых средств, для которых наиболее предпочтительна открытость и прозрачность использования. Поэтому в условиях отсутствия информации сложно создать эффективный институт венчурного финансирования.

Опыт стран, сопоставимых с Россией по уровню развития, показывает, что вмешательство государства в инновационные процессы нужно для того, чтобы в самом частном секторе создать стимулы к инновациям – для внедрения новых технологий, для выхода на новые рынки и для запуска собственных технологических производств.

Сложившаяся в Российской Федерации практика свидетельствует о том, что Государственные научно-исследовательские учреждения осуществляют разработку более 50% от всех инноваций, однако они не занимаются их практической реализацией и освоением. В практику внедряются лишь от 1 до 5% отечественных НИОКР, и происходит это в основном за счет средств финансово-промышленных групп. В то же время наблюдается крайне слабое участие государственных и коммерческих банков в кредитовании венчурных инновационных проектов.

Поэтому государственная поддержка венчурного бизнеса в России может оказываться по следующим направлениям через [5, с.52]:

1) нормативно-правовое регулирование научно-технической, инновационной, венчурной деятельности;
2) решение правовых проблем, связанных с вопросами интеллектуальной собственности, системы льгот, мотивации труда, а также на основе статуса территорий с высокой концентрацией научно-технического потенциала;
3) создание и поддержку экономических условий и стимулов развития венчурного инвестирования посредством системы госзаказа, совершенствования планирования и прогнозирования научно-технического прогресса, эффективных финансово-кредитных и других рычагов;
4) организацию управленческих условий венчурного инвестирования в результате совершенствования управления государственной собственностью, повышения эффективности управления государственными пакетами акций, обеспечения технологической безопасности, соблюдения национальных интересов, подготовки и переподготовки персонала.

Данные мероприятия должны быть интегрированы в единую стратегическую государственную концепцию развития отечественной инновационной и инвестиционной деятельности в области венчурного бизнеса.

СПИСОК ЛИТЕРАТУРЫ

1. *Зверев В.А.* Венчурный бизнес в России. Инвестиционные проекты и предложения. 2010, С. 55
2. *Кольцова Н.В.* Венчурное финансирование малого инновационного предпринимательства в России и ее регионах: проблемы и тенденции развития. 2010, С. 49
3. *Пеникас Г., Маленко А.,* Высшая школа экономики, 2014, С. 56.
4. *Родионов И.И.* Модели формирования института венчурных инвестиций 2010, С. 26.
5. *Суворинов Н.В.* О развитии инновационной деятельности в регионах России. 2009. С. 52.

М.Л. Мухитдинова , В.А. Каримова

АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ ЗАПАСАМИ ПРЕДПРИЯТИЯ НА ОСНОВЕ МЕТОДА СОВМЕЩЕННОГО ABC И XYZ АНАЛИЗА

Ташкентский университет информационных технологий, Ташкент, Узбекистан

Ключевые слова: информационные технологии, ABC-анализ, XYZ-анализ, принцип Парето, коэффициент вариации.

В статье рассмотрены проблемы анализа процесса управления запасами предприятия на основе метода совмещенного ABC и XYZ анализа. Представлен пример решения задачи для автоматизации процесса управления запасами предприятия, а также его прогнозирования на будущие сроки.

M.L. Mukhitdinova, V.A. Karimova

THE ANALYSIS OF PROCESS OF THE ENTERPRISE STOCKS MANAGEMENT ON THE BASIS OF THE COMBINED ABC AND XYZ ANALYSIS METHOD

Tashkent university of information technologies, Tashkent, Uzbekistan

Keywords: information technologies, ABC analysis, XYZ analysis, Pareto principle, variation coefficient.

In the article problems of the analysis of process of the enterprise stocks management on the basis of the combined ABC and XYZ analysis method are considered. The example of the task solution for automation of process of the enterprise stocks management, and also his forecasting for future terms is presented.

В условиях современных рыночных отношений одном из важных преимуществ любого предприятия является его эффективная система управления. Одним из важных вопросов при управлении предприятием является процесс управления запасами. [1]

Автоматизация данного процесса позволит предприятиям обрабатывать большое количество информации в минимальные сроки и на основе полученных результатов прогнозировать последующие запасы. На сегодняшний день существуют различные методы и методологии для управления запасами на предприятии. Наибольшей популярностью пользуются такие методы как метод АВС анализа и метод XYZ анализа.

АВС-анализ – это метод, который позволяет классифицировать ресурсы предприятия по степени их важности. Данный метод основан на принципе Парето, который гласит, что 20 % всех товаров дают 80 % оборота. [2] Применительно к управлению запасами предприятия - контроль 20 % категорий всех запасов позволяет на 80 % контролировать систему выдачи запасов. АВС-анализ основан на делении всех категорий запасов на 3 категории, которые можно определить по объему выдачи:

1) А – наиболее важные, 20 % - категорий запасов; 80 % - объем выдачи
2) В – средней важности, 30 % - категорий запасов; 15 % - объем выдачи
3) С – наименее важные, 50 % - категорий запасов; 5 % - объем выдачи.

По сути, АВС-анализ – это ранжирование каких-либо ресурсов (в нашем случае запасов) по разным характеристикам. Результатом АВС анализа является группировка объектов по степени влияния на общий результат. [2]

XYZ-анализ позволяет произвести классификацию ресурсов предприятия в зависимости от характера их потребления и точности прогнозирования изменений в их потребности в течение определенного временного цикла. [3]

Для получения результатов XYZ-анализа необходимо:

1) Определить коэффициент вариации для каждой категории;
2) В соответствии с возрастанием коэффициента вариации распределить запасы по категориям X, Y, Z.

Категория X – ресурсы характеризуются стабильной величиной потребления, незначительными колебаниями в их расходе и высокой точностью прогноза. Значение коэффициента вариации находится в интервале от 0 до 10 %. Категория Y – ресурсы характеризуются известными тенденциями определения потребности в них (например, сезонными колебаниями) и средними возможностями их прогнозирования. Значение коэффициента вариации – от 10 до 25 %. Категория Z – потребление ресурсов нерегулярно, какие-либо тенденции отсутствуют, точность прогнозирования невысокая. Значение коэффициента вариации – свыше 25 %. [3]

Оба данных метода имеют погрешности определения, однако могут дать эффективные результаты, если использовать их совмещенно.

Рассмотрим на примере использование метода совмещенного АВС и XYZ анализа для управления запасами предприятия. Данные по категориям запасов и вычисленная

общая сумма выдачи запасов за период (в данном случае 6 месяцев) приведены в таблице 1 (табл.1)

Табл. 1

	Объем выдачи запасов на предприятии по месяцам						**Итого сумма**
Категории	**Месяц 1**	**Месяц 2**	**Месяц 3**	**Месяц 4**	**Месяц 5**	**Месяц 6**	
Категория 1	190	220	220	280	250	300	1460
Категория 2	250	264	200	252	248	239	1453
Категория 3	251	223	256	287	265	290	1572
Категория 4	752	761	775	800	792	858	4738
Категория 5	200	192	202	201	230	210	1235
Категория 6	-	-	261	324	424	520	1529
Категория 7	2 500	2 400	2 721	2 320	2 692	2 604	15237
Категория 8	101	151	290	300	305	371	1518
Категория 9	1 704	1 766	1 434	1 000	1 753	1 550	9207
Категория 10	300	220	190	240	250	230	1430

Затем необходимо отсортировать результаты общей суммы выдачи по убыванию и определить долю выдачи запасов по каждой категории в общей сумме выдачи. Также определяем долю нарастающим итогом. При ранжировании данных, категории товаров с долей нарастающего итога от 0 % до 80 % будут относиться к группе А, от 80 % до 95 % - к группе В, от 95 % до 100 % - к группе С. Результаты представлены в таблице 2 (табл.2)

Табл.2

Категории	**Общая сумма**	**Доля**	**Доля с нарастающим итогом**	**Группа**
Категория 7	15237	38,69 %	38,69 %	A
Категория 9	9207	23,38 %	62,07 %	A
Категория 4	4738	12,03 %	74,11 %	A
Категория 3	1572	3,99 %	78,10 %	A
Категория 6	1529	3,88 %	81,98 %	B
Категория 8	1518	3,85 %	85,84 %	B
Категория 1	1460	3,71 %	89,54 %	B
Категория 2	1453	3,69 %	93,23 %	B
Категория 10	1430	3,63 %	96,86 %	C
Категория 5	1235	3,14 %	100,00 %	C
Итого	**39379**	**100,00 %**		

Таким образом, в группе А - 4 категории, в группе В – 4 категории, в группе С - 2 категории. Общее количество категорий в нашем примере 10. Следовательно, доля количества категорий в каждой группе составляет: группа А – 40 %, группа В – 40 %, группа С – 20 %.

Сравним результат ABC-анализа с рекомендуемыми значениями.

Группа А – 78,10 % выдачи (рекомендуемые – 80 %), 40 % категорий (рекомендуемые – 20 %)

Группа В – 15,13 % выдачи (рекомендуемые – 15 %), 40 % категорий (рекомендуемые – 30 %)

Группа С – 6,77 % выдачи (рекомендуемые – 5 %), 20 % категорий (рекомендуемые – 50 %)

После того, как проведен ABC-анализ с разбиением на группы, необходимо провести XYZ анализ. Данный метод заключается в группировке товаров по трем группам на основе изменчивости их результатов за прошлые периоды.

Для каждой категории (из табл.1) необходимо вычислить коэффициент вариации по формуле (1):

$$v = \frac{S}{R_{\text{ср}}} * 100\%$$

где, S – среднеквадратическое отклонение; $R_{ср}$ – средний объем выдачи запасов.

Результаты вычисления коэффициентов вариации и распределение по группам представлены в таблице 3 (табл.3).

Табл.3

	Объем выдачи запасов на предприятии по месяцам						**v, %**	**Группа**
Категории	**Месяц 1**	**Месяц 2**	**Месяц 3**	**Месяц 4**	**Месяц 5**	**Месяц 6**		
Категория 1	190	220	220	280	250	300	15,50	Z
Категория 2	250	264	200	252	248	239	8,36	X
Категория 3	251	223	256	287	265	290	8,67	X
Категория 4	752	761	775	800	792	858	4,40	X
Категория 5	200	192	202	201	230	210	5,83	X
Категория 6	-	-	261	324	424	520	77,43	Z
Категория 7	2 500	2 400	2 721	2 320	2 692	2 604	5,79	X
Категория 8	101	151	290	300	305	371	37,40	Z
Категория 9	1 704	1 766	1 434	1 000	1 753	1 550	17,37	Y
Категория 10	300	220	190	240	250	230	14,00	Y

В соответствии со значением коэффициента вариации все категории запасов делятся на три группы: X, Y и Z. В группу X попадают категории с коэффициентом вариации менее 10%. В группу Y – категории с коэффициентом вариации от 10% до 25%. В группу Z – категории с коэффициентом вариации более 25%. [3]

После применения ABC и XYZ анализа, совмещаем полученные результаты и представляем их в итоговой матрице (табл.4)

Табл.4

	Группа А	**Группа В**	**Группа С**
Группа X	3, 4, 7	2	5
Группа Y	9		10
Группа Z		1, 6, 8	

Из полученных данных можно сделать следующие выводы:

– Наиболее важными для предприятия является наличие запасов категорий групп А и В, следовательно, на предприятии должно быть обеспечено постоянное их наличие. При этом, категории запасов группы А должны быть обеспечены с избытком, а категории запасов группы В должны быть в достаточном количестве. Применение XYZ анализа показывает более точное распределение.
– Категории 2, 3, 4 и 7 стабильны по объему выдачи, поэтому наличие данных категорий запасов должно быть постоянным. Объем выдачи запасов указанных категорий хорошо прогнозируется.
– Категория 9 имеют недостаточную стабильность выдачи запасов, и, как следствие, для того, чтобы обеспечить постоянное наличие, нужно увеличить страховой запас.
– Категории 1, 6, 8 отличаются низкой прогнозируемостью выдачи объемов запасов на предприятии. Необходимо пересмотреть управление запасами в данных категориях.
– Категории группы С (5, 10) составляют до 80 % оставшихся запасов на предприятии.
– Категория 5 характеризуется хорошей стабильностью, и предполагает снижение страхового товарного запаса.
– Для категории 10 необходимо увеличить страховой запас, исходя из имеющихся у предприятия финансовых возможностей.

Таким образом, применение совмещенного АВС и XYZ-анализа позволяет повысить эффективность системы управления запасами предприятия. Применение данной методики на практике позволит выявить наиболее важные категории запасов и спрогнозировать оптимальный и эффективный запас на будущие сроки.

СПИСОК ЛИТЕРАТУРЫ

1. *Джон Шрайбфедер* Эффективное управление запасами // Изд-во: Альпина Паблишер, 2016, с. 15-35.
2. *Алесинская Т.В.* Основы логистики. Функциональные области логистического управления // ЛОГИСТИКА ЗАПАСОВ, Таганрог: Изд-во ТТИ ЮФУ, 2009. 79 с.
3. *Бодряков Р.Е.* АВС и XYZ: составление и анализ итоговой матрицы [Электронный ресурс] – Режим доступа – URL: http://www.rombcons.ru/logistik2.htm
4. *Ксенофонтова О.Л., Новосельская Н.А.* ABC-XYZ - анализ как средство управления товарным ассортиментом торгового предприятия // Экономические науки, выпуск 2, 2013, с.70-76

***В.А. Погорелов, *А.О. Семилеткин, **С.А. Швидченко**

ИССЛЕДОВАНИЕ МЕТОДА ПАРАМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ДИНАМИЧЕСКОЙ СИСТЕМЫ В УСЛОВИЯХ ДЕЙСТВИЯ ПОМЕХ

* ФНПЦ ФГУП «Ростовский-на-Дону НИИ радиосвязи», Ростов-на-Дону, Россия
**Донской государственный технический университет, Ростов-на-Дону, Россия

Ключевые слова: распределение Пирсона, идентификация, стохастическая фильтрация.

В статье исследован 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**

THE RESEARCH METHOD OF PARAMETRIC IDENTIFICATION OF DYNAMIC SYSTEMS IN CONDITIONS OF INTERFERENCE

*Federal State Unitarian Enterprise Scientific Research Institute of Radio Communication – Federal Scientific Production Center, Rostov-on-Don, Russia
** 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 $$L\{q,b,\rho_z\} = -\frac{\partial}{\partial Y}[q(Y,t)\rho_z] + \frac{1}{2}\frac{\partial^2}{\partial Y^2}[b(Y,t)\rho_z],$$

$$q(Y,t)=f_1(Y,t)+\frac{1}{2}\frac{\partial}{\partial Y}f_0^2(Y,t),\qquad b(Y,t)=f_0^2(Y,t),$$

$$R=R(Y,t)=-\frac{1}{2}[Z-h(Y,t)]^T D_W^{-1}[Z-h(Y,t)],\ R_0=\int_{-\infty}^{\infty}R(Y,t)\rho_z(Y,t)dY.$$

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:

$$J=-\int_T\int_{Y_*}\mathbf{\Phi}[\rho_z(Y,Q,t/Z(t))]dYdt, \tag{1.4}$$

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:

$$\dot{Y}=\sum_{i=0}^{N_0}f_{1_i}(t)Y^i+\sum_{i=0}^{N_1}Q_iY^i+\left[\sum_{i=0}^{N_2}f_{0_i}(t)Y^i\right]V_t, \tag{2.1}$$

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:

$$\dot{m}_j = j\sum_{i=0}^{N_0}\left[f_{1_i} + \frac{D_v}{2}\sum_{k=0}^{i} f_{0k} f_{0(i-k+1)}(i+1-k)\right]m_{i+j-1} + \frac{D_v}{2} j(j-1)\sum_{i=0}^{N_2}\left[\sum_{k=0}^{i} f_{0k} f_{0(i-k)}\right]m_{i+j-2} + \tag{2.2}$$

$$+\sum_{i=1}^{N_0} h_i\left(m_{i+j} - m_i m_j\right) + j\sum_{i=0}^{N_1} Q_i m_{i+j-1},$$

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 $M = \left|m_1 \ \ldots \ m_l\right|^T$, $F_1 = \left|f_{1_0} \ \ldots \ f_{1_N}\right|$, $F_0 = \left|f_{0_0} \ \ldots \ f_{0_N}\right|$, $G(M, F_1, F_0)$ – известная нелинейная вектор-функция компоненты, которой определяются из (2.5), $N(M) = \left|i m_{i+j-1}\right|\left(i = \overline{1,l};\ j = \overline{0,N}\right)$ – 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

$$\dot{\lambda}(t) = -\left[\frac{\partial}{\partial M} \int_{Y*} \mathbf{\Phi}_1 [\rho_z(Y, M, t)] dY \right]^T - \left[\frac{\partial G(M, F_1, F_0)}{\partial M} + \frac{\partial N(M)}{\partial M} Q \right]^T \lambda, \tag{2.9}$$

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

$$\dot{\tilde{M}} = G(\tilde{M}, F_1, F_0) - D\left[\frac{\partial}{\partial \tilde{M}} \int_{Y_*} \mathbf{\Phi}_1 [\rho_z(Y, \tilde{M}, t)] dY \right]^T, \tag{2.10}$$

$$\dot{D} = 2\left[\frac{\partial G}{\partial \tilde{M}} + \frac{\partial N}{\partial \tilde{M}} Q(\tilde{M}, 0) + N(\tilde{M}) \frac{\partial Q(\tilde{M}, 0)}{\partial \lambda} \right] D +$$

$$+ D\left[\frac{\partial G}{\partial \tilde{M}} + \frac{\partial N}{\partial \tilde{M}} Q(\tilde{M}, 0) \right] - N(\tilde{M}) \frac{\partial Q(\tilde{M}, 0)}{\partial \lambda} - 2D\left[\frac{\partial}{\partial \tilde{M}} \left[\frac{\partial}{\partial \tilde{M}} \int_{Y*} \mathbf{\Phi}_1 [\rho_z(Y, \tilde{M}, t)] dY \right]^T \right] D,$$

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%.

Заключение.

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.

СПИСОК ЛИТЕРАТУРЫ

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) – 2013.
13. *Погорелов В.А., Семилеткин А.О., Швидченко С.А.* Решение задачи идентификации на основе негауссовской аппроксимации апостериорной плотности вероятности. Труды Северо-Кавказского филиала Московского технического университета связи и информатики № 1 – 2015.

М.А. Пташинский, А.И. Момот

ОСОБЕННОСТИ ПЕРЕХОДА НА ВЕРСИЮ ИННОВАЦИОННОГО СТАНДАРТА ИСО 9001-2015

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: международный стандарт, система менеджмента качества, новая версия, философия, персонал, инновация

Рассматриваются вопросы перехода системы менеджмента качества предприятия отрасли связи на новую версию международного стандарта ISO 9001:2015. Приведены рекомендации по переходу.

M.A. Ptashinskiy, A.I. Momot

FEATURES OF TRANSITION TO VERSION OF INNOVATION STANDARD ISO 9001-2015

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

Keywords: international standard, quality management system, new version, philosophy, personnel, innovation

The issues of the transition of the quality management system of the communication industry enterprise to the new version of the international standard ISO 9001:2015 are considered. The recommendations on the transition are given.

Скоро подойдет к концу время, отведенное на завершение действия международного стандарта ISO 9001 версии 2008 г. (ГОСТ Р ИСО 9001-2008). Однако уже многие предприятия, не дожидаясь окончания действия предыдущего стандарта, активно переходят на новую, пятую его версию ISO 9001:2015. В Росстандарте утверждение национальных российских стандартов на системы менеджмента качества ГОСТ Р ИСО 9000 – 2015 и ГОСТ Р ИСО 9001 – 2015 произошло практически одновременно с международными стандартами ISO 9000:2015 и ISO 9001:2015. Стандарты ГОСТ Р ИСО 9000 – 2015 и ГОСТ Р ИСО 9001 – 2015 были введены в действие 1 ноября 2015 г. [1-2]

Введенный стандарт ГОСТ Р ИСО 9001-2015 «Системы менеджмента качества. Требования» аутентичен с ISO 9001:2015 «Системы менеджмента качества. Требования» и определяет требования к системе управления качеством. Требования вышеуказанного

документа являются общими для использования в любом предприятии и занимающимся любым видом деятельности. ГОСТ Р ИСО 9000-2015«Системы менеджмента качества. Основные положения и словарь» также аутентичен с ISO 9000:2015«Системы менеджмента качества. Основные положения и словарь». Настоящий стандарт устанавливает основные понятия и принципы менеджмента качества, а термины и определения, применяемые во всех стандартах в области менеджмента качества и стандартах на системы менеджмента качества, разработанные техническим комитетом ИСО/ТК 176 [15 - 16].

Новая версия стандарта ISO 9001:2015 была разработана на основе долголетних связей с ведущими международными кампаниями, участниками международной организации ISO, сформировавшими свои собственные системы управленческих технологий, опирающихся на многолетние результаты работы ученых международного уровня, таких как Э.Деминг, Д.Джуран, Ф.Кросби, К.Исикавы и многих других. Стандарт вобрал в себя самые эффективные технологии, которые ориентированы не сколько на выполнение требований по документированию всех процессов, сколько на постановку целей и задач в области бизнеса, изменения мышления в пользу бизнеса и эффективности результатов деятельности кампаний. Особое значение придается достижению удовлетворенности всех заинтересованных сторон.

Существенно отличаясь от старого издания, новая версия в качестве приоритетных направлений все ближе подходит к основным принципам менеджмента успешных предприятий и организаций, разработанных ведущими предприятиями мирового уровня и апробированные на протяжении многих десятков лет. В основу этих принципов, а, следовательно, и принципов новой версии международных стандартов в области менеджмента качества, положены принципы лидерства, ориентации на потребителя, оценке эффективности и результативности бизнес-процессов, управлении рисками, обеспечения одинаковой заинтересованности всех участников и партнеров организаций. Особенно это актуально для клиентов и самой организации ФГУП «Почта России».

Новая версия ISO 9001:2015 (ГОСТ Р ИСО 9001-2015), значительно отличающаяся от предыдущих, направлена на улучшение всей деятельности современного предприятия. Был создан новый стандарт для единой новой структуры всех серий систем менеджмента. Данная новая структура стала называться «Структура высокого уровня», и в соответствии с ней будут строиться стандарты всех остальных серий. В новой структуре активно используется процессный подход. Данный стандарт носит ярко выраженный инновационный характер.

В связи со значительными изменениями в стандарте ISO серии 9001 версии 2015 г. для всех предприятий отрасли связи, в которых функционирует данная система менеджмента качества, необходимо внесение всех соответствующих изменений. Эти изменения будут заключаться в нижеприведенных рекомендациях.

При построении системы управления качеством на соответствие требований новой версии международного стандартов ISO 9001:2015 (ГОСТ Р ИСО 9001-2015), прежде всего, следует учесть изменения базовых принципов менеджмента качества, которые представлены в таблице 1.

Базовые принципы служат основой для изменения, прежде всего, мышления персонала и направлены на боле тесные взаимоотношения со всеми партнерами предприятия, их еще можно назвать взаимозаинтересованными сторонами. Однако, на

нащ взгляд, к партнерам предприятия можно отнести не только внешних участников взаимоотношений, но и внутренних. Среди всех партнеров предприятия можно выделить несколько групп взаимозаинтересованных сторон, к которым можно отнести:

- акционеров;
- совет директоров;
- топ-менеджеров;
- потребителей;
- государство;
- общество;
- персонал;
- партнеров

Таблица 1 - Изменения базовых принципов менеджмента качества [1; 2; 3; 4]

1	Ориентация на потребителя	1	Ориентация на потребителя
2	Роль руководства	2	Лидерство
3	Вовлечение персонала	3	Вовлечение персонала
4	Процессный подход	4	Процессный подход
5	Системный подход		
6	Постоянное улучшение	5	Улучшения
7	Принятие решений на основе фактов	6	Принятие решений на основе фактов (свидетельств)
8	Взаимовыгодные отношения с поставщиками	7	Управление взаимоотношениями с заинтересованными сторонами

При разработке системы менеджмента качества на основе версии ISO 9001:2015 (ГОСТ Р ИСО 9001-2015) следует внести изменения и в структуру Руководства по качеству, которая может основываться на структуре новой версии стандарта.

В таблице 2 представлена старая и новая структуры международного стандарта. Более подробные рекомендации по каждому разделу приведены ниже.

Введение (основная информация о методе PDCA, менеджменте рисков, процессном подходе, взаимодействии с остальными стандартами);

1. Области использования;
2. Нормативные ссылки;
3. Термины и определения;
4. Окружение предприятия (приняты два новых раздела, о сущности самой кампании);
5. Лидерство (в новой редакции повышены требования к лидерству);
6. Планирование системы качества (принят новый блок требований);

7. Обеспечение;
8. Процессы;
9. Оценка функционирования (мониторинг, измерение, анализ, оценка деятельности организации и удовлетворенности потребителей, внутренний аудит, анализ СМК);
10. Совершенствование (непрерывное улучшение продуктов/услуг, а также системы менеджмента, выявление несоответствий и корректирующие действия).

Были несколько изменены основные принципы системы качества. Системный подход перестал использоваться в этой версии, как устаревший. По новому стал определяться принцип «Управление взаимоотношениями с заинтересованными сторонами», в котором отношения с участниками деятельности стали пониматься гораздо шире. Получил новое понимание принцип о роли руководства, который стал называться в «Лидерство» [6].

Одним из важнейших нововведений версии стандарта ISO 9001:2015 стало введение новых понятий, таких как: «Организационная среда», «Заинтересованная сторона», «Знания организации».

В новом тексте стандарта произошло, также, упразднение отдельных требований, хотя следует отметить, что некоторые положения не совсем исчезли из ISO 9001:2015, а лишь поменяли свой статус: из обязательных стали рекомендательными.

Таблица 2 - Сравнительный анализ структур стандартов версий ISO 9001:2008 и ISO 9001:2015 [3; 5]

	МС ISO 9001:2008 ГОСТ Р ИСО 9001-2009		МС ISO 9001:2015 ГОСТ Р ИСО 9001-2015
0	Введение	0	Введение
1	Назначение	1	Область применения
2	Нормативные ссылки	2	Нормативные ссылки
3	Термины и определения	3	Термины и определения
4	Система управления качеством	4	Окружение организации
5	Ответственность руководства	5	Лидерство
6	Управление ресурсами	6	Планирование
7	Производство продукции (осуществление услуг)	7	Обеспечение
8	Измерения, анализ и совершенствование	8	Процессы
		9	Проведение оценки
		10	Улучшения

Перестали использоваться обязательные требования по разработке шести документированных процедур, также как и создание Руководства по качеству стало не обязательным, однако организации вправе продолжать применять их на свое усмотрение. Вследствие широкого распространения электронного документооборота были отменены понятия «протокол качества» и «документ». Вместо этого был введен термин «документированная информация», в котором осталось требование по обеспечению наличия информации в электронной или бумажной форме. Также ликвидируется понятие «предупреждающие меры», которые теперь является составляющим элементом механизма управления рисками [1].

Очень важным и принципиальным изменением становится требование руководителю предприятия нести всю полноту ответственности напрямую за процессы системы качества, вместо существовавшей до этого практики назначать для выполнения этой задачи представителя руководства по системе менеджмента качества.

Кратко, необходимые изменения в СМК можно свести к следующему:

1) изменение базовых принципов;
2) изменения в структуре стандарта и Руководства по качеству;
3) упразднение должности представителя руководства по качеству и передача данных функций руководителю предприятия;
4) изменение философии качества должно быть осознанным для населения

СПИСОК ЛИТЕРАТУРЫ

1. Государственный стандарт РФ ГОСТ Р ИСО 9000-2015 «Системы менеджмента качества. Основные положения и словарь»: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28.09.2015г. № 1390-ст. - М.: Издательство стандартов, 2015;
2. Государственный стандарт РФ ГОСТ Р ИСО 9001-2015 «Системы менеджмента качества. Требования»: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28.09.2015г. № 1391-ст. - М.: Издательство стандартов, 2015;
3. Государственный стандарт РФ ГОСТ Р ИСО 9000-2008 «Системы менеджмента качества. Основные положения и словарь»: принят и введен в действие приказом Федерального Агентства по техническому урегулированию и метрологии от 18.12.2008г. № 470-ст. - М.: Издательство стандартов, 2009;
4. Государственный стандарт РФ ГОСТ Р ИСО 9001-2008 «Системы менеджмента качества. Требования»: принят и введен в действие приказом Федерального Агентства по техническому урегулированию и метрологии от 18.12.2008г. № 470-ст. - М.: Издательство стандартов, 2009;
5. Новый стандарт ISO 9001:2015. Риски и потенциал для предприятий. Переход системы менеджмента качества на новую версию стандарта. Режим доступа: http://gnexpert.ru/1447860885
6. ISO 31000 Менеджмент риска. Принципы и руководство http://gostrf.com/normadata/1/4293795/4293795643.pdf

Е.Г. Ротова, А.И. Момот

ИСПОЛЬЗОВАНИЕ ПРОЦЕССНОГО ПОДХОДА ПРИ ОСУЩЕСТВЛЕНИИ ЗАКУПОЧНОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова статьи: закупочная деятельность, процессы, эффективность, технологии, логистика, закупки, выбор потенциальных поставщиков

Рассматриваются вопросы осуществления закупочной деятельности на основе процессного подхода. Приведена методика выбора альтернативных поставщиков, сделан расчет о степени предпочтительности поставщиков.

E.G. Rotova, A.I. Momot

USE OF THE PROCESS APPROACH WHEN PERFORMING PURCHASING ACTIVITY OF THE ENTERPRISE

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

Keywords: procurement activity, processes, efficiency, technology, logistics, procurement, selection of potential suppliers

The issues of procurement activities are considered on the basis of the process approach. The method of choosing alternative suppliers is given, the calculation is made about the degree of preference of suppliers.

В любой организации закупочная деятельность занимает важную роль в системе логистики, являясь главным источником поступления товаров. Деятельность по закупкам должна быть построена таким образом, чтобы получать от нее доход за счет приобретения товаров по выгодным и приемлемым ценам, не допуская нарушения сроков поставок и выполнения планов по количеству и качеству.

Иначе говоря, закупочная деятельность представляет собой процессы по приобретению продукции соответствующего качества в необходимом количестве, которые могут быть поставлены из нужного источника по достаточно приемлемой цене, и быть доставлены в необходимое место и в конкретное время. Эффективность такой работы во многом зависит от квалификации и добросовестности персонала, его умению работать как с поставщиками, так и с покупателями [2, с.22]. Основной проблемой при осуществлении закупочной деятельности любой компании является параллельная работа по продаже этой закупленной продукции.

Поэтому очень важным для получения прибыли и сохранением оптимальных затрат является слаженная, четкая работа и скоординированное взаимодействие подразделений по закупкам и продажам. С этой целью подразделения по закупкам должны осуществлять свою деятельность на основе использования современных управленческих, логистических, складских, маркетинговых технологий [4; 5].

Закупочной деятельности предприятий характерна высокая динамика, обусловленная изменениями во внутренней и внешней среде, ресурсном потенциале, технологии торговли, финансовом состоянии, а эффективная деятельность по закупкам обеспечивает устойчивое развитие предприятия, его конкурентоспособность.

Только в условиях полной координации работы всех подразделений возможна безубыточная деятельность организации и обеспечение ее высокой конкурентоспособности на всех этапах развития рыночной экономики. Положение усложняется еще и тем, что в настоящее время остается значительное количество факторов, негативно влияющих на эту деятельность.

Особую важность приобретают механизмы проведения закупок на основе использования процессного подхода, получившего распространение в последние десятилетия, как во всем мире, так и в Российской Федерации. Получившие распространения технологии бережливого производства, Канбан, «Точно-во-время» и многие другие позволяют значительно сокращать размеры товарных запасов, ускорять время товарооборачиваемости, не нести не нужных расходов и значительно сократить издержки, связанные с закупочной деятельностью.

Управление закупками сегодня можно рассматривать с точки зрения процессного подхода, являющегося одним из доминирующих методических подходов, применяемых в менеджменте. В соответствии со стандартом ГОСТ Р ИСО 9001-2009 любая деятельность или комплекс деятельности, в которой используются ресурсы для преобразования входов в выходы, может рассматриваться как процесс» (рисунок 1) [9].

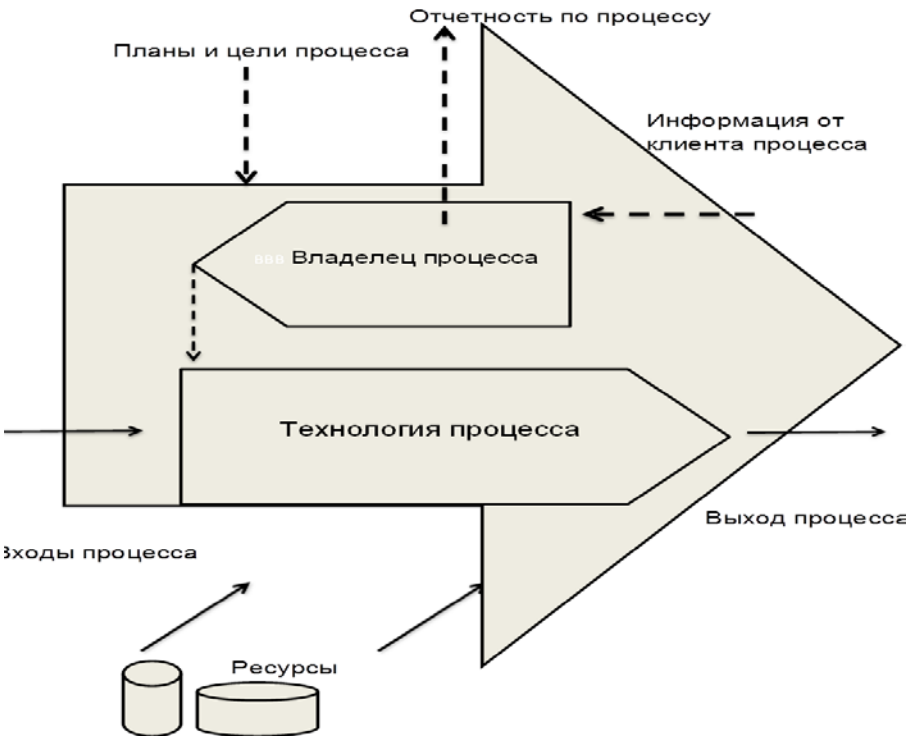


Рисунок 1- Концептуальная схема управления процессов

При этом система управления компанией ориентируется как на управление каждым бизнес-процессом в отдельности, так и всеми бизнес-процессами предприятия в целом. При этом система качества предприятия обеспечивает качество технологии выполнения бизнес-процессов.

Отличие процессного подхода в том, что он ориентирован, в первую очередь, не на организационную структуру предприятия, не на функции подразделений, а на бизнес-процессы, конечными целями выполнения которых, является создание продуктов или услуг, представляющих ценность для внешних или внутренних потребителей.

Требования к результату процесса и его характеристик идут от потребителя процесса, которым может быть либо внешний в отношении организации субъект, или структурное подразделение самой организации. В свою очередь, руководители и участники процесса выдвигают требования к входам процесса и, соответственно, к его поставщикам - внешним поставщикам организации или ее структурным подразделениям [3].

На конечный результат деятельности компании оказывает качество закупаемой продукции, которое напрямую зависит от наличия эффективной системы управлением процесса закупок. Одним из главных элементов при осуществлении процесса управления закупками является правильный выбор потенциальных поставщиков. Этот выбор проводится в два этапа [6]:

1 этап. Поиск потенциальных поставщиков.

2 этап. Выбор потенциальных поставщиков.

В компании поиск потенциальных поставщиков начинается с рассылки коммерческих писем, главной целью которых является получение оферты с полной информации о поставщике и возможностях по поставке необходимой продукции. На основе полученных ответов формируется перечень постоянных поставщиков. Данный перечень не является постоянным и утверждается каждый год директором компании.

На втором этапе при проведении выбора проводится предварительный анализ. В этом случае может быть применена рейтинговая система оценок поставщиков [7; 8]. Рассмотрим схему проведения процессов закупок на рисунке 2, которая представлена в виде блок схемы управления процессами .Порядок проведения закупок осуществляется в следующей последовательности [1]:

1) подготовка и подача заявки на приобретение материально-технических ресурсов,
2) определение требований к закупаемых материалов
3) подготовка документации;
4) передача документация на закупку материалов;
5) осуществление контроля документации на закупку материалов;
6) принятие решения о документации на закупку материалов;
7) выбор и оценка поставщиков;
8) корректировка документации на закупку материалов;
9) представление документации на поставку материалов;
10) приобретение и доставка материалов;
11) контроль сопроводительной документации и входной контроль материалов;
12) принятие решения по результатам контроля;
13) проведение замены материалов или возврат поставщику;
14) направление материалов на производство или для продажи.

Подразделением по закупкам предприятия проводится выбор по двум критериям:

1) цена продукции;
2) качество продукции.

Однако анализ результатов поставок и разработка предложений по повышению их эффективности проводится не на постоянной основе и не достаточно часто. Как правило, поставщики выбираются из перечня, который был сформирован раньше, без анализа их поставок, основываясь на сложившихся взаимоотношениях. Подход, рассмотренный выше, осуществляется на многих предприятиях.

Но, в настоящее время для повышения эффективности деятельности предприятия в условиях высокой конкуренции необходимо сокращать затраты в целях обеспечения конкурентоспособной цены.

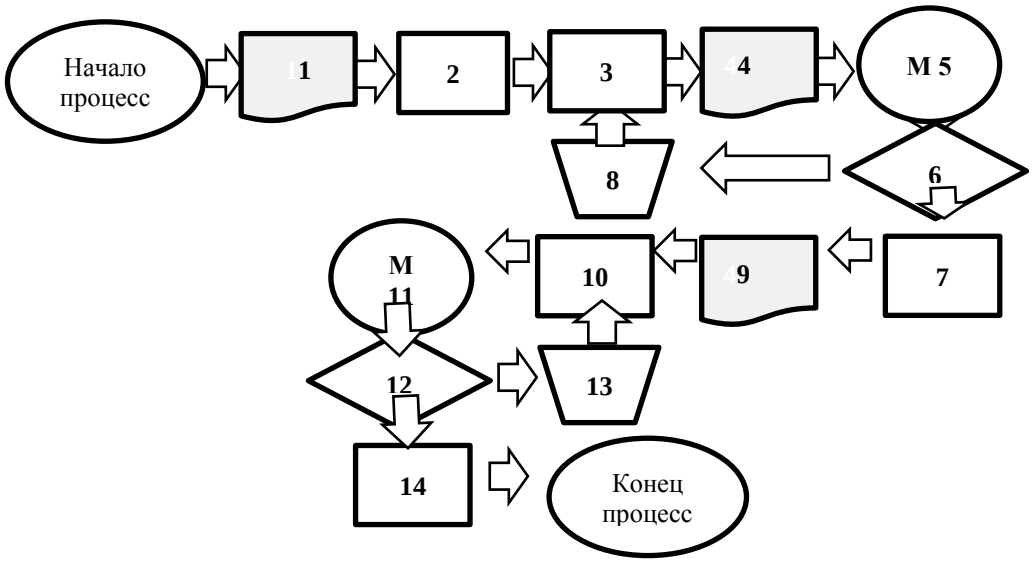


Рисунок 2-Схема проведения закупок продукции в компании [3]

Поэтому затраты, связанные с поставкой продукции могут иметь значительную величину, что может быть помехой при формировании оптимальной цены на продукцию. Кроме того, на наш взгляд, целесообразно расширить перечень критериев и включить в него следующие их виды: - надежность поставок продукции; - цена поставляемой продукции; - качество; - сроки выполнения поставок продукции; - удаленность поставщика от предприятия.

Ниже в таблице 1 приведены характеристики по 5-бальной шкале критерия выбора поставщиков «Надежность поставок продукции» [7].

Таблица 1 – Расчет рейтинга поставщиков продукции на предприятии

№ п/п	Разработанные критерии поставок	Среднее значение оценки критерия поставщика			Критерий коэффициента весомости фактора поставки	Произведение среднего значения оценки поставщика на весовой коэффициент весомости фактора поставки		
		1	2	3		1	2	3
Продолжение таблицы 1								
1	Надежность поставок продукции	4,0	3,6	3,0	0,23	0,92	0,83	0,69
2	Цена поставляемой продукции	3,8	3,4	3,6	0,22	0,84	0,75	0,79
3	Качество поставляемой продукции	3,4	3,8	3,2	0,24	0,82	0,91	0,77
4	Сроки выполнения поставок продукции	3,2	3,6	3,0	0,20	0,64	0,72	0,6
5	Удаленность поставщика от ПАО «Ростелеком»	3,2	3,0	3,2	0,11	0,35	0,33	0,35
	Всего	17,6	17,4	16,0	1,0	3,57	3,54	3,2

На основе анализа предложенных критериев поставок в таблице 1 были сделаны выводы о степени предпочтительности поставщиков. Наиболее предпочтительным поставщиком по данному виду продукции на основе экспертных оценок стал поставщик 1. Вторым по степени значимости и целесообразности определен поставщик 2, и наименее предпочтительный оказался поставщик 3.

После проведенных расчетов коммерческий директор предприятия делает предложение по выбору поставщиков, однако окончательное решение принимает директор.

СПИСОК ЛИТЕРАТУРЫ

1. Алгоритмы некоторых процессов [Электронный ресурс]. – Режим доступа: http://www.ingener-alians.ru/algoritm/alg01.shtml.
2. ГОСТ Р ИСО 9001-2009 Системы менеджмента качества. Требования. – 23 с.
3. ГОСТ 701-90 (ИСО 5807-85) «Схемы алгоритмов, программ, данных и систем»
4. *Кузовкова Т.А., Женчур М. А., Кузовков А. Д.* Методический аппарат комплексного прогнозирования развития инфокоммуникаций. // Системы управления, связи и безопасности, 2016, № 1. – С. 146-190
5. Логистическое управление закупками и поставками [Электронный ресурс]. – Режим доступа: http://ua.coolreferat.com/Логистическое_управление_закупками_и_поставками

7. Поиск, оценка и выбор поставщика [Электронный ресурс]. – Режим доступа:http://www.1snabport.org/index.php?option=com_content&view=article&id=54&Itemid=58.
8. Рейтинговая оценка поставщиков сырья [Электронный ресурс]. – Режим доступа: http://science-bsea.narod.ru/2006/ekonom_2006/zvarygina_reiting.htm.
9. *Репин.* Бизнес-процессы компании. // СПб.: Виктория плюс, 2002. – 187 с.
10. ISO/TC 176/SC 2/N 544R2(r) «Руководство по концепции и применению процессного подхода к системам менеджмента».

А.А. Санников, В.Т. Куанышев

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ОБРАБОТКА БОЛЬШИХ МАССИВОВ ДАННЫХ В СФЕРЕ ОБРАЗОВАНИЯ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», г. Екатеринбург, Россия

Ключевые слова: большие данные, массивы, данные, система, обработка, сервер, принципы, программное обеспечение

В работе описывается технический подход для обработки больших массивов данных в сфере образования, на примере системы для контроля за программных обеспечением.

A.A. Sannikov, V.T. Kuanyshev

INFORMATION TECHNOLOGIES AND PROCESSING BIG DATA IN EDUCATION

Keywords: big data, arrays, data, system, processing, server, principles, software

The paper describes the technical approach for processing of big data sets in education, for example, the system for monitoring software.

Введение

В сфере образования регулярно обновляются и появляются информационные технологии, которые позволяют совершенствовать процесс обучения. Информационные технологии имеют различное применение и соответствующие архитектурные решения, при этом, если одна технология позволяет совершенствовать процесс обучения, то другая может выполнять функции контроля за различными сегментами образовательного учреждения и т.д.

Принципиальным здесь является то, что все они тесно связаны друг с другом на функциональном и структурном уровне, а также то, что работают с большим объёмом данных (Big data).

Big data – большой объем (массив) данных, который может быть представлен как в структурированном виде, так и не в структурированном [1].

В данной работе под большим массивом данных понимаются в первую очередь не собственно объёмы данных, а методы их обработки. Обрабатывать такие массивы, можно разными методами и способами [1]. После этапа обработки необходимо проводить анализ данных, на основе которого строится соответствующий вычислительный алгоритм извлечения некоторого знания из полученных данных. В общем случае анализ данных основан на применении разнообразных методов, например, машинное обучение, технологии Data Mining [2].

Обработка данных поисковыми системами в реальном времени

Рассмотрим небольшой пример, связанный с обработкой данных поисковыми системами в режиме реального времени. Для того чтобы обрабатывать запросы поисковых систем нужно иметь на аппаратном уровне достаточно мощные вычислительные ресурсы. Такие компании, как Google и Yandex, имеют очень сильную базу для обработки, но и в этом случае у каждой базы есть предел. Когда он будет достигнут, егонужно будет расширять. Поэтому поисковые системы используют различные методы и технологии (например, технология Apache Spark [3]) для оптимизации всех запросов.

Здесь важно понимать, что обработка Big data позиционируется на нескольких основных принципах:

- горизонтальная масштабируемость;
- отказоустойчивость;
- локальность данных.

Опишем кратко некоторые из этих основополагающих принципов.

Горизонтальная масштабируемость. Исходя из того, что у нас имеются большие объёмы данных, наша система должна иметь возможность расширять свою техническую и вычислительную базу.

Отказоустойчивость. Поскольку в нашей системе присутствует возможность расширения мощностей, то какая-то часть оборудования в нашей системе будет выходить из строя. И система должна переживать эти моменты, без каких-либо неприятных последствий.

Локальность данных. Если наши данные хранятся на одном из серверов, а обрабатываются они уже другим сервером, то это может вызвать проблему. Потому что затраты на передачу данных могут превысить саму обработку. Исходя из этих данных, нужно спроектировать систему таким образом, чтобы данные хранились, обрабатывались и передавались одним сервером.

Так или иначе, все системы, которые работают с Bigdata, придерживаются этих основных принципов функционирования.

После определения больших массивов данных, можно переходить к информационной технологии в выбранной сфере, в данном случае, области образования. Соответствующая вышеперечисленным принципам разработанная системадолжна осуществлять контроль за программным обеспечением.

Суть технологии заключается в следующем: в любом образовательном учреждении есть персональные компьютеры, на которых установлено платное и бесплатное программное обеспечение. Наша система будет хранить и обрабатывать всю информацию об этом программном обеспечении.

Блочная структура системы показана на рисунке 1.

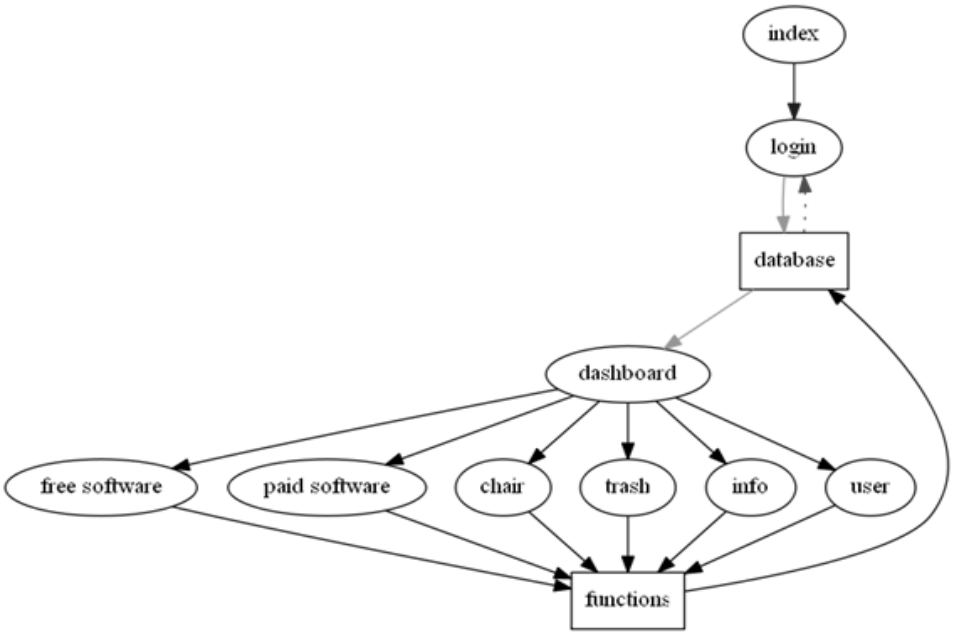


Рисунок 1 – Блочная структура системы обработки больших данных

Структура системы была разработана в виде орграфов, при помощи программного обеспечения GraphViz, на языке DOT.

Пояснения к структуре:

- администратор открывает главную страницу (index);
- затем переходит на страницу авторизации (login), после того, как были введены данные, выполняется запрос к базе данных, если все данные были введены верно система осуществляет перенаправление (редирект) на страницу (dashboard);
- на странице управления (dashboard) администратор может попасть в любой раздел: платное ПО, бесплатное ПО, кафедры, корзина, информация и данные пользователя;
- все запросы на страницах обрабатываются файлом functions, и передаются в базу данных.

Данная система может работать, как на локальном сервере, так и на виртуальном под управлением операционной системы Windows, Ubuntu, FreeBSD и др.

Вся информация о программном обеспечении, данных пользователя, информации об образовательном учреждении и кафедрах, хранится и обрабатывается на одном сервере. Это в свою очередь позволит систематизировать и структурировать данные, которые можно будет использовать в стороннем программном обеспечении. Тем самым появляется возможность создавать гибкую связь между несколькими программными продуктами.

СПИСОК ЛИТЕРАТУРЫ

1. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма Map Reduce / Блог компании DCA (Data-Centric Alliance) / Электронный ресурс: https://habrahabr.ru/company/dca/blog/267361/]
2. *Золотых Н.Ю.* Машинное обучение. – Электронный ресурс: http://www.machine learning.ru
3. Spark для профессионалов: современные паттерны для обработки больших данных / Сэнди Риза, Ури Лезерсон, Шон Оуэн, Джош Уиллс. – С.-Пб: Изд. дом «ПИТЕР», 2017. - 272 с.

Е.А. Свирщ

ИНФОРМАЦИОННАЯ КОМПЕТЕНТНОСТЬ ЭКОНОМИСТОВ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО "Сибирский государственный университет телекоммуникаций и информатики" в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: информатизация образовательного пространства вуза, информационная компетентность профессорско - преподавательского состава, использование информационных ресурсов вуза в образовательном процессе, информационная компетентность выпускников.

В статье рассмотрены современные требования подготовки экономистов и их информационная компетентность, информатизация образовательного процесса .

E.A. Svirsch

INFORMATION COMPETENCE OF ECONOMISTS

Ural Technical Institute of Communications and Informatics (branch) FGBOU VO "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibGUTI)

Key words: informatization of the educational space of the university, information competence of the teaching staff, use of information resources of the university in the educational process, informational competence of the graduates.

The article considers modern requirements of training economists and their information competence, informatization of the educational process.

Профессиональная подготовка экономистов с настоящее время невозможна без широкого использования инфокоммуникационных технологий, но выпускники ВУЗов не всегда соответствуют требованиям , предъявляемым к ним работодателями. Причинами этого являются противоречия между существующей теорией и практикой профессиональной подготовки специалистов и требованием времени в специалистах, умеющих гибко перестраиваться в соответствии с требованиями постоянно изменяющегося информационного пространства. Не всегда преподаватели применяют инновационные формы преподавания, связанные с применением инфокоммуникационных технологий, чаще используются традиционные формы учебно-методического обучения. Недостаточно разработаны содержание и условия обеспечения эффективности процесса обучения.

В условиях перехода к информационному обществу особенно актуальной становится проблема профессиональной подготовки экономистов с высокой информационной грамотностью. Требования работодателей к кандидатам на вакантную должность экономиста однозначны – помимо опыта работы, профессиональных знаний требуется умение использовать информационные технологии для решения экономических задач на предприятии .

С другой стороны внедрение информационных технологий в учебный процесс позволяет сократить время на выполнение рутинных операций и повысить эффективность обучения.

Информационные технологии позволяют:

- получить необходимую информацию и быстрее повысить уровень актуальных в настоящий момент знаний;
- систематизировать информацию, пользуясь электронными словарями, справочникам и электронными библиотеками;
- отработать различные навыки и умения, используя программных продукты по заполнению первичных документов, финансовому анализу;
- визуализировать информацию (например, на презентациях);
- проводить сложные расчеты и автоматизировать рутинные операции;
- обмениваться информацией между пользователями, находящимися на большом расстоянии друг от друга.

Информатизация общества приводит к необходимости существенного изменения методики подготовки экономистов.

Прослеживается логическая связь: информатизация общества – информатизация образовательного пространства вуза - информационная компетентность профессорско - преподавательского состава – использование информационных ресурсов вуза в образовательном процессе - информационная компетентность выпускников.

Информатизация образовательного пространства вуза позволит наиболее эффективно использовать все возможности информационных технологий. Это и дистанционное обучение, и создание единой системы мониторинга и оценки качества образования, организация сетевого взаимодействия структурных подразделений, оптимизация управления образовательным учреждением, достижение нового качества образовательной деятельности за счет использования инновационных информационных технологий.

Главнейшей задачей информатизации процесса образования является создание системы повышения квалификации преподавателей. В программах повышения квалификации должны быть наравне с профессиональными вопросами, вопросами охраны труда и безопасности жизнедеятельности присутствовать вопросы повышения информационной грамотности.

Информационная компетентность преподавателя характеризуется умениями осуществлять поиск, анализ и использование информации для построения профессиональной карьеры. Информационная компетенция преподавателя включает в себя следующие умения и навыки::

- умение осуществлять познавательную деятельность в области информационных технологий;
- знание способов информационной деятельности в своей предметной области (решение методических, проектных, задач с использованием информационных технологий) в форме действий по алгоритму;
- умение принимать эффективные педагогические решения в учебных ситуациях.

Одним из важных показателей информационной компетенции преподавателя является владение информационными технологиями. Обычно выделяют три уровня владения информационными компетенциями:

- базовый - на данном уровне накапливаются базовые знания, умения и навыки, необходимые для знакомства с компьютерной грамотностью; применение информационных технологий на данном уровне минимально (владение общими приемами создания, редактирования, сохранения, копирования и переноса информации в электронном виде, представление информации средствами презентационных технологий, освоение навыков поиска информации в сети Интернет и т.д., выбор способа сетевого взаимодействия (или их комбинации), наиболее соответствующего характеру проблемы и позволяющего выработать пути ее решения наиболее оптимальными способами);
- технологический (на данном уровне информационные технологии становятся инструментом в осуществлении прикладной деятельности (оценка потенциала Интернет-ресурсов, степени их интерактивности и информативности с позиций целевой предметной области; анализ программных средств и ресурсов сети глобальной компьютерной сети с учетом основных технологических, экономических, эргономических и технических требований; оценка качества, средств и форм представления в глобальной сети Интернет программно-технологического и информационного обеспечения и др.);
- практический (профессиональный) - на данном уровне целесообразно говорить о создании новых инструментов для осуществления информационной деятельности.

Основные информационные образовательные ресурсы:

1. Электронная библиотека - это информационная система, позволяющую сохранять и эффективно использовать коллекции электронных документов через глобальные сети передачи данных в удобном для конечного пользователя виде.

   Признаки электронной библиотеки:

   – управление ресурсами через компьютер;
   – способность связывать поставщика информации с потребителем через электронные каналы;

- способность персонала вмешиваться в электронные процессы, когда это необходимо;
- способность хранить, организовывать и передавать информацию пользователю с использованием электронных средств.

2. Электронные учебники и электронные учебные высоко эффективны при подготовке экономистов.

Электронные учебники – это программно-методические комплексы, обеспечивающие возможность самостоятельного усвоения учебного курса или большого раздела . Электронные учебные пособия это компонент поддержки учебного процесса. Основное отличие от электронного учебника – большая степень автономности, охват небольшого раздела дисциплины. В электронном пособии могут использоваться мультимедиа и гипермедиа ресурсы, позволяющие объединить в компьютерной системе текст, звук, видеоизображение, графическое изображение и анимацию.

3. Интернет позволяет создавать единую информационную образовательную среду для всех категорий пользователей. Интернет позволяет актуализировать информацию, получить доступ к новым нормативные документам, приказам, положениям. Собрать статистические данные и финансовые отчеты организаций; изображения, видео- и звуковые файлы; обучающие программы.

Важным аспектом организации учебно-познавательной деятельности студентов является развитие самостоятельности, как необходимого качества личности будущего специалиста. Необходимо привить студентам потребность в самостоятельном изучении учебной и научной литературы, в самообразовании и саморазвитии посредством активной познавательной деятельности по собственной инициативе, вызванной познавательной потребностью.

Самостоятельная работа требует соответствующего информационно – предметного обеспечения. Наряду с учебниками, ученьми пособиями, конспектами лекций, научной литературой и т.п. целесообразно использование в самостоятельной работе студентов электронных информационных образовательных ресурсов. Имея в своем распоряжении электронный учебник, практикум по курсу, рекомендации по решению типовых задач, электронные справочники, перечень вопросов к семинарам и экзаменам, студент может эффективно организовывать свою самостоятельную работу с учетом собственных возможностей и потребностей.

Информационная компетентность выпускников это умение работать с информацией, представленной в различных формах.

Выпускник по направлению подготовки «Экономика» должен иметь определенный уровень знаний, умений и навыков, позволяющих решать актуальные практические задачи, и быстро ориентироваться в информационном пространстве, иметь опыт в поиске, хранении и передаче информации, полученной с помощью технических средств и информационных технологий, готовность и способность личности к организации использования информации, технических средств и средств информационных технологий в профессиональных целях.

Включение современных информационных технологий в образовательный процесс позволяет повысить качество образовательных услуг

Информатизация образования является одним из приоритетов развития социальной сферы и органически связана с процессом модернизации образования.

СПИСОК ЛИТЕРАТУРЫ.

1. *Акулова О.В.* Компетентностный подход в информационном обществе: тенденции и проблемы. – Режим доступа: ftp://lib.herzen.spb.ru/text/akulova_6_17_16.pdf
2. *Бейсетаев Д.Б., Султанова Б.К.* Создание единого информационного пространства вуза // Молодой ученый. — 2015. — №23. — С. 107-110.
3. *Савостьянова И.Л.* Состояние проблемы определения понятия профессиональной информационной компетентности экономиста // Молодой ученый. — 2013. — №11. — С. 640-643.
4. *Шапиева М.С.* Использование информационных технологий при обучении в системе образования вуза // Молодой ученый. — 2014. — №5. — С. 572-574.

Т.В. Сидорина

ОБЕСПЕЧЕНИЕ БЕЗОПАНОСТИ НА ПРЕДПРИЯТИЯХ ПОЧТОВОЙ СВЯЗИ

Донской государственный технический университет, федеральное государственное бюджетное образовательное учреждение высшего профессионального образования,
г. Ростов-на-Дону, Россия

Ключевые слова: почтовая безопасность, информационная безопасность, административный уровень информационной безопасности.

Успех обеспечения сохранности и защиты информации на предприятии зависит, прежде всего, от разработанных на нем политик безопасности. В статье рассмотрены проблемы обеспечения безопасности на предприятиях почтовой связи и способы их обеспечения подразделениями почтовой безопасности Почты России на административном уровне.

T.V. Sidorina

PROVIDING OF SECURITY ON ENTERPRISES OF POSTAL CONNECTION

Don state technical university,
federal public budgetary educational institution of higher professional education,
Rostov-on-Don, Russia

Keywords: postal safety, informative safety, administrative informative strength security.

Success of providing of safety and priv depends on an enterprise, foremost, from worked out on him politician of safety. In the article the problems of providing of safety on the enterprises of postal connection and methods of their providing subdivisions of postal safety of Mail of Russia are considered at administrative level.

ФГУП «Почта России» – национальный почтовый оператор, предоставляющий универсальные услуги почтовой связи на всей территории Российской Федерации, присутствует в трех секторах экономики: перевозки и логистика, почтовые услуги, а также финансовый сегмент. Ее предназначение и прямая обязанность заключается в обеспечении граждан доступной, надежной и безопасной связью, что требует защиты почтовых каналов и недопущения их использования в ущерб общественным интересам.

Почтовая безопасность является неотъемлемой составляющей качества услуг почтовой связи. От ее уровня напрямую зависит доверие клиентов почтового оператора.

Почта России является участником глобального сотрудничества в области обеспечения почтовой безопасности в рамках Всемирного почтового союза (ВПС) - главной международной почтовой организации.

В настоящее время основная деятельность почты все больше ориентирована на расширение спектра финансовых услуг. В их числе: электронные денежные переводы (проект "КиберДеньги") по России, в странах ближнего и дальнего зарубежья, погашение кредитов, выплата пенсий и пособий. В этом же ряду – прием коммунальных платежей, платежей за услуги связи, Интернет и телевидение, прием платежей на терминалах самообслуживания, страховые услуги и финансовое посредничество, обслуживание банковских карт. Особое место в системе электронных денежных переводов занимают вопросы защиты информации.

Хищения и злоупотребления в органах связи были всегда. В тридцатые годы прошлого века они достигли таких размеров, что в целом ряде случаев приобрели значение политического бедствия. Количество потерянных, похищенных и неврученных посылок, в первом квартале 1933 г. достигло 6 млн руб., а в третьем квартале – 3,5 млн руб. Огромный удельный вес во всех злоупотреблениях занимают злоупотребления с денежными посылками [3].

Со стороны работников почты совершаются различные виды мошенничества. Мошенничество – это преступление, при котором преступник обманным путем или войдя в доверие потерпевшего завладевает его имуществом или денежными средствами (ст. 159 УК РФ) [1].

В ряде случаев, используя свое должностное положение, имея доступ к персональным данным клиентов, руководители отделений снимали денежные средства пенсионеров и использовали их в своих личных целях. При этом вносились заведомо ложные сведения в итоговый реестр якобы о получении ими денежных средств. В случае обращения граждан на почту о расхождении в счете, им выдавались недостающие деньги, а недостачу покрывалась путем снятия средств с другого счета.

Также имеют место быть хищения со стороны начальников почтовых отделений путем подделки подписи пенсионеров, получателей детских пособий и денежных переводов, с последующим их присвоением. Присваиваются не только деньги пенсионеров, но и средства, принятые от населения в счет оплаты коммунальных услуг, а также от реализации принадлежащих почтовому отделению товаров и периодических

изданий. Подделка подписей происходит и со стороны почтальона, что ведет к обсчету пенсионеров.

Не имея права осуществлять кассовые операции по приему денежных средств у населения, злоупотребляя доверием граждан, ряд начальников отделений почтовой связи похищали денежные средства клиентов, оплачивающих на почте коммунальные услуги, а также налоги и сборы (преступления, предусмотренные ч. 1 ст. 159 УК РФ, то есть хищения чужого имущества путем обмана) [1].

Одним из распространенных правонарушений на почте является хищение пенсий, работниками отделений путем снятия средств со счетов пенсионеров, и получения от их имени потребительских кредитов. Этому способствует, то, что операторы почты, являющейся агентом банка, имеют слишком широкий доступ к манипуляциям со счетами пенсионеров, при слабом за ними контроле.

Мошенничество присутствует и при присвоении денег, предназначенных для кредитования, путем осуществления подписи в ордерах о получении кредитов. Подделывая подписи клиентов, воспользовавшись их документами, оформлялся кредит, с последующим присвоением денежных средств.

Имеют место быть случаи похищения денежные средства с кредитной карты, присланной по почте жителям населенных пунктов. Позвонив в банк, почтальон, представившись владельцем кредитной карты, сообщив чужие паспортные данные, вводит в заблуждение работника кредитной организации. После активации кредитной карты происходило похищение находившиеся на ней денежных средств. В этих случаях действия почтальона органами следствия квалифицируются по ч. 1 ст. 159.3 УК РФ – мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием принадлежащей другому лицу кредитной карты путем обмана уполномоченного работника кредитной организации [1].

Факты хищений почтовых переводов вскрываются в ходе внутренней ревизии, проведенной ведомственной службой безопасности. Нередко, пользуясь своим служебным положением, начальники почтовых отделений осуществляли хищение почтовых переводов, посредством подделки отчетных документов, используя из архивных записей паспортное данные граждан, которым уже не первый раз приходили почтовые переводы. Подделывались подписи получателей, вносились заведомо ложные данные в отчеты, и в результате происходило похищение денежных средств. В большинстве своем это были алименты. Некоторые из получателей, так и не дождавшись своих денег, приходили на почту, чтобы разобраться в ситуации. Но их уверяли в том, что никаких переводов алиментов не было.

При оформлении выдачи почтовых отправлений с наложным платежом, начальники почтовых отделений получали деньги, которые должны быть направлены на адрес отправителя, но в кассу они не оформлялись, почтовый перевод не пересылался, а происходило присвоение средств. Для того, чтобы скрыть хищение денег, ими сообщалось в местный информационный пункт о том, что регистрируемые почтовые отправления возвращены, указывая вымышленный номер накладной или указывала номер несуществующего перевода.

Хищение денежных переводов осуществляется и операторами филиалов ФГУП «Почта России», которые также используя свое служебное положение, расписывались в бланках электронно-оплаченного перевода за граждан, на имя которых приходили

денежные переводы, связанные с выплатой алиментов, пенсий, иных перечислений. В последующем пришедшие на имя граждан денежные средства ими попросту похищались.

Нередко для сокрытия образовывающейся в результате хищения недостачи вызванной хищением денежных переводов, операторами почтовых отделений распечатывались бланки извещений на получение денежных переводов, собственноручно заполнялись ими от имени адресата, делалась ложная отметка о выдаче денег в базе данных. Из-за указанных действий выявление совершенного преступления путем сверки наличия денежных средств в кассе с документами финансового контроля и отчетности становилось невозможным.

В случае явки адресата для получения перевода, который уже был оформлен злоумышленниками как ложно выданный, ему выдавались денежные средства из кассы согласно ранее оформленному извещению на получение перевода. Недостача, образовавшаяся в результате реальной выдачи перевода, скрывалась путем оформления ложной выдачи денежного перевода на имя другого адресата с дальнейшим повторением описанных действий неопределенное количество.

Хищения происходят и при оформлении отправлений денежных переводов, которые предназначаются адресату, но при этом деньги клиентов в кассу не вносятся и почтовый перевод не отправляется.

В качестве похитителей денежных средств выступают и операторы главной распределительной кассы почтамта, присваивая из хранилища главной распределительной кассы деньги, предназначенные для перераспределения наличных сумм одного из почтамта между банковскими счетами и кассами отделений почтовой связи. Для скрытия следов преступления, ими вносились ложные сведения в документы о движении денежных средств.

Специалистами управления Федеральной почтовой связи (УФПС) имеющими доступ к электронным платежным поручениям, изготавливались подложные финансовые документы, что позволяло им направлять денежные средства УФПС на контролируемые ими счета.

Имеют место и использование своего служебного положения со стороны начальников отделений почтовой связи, мошеннические действия, связанные с безвозмездным изъятием из кассы вверенных им денежных средств, вырученных от реализации товаров народного потребления (без надлежащего оформления и соответствующих расходно-кассовых документов), периодических изданий, лотерейных билетов, государственных знаков почтовой оплаты и денег, предназначенных для выплаты пенсий, пособий, денежных переводов, а также совершение присвоения денежных средств, полагающихся в качестве заработной платы работникам вверенного им почтового отделения.

Присвоенными от этого денежными средствами они распоряжались по собственному усмотрению, что является преступлением, предусмотренным ч. 3 ст. 160 УК РФ (присвоение, то есть хищение чужого имущества, вверенного виновному, совершенное лицом с использованием своего служебного положения).

Являясь материально-ответственными и должностными лицами, обязанными осуществлять и выполнять административно-хозяйственные функции по руководству финансово-хозяйственной деятельностью отделения почтовой связи, начальники этих отделений присваивают вверенные им товарно-материальные ценности, а также

непосредственно сами товары, которые поступали в почтовое отделение для реализации, и в дальнейшем использовались в личных целях. При этом ими вносятся в ежемесячные отчеты ложные сведения, чтобы скрыть похищенные из отделений почтовой связи денежные средства и товары.

За последние годы во ФГУП «Почта России» реализуются мероприятия внутреннего контроля, направленные на снижение рисков хищений денежных средств, как следствие этого в 2013 – 2014 годах на предприятии проведено 68 комплексных внутренних проверок финансово-хозяйственной деятельности филиалов, 1037 почтамтов, 2989 отделений почтовой связи, размер недостач и хищений по вине работников в указанный период составил 0,001% (64 млн. руб.) от общего объема выплаченных песий и пособий [2].

В 2015 году службой безопасности ФГУП уже проведено более 60 тыс. внутренних проверок различного уровня, по итогам которых правоохранительными органами было возбуждено 463 уголовных дела, 118 пришлось на злоупотребления с почтовыми отправлениями, а 12 касались руководителей региональных филиалов Почты России, осуждены семь человек, более 50 почтовых работников уволены [2].

Основной массив составляют уголовные дела по признакам составов преступлений, предусмотренных ч. 3 ст. 159 и ч. 3 ст. 160 Уголовного кодекса РФ (мошенничество, а также присвоение и (или) растрата чужого имущества, вверенного виновному, совершенные с использованием служебного положения) [1].

Факты присвоения денежных средств работниками почтовых отделений связи выявляются в результате проводимых службой почтовой безопасности почтамта внутренних ревизий.

Обеспечение сохранности и защиты информации на предприятии зависит, прежде всего, от разработанных политик безопасности на предприятии. В информационной безопасности следует выделить административный уровень информационной безопасности предприятия, то есть меры, предпринимаемые руководством организации. В основе всех мероприятий административного уровня лежит документ, часто называемый политикой информационной безопасности предприятия, под которой следует понимать совокупность документированных управленческих решений и разработанных превентивных мер, направленных на защиту информационных ресурсов.

Одна из актуальнейших задач Почты – это улучшение качества обслуживания клиентов. Отделения связи должны быть максимально привлекательными для посетителей. Упрощение работы и повышение качества услуг требует внедрения современных информационных технологий.

Успехом обеспечения сохранности и защиты информации на предприятии зависит, прежде всего, от разработанных политик безопасности на предприятии.

Обеспечение почтовой безопасности - задача, требующая комплексного подхода и учета всех факторов. Основной целью мероприятий, проводимых подразделениями почтовой безопасности Почты России, является предотвращение совершения преступлений, как в отношении почтовой сети, так и с ее использованием.

На сегодняшний день Почтой России совместно с МВД разработан план комплексных мероприятий по предотвращению, пресечению и раскрытию преступлений, связанных с хищениями денежных средств. Усиление внутреннего контроля и взаимодействие с силовыми ведомствами должно быть направлено на снижение уровня

противоправных действий сотрудников, позволяющее оперативно выявлять, предотвращать пресекать преступления связанные с хищениями денежных средств.

Выявлению недобросовестных работников способствует внедрение трекеров ГЛОНАСС, кейсов для транспортировки и кратковременного хранения денежных средств с функцией защиты содержимого.

На минимизацию рисков потери доходов предприятия в результате противоправных действий ее собственных работников, в рамках работы по обеспечению финансовой безопасности направлена автоматизированная система защиты доходов предприятия, которая исключит возможность злоупотреблений при использовании франкировальных машин и пересылки не оплаченных в официальном порядке почтовых отправлений, так называемой серой почты.

Необходимо разграничение прав и уровня доступа к клиентской базе данных, к финансово-бухгалтерской информации и т.д.

Чтобы минимизировать и исключить случаи злоупотребления служебным положением, необходимо ужесточать систему отбора и контроля персонала.

Сотрудникам, которые работают с денежными средствами, следует уделять особое внимание, дополнительно изучать их профессиональные и деловые качества, в том числе и на этапе прохождения ими испытательного срока при приеме на работу в систему связи.

При приеме на работу должностных лиц, несущих материальную ответственность, совместно блоком безопасности и блоком по управлению персоналом, должна осуществляться проверка каждого кандидата путем тестирования, определения личностных характеристик и наклонностей, проверка предыдущих мест работы, а также проверка на наличие судимостей и административных правонарушений.

Необходимо предъявлять повышенный спрос к сотрудникам за нарушение финансово-хозяйственной дисциплины, усиливать административные меры взыскания для почтовых работников, недобросовестно выполняющих свои должностные обязанности.

Важной составляющей безопасности должна являться профилактическая работу с сотрудниками и клиентами предприятия.

Постоянный контроль за действиями персонала, применение различных средств мониторинга сетевого трафика, анализа сетевой активности, камеры видеонаблюдения и фиксация телефонных звонков могут оказать в плане обеспечения безопасности. Так как понимание персонала того, что любое их действие фиксируется, заставляет по-другому относиться не только к вопросам безопасности, но и к эффективности работы на протяжении всего рабочего дня.

Сокращение и предотвращение правонарушений в подразделениях почтового оператора будет способствовать росту уровня почтовой безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63–ФЗ (ред. от 30.12.2015) [Электронный ресурс]. – Режим доступа: http://www. consultant.ru /popular/ukrf/10_30.html.
2. Почта России увеличила количество выявленных нарушений [Электронный ресурс]. – Режим доступа: http://tass.ru/proisshestviya/2624480.

3. Ъ-Деньги – Дело о рекордном воровстве на почте [Электронный ресурс]. – Режим доступа: http://kommersant.ru›doc/2341435.

Е.А. Скоробогатова

ВЛИЯНИЕ ИНФОКОММУНИКАЦИОННЫХ УСЛУГ НА ЭФФЕКТИВНОСТЬ ДЕЯТЕЛЬНОСТИ СБЕРБАНКА

Уральский технический институт связи информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: инновации в сфере банковских услуг

В статье рассмотрено приоритетное развитие банковского сектора РФ.

E.A. Skorobogatova

INFOCOMMUNICATION SERVICES INFLUENCE FOR EFFICIENCY OF SBERBANK ACTIVITY

Ural Technical Institute of Communication and Computer Sciences (branch) “Siberian State University of Telecommunications and Informatics” in Ekaterinburg.

Key words: innovations in the sphere of bank services.

The foreground development of Russian Federation bank segment is discussed in the article.

Инфокоммуникации – конвергентный сектор экономической деятельности, основу которой составляют процессы информатизации, реализованные посредством использования информационно- коммуникационной инфраструктуры для удовлетворения информационных потребностей граждан, организаций и государства.

Инфокоммуникационная услуга – согласованный на договорной основе процесс взаимодействия субъектов информационных отношений, осуществляемый с применением инфокоммуникационных технологий, систем и сетей в соответствии с требованиями действующего законодательства и защиты прав интеллектуальной собственности, направленный на обеспечение гарантированного качества информационного обмена в электронном виде и получения положительных эффектов.

На сегодняшний день классификации инфокоммуникационных услуг уточняются и расширяются. Наиболее существенными являются следующие классификационные признаки:

– принадлежность к сложившимся индустриям: услуги связи, услуги на основе инфокумманиционных технологий;

- вид экономической деятельности: услуги издательской деятельности и в сфере аудио и видеозаписи, воспроизведения и вещания; услуги телекоммуникаций; услуги информационных технологий и информационного обслуживания;
- важность для потребителей: основные услуги, дополнительные услуги;
- категория доступа к информационным ресурсам: общедоступная услуга, услуга с ограниченным доступом;
- категория владельцев информационных ресурсов: государственные и негосударственные услуги;
- отношение к универсальной услуге (службе): услуги, входящие в состав универсальной услуги; услуги, не входящие в состав универсальной услуги;
- метод обслуживания потребителей: абонентские услуги, клиентские услуги;
- стоимостные характеристики: платные услуги, бесплатные услуги;
- субъекты, потребляющие инфокоммуникационные услуги: услуги для корпоративных клиентов, услуги для частных клиентов;
- способ (электронный канал) предоставления: телефонные услуги, компьютерные услуги, услуги интерактивного цифрового телевидения, терминальные услуги и др.;
- виды связи: услуги стационарной телефонной связи, услуги сотовой подвижной электросвязи, услуги почтовой связи, интернет-услуги и др.;
- степень временного взаимодействия: непрерывные услуги, сеансовые услуги, транзакционные услуги, комбинированные услуги;
- степень участия потребителя в производстве и реализации инфокоммуникационной услуги: распределительные услуги, диалоговые услуги, интерактивные услуги, комбинированные услуги;
- количество потребителей: индивидуальные услуги, коллективные услуги, услуги массового обслуживания;
- прикладная область применения: электронное правительство, электронная коммерция, электронное образование, электронная медицина, электронная таможня и др.;
- вид передаваемых сообщений: мономедийные услуги, мультимедийные услуги;
- количество одновременно предоставляемых услуг: базовые услуги, мультисервисные услуги;

К специфическим услугам банков оказываемых с применением телекоммуникационной среды относятся типичные для них формы работы:

- осуществление денежных переводов по средствам международных систем денежных переводов;
- безналичные расчеты с использованием пластиковых карт осуществляемые посредством банкоматов и оборудования эквайринга;
- удаленное банковское обслуживание клиентов с использованием сети Интернет и мобильного телефона (интернет-банкинг, мобильный-банкинг);
- оказание дополнительных услуг по применению того или иного банковского продукта[2].

Для достижения целей, которые стоят перед банком, нужны преобразования, которые предполагают значимые изменения во всех областях его деятельности

Принципиально важным направлением развития банка станут максимальная ориентация на клиента и в этом смысле превращение Сбербанка в «сервисную»

компанию. Это значит, что банк будет стремиться удовлетворить максимальный объем потребностей в финансовых услугах каждого своего клиента и тем самым максимизировать свои доходы от каждого набора клиентских отношений. Это означает, что качество и глубина взаимоотношений с клиентом, а также навыки и возможности банка в области продаж и обслуживания, которые обеспечат поддержание и развитие этих отношений, станут важной основой конкурентного преимущества банка. С практической точки зрения, для того чтобы ориентация на клиента не осталась лозунгом, банк существенным образом изменит очень многие элементы своей работы, начиная от логики продуктового предложения и создания внутри банка выделенной вертикали продаж и обслуживания в рознице и заканчивая новой моделью клиентской работы в корпоративном блоке и изменением процессов и процедур в бэк- и мидл-офисе.

Реализация выбранного сценария «модернизации» предполагает комплексную перестройку процессов и систем и их перевод на новую «промышленную» основу. Подобная «индустриализация» систем и процессов в Банке повысит уровень управляемости и масштабируемости, снизит затраты, улучшит качество обслуживания клиентов и позволит банку более эффективно управлять кредитными и другими видами рисков. Построение промышленных систем и процессов во многих случаях подразумевает консолидацию или централизацию функций как инструмента повышения управляемости и снижения затрат, а также пересмотр многих основных процессов, большую формализацию методик работы (например, оценку рисков) и построение современных систем электронного документооборота, способных работать в масштабах всего банка. Это также потребует существенного развития информационных систем.

В результате используемые системы не только смогут «справляться» с масштабом операций банка, но и позволят банку сделать масштаб своих операций важнейшим источником формирования конкурентных преимуществ. Наиболее очевидные проявления этих изменений связаны с планами консолидации, а также с построением новых систем управления кредитными рисками. Однако эти изменения также весьма значимо затронут и бизнес - подразделения банка, в частности в контексте построения систем управления взаимоотношениями с клиентами и поддержки клиентской работы в корпоративном и розничном бизнесе.

«Индустриализация» позволит повысить эффективность, управляемость и качество, принципиально и «разово» меняя логику работы систем и процессов «сверху вниз». Руководство банка глубоко убеждено, что этого недостаточно для выполнения стратегических целей и миссии банка.

Осознавая важность и приоритет российского рынка банковских услуг для развития бизнеса, банк ставит перед собой задачу стать значимым участником мировой финансовой системы, поэтому выделяет развитие операций на международных рынках как одно из приоритетных направлений. При этом банк понимает, что развитие его международного присутствия и повышение его значимости (не только с точки зрения размера, но и степени участия в мировом финансовом секторе) будет достаточно медленным и постепенным процессом. Это еще больше подчеркивает необходимость того, чтобы первые шаги на пути превращения Сбербанка из крупного национального в международный банк делались уже сейчас.

В последнее время наблюдается тенденция роста числа электронных банковских продуктов, предлагаемых на рынке. Высокая конкуренция среди коммерческих банков,

стремление занять новые ниши, борьба за клиента способствуют созданию новейших банковских продуктов.

Наибольшее распространение в сфере банковского обслуживания получило дистанционное банковское обслуживание, в особенности, интернет-банкинг и sms-банкинг. Электронный банкинг позволяет клиенту реагировать на изменения финансового рынка, пользоваться услугами 24 часа в сутки вне зависимости от местонахождения при условии свободного доступа к Интернету.

В развитии электронного банкинга заинтересованы и сами банки, т.к. электронные платежи существенно сокращают операционные расходы, а затраты на разработку и введение новых технологий быстро окупаются за счет абонентской платы. Однако наравне с явными преимуществами введение электронного банкинга создает предпосылки к появлению дополнительных рисков[3].

По мнению специалистов, в России существует немало вариантов дистанционного обслуживания клиентов банка, однако их популярность в настоящее время не превышает 10% всех пользователей банковских услуг, что связано, во-первых, с низким уровнем материального благополучия, а во-вторых, с непониманием достоинств электронного банкинга и недоверием к работе в сети Интернет.

Инновации в сфере банковских услуг не создают абсолютно новых видов рисков для банков, они усиливают уже имеющиеся риски, поэтому для предотвращения проблем, связанных с использованием новых банковских продуктов, необходимо создание эффективной системы управления рисками.

С развитием электронного банкинга появляются новые компоненты уже имеющихся рисков, которые способствуют появлению таких рисков, как отрицания транзакций, деловой, хищений идентификационных данных, безопасности, отмывания денег, мошеннических действий со счетами, обезличивания индивидуальности. Предоставляя дистанционные банковские услуги, кредитная организация не всегда может быть полностью уверена, что из виртуального пространства поступают ордера, формируемые официальным клиентом. Со стороны кредитной организации возможно совершение мошеннических действий, к которым она отношения не имеет, но банковские технологии которой этому способствует. Кроме того, клиенты тоже не всегда могут быть уверены в том, что взаимодействуют со «своей» кредитной организацией.

Одним из наиболее известных способов мошенничества в Интернете является «фишинг» – мошенничество, при котором злоумышленник рассылает сообщения по электронной почте для получения личной и финансовой информации о потенциальных жертвах (для дальнейшего доступа к их банковским счетам и другим важным ресурсам). В случае с электронным банкингом, как правило, такое письмо содержит информацию о внезапно возникших технических проблемах на сервере банка, в связи с чем возникла необходимость проверки учетных записей и регистрационных данных пользователей. Далее жертве предлагается открыть «регистрационную форму» и ввести интересующие мошенника данные. Получив эти данные, мошенник распоряжается банковским счетом жертвы и кредитной картой по своему усмотрению.

Распространены традиционные способы кражи данных при считывании идентификаторов и паролей программами перехвата клавиатурного ввода, сетевого прослушивания в результате хакерских атак и так далее, интернет и банкоматных мошенничеств с банковскими картами и других вариантов противоправной деятельности.

В последнее время достаточно серьезные угрозы исходят от троянских программ. Троянские программы могут находиться долгое время в системе, выполняя задачу по похищению данных[1].

Очевидно, что в будущем угрозы станут более опасными. Уже сегодня многие атаки – это комбинации различных методов. Кредитные организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие продолжают выдумывать и создавать новые техники атак. Целесообразно помнить о том, что любые претензии к кредитной организации со стороны клиентов могут оказаться для нее источниками репутационного, правового, стратегического рисков в том случае, если она не предупреждала пользователей о возможных источниках рисков, связанных с использованием дистанционного банковского обслуживания.

Несмотря на неоспоримые преимущества электронного банкинга, любые технологические нововведения повышают и усложняют банковские риски, а, следовательно, снижают надежность и устойчивость коммерческих банков. Необходимо предъявлять серьезные требования к проверке новых технологий для обеспечения гарантий соблюдения правил выполнения банковских операций, бухгалтерского учета, сохранения банковской тайны и активов клиентов, а также высокого качества работы.

СПИСОК ЛИТЕРАТУРЫ:

1. Банковское дело: учебник для вузов/ Г.Н. Белоглазова [и др.]; под ред. Г.Н. Белоглазовой, Л.П. Кровелицкой. - 5-е изд., перераб. И дополн. - М.: Финансы и статистика, 2009 г.
2. Банковское дело [Текст]: учебник для студентов вузов, обучающихся по экономическим специальностям и специальности 060400 «Финансы и кредит»/ Под ред. Е.Ф. Жукова, Н.Д. Эриашвили. - М.: ЮНИТИ - ДАНА: Единство, 2008. - 575 с.
3. Глушкова Н.Б. Банковское дело: учебное пособие для вузов/ Н.Б. Глушкова. - М.: Акад. Проект: Альма Матер, 2007 г.

И.А. Степская, С.А. Уколова, А.И. Момот

ОЦЕНКА КОНКУРЕНТОСПОСОБНОСТИ УСЛУГИ ПО ПРИЕМУ КОММУНАЛЬНЫХ ПЛАТЕЖЕЙ УФПС РОСТОВСКОЙ ОБЛАСТИ – ФИЛИАЛА ФГУП «ПОЧТА РОССИИ»

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: финансовые услуги, почтовая связь, Почта России, коммунальные платежи

Рассмотрены вопросы обновления процессов предоставления услуги по приему коммунальных платежей населению Ростовской области. Сделан анализ необходимости в разработке ряда мероприятий, направленных на развитие услуги.

I.A. Stepskaya, S.A. Ukolova, A.I. Момот

EVALUATION OF THE COMPETITIVENESS OF SERVICES FOR THE RECEIPT OF UTILITY BILLS IN THE ORGANIZATION «POST OF RUSSIA»

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

Keywords: financial services, postal service, Russian Post, utility payments

The issues of updating the processes of providing services for receiving communal payments to the population of the Rostov region are considered. An analysis was made of the need to develop a number of measures aimed at developing the service.

Актуальность данной темы обусловлена тем, что населению, проживающему в отдаленных и труднодоступных районах, получение финансовых услуг, таких как отправка и вручение переводов денежных средств, оплата коммунальных платежей или налогов и других платежей, оформление страховых полисов недоступно по месту жительства.

Одним из крупнейших операторов, предоставляющих почтовые, финансовые услуги, прием и выдачу посылок на всей территории нашей страны, включая отдаленные и труднодоступные районы, является ФГУП «Почта России» - одновременно коммерческое и социально направленное предприятие.

Развитие всех видов услуг, которые осуществляет Почта России и особенно сегмента финансовых услуг, не ограничивается реализацией проекта по созданию почтового банка – санация продуктового портфеля и новая политика по работе с партнерами приносят первые, ощутимые результаты. Обновление процессов оказания всех видов услуг, и особенно финансовых услуг таким бенефитам как, государство, население и бизнес, необходимость разработки ряда мероприятий, направленных на развитие финансовых услуг, рассмотренная на примере УФПС Ростовской области – филиала ФГУП «Почта России» является целью, поставленной в данной работе.

С целью оценки позиции УФПС Ростовской области – филиала ФГУП «Почта России» на рынке финансовых услуг в данной статье определены основные игроки рынка Ростовской области по оказанию услуги приема коммунальных и прочих платежей:

- ПАО «Сбербанк»;
- ПАО КБ Центр – Инвест;
- Ростовский филиал Россельхозбанка;
- ПАО «Донкомбанк»:

По результатам произведенного подсчета количества принятых коммунальных платежей в 2016 году на территории Ростовской области двумя наиболее значимыми игроками финансового рынка - УФПС Ростовской области – филиал ФГУП «Почта России» и ПАО «Сбербанк» доля присутствия УФПС Ростовской области составила 48%.

При проведении анализа доли рынка в разрезе территорий Ростовской области, были выявлены районы (в основном сельская местность), где количество принятых Почтой России переводов достигло до 89%, от принятых остальными альтернативными структурами платежей. В районных городах Ростовской области средний процент приема почтой коммунальных платежей составил – 55%, и в г. Ростове-на-Дону – 6%.

Из вышеизложенного, можно сделать вывод о том, что услуга приема коммунальных платежей УФПС Ростовской области от населения, проживающего в сельской местности и небольших районных городах достаточно востребована и конкурентоспособна. Однако, развитие и совершенствование услуги приема коммунальных платежей в отделениях почтовой связи города Ростова-на-Дону, в котором проживает одна четвертая часть всего населения Ростовской области и дислоцируется широкая сеть филиалов ПАО «Сбербанк», требует дополнительного внимания и осуществления ряда мероприятий, позволяющих увеличить долю присутствия УФПС Ростовской области на рынке приема коммунальных платежей.

В 2016 году, среди городского сегмента – физических лиц, проведено анкетирование, на основании которого, были выявлены три основных критерия выбора клиентом поставщика рассматриваемой в статье услуги и определен удельный вес каждого критерия.

- Доступность услуги – 40%,
- Стоимость услуги – 45%,
- Качество услуги – 15%.

По критерию доступности услуги:

УФПС Ростовской области и ПАО «Сбербанк» имеют приоритетные позиции 100 балов из 100 возможных. ПАО КБ Центр – Инвест 90 балов, Ростовский филиал Россельхозбанка 50 балов и ПАО «Донкомбанк» всего 10 балов из 100 возможных.

По критерию стоимости услуги:

Наиболее высокий тарифный сбор за оказание услуги приема коммунальных платежей от населения осуществляет ПАО «Сбербанк» - 2,4% от суммы коммунального платежа, тарифный сбор Почты Россия составляет – 2.1%. Тарифный сбор ПАО КБ Центр – Инвест и ПАО «Донкомбанк» - 1,5%, и Ростовскоий филиал Россельхозбанк взымает самый низкий тариф с суммы коммунального платежа – 0,5%. Информация, собрана и актуальна по состоянию на 28.10.2016 г. При проведении анализа для сравнения использовались средние значения внешних комиссий по приему платежей в процентном выражении. На их основании рассчитан среднерыночный тариф, выведены отклонения.

Таблица 1 - Сравнительный анализ тарифов на оказание услуги приема коммунальных и прочих видов платежей.

Игроки рынка	**Тариф услуги по приему платежей ЖКХ**
Почта России	2,1%
ПАО «Сбербанк»	2,4%
ПАО КБ Центр - Инвест	1,5%
Ростовский филиал Россельхозбанк	0,5%
ПАО «Донкомбанк»	1,5%
Среднерыночный тариф	1,4%
Процент отклонения тарифа Почты России от среднерыночного, на территории Ростовской области	0,7%

По критерию качества осуществления услуги:

ПАО «Сбербанк», ПАО КБ Центр – Инвест, ПАО «Донкомбанк» и Ростовский филиал Россельхозбанка имеют приоритетные позиции – 100 балов из 100, УФПС Ростовской области – 90 балов их 100 возможных.

Несмотря на то, что критерий качества услуги определен при анкетировании клиентов с самым низким процентом значимости, и по качеству осуществления услуги УФПС Ростовской области абсолютно незначительно уступает альтернативным структурам, почте, с целью увеличения своей доли на рынке приема денежных переводов в столице Ростовской области, необходимо довести данный критерий до полного удовлетворения потребности клиентов.

На наш взгляд, повышение качества предоставления услуг возможно путем дополнительного обучения персонала:

- обучение вновь принятого персонала в Ростовском учебном центре;
- введение системы наставничества;
- дистанционное обучение персонала при внедрении новых, или изменении технологии оказания существующих услуг;
- на постоянной основе ответственными работниками аппарата управления УФПС Ростовской области – филиалом ФГУП «Почта России» организация проведения аудио, видео - конференций с целью обучения менеджеров почтамтов.

Повышение качества оказания услуги и клиенто-ориентированности персонала, возможно путем создания отделений почтовой связи нового формата обслуживания - это:

- улучшение клиентского обслуживания;
- внедрение лучших мировых практик;
- внедрение новых технологий;
- наличие простой и четкой навигации в отделении почтовой связи;
- интуитивно понятный процесс обслуживания;
- сокращение времени ожидания в очередях;
- клиенто - ориентированность сотрудников;

- комфортная среда для клиентов;
- внедрение новой ИТ – платформы «ЕАС ОПС» (единая автоматизированная система отделения почтовой связи).

Проект создания и внедрения новой, уникальной на настоящий момент услуги – прием коммунальных платежей от физических лиц на дому:

По итогам 2016 года, каждый второй почтальон УФПС Ростовской области оснащен мобильным почтово-кассовым терминалом (МПКТ) – устройством, с помощью которого, почтальон может осуществить прием коммунального платежа на дому, по желанию клиента, с обязательной выдачей кассового чека, при доставке почтовой корреспонденции в пределах почтового маршрута.

Данная услуга, на территории Ростовской области предоставляется только Почтой России, и по результатам подсчета количества принятых в 2016 году коммунальных платежей на дому, демонстрирует свою востребованность. Тарифный сбор, за ее осуществление не отличается от тарифного сбора при приеме коммунального перевода в кассе отделения почтовой связи. Основной сегмент потребителей данной услуги – население пожилого возраста, домохозяйки.

Еще одно из преимуществ приема коммунальных платежей через мобильные почтово-кассовые терминалы – это возможность прихода почтальона с МПКТ на предприятие или в организацию в определенную по договоренности с руководством предприятий и организаций дату.

Оплата коммунального платежа на рабочем месте очень удобна населению Ростовской области, а УФПС Ростовской области, позволяет увеличить объем принятых платежей и доходы от предоставления населению услуг по приему коммунальных платежей, так как клиенты выбирают поставщика услуги по критерию доступности - почтальон пришел к клиенту на рабочее место. Осуществление данного мероприятия в прогнозе на 2017 год, обещает получение экономического эффекта именно в г. Ростове-на-Дону и других крупных городах Ростовской области, по месту дислокации предприятий крупного и среднего бизнеса. И как следствие, мероприятие позволяет увеличить объем принятых платежей путем перевода клиентов из банковского сектора на обслуживание в УФПС Ростовской области – филиала ФГУП «Почта России», особенно в г. Ростове–на–Дону и прочих крупных областных городах.

СПИСОК ЛИТЕРАТУРЫ

1. *Страшнов Д.* Почта без границ//Почта России, 2015 - №3, 56с.
2. http://www.pochta.ru
3. http://www.sberbank.ru
4. http//www.donland.ru/economy/Svyaz/?pageid=75904
5. https://www.centrinvest.ru/
6. http://www.rshb.ru/branches/rostov/

В.Н. Трофименко, А.В. Павлова, К.В. Пащенко

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ КОНТУРА УГЛОВОЙ СТАБИЛИЗАЦИИ САМОЛЕТА

Донской государственный технический университет (ДГТУ), Ростов-на-Дону, Россия
trofimvn@mail.ru

Ключевые слова: информационные технологии, образовательный процесс, самолет, имитационное моделирование, угловая стабилизация.

В статье рассмотрены вопросы использования инфокоммуникационных технологий в учебном процессе, представлена имитационная модель продольной угловой стабилизации самолета, которую можно использовать при проведении учебных занятий при подготовке специалистов инженерных направлений, представлены результаты моделирования.

V.N. Trofimenko, A.V. Pavlova, K.V. Pashchenko

OF THE PLANE IMITATING MODELLING OF THE CONTOUR OF ANGULAR STABILIZATION

Don state technical university (DSTU), Rostov-on-Don, Russia
trofimvn@mail.ru

Keywords: information technologies, educational process, imitating modeling, plane, angular stabilization.

In article questions of use of infocommunication technologies in educational process are considered, the imitating model of longitudinal angular stabilization of the plane which can be used when carrying out studies at training of specialists of the engineering directions is presented, results of modeling are presented.

Применение современных инфокоммуникационных технологий в обучении является неотъемлемой составляющей образовательного процесса в ВУЗе. Их применение позволяет повышать эффективность обучения за счет обеспечения обратной связи в учебном процессе с обучаемыми; обеспечения индивидуализации учебного процесса; повышения наглядности учебного процесса; организации коллективной и групповой работы [1].

Одним из направлений применения инфокоммуникационных технологий является создание и использование библиотек автоматизированных лабораторных практикумов [2], которые могут быть использованы в том числе и для дистанционного обучения. Лабораторные занятия является одним из базовых видов учебных занятий при подготовке специалистов инженерных специальностей. Так изучение и исследование на лабораторных занятиях систем автоматического управления полетом студентами

авиационных специальностей невозможно без применения вычислительной техники и математического моделирования. В [3, с. 3] для исследований автопилотов предлагается программа, позволяющая получить серию графиков переходных процессов для заданных законов управления. Однако программа включает математические модели, закрытые для обучаемых. В данной работе представлена программа математического моделирования стабилизации угла тангажа, позволяющая не только получать графики соответствующих переходных процессов, но и исследовать математическую модель.

Рассмотрим автопилот стабилизации угла тангажа, с пропорционально-дифференциально-интегральным законом управления [3, с. 9-10]

$$\frac{T_И p}{T_И p+1}\delta_B = k_\vartheta(\vartheta-\vartheta_З)+k_{\omega_Z}\omega_Z. \qquad (12)$$

Система дифференциальных уравнений в операторной форме имеет вид:

$$\begin{aligned}&(p^2+a_{m_Z}^{\omega_Z}p)\vartheta+(a_{m_Z}^{\dot\alpha}p+a_{m_Z}^{\alpha})\alpha+a_{m_Z}^{\delta_B}\delta_B = a_{m_Z}^{M_Z}M_Z+a_{m_Z}^{\dot\alpha}p\alpha_B\\ &-p\vartheta+(p+a_y^{\alpha})\alpha = p\alpha_B,\\ &\frac{T_И p}{T_И p+1}\delta_B = k_\vartheta(\vartheta-\vartheta_З)+k_{\omega_Z}\omega_Z.\end{aligned} \qquad (13)$$

В выражениях (12), (13) α - приращение угла атаки - град; ϑ - приращение угла тангажа, град; δ_B - приращение угла отклонения руля высоты, град; α_B - приращение угла между вектором воздушной скорости и вектором путевой скорости, обусловленное действием вертикальной составляющей ветра, град; M_Z - приращение возмущающих моментов соответственно относительно оси OZ связанной системы координат, кГ м; $a_{m_Z}^{\omega_Z}=0.8,\ a_{m_Z}^{\dot\alpha}=0.18,\ a_{m_Z}^{\alpha}=3.4,\ a_{m_Z}^{\delta_B}=1.9,\ a_{m_Z}^{M_Z}=9.5\cdot10^{-7},\ a_{m_Z}^{\dot\alpha}=0.8,\ a_y^{\alpha}=0.9$ - линеаризованные коэффициенты модели определяются выражениями, представленными в [4]; $k_\vartheta=0.04,\ k_{\omega_Z}=1.888$ - коэффициенты передачи автопилота по углу тангажа и по угловой скорости по оси *Z*, соответственно.

Запишем систему уравнений (13) в дифференциальной форме при заданном значении программного угла тангажа и без учета вертикальной составляющей скорости ветра:

$$\begin{aligned}&\frac{d^2\vartheta}{dt^2}+a_{m_Z}^{\omega_Z}\frac{d\vartheta}{dt}+a_{m_Z}^{\dot\alpha}\frac{d\alpha}{dt}+a_{m_Z}^{\alpha}\alpha+a_{m_Z}^{\delta_B}\delta_B = a_{m_Z}^{M_Z}M_Z,\\ &-\frac{d\vartheta}{dt}+\frac{d\alpha}{dt}+a_y^{\alpha}\alpha=0,\\ &\frac{d\delta_B}{dt}=\frac{k_\vartheta}{T_И}(\vartheta-\vartheta_З)+(k_\vartheta+\frac{k_{\omega_Z}}{T_И})\frac{d\vartheta}{dt}+k_{\omega_Z}\frac{d^2\vartheta}{dt^2}.\end{aligned} \qquad (14)$$

Представим систему уравнений (14) в форме Коши, обозначив переменные состояния через компоненты вектора *x*:

$$
\begin{aligned}
&\frac{dx_1}{dt} + a_{m_z}^{\omega_z} x_1 + a_{m_z}^{\dot{\alpha}} \left(-a_y^{\alpha} x_3 + x_1\right) + a_{m_z}^{\alpha} x_3 + a_{m_z}^{\delta_B} x_4 = a_{m_z}^{M_Z} M_Z,\\
&\frac{dx_2}{dt} = x_1,\\
&\frac{dx_3}{dt} = -a_y^{\alpha} x_3 + x_1,\\
&\frac{dx_4}{dt} = k_{\vartheta} T_{\vartheta} x_1 + k_{\omega_z} \left(-a_{m_z}^{\omega_z} x_1 - a_{m_z}^{\dot{\alpha}} \left(-a_y^{\alpha} x_3 + x_1\right) - a_{m_z}^{\alpha} x_3 - a_{m_z}^{\delta_B} x_4 + a_{m_z}^{M_Z} M_Z\right),
\end{aligned}
\qquad (15)
$$

где компоненты вектора $x - \; x_1 = \frac{d\vartheta}{dt} = \omega_Z,\; x_2 = \vartheta,\; x_3 = \alpha,\; x_4 = \delta_B.$

Для составления имитационной модели стабилизации продольного углового движения, позволяющего исследовать работу автопилота, был использован пакет математического моделирования Mathcad [5]. Решение системы дифференциальных уравнений выполним методом Рунге-Кутта с постоянным шагом при помощи функции *rkfixed()*. На рис. 1 представлена векторная функция правых частей системы дифференциальных уравнений (15) в рабочем листе Mathcad.

На рис. 2 и рис. 3 представлены результаты моделирования изменения угла тангажа на 5 град, время моделирования – 180 сек.

D1(t ,x) :=

$$
\begin{bmatrix}
-a_{mz\omega z} \cdot x_0 - a_{mz\dot{\alpha}} \cdot \left(-a_{y\alpha} \cdot x_2 + x_0\right) - a_{mz\alpha} \cdot x_2 - a_{mz\delta\hat{a}} \cdot (x_3) + a_{mzMz} Mz \\
x_0 \\
-a_{y\alpha} \cdot x_2 + x_0 \\
\frac{k_\vartheta}{T_\vartheta}\left(x_1 - \vartheta_0\right) + \left(k_\vartheta + \frac{-k_{\omega z2}(1)}{T_\vartheta}\right) \cdot x_0 + -k_{\omega z2}(1) \cdot \left[-a_{mz\omega z} \cdot x_0 - a_{mz\dot{\alpha}} \cdot \left(-a_{y\alpha} \cdot x_2 + x_0\right) - a_{mz\alpha} \cdot x_2 - a_{mz\delta\hat{a}} \cdot x_3 + a_{mzMz} Mz\right]
\end{bmatrix}
$$

Рис. 1 – Векторная функция правых частей системы дифференциальных уравнений (15)

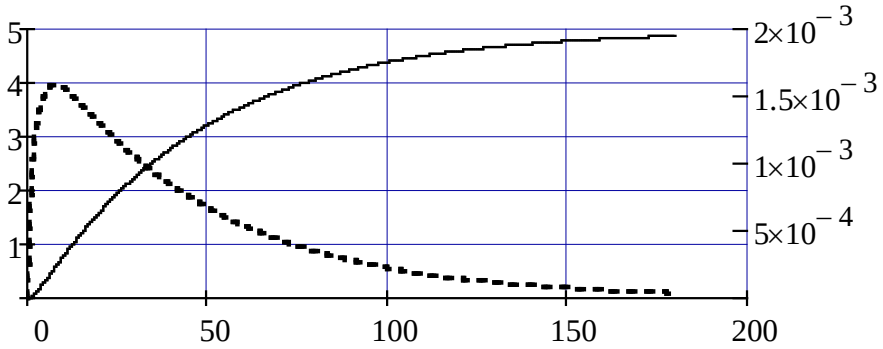


Рис. 2 – Динамика угла тангажа ϑ (___), град, лев. шкала и угловой скорости ω_Z (**…..**), рад/сек, прав. шкала

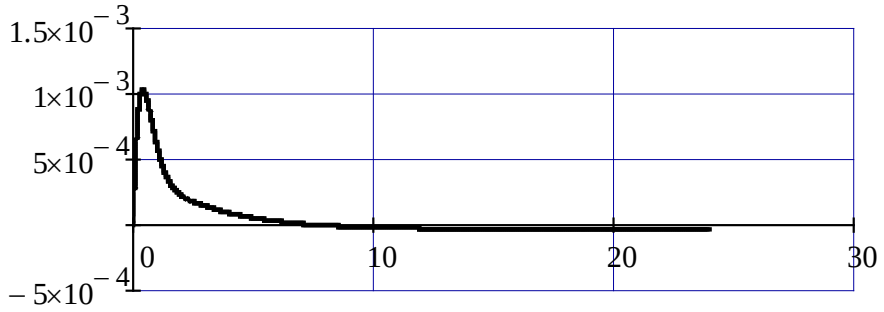


Рис. 3 – Динамика углового ускорения $\dot{\omega}_Z$, рад/сек^2 (интервал – 0-25 сек)

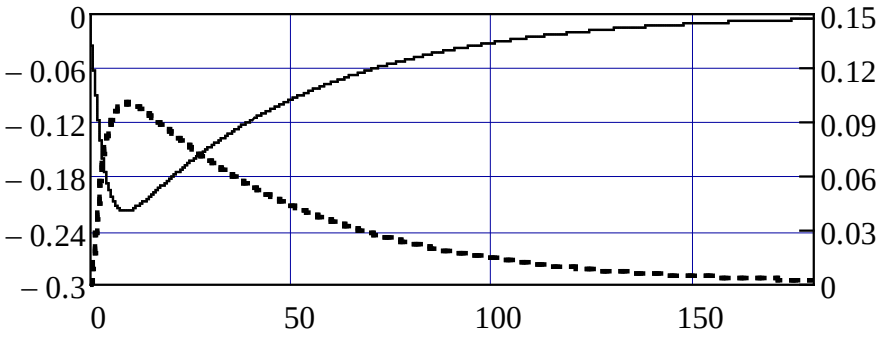


Рис. 4 – Динамика угла отклонения руля высоты δ_B (___), град, лев. шкала и угла атаки α (**.....**), град, правая шкала

Полученные при моделировании графики соответствуют переходным процессам, представленным в [5]. Это подтверждает корректность представленной программы имитационного моделирования.

Таким образом, представленная имитационная модель позволяет проводить лабораторные исследования и практические занятия как по дисциплинам, направленным на изучение систем автоматического управления полетом, так и по дисциплинам математического моделирования.

Представленная имитационная модель может быть использована в качестве элемента библиотеки автоматизированных лабораторных практикумов, в том числе и для дистанционного обучения студентов.

СПИСОК ЛИТЕРАТУРЫ

1. *Беленький П. П., Манин А.А.* Unify Communications: будущее в настоящем. // Аккредитация в образовании. 2015, № 3 (79), с. 34.
2. *Братченко Н. Ю., Михайличенко Т.А.* Инфокоммуникационные технологии как инновационная образовательная среда в техническом вузе. // Инженерное образование. – 2012, №11, с. 131.

3. *Гусев А. А.* Системы автоматического управления полетом: Пособие по выполнению лабораторной работы «Изучение и исследование контуров угловой стабилизации самолета» для студентов IV и V курсов специальности 160903. – М.: МГТУ ГА, 2009, с. 3-17.
4. *Кузнецов С. В., Гусев А. А.* Методические указания по изучению дисциплины “Системы автоматического управления полетом” и контрольное задание для студентов V курса специальности 131000 заочного обучения. – М.: МГТУ ГА, 2004, с. 3-7.
5. MATCHCAD 6.0 PLUS. Финансовые, инженерные и научные расчеты в среде Windows 95. – М.: Информационно-издательский дом "Филинъ", 1997, с. 362-369/
6. *Воробьев В. Г., Кузнецов С. В.* Автоматическое управление полетом самолетов: Учеб. для вузов.-М.: Транспорт. 1995, с. 272-274.

Д.Л. Устименко, Е.А. Гатилова

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КОМПЬЮТЕРНОГО ДИЗАЙНА В СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: интерфейс, инфокоммуникационная система, HMI, информация, дизайн, сайты, приложения.

В статье рассмотрены проблемы и актуальные тенденции развития компьютерного дизайна в сфере инфокоммуникационных технологий.

D.L. Ustimenko, E.A. Gatilova

ACTUAL PROBLEMS OF COMPUTER DESIGN IN THE MODERN INFORMATION AND COMMUNICATION TECHNOLOGIES

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

Keywords: interface, information and communication system, HMI, information, design, websites, applications.

The article considers problems and trends of development of computer design in the field of information and communication technologies.

Компьютерные технологии всё глубже проникают во все сферы человеческой деятельности. Общество, безусловно, волнует не только технические характеристики, но и зрительная составляющая. Благодаря развитию инфокоммуникационных систем на данный момент есть все необходимые программные продукты для создания дизайна сайтов и компьютерных приложений, и теперь перед разработчиками стоит задача продвижения своего продукта.(1) В этом им помогает развитие компьютерного дизайна и маркетинг в целом. Компьютерная графика – это та дисциплина, которую можно применять в любой современной области деятельности человека, прежде всего, как инструмент наглядной демонстрации различных понятий и привлечения клиентов к какому-либо товару с помощью графических изображений. Современное программное обеспечение позволяет автоматизировать и визуализировать сложные графические построения, что многократно сокращает время работы над проектом.

Создатели интерфейсов – это в большинстве своем люди с высокими аналитическими способностями. Они владеют развитой логикой, безошибочно просчитывают действия других людей. С увеличением возможностей компьютера, аппаратного и программного обеспечения, дизайнеры интерфейсов начали обращать внимание на то, как люди взаимодействуют с компьютерами и как должны быть разработаны интерфейсы для облегчения этого взаимодействия. Годы исследований человеческих факторов и эргономики привели к тому, что уже появился большой объем информации о том, как проектировать продукты, так что все, что человек хочет или должен делать с ними, было бы легко сделать.(3) Тем самым главной целью разработчиков являлось создание понятого, удобного и практического продукта. С результатами исследований человеческого фактора и вызванного им дорогостоящих промышленных аварий, люди в этой отрасли все чаще обращают внимание на качество HMI, и начинает иметь значение действительно полезный операторский интерфейс. Исследовательский центр NASA «Ames» поддерживает исследования по науке цвета и его использованию в сложных информационных дисплеях. Центр по производительности операторов (Center for Operator Performance) публикует исследования о квалификации, обучении и условиях работы операторов, а также о системах автоматизации и сигнализации. При международной ассоциации стандартов (ISA) был создан комитет по стандартам человеко-машинных интерфейсов в обрабатывающей промышленности.(2)

Сегодня композиционные особенности дизайн-продуктов складываются в русле трех направлений:

1. Плоскостная композиция изобразительных пространственных искусств и, соответственно, организация статичной формы продукта дизайна (графический дизайн, иллюстрация).
2. Композиция изобразительных пространственно-временных искусств с ее динамичной формой организации произведения во времени (дизайн, кинематограф, анимация, мультипликация).
3. Организация пользовательского интерфейса — эргономичного механизма взаимодействия между человеком и цифровым устройством для манипулирования статичными и динамичными объектами Новых медиа (дизайн пользовательских интерфейсов, программирование).

Каждое из приведенных направлений является самостоятельной областью деятельности. Изучив подробно роль каждого можно сделать вывод, что они несомненно

дополняют друг друга. В течение ближайших десятилетий подобные изменения будут продолжаться естественным путем – под давлением рынка в сочетании с дальнейшим технологическим прогрессом.

В настоящее время одной из главных задач компьютерного дизайна можно назвать максимальное упрощение приложений, информацию делают более доступной, поверхностной. Также дизайнерам необходимо бороться с повторяющимся контентом. Сейчас мы сталкиваемся с тем, что для большинства людей, работающих в интернете, все сайты выглядят одинаково. Заголовки выглядят очень похоже, что является не интересным для пользователя. Пользователи отдают предпочтение структурам, позволяющим получить быстрый, качественный и результат. Им просто нужно отыскать интересующую вещь. Они не хотят разбираться в нечитаемых шрифтах или хитросплетениях функций. По большому счёту всех больше интересует результат, притом полученный быстрым, и не навязчивым путём. Это две фундаментально разных концепции – удобство использования, и результативность.(4)

В заключение хотелось бы сказать, что, самой главной и основной задачей компьютерного дизайна на данный момент является создание более простого, понятного и удобного интерфейса. В наше время людей сложно удивить спецэффектами и превосходной графикой, а удобство и простота в использовании, безусловно, актуальна.

СПИСОК ЛИТЕРАТУРЫ

1. *Гофман А.Б.* Мода и люди. Новая теория моды и модного поведения. М., 2010.
2. *Давыдова Т.Ю., Шелобаев С.И., Арсеньев Ю.Н.* Информационные системы и технологии. Экономика. Управление. Бизнес: Учебное пособие. – Юнити-Дана, 2012
3. *Новикова Я.Н.* Пропедевтический подход к многоуровневой подготовке дизайнеров // Вестник Новгородского государственного университета. 2008.
4. *Храмкова Е.Л.* Промышленный дизайн как стратегический инструмент бизнеса // Стратегический менеджмент. 2008. .

В.В. Федотов, Е.Н. Тищенко, А.А. Яковенко

ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ЖИЗНЕННОГО ЦИКЛА ПРОЕКТИРОВАНИЯ И ПРОИЗВОДСТВА НАУКОЕМКОЙ ТЕЛЕКОММУНИКАЦИОННОЙ ПРОДУКЦИИ НА БАЗЕ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ВИДЕ ВИРТУАЛЬНОГО ПРЕДПРИЯТИЯ МЕЖДУ ПАО «РОСТЕЛЕКОМ» И ВЕДУЩИМИ ПРОИЗВОДИТЕЛЯМИ, ПРОЕКТИРОВЩИКАМИ ТК МАТЕРИАЛОВ И ОБОРУДОВАНИЯ, СТРОИТЕЛЬНЫМИ ТК КОМПАНИЯМИ

ПАО «Ростелеком», Ростов-на-Дону, Россия
Ростовский Государственный Экономический Университет, Ростов-на-Дону, Россия
Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: бизнес процессы, аналитические системы управления производством, телекоммуникации, виртуальное предприятие

Виртуальные предприятия – одна из новых организационных форм предприятий. На развитие этих форм организации и управления предприятием в значительной степени повлияли такие тенденции развития современных рынков, как их глобализация, рост значения качества товара, его цены и степень удовлетворения потребителей, повышение важности устойчивых отношений с потребителями (индивидуализация обслуживания заказчиков), а также растущее значение использования новых информационных и коммуникационных технологий.

V.V. Fedotov, E.N. Tishchenko, A.A. Yakovenko

BUILDING A SYSTEM OF INFORMATION SUPPORT OF LIFE CYCLE DESIGN AND PRODUCTION OF SCIENCE-INTENSIVE TELECOMMUNICATION PRODUCTS BASED ON A COMMON INFORMATION SPACE IN THE FORM OF A VIRTUAL ENTERPRISE BETWEEN PJSC ROSTELECOM AND LEADING MANUFACTURERS AND DESIGNERS OF TC MATERIALS AND EQUIPMENT, CONSTRUCTION OF TC COMPANIES

PJSC "Rostelecom", Rostov-on-don, Russia
Rostov State Economic University, Rostov-on-don, Russia
North-Caucasian branch of Moscow Technical University of Communication and Informatics, Rostov-on-don, Russia

Keywords: business processes, analytical system of production management, telecommunications, virtual enterprise

The virtual enterprise is one of the new organizational forms of enterprises. The development of these forms of organization and management of an enterprise are largely influenced by such trends of development of modern markets, such as globalization, the growing importance of the quality of the product, its price and the degree of satisfaction of customers, raising the importance of sustainable relationships with customers (individual customer service), as well as the growing importance of the use of new information and communication technologies.

Суть проблемы

Крупные предприятия в современных рыночных условиях заинтересованы:

- в снижении затрат, связанных с уменьшением стоимости оборудования, приобретением его функциональных блоков;
- в максимальном удовлетворении потребностей своей сети связи в современных тактико-технических и экономических характеристиках и параметрах, максимально приближенным к современным, постоянно изменяющимся к условиям эксплуатации и развития в телекоммуникационном секторе экономики;
- в снижении эксплуатационных затрат и вытекающему из этого уменьшению себестоимости услуг связи.
- разработке и внедрении новых типов линейно-кабельной продукции, к примеру ленточных оптических кабелей.
- доведению до подрядных организаций меняющимся принципах и особенностях строительства сетей связи
- проектированию новых сервисов и услуг
- разработке перспективных схем предоставления сервисов для конкретных крупных клиентов (банки, госструктуры)
- развитие непрофильных направлений и услуг

Любой продукт на рынке телекоммуникаций (наукоемкое оборудование связи или новые типы кабельной продукции) создается производителем на основе ориентировочных маркетинговых данных, спроса на определенный тип портов, его протоколы, емкость с учетом информации, полученной в процессе эксплуатации или реализации крупной программы по подключению клиентов, поступаемой, как правило, от крупных операторов связи. Создание ПАО Ростелеком совместно минимум с 2-мя – максимум с 10-ю крупнейшими наукоемкими производителями телекоммуникационных компонентов сетей связи (Huawei, НТЦ «Натекс», НПП «Спецстрой-Связь» (желательно отечественные производители)) единого информационного пространства (ЕИП) на основе CALS-технологии (Continuous Acquisition and Life Cycle Support), что позволит оптимизировать и сократить процессы проектирования, внося дополнительные предложения, замечания по конструкторской оптимизации любого телекоммуникационного продукта (улучшение конструкции, мощности, производительности, дооборудование функциями, удаление излишеств, повышение надежности, уменьшение себестоимости) в любой точке жизненного цикла (ЖЦ) товара (наукоемкого телекоммуникационного оборудования). Предложения и коррекции вносятся как оператором, так и производителем.

Актуальность внедрения ЕИП на основе CALS-технологии проектирования в первую очередь обусловлено необходимостью снижения рисков при переходе на новую версию

или тип оборудования и обеспечения скорейшего возврата инвестиций, уменьшение сроков реализации, внедрения и получения дохода.

Создание своеобразного виртуального предприятия для информационной поддержки ЖЦ наукоемкой ТК продукции создается путем отбора требующихся организационно-технологических ресурсов от различных предприятий и их интеграции с помощью компьютерной сети Internet в гибкую и динамическую структуру, приспособленную для скорейшего выпуска новой продукции и ее оперативной поставки на рынок. Особенностью функционирования виртуального предприятия является то, что персонал такого объединения территориально размещается в различных регионах страны, а в общем случае и в различных странах.

Предполагаемый бизнес-результат

- в снижении затрат, связанных с уменьшением стоимости оборудования, приобретением его функциональных блоков;
- в максимальном удовлетворении потребностей своей сети связи в оборудовании по тактико-техническим и экономическим характеристикам и параметрам максимально приближенным к современным, постоянно изменяющимся условиям эксплуатации и развития в телекоммуникационном секторе экономики;
- в снижении эксплуатационных затрат и вытекающем из этого уменьшением себестоимости услуг связи.
- разработке и внедрении новых типов линейно-кабельной продукции, к примеру ленточных оптических кабелей.
- доведение до подрядных организаций меняющихся принципов и особенностей строительства сетей связи
- проектировании новых сервисов и услуг

Экономический эффект

Снижение операционных затрат на 20%

Повышение эффективности работы оборудования на 30%

Оперативное разворачивание ТК ресурсов

Оперативное удовлетворение услугами связи потребителей

Снижение себестоимости не менее 15%

Снижение стоимости закупок не менее чем на 15%

Уменьшение затрат на логистику не менее 20%

Это миллионы рублей в год и факт повышения эффективности производственных процессов

Приток наукоемких технологий

Что предлагается предпринять для решения проблемы? Заключить соглашение с обозначенным количеством производителей , проектировщиков, подрядчиков. Создать единое информационное пространство, обеспечить его выносными рабочими местами и серверным оборудованием. Организовать на каждом предприятии-участнике структурное подразделение с экономическими, техническими и коммерческими навыками.

Необходимые для реализации ресурсы.

Серверное оборудование. Медийный ресурс должен быть закреплен за Ростелеком, Выделение среди существующих сотрудников новых членов структурного подразделения. Общая численность штата не должна быть увеличена. Обеспечение их соответствующими полномочиями. Умственные способности. Общие капитальные вложения по проекту должны составит максимум 5 млн руб. Фонд оплаты труда существующий. Количество человек - 6. Центр обработки данных существующий

СПИСОК ЛИТЕРАТУРЫ

1. *Федотов В.В. Борисов Б.П.* «МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ И ИНФОРМАЦИОННОЙ ИНТЕГРАЦИИ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ» Сборник Трудов СКФ МТУСИ 2015
2. *Федотов В.В. Тищенко Е.Н.* «ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА ПРИНЯТИЯ РЕШЕНИЯ ДЛЯ НЕПРЕРЫВНОЙ ПОДДЕРЖКИ И ОПТИМИЗАЦИИ ПРОИЗВОДСТВА НАУКОЕМКОЙ ПРОДУКЦИИ» Сборник Трудов СКФ МТУСИ 2015
3. *Федотов В.В.* "Инструментальные методы исследования качества жизненного цикла ", с номером ISBN 978-3-659-62673-9 Издательство «Lambert Academic Publishing» Saarbrücken, Germany
4. *Федотов В.В.* БИЗНЕС-ПРОЦЕССЫ: ОТ ОСНОВ К СОВЕРШЕНСТВУ Теоретические и прикладные вопросы экономики и сферы услуг № 4, 2014
5. *В.В. Федотов, Д.О. Осадчий, Н.А. Пасенко* Применение аналитических и информационных систем принятия решений для непрерывной поддержки и

оптимизации процесса производства аппаратуры связи. Сборник Трудов СКФ МТУСИ 2016
6. *В.В. Федотов, Е.Н. Тищенко, Б.П. Борисов* Возможность применения интеллектуальных информационных систем в организационных структурах. Сборник Трудов СКФ МТУСИ 2016

П.Ч.Е. Федотова, Н.В. Будылдина

РЕАЛИЗАЦИЯ В РОССИИ ИНДУСТРИАЛЬНЫХ ИНТЕРНЕТ ВЕЩЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: информационные технологии, новые технологии, индустриальный интернет вещей.

В статье рассмотрены проблемы развития индустриальных Интернет вещей, представлены основные задачи для реализации системы интернет вещей в России.

P.C.E. Fedotova, N.V. Budyldina

REALIZATION INDUSTRIAL INTERNET OF THING IN RUSSIA

Ural Technical Institute of Communications and Informatics (branch) FGBOU VO "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibGUTI), Russia

Keywords: information technology, new technologies, Industrial Internet of Things.

The article deals with the problems of the industrial Internet of Things, presents the basic tasks for the realization of the Internet of Things system in the Russia.

Интернет Вещей (IoT, Internet of Things) – система объединенных компьютерных сетей и подключенных физических объектов (Вещей) со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека [2].

Специалисты компании IDC определяют Интернет вещей (Internet of Things, IoT) как сеть сетей, состоящих из уникально идентифицируемых объектов (вещей), способных взаимодействовать друг с другом без вмешательства человека, через IP-подключение. Основным фактором этого определения является наличие автономности устройств и их способности передачи данных самостоятельно, без участия человека [3].

Интернет вещей подразделяют на потребительский (массовый) и корпоративный (бизнес) сегменты. В потребительский сегмент входят персональные подключенный устройства, например, различные смарт вещи, такие как смарт-часы, автомобили, устройства умного дома и так далее. К корпоративному сегменту относятся отраслевые и межотраслевые рынки, например, промышленность, сельское хозяйство, транспорт, энергетика, умный город (Smart City) и другие [2].

Индустриальный Интернет Вещей (Industrial Internet of Things, IIoT) – Интернет Вещей для корпоративного применения – это система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека [3].

Внедрение Индустриального Интернета вещей на данный момент происходит внутри компаний, однако с помощью традиционных систем хранения и аналитических решений осуществляется сбор и анализ данных. Тем не менее, спрос на решения в области больших данных и облачных услуг растет, это приведет к легкому масштабированию решений и выходу за рамки отдельных компаний, в зависимости от темпов роста генерируемых объемов данных.

На данный момент для того, чтобы реализовать в России Индустриальный Интернет вещей заказчикам необходимо быть уверенными в необходимости и ценности предлагаемого им подхода, а также осуществляемых комплексных решений. Некоторые полагают, что Индустриальный Интернет вещей это сбор данных с устройств и их анализ, при этом очень часто упускается важная часть того, что для передачи стремительно растущего объема данных в центры обработки требуются новые технологические решения. Однако аналитический компонент Интернет вещей, включая и на конечных устройствах, пока не воспринимается как неотъемлемая часть IoT-решений.

Для того чтобы наиболее быстрее развивался Индустриальный Интернет вещей необходимо, чтобы бизнес-пользователи были более заинтересованы, таким образом, возрастут результаты от внедрений успешных проектов. Следовательно, в результате формирования изолированных систем в рамках отдельных компаний при реализации пилотных проектов, увеличивается опыт по оцифровыванию данных и реализации технологий в постановке бизнес-задач. Таким образом, между партнерскими и клиентскими сетями становится возможным установление связей, то есть облегчает дальнейшую интеграцию с другими системами [3].

На данный момент во многих странах, которые намерены использовать технологии Индустриального Интернета вещей, существуют ассоциации, которые рассматривают проблемы Интернета вещей. Также созданы интернациональные консорциумы, которые занимаются разработкой стандартов в области безопасности и обмена данными [3].

Большое влияние на экономику страны и отдельных компаний оказывает Индустриальный Интернет вещей. В будущем это будет способствовать росту валового национального продукта, повышению производительности труда, положительно окажет влияние на условия труда и профессиональный рост сотрудников. Оцифровка производства, обмен данными и аналитика больших объемов информации является основой сервисной модели экономики, которая создается благодаря этому переходу. На данный момент существуют только пилотные проекты российских компаниях, однако они

активно развиваются и в скором времени ожидается момент, когда эти результаты опубликуют и станут достоянием общественности. Этап создания цифровых моделей продукции и связей между технологическими процессами и критически важными инфокоммуникационными процессам внутри корпорации является крайне важным этапом в развитии Индустриального Интернета вещей.

Для дальнейшего развития Индустриального Интернета вещей требуются внешняя поддержка, нормативные базы, эффективная инфраструктура взаимодействия и общих стандартов. Чтобы компании могли пользоваться всеми достоинствами цифрового производства необходимо установить эффективные партнерские отношения с целью разработки инновационных продуктов и услуг, а для этого требуется стратегическое лидерство. Компания IDC считает, таким лидером может стать компания «Ростелеком», которая возьмет на себя заботу о стандартах и обеспечит взаимодействие всех участников процесса создания решений в области Индустриальных Интернет вещей в России, а также взаимодействие с ведущими мировыми поставщиками технологий [3].

В России только начинается формирование рынка Интернета вещей. Во многих компаниях решаются такие задачи как автоматизированный обмен и управление данными за счет решений и протоколов компании, которые, в основном, сложны для расширения и интеграции с внешними системами [2].

Считается, что наиболее активно используют возможности Интернета вещей такие отрасли как жилищно-коммунальное хозяйство, транспортная система и производство. Однако, за счет стремительно развивающейся концепции «Умный город», которая во многом использует технологии IoT, ситуация на рынке склонна к изменениям. На данный момент в России реализуются фундаментальная ступень «Умного города» - система «Безопасный город», который является аппаратно-программным комплексом, реализующим контроль за безопасностью за счет видеонаблюдения [4]. На данный момент в г. Екатеринбурге происходит реализация инновационного проекта «Умный город» в районе «Академический». Также в г. Казани компании Cisco и «Таттелеком» осуществляют проект «Умный и безопасный город Казань», который включает в себя единую городскую сеть Wi-Fi, интеллектуальные видеонаблюдение, парковку, транспортную систему, уличное освещение и ЖКХ.

Также компаниями «Техносерв» и «Акадо телеком» для Московсковской объединенной энергетической компании была разработана система, которая позволяет удаленно считывать расход тепловой энергии в жилых домах, таким образом, система может оповещать энергетиков о сбоях в теплоснабжении или прогнозировать возможные поломки [5].

Компания «Автоваз» выпустили первый серийный автомобиль, который оснащен системой экстренного оповещения «ЭРА-ГЛОНАСС». С помощью данной системы происходит передача сигнала о ДТП, о нарушении скоростного режима, а также позволяет производить отключение двигателей автомобилей удаленно.

Для оптимизации процесса производства и исключения воровства на заводе «Северсталь» была реализована беспроводная система отслеживания передвижения грузов.

Технология IoT также используется в различных агрохолдингах. Например, на заводе «Дамате» была внедрена беспроводная система Eaton для того, чтобы процесс разделки индейки был более автоматизирован, то есть при отключениях электроэнергии

простои линии сводились к минимуму; в агрохолдинге «Русагро» была внедрена умная система хранения сахарной свеклы, которая заключается в фиксировании датчиками условий и мест хранения, при этом система показывает наиболее рациональный подход переработки необходимого сырья.

Интернет вещей также используют российские нефтяники, для того, чтобы создавать «умные скважины». С помощью датчиков инженерам в режиме реального времени поступают сведения о температуре и давлении в скважине, что благоприятно сказывается на эффективности нефтеотдачи и предоставляет возможность управлять нефтедобычей удаленно [5].

Существует несколько факторов, которые препятствуют широкому распространению концепций Интернета вещей, «Умного дома», «Умного города» и так далее в России на данный момент. А именно, это различные барьеры, такие как финансовые и психологические, даже для тестирования таких услуг, отсутствие понимания большинства пользователей в практическом применении данных услуг, следовательно, низкая покупательная способность, также отсутствие технических, юридических и интегрированных решений с управляющими компаниями. При этом необходима поддержка со стороны государства для того, чтобы было возможно реализовать именно юридические аспекты в части разработки и принятия единой нормативной базы для внедрения новых типов датчиков, измерительных приборов и управляющих систем в деятельность организаций ЖКХ. Таким образом, необходимо устранять основные факторы, которые препятствуют развитию системы Интернет вещей, для того, чтобы в любом населенном пункте России жители могли стать потребителями данных услуг [2].

СПИСОК ЛИТЕРАТУРЫ

1. *Росляков А.В., Ваняшин С.В., Гребешков А.Ю.* Интернет вещей. // Учебное пособие Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015 – 200 с.
2. JSON.TV [Электронный ресурс] – Ресурс доступа: http://json.tv – Загл. с экрана
3. Семеновская Е. Индустриальный интернет вещей перспективы Российского рынка. // IDC – 2016.
5. Журнал Коммерсант.ru [Электронный ресурс] – Ресурс доступа: http://www.kommersant.ru – Загл. с экрана
6. RUSBASE [Электронный ресурс] – Ресурс доступа: http://rb.ru – Загл. с экрана

О.И. Шаравова , М.П. Белянчикова, И.А. Новикова

РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОЙ ОЦЕНКИ ФИНАНСОВОГО ПОЛОЖЕНИЯ КРУПНЕЙШИХ РОССИЙСКИХ ОПЕРАТОРОВ ПОДВИЖНОЙ СВЯЗИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технический университет связи и информатики», Москва, Россия

Ключевые слова: подвижная связь, финансовое положение, перспективная оценка финансового состояния, финансовая устойчивость.

В статье рассмотрены результаты сравнительной текущей и перспективной оценки финансового положения ведущих операторов подвижной связи России, обоснована целесообразность применения для прогнозирования финансового положения организаций подвижной связи модели перспективной финансовой устойчивости.

O.I. Sharavova, M.P. Belyanchikova, I.A. Novikova

THE RESULTS OF THE COMPARATIVE EVALUATION OF THE FINANCIAL SITUATION OF THE LARGEST RUSSIAN OPERATORS MOBILE

Moscow Technical University of Communications and Informatics, Moscow, Russia

Keywords: mobile communications, financial position, prospects and financial condition, financial sustainability.

In the article the results of comparative current and prospective assessment the financial situation of the leading mobile operators of Russia, the expediency of application for forecasting the financial situation of organizations of mobile connection model perspective of financial stability.

Финансовая устойчивость организаций подвижной связи является важнейшим показателем текущего и перспективного состояния финансовых ресурсов, от которого зависит обеспечение нормального функционирования организации подвижной связи, способность предоставлять доступные услуги пользователям.

На основании данных публичной финансовой отчетности крупнейших операторов подвижной связи России: ПАО «Мобильные Телесистемы», ПАО «ВымпелКом» и ПАО «МегаФон», был проведен сравнительный анализ их финансового положения.

Анализ имущества ведущих российских операторов подвижной связи позволяет оценить общую стоимость имущества изучаемых компаний на уровне свыше 400 млрд. руб., причем наибольшими активами в размере 539135,981 млн. руб. в конце отчетного периода располагало ПАО «МТС». Следует отметить, что стоимость имущества ПАО «ВымпелКом» в анализируемом периоде снизилась с 639669,555 млн. руб. до 477898,251

млн. руб., в то время как активы двух других анализируемых компаний в отчетном периоде увеличились.

В результате анализа выявлено преобладание удельного веса иммобилизованных средств в общей стоимости активов, на долю которых приходится более 75 % имущества, в то время как удельный вес мобильных (оборотных) средств в общей стоимости имущества составлял от 12,90 % (в 2014 г. у ПАО «ВымпелКом») до 24, 16 % (в 2015 г. у ПАО «МТС»).

Кроме того, следует отметить незначительное снижение (на 0,34 %) в отчетном периоде удельного веса мобильных средств в структуре имущества ПАО «МегаФон».

Наибольший удельный вес в структуре источников имущества ведущих российских операторов подвижной связи занимают заемные средства, их доля составляет от 66 – 67% у ПАО «МегаФон» до 93 % у ПАО «МТС». Необходимо отметить, что имело место незначительное снижение удельного веса заемных средств в общей стоимости пассивов у ПАО «ВымпелКом» с 86,42% до 75,00%. Тревогу, с точки зрения, обеспеченности имущества собственными источниками вызывает тот факт, что величина собственного капитала всех анализируемых компаний подвижной связи не превышает 34 %, а у ПАО «МТС» этот показатель в 2015 году составляет лишь 6,64% против 16,48 % в 2014 году. То есть ПАО «МТС», не располагая достаточным количеством собственных средств для осуществления основной деятельности, предоставления качественных услуг пользователям, вынуждено было увеличить капитал за счет дополнительного привлечения заемных средств.

Собственный капитал ПАО «ВымпелКом» в анализируемом периоде незначительно возрос с 13,58% до 25%, однако очевидно, что такие изменения, не смотря на положительную динамику, не обеспечат независимость средств организации от заемных источников.

Сравнение дебиторской и кредиторской задолженностей показало, что величины дебиторской задолженности ПАО «ВымпелКом» и ПАО «МТС» превышают стоимость кредиторских задолженностей на обе отчетные даты, что положительно характеризует способность этих организаций своевременно рассчитываться по своим обязательствам, в то время как у ПАО «МегаФон» кредиторская задолженность превышает дебиторскую более, чем в 2 раза, что влечет за собой неспособность полностью и в срок погашать текущие обязательства.

Финансовая устойчивость всех изучаемых компаний подвижной связи в краткосрочной и долгосрочной перспективах оценивается как кризисная (кроме ПАО «МегаФон» в 2015 году, где в краткосрочной перспективе финансовая устойчивость определяется как предкризисная), на фоне того, что в текущей перспективе ПАО «ВымпелКом», ПАО «МТС» и ПАО «МегаФон» в отчетном году – нормальную. Такая оценка характеризует довольную рисковую финансовую ситуацию в будущем, которая в случае непринятия менеджментом операторов мер по улучшению финансового положения грозит финансовой неустойчивостью, отсутствием платежеспособности.

Более детально финансовое положение было оценено с помощью финансовых коэффициентов, характеризующих различные стороны финансово-хозяйственной деятельности, результаты расчета которых представлены в таблице 1. Следует отметить, что значения коэффициента автономии не удовлетворяют нормативным ограничениям у всех изучаемых компаний подвижной связи, что является крайне нехарактерной

ситуацией для организаций подвижной связи, в частности, и инфокоммуникационного комплекса в целом. Это объясняется тем, что величина собственных средств данных операторов значительно ниже заемного капитала, т.е. все компании зависимы от заемных источников. Кроме того, отрицательные значения коэффициентов маневренности и обеспеченности оборотных средств собственными источниками свидетельствуют о недопустимо низком уровне собственного капитала, необходимого для формирования достаточного количества оборотных средств, а также о недостаточной доле средств, находящихся в мобильной форме, позволяющей свободно маневрировать этими средствами.

Таблица 1 – Результаты расчета финансовых коэффициентов ведущих российских операторов подвижной связи

Наименование показателя	Значение показателя, отн. ед.	
	в баз. году	в отч. году
1. ПАО «ВымпелКом»		
1.1. Коэффициент автономии	0,14	0,25
1.2. Коэффициент финансовой устойчивости	0,90	0,86
1.3. Коэффициент финансирования	0,16	0,33
1.4. Коэффициент инвестирования	0,16	0,31
1.5. Коэффициент соотношения заемных и собственных средств	6,25	3,03
1.6. Коэффициент соотношения мобильных и иммобилизованных средств	0,15	0,22
1.7. Коэффициент маневренности	-5,42	-2,27
1.8. Коэффициент имущества производственного назначения	0,88	0,83
1.9. Коэффициент обеспеченности оборотных средств собственными источниками	-0,74	-3,09
2. ПАО «МТС»		
2.1. Коэффициент автономии	0,27	0,16
2.2. Коэффициент финансовой устойчивости	0,78	0,74
2.3. Коэффициент финансирования	0,38	0,20
2.4. Коэффициент инвестирования	0,32	0,20
2.5. Коэффициент соотношения заемных и собственных средств	2,64	5,07
2.6. Коэффициент соотношения мобильных и иммобилизованных средств	0,17	0,23
2.7. Коэффициент маневренности	-2,10	-3,95
2.8. Коэффициент имущества производственного назначения	0,86	0,83
2.9. Коэффициент обеспеченности оборотных средств собственными источниками	-3,88	-3,54

Продолжение таблицы 1

3. ПАО «МегаФон»		
3.1. Коэффициент автономии	0,38	0,37
3.2. Коэффициент финансовой устойчивости	0,92	0,92
3.3. Коэффициент финансирования	0,62	0,58
3.4. Коэффициент инвестирования	0,48	0,47
3.5. Коэффициент соотношения заемных и собственных средств	1,61	1,71
3.6. Коэффициент соотношения мобильных и иммобилизованных средств	0,25	0,29
3.7. Коэффициент маневренности	-1,09	-1,11
3.8. Коэффициент имущества производственного назначения	0,88	0,84
3.9. Коэффициент обеспеченности оборотных средств собственными источниками	-2,12	-1,85

Анализ финансовых коэффициентов подтвердил сложную финансовую ситуацию во всех изучаемых компаниях подвижной связи.

Ликвидность баланса оператора подвижной связи выражается в степени покрытия обязательств его активами, срок превращения которых в деньги соответствует сроку погашения обязательств.

Сравнение средств по активу, сгруппированных по степени ликвидности, со средствами по пассиву, сгруппированными по срокам погашения обязательств ПАО «МТС», ПАО «МегаФон» и ПАО «ВымпелКом» позволили сделать вывод об отсутствии абсолютной ликвидности у всех анализируемых операторов, поскольку знаки в системе неравенств [3, с. 38] отличаются от зафиксированных в оптимальном варианте.

Детальную характеристику ликвидности баланса рассматриваемых компаний позволяют получить относительные показатели – коэффициенты ликвидности, результаты расчета которых приведены в таблице 2.

Проведенный анализ показателей ликвидности ведущих российских операторов подвижной связи показал, что значения коэффициента текущей ликвидности ни в одном случае не удовлетворяют нормативным ограничениям, принятым для инфокоммуникационных компаний [3, с. 39]. Кроме того, значения всех показателей ликвидности баланса ПАО «ВымпелКом» не соответствуют нормативам. В целом можно отметить, что все представленные организации испытывают серьезные проблемы при расчетах по своим обязательствам ввиду недостаточности оборотных средств, а у ПАО «ВымпелКом» и денежных средств.

Таблица 2 – Результаты расчета показатели ликвидности баланса ведущих российских операторов подвижной связи

Наименование показателя	Значение показателя, отн. ед.	
	в баз. году	в отч. году
1. ПАО «ВымпелКом»		
1.1. Коэффициент абсолютной ликвидности	0,12	0,08
1.2. Коэффициент ликвидности	0,15	0,51
1.3. Коэффициент текущей ликвидности (покрытия)	0,54	0,72
2. ПАО «МТС»		
2.1. Коэффициент абсолютной ликвидности	0,24	0,32
2.2. Коэффициент ликвидности	0,61	0,66
2.3. Коэффициент текущей ликвидности (покрытия)	0,67	0,71
3. ПАО «МегаФон»		
3.1. Коэффициент абсолютной ликвидности	0,61	0,71
3.2. Коэффициент ликвидности	0,75	0,92
3.3. Коэффициент текущей ликвидности (покрытия)	0,77	0,93

Результаты расчета показателей рентабельности и деловой активности [2, с. 465-466; 3, 41-43] крупнейших российских операторов подвижной связи, являющихся показателями эффективности их финансово-хозяйственной деятельности и использования ресурсов соответственно, свидетельствуют о том, что почти все анализируемые компании подвижной связи обладают рентабельностью реализации на уровне, превышающем 20% (кроме ПАО «ВымпелКом» в 2015 г. – 18%) , т.е. можно сделать вывод об эффективной финансово-хозяйственной деятельности этих компаний.

Скорость оборота дебиторской задолженности у всех анализируемых операторов превышает скорость оборота кредиторской задолженности, что характеризует некоторое замедление оборачиваемости кредиторской задолженности по сравнению с дебиторской.

Кроме того, в 2015 году снизилась рентабельность общей стоимости активов ПАО «МТС» и ПАО «МегаФон», а рост данного показателя для ПАО «ВымпелКом» хоть и отражает положительную динамику, пока не может означать эффективность использования активов, поскольку значение этого показателя как в базисном, так и в отчетном периодах, имеет невысокий уровень.

Результаты анализа текущего финансового положения компаний подвижной связи являются основой для прогнозирования перспективного финансового состояния.

Оценка перспективной финансовой ситуации ПАО «МТС», ПАО «МегаФон» и ПАО «ВымпелКом» на основании модели оценки возможной платежеспособности организаций связи [2, с. 468; 4] представлена в таблице 3.

Таблица 3 - Результаты оценки возможной платежеспособности ведущих российских операторов подвижной связи

Удельный вес излишка или недостатка величины источников формирования оборотного капитала в общем итоге аналитического баланса	Значение показателя в отчетном году, отн. ед.
ПАО «ВымпелКом»	-0,48
ПАО «МТС»	-1,53
ПАО «МегаФон»	-0,48

На основании данных таблицы 3 можно сделать вывод о перспективной финансовой неустойчивости всех изучаемых операторов подвижной связи, в случае, если условия финансово-хозяйственной деятельности останутся неизменными, поскольку значения показателя удельного веса излишка или недостатка величины источников формирования оборотного капитала в общем итоге аналитического баланса представляют собой отрицательные величины. Поэтому менеджменту компании следует принять срочные меры по увеличению собственного капитала и собственных оборотных средств.

Результаты расчета операционного рычага [2, с. 470; 3, с. 46] показывают, что при изменении выручки от реализации услуг подвижной связи на 1 % прибыль ПАО «ВымпелКом» изменяется на 24,95 %, ПАО «МТС» - на 28,41 %, а ПАО «МегаФон» - на 5,23%. Такие величины показателя операционного рычага свидетельствуют, что ПАО «МегаФон» подстерегает большая опасность, а ПАО «МТС» и «ВымпелКом» - огромная, при снижении объема оказания услуг, например, вследствие падения спроса. Менеджменту компаний необходимо принимать во внимание эти факты при принятии решений в области ценообразования и тарифной политики.

В 2016 году была разработана новая модель прогнозирования финансового положения организаций подвижной связи - [1, 5, 6]:

$$y = 0.659k_{ФУ} + 0.168k_{З/С} + 0.481k_{ОС},$$

где $k_{ФУ}, k_{З/С}, k_{ОС}$ – коэффициенты финансовой устойчивости, соотношения заемных и собственных средств, обеспеченности оборотных средств собственными источниками соответственно.

Оценка перспективной финансовой ситуации ведущих российских операторов подвижной связи на основе *эконометрической модели оценки перспективной финансовой устойчивости*, представлена в таблице 4.

На основании данных таблицы 4 можно сделать вывод о перспективной финансовой неустойчивости ПАО «ВымпелКом», ПАО «МТС» и минимальной финансовой устойчивости ПАО «МегаФон». Сравнивая полученные результаты с результатами прогнозирования на основе модели оценки возможной платежеспособности, представленными в таблице 3, можно отметить, что ПАО «ВымпелКом» и ПАО «МТС» характеризуются перспективной финансовой неустойчивостью, возникающей при отсутствии платежеспособности. А минимальная финансовая устойчивость ПАО «МегаФон» определяется меньшим эффектом операционного рычага. Вследствие этого, можно утверждать, что модель оценки перспективной финансовой устойчивости точнее

описывает перспективную финансовую ситуацию оператора подвижной связи и ее применение для финансового прогнозирования видится целесообразным.

Таблица 4 - Исходные данные и результаты оценки перспективной финансовой устойчивости ведущих российских операторов подвижной связи

Удельный вес излишка или недостатка величины собственных и долгосрочных заемных источников формирования оборотных активов в общем итоге аналитического баланса	Значение показателя в отчетном году, отн. ед.
ПАО «ВымпелКом»	-0,41
ПАО «МТС»	-0,36
ПАО «МегаФон»	0,004

Полученные в результате сравнительного анализа финансового положения организаций подвижной связи результаты и выводы способствуют развитию аналитико-прогнозной методологии в области диагностики и прогнозирования финансового состояния компаний подвижной связи.

СПИСОК ЛИТЕРАТУРЫ

1. *Белянчикова М.П., Шаравова О.И.* Финансовое прогнозирование – инструмент повышения стабильности и устойчивости в сфере ИКТ. / Сборник материалов XXIX Конгресса «Безопасность и качество в сфере ИКТ». - 2016. - С. 43-47.
2. *Кузовкова Т.А., Салютина Т.Ю., Шаравова О.И.* Статистика инфокоммуникаций. Учебник для вузов / Под ред. Т.А. Кузовковой. – М.: Горячая линия – Телеком, 2015. – 554 с.
3. *Кузовкова Т.А., Шаравова О.И., Зайцев Е.М.* Финансы и кредит: Учебное пособие / МТУСИ. – М., 2010. – 140 с.
4. *Кузовкова Т.А., Шаравова О.И., Терехова Ю.С.* Финансовое прогнозирование в организациях инфокоммуникаций // T-Comm: Телекоммуникации и транспорт. - 2015. Т. 9. № 8. - С. 84-89.
5. *Шаравова О.И., Белянчикова М.П.* Диагностика финансовой устойчивости организаций подвижной связи / Труды Северо-Кавказского филиала Московского технического университета связи и информатики. - 2016. Т.1. № 9. - С. 603-606.
6. *Шаравова О.И., Белянчикова М.П.* Прогнозирование финансового состояния организаций подвижной связи (DOI 10.18454/IRJ.2016.45.065). // Международный научно-исследовательский журнал. - 2016 - №3 (45). Часть 1. - С. 79-80.

А.А. Яковенко, М.А. Галухин

ТРАНСФОРМАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА И ИННОВАЦИИ В УПРАВЛЕНИИ ПЕРСОНАЛОМ

Ключевые слова: Управление трудовыми ресурсами,Управление человеческим капиталом, Управление персоналом, коучинг

Аннотация: В статье рассматривается возможность удовлетворения своих личные качества, работая в организации. Трудовая деятельность как форма реализации соц. и личных потребностей

A.A. Yakovenko, M.A. Galukhin

MODERN SOCIETY TRANSFORMATIONS AND HUMAN RESOURCES MANAGEMENT INNOVATIONS

Keywords: Human Resource Management, Human Capital Management, Human Resources Management, Coaching

Abstract: The article considers the possibility of satisfying one's personal qualities by working in an organization. Labor activity as a form of realization social. And personal needs

Стремительные изменения современного мира, включая технологические и социальные революции не могли не затронуть сферу управления персоналом. Появились новые понятия, новые нелинейные формы организационных структур, на фоне высокой конкуренции и насыщенности рынка особое значение приобрели маркетинг и стратегическое управление, брендинг, социальные инновации и человеческий капитал. В управлении персоналом появились идеи, методы и концепции, отвечающие современным социокультурным условиям ведения бизнеса. Возникли технологии, позволяющие более успешно руководить людьми. Всевозможные аттестации, мероприятия, направленные на развитие корпоративной культуры и поддержание корпоративного духа, управление по целям, тренинги, коучинг, действия, призванные ускорить адаптацию вновь поступающих сотрудников, работа с резервом - это далеко не полный перечень того, что проводится в современной организации. Если в недавнем прошлом нормой считалось отношение к сотруднику как к исполнителю определенных функций, то современный стиль управления предоставляет работнику гораздо больше возможностей реализации и самоорганизации, предполагает проявление инициативы и творческих сил.

Управление персоналом (англ. Human Resource Management, HRM) в большинстве источников определяется как область знаний и практической деятельности, направленная на обеспечение организации «качественным» персоналом (способным выполнять возложенные на него трудовые функции) и оптимальное его использование. Оптимальное использование персонала в концепции «Управления персоналом» достигается за счёт выявления положительных и отрицательных мотивов индивидуумов и групп в организации и соответствующего стимулирования положительных мотивов и

«погашения» отрицательных мотивов, а также анализа таковых воздействий. В различных источниках могут встречаться и другие названия: управление трудовыми ресурсами, управление человеческим капиталом, кадровый менеджмент, менеджмент персонала.

Сущность философии управления персоналом организации заключается в том, что работники обладают возможностью удовлетворять свои личные потребности, работая в организации. В то же время в практике управления можно наблюдать отсутствие современной системы управления персоналом, когда работники не находят условий для реализации и удовлетворения своих социальных, личных, человеческих потребностей в организации. Труд только истощает силы сотрудников и становится своеобразной жертвой ради денег, получаемых в качестве компенсации. Тогда можно говорить об отчуждении сотрудника от собственной человеческой сущности в процессе труда. В таком случае можно утверждать, что грамотная система управления персоналом способна преодолеть отчуждение и сформировать условия для раскрытия, реализации человека в профессиональной деятельности, включения его в более широкий контекст общественной жизни. Актуальная для многих современных руководителей тема нематериальной мотивации также решается в процессе эффективного управления персоналом.

Итак, сформулируем теоретические, философские основы управления персоналом:

Смысл системы управления персоналом заключается в обеспечении возможностей реализации сотрудниками своих личных потребностей и гармоничной увязке этих потребностей с целями организации.

Цель системы управления персоналом – формирование необходимого кадрового потенциала для реализации целей организации.

Система управления персоналом методологически связывает собой материалистическую экономику, в которой основным показателем эффективности является, в общем-то, прибыль собственников и гуманистическую психологию, в которой показателем становится удовлетворение потребностей человека. Еще в первой половине прошлого века прозвучала и была доказана идея о том, что забота о человеке экономически выгодна.

Предметом исследования данной отрасли знания является человек в его связи с другими людьми в организации, а также его способность быть эффективным в отношении личных и организационных целей.

Система управления персоналом неэффективна в том случае, если в организации отсутствует система манеджмента качества и контроль отдачи затрат на управление персоналом.

Управление персоналом включает в себя: поиск и адаптацию персонала, оперативную работу с персоналом (обучение и развитие персонала, оперативная оценка персонала, управление бизнес-коммуникациями, мотивацию персонала и его оплату, организацию труда), стратегическую работу с персоналом (управление корпоративной культурой).

В ходе развития менеджмента (весь двадцатый, начало двадцать первого века) можно проследить такие тенденции, как:

– постепенная децентрализация управления: переход от иерархических линейно-функциональных организационных структур к дивизионным, матричным, сетевым – более гибким, пластичным и допускающим большую долю автономии сотрудников, которые зачастую участвуют как в управлении, так и в прибылях;

– рост значимости и ценности личности в экономике: человеческого капитала, креативных способностей, способностей генерировать новые идеи, что можно связать с ростом конкуренции и насыщением рынка. Человеческий капитал становится ресурсом и фактором конкурентоспособности организации;
– отношения подчинения все больше уступают место отношениям партнерства, грань между начальником и подчиненными на всех уровнях управленческой иерархии сгладились. Экономическая культура постиндустриального общества все больше носит «сотрудничающий» характер;
– возникает необходимость в постоянном образовании и повышении квалификации сотрудников организаций;
– все больше используются методы психологии в управлении персоналом (тренинги и др.);
– усилилось внимание к организационной культуре, а также разнообразным формам демократизации, участию рядовых работников в прибылях и осуществлении управленческих функций.

Концепция управления персоналом - система - теоретико-методологических взглядов на понимание и определение сущности, содержания, целей, задач, критериев, принципов и методов управления персоналом. На сегодняшний момент сформировалось и действует несколько концепций управления персоналом:

Контроллинг персонала - концепция управления персоналом, интегрированная с контроллингом экономического и социального компонентов эффективности. Основными функциями контроллинга персонала являются:
– анализ использования персонала и достигнутых за счет этого результатов;
– координация планирования персонала с другими сферами планирования;
– создание и поддержание интегрированной базы данных по персоналу в соответствии с поставленными целями.

Маркетинговая концепция управления персоналом - утверждение, согласно которому важнейшим условием достижения целей организации является четкое определение требований к персоналу, его социальных потребностей в профессиональной деятельности и обеспечение удовлетворения этих требований и потребностей более эффективными, чем у конкурентов, способами.

Персонал-издержки - концепция управления персоналом, согласно которой персонал рассматривается как издержки организации, которые необходимо сокращать.

Персонал-ресурс - концепция управления персоналом, рассматривающая персонал как один из основных ресурсов организации, которым надо грамотно управлять. Эта концепция предполагает:
– построение работы с персоналом в соответствии со стратегией развития организации;
– качественный и количественный прогноз персонал-ресурса;
– оптимизацию и расчет персонал-ресурса на длительную перспективу;
– ориентацию на качественные показатели деятельности работников;
– значительную степень автономии и самостоятельности специалистов при выполнении работ;
– инвестиции в персонал.

В первую очередь приход современного HRM существенно изменил сам стиль управления персоналом. Возникла новая культура управления и организационная культура в принципе. Человеческий потенциал компании стал основой для ее стратегического развития и грамотные вложения в него – одним из лучших способов инвестирования. Одной из относительных новаций (возникла на Западе в девяностые годы двадцатого века) в управлении персоналом стал коучинг. По данным исследования Manchester Inc., организации, инвестирующие в коучинг для своих топ-менеджеров, получили почти шестикратную прибыль. Во-первых, это объясняется тем, что коучинг сосредотачивает людей на выполнении дел, которые увеличивают прибыль организации. Во-вторых, он дает компании-клиенту «капитал» самомотивации и ответственности персонала, которые максимизируют продуктивность и эффективность организации, что опять же ведет к увеличению прибыли.

Пик популярности коучинга на Западе пришелся на девяностые годы двадцатого века. Тогда же Д. Уитмор, который создал основы этого метода и стал работать с его помощью с руководителями и бизнесменами, привез его в Россию. Но и сейчас, например, в Ростове-на-Дону такая профессия как коуч только формируется, только появляются попытки распространять коучинговую культуру в организациях, сам термин практически малоизвестен. Полагаю, что для большинства российских организаций переход с изжившего себя авторитарно-директивного стиля управления на более современный, предполагающий децентрализацию власти стиль актуален и возможен вместе с началом использования метода коучинга в практике менеджмента.

Коучинг рассматривают и как консультативную работу, и как стиль менеджмента. И в том и в другом случае он формирует особую психологическую среду, позволяющую каждому сотруднику организации эффективно реализовывать поставленные цели, достигать более высоких профессиональных уровней, получать большее удовлетворение от жизни в целом, формировать нематериальную мотивацию. Только в первом случае его проводит специально нанятый консультант – коуч, во втором его использует сам менеджер в ходе работы, если он прошел соответствующее обучение. Коуч может проводить как индивидуальную, так и групповую работу.

Коучинг в процессе управления предполагает переход от вертикальных отношений подчиненный-начальник к горизонтальным, когда руководитель выступает своеобразным тренером, помощником работника в достижении им лучших результатов. Главной ценностью здесь является человек.

Международная Федерация Коучинга (ICF) даёт следующее определение процесса коучинга: «Коучинг (coaching) – это непрерывное сотрудничество, которое помогает клиентам (работникам) достигать реальных результатов в своей личной и профессиональной жизни. Посредством процесса коучинга клиенты углубляют свои знания, повышают свой КПД и улучшают качество жизни.

Коучинг как метод представляет собой диалог, когда коуч задает вопросы, проясняющие ситуацию клиента, его цели, необходимые шаги для достижения этих целей, а также найти все необходимые психологические и материальные ресурсы для этого. Помогает преодолеть реальные и мнимые препятствия. При этом предполагается, что клиент обладает всеми нужными ресурсами и способностями для принятия нужных решений. Коуч ничего не советует. Он в первую очередь умеет слушать (что в наше время

является в общем-то редкостью, особенно для руководителей) и задавать эффективные вопросы.

Особенностью общения коуча и клиента является то, что коуч не занимает роль эксперта, может вообще не владеть темой. Уитмор подчеркивает, что клиент достигает больших результатов когда коуч не владеет темой, потому что тогда он не дает советов и не переносит личный опыт в сферу работы клиента. Он помогает клиенту лучше сконцентрироваться и поддерживает, чтобы продлить его импульс к действию.

Тимоти Гэлвэй - один из основоположников коучинга так определил его сущность: «Коучинг - это раскрытие потенциала человека с целью максимального повышения его эффективности. Коучинг не учит, а помогает учиться». Методики коучинга уходят в тренерскую работу, опираются на гуманистическую психологию, работы Дэниела Гоулмена в сфере эмоционального интеллекта, традицию сократовских диалогов и ориентированы прежде всего не на точное выполнение инструкций, а на раскрытие внутреннего потенциала. Смысл коучинга заключается в пробуждении и развитии потенциала личности в процессе труда, которое достигается за счет повышения осознания (своих целей, возможностей, ресурсов). На эффективность работы организации влияет не только то, что знает и умеет персонал, а то, что он хочет делать и как это делает. Коучинг позволяет получить инициативных и деятельных сотрудников, которые по собственному желанию делают максимум из того, на что способны в данный момент.

Включая незадействованные ресурсы личности (а как известно человек в среднем использует лишь небольшую долю своих потенциальных возможностей), коучинг позволяет добиваться результатов экологично, действуя в большей степени на вдохновении, чем на напряжении. Между тем напряжение свойственно российскому менталитету. Как верно заметил автор одной из книг о коучинге «наш менталитет за бесконечно долгие годы крепостничества и революций дошел до непоколебимой аксиомы, что все великое и хорошее надо выстрадать. Глубоко выстрадать, помучиться до боли, до стискивания зубов, до хруста в суставах. И только тогда может родиться то, что действительно достойно назвать ценным. Это наше видение мы переносим на все - на работу, любовь, коллег, постройку дома, вождение автомобиля. Обратите внимание на выражение лица водителей в мегаполисе - обреченная напряженность и стойкая высокомерность. Полная готовность вступить, если не в бой, так к финальному участию в гонке на выживание. Именно напряженность, а не сосредоточенность» [1, с. 15].

Коучинг включает два уровня обучения. Первый уровень - создание нового сценария своих действий. Второй - человек приобретает уверенность и способность в принципе самостоятельно разрабатывать новые сценарии. Очень наглядно это отражает китайская пословица: «Если вы дали человеку рыбу, вы его накормили на день, если вы его научили ловить рыбу, вы его обеспечили пищей на всю жизнь». Если вы обучили сотрудника одной конкретной методике — это одно, если вы его обучили на примере конкретной методики самому разрабатывать новые методики для выполнения разнообразных задач — это совсем другое. Быть коучем означает, помочь поймать конкретную рыбу и одновременно научить ловить все виды остальных [1, с. 127].

Коучинг предполагает стиль исключения в руководстве людьми. Руководить в русском языке буквально означает «водить за руку». В английском языке слово «руководить» имеет древние корни и переводиться как «знать». Нашим подчиненным важно знать, куда они идут, а идеально иметь на руках карту этой «местности». Коуч -

менеджер, он же проводник, он же ведущий за руку, он же знаток карты, имеющий опыт и уже определивший все механизмы, закономерности и обычаи этой местности. Но, его ведение и контроль не постоянны. Коуч или менеджер работающий в стиле коучинга, вмешивается в процесс клиента (подчиненного) только тогда, когда возникают заминки при его продвижении вперед, когда он действительно в чем-то нуждается. А пока события развиваются в правильном направлении, или наблюдается явный прогресс опекаемого, руководитель, он же опекун, не вмешивается. Принцип коучинга: «Если что-то работает - не трогайте». Стиль исключения, правильно дозируя самостоятельность и ответственность, позволяет воспитать лидеров. Дозированное опекание - ключ к раннему проявлению самостоятельности [1, с. 131].

Основным результатом коучинга является достижение жизненных целей. привнесение гармонии в личную и профессиональную жизнь, обретение силы и усиление жизненной мотивации. Коуч помогает клиенту сосредоточиться на том, что наиболее важно для него, и действовать согласно этим ценностям. Воодушевление, мотивация и удовольствие - вот что обычно сопровождает процесс этого взаимодействия.

Предпосылки коучинга.

Все люди обладают способностью к развитию.

Наши убеждения, относящиеся к собственному потенциалу, прямо связаны с нашей успешностью.

Люди способны изменяться только в тех случаях, когда хотят этого и готовы к этому.

То, как мы определяем успех, окажет прямое воздействие на наши достижения.

Люди учатся только тогда, когда по-настоящему вовлечены в процесс.

Мы ограничиваем наш потенциал рамками наших убеждений (например, считая, что определенные вещи невозможны из-за внешних или ситуационных барьеров).

Для того чтобы помогать другим, мы должны непрерывно прогрессировать сами.

Мы можем учиться с помощью всего, что мы делаем, однако обучение происходит только тогда, когда мы мыслим и строим планы на будущее (теория обучения Колба).

Цель современных технологий по управлению персоналом, в том числе коучинга, состоит в преодолении отчужденности сотрудника от организации, согласовании личных и организационных целей, поиске возможностей для реализации сотрудников в компании, возрастании человеческого капитала организации. Можно утверждать, что конечной целью кадрового менеджмента является индивидуация и рост ресурсов сотрудников, которые напрямую влияют на качество выполняемого им труда. Термин «индивидуация» использовал К. Г. Юнг для обозначения процесса развития человека, достижения им большей психологической целостности. Я бы использовала его, добавив еще некоторые оттенки смысла. Индивидуация – это процесс раскрытия потенциала человека, становление его индивидуальности посредством социализации в организации и через организацию в общественную жизнь в целом, процесс роста внешних и внутренних ресурсов. Индивидуация – процесс противоположный по своим характеристикам отчуждению – постепенному истощению сил в процессе труда. Можно также сказать, что если индивидуация подразумевает рост осознания, то отчуждение - постепенное рассеивание осознания, «замыливание» взгляда, превращение труда в рутину, работу «на автомате» [2].

Индивидуальность – результат процесса индивидуации, не определяема внешними причинами в отличие от вещи, способна создавать нечто новое: в решениях, идеях, инновациях. Индивидуальность способна сделать проводником своего влияния любое материальное образование. Что такое бренд сегодня? Это вещь, которая стала нести в себе отпечаток некой личности, вещь, которая стала проводником некой индивидуальности, за которую потребитель готов платить дополнительную стоимость. Сегодня, в условиях насыщенности рынка в развитых странах индивидуальность становится самым дорогим товаром. Индивидуальность подразумевает способность к творчеству - создавать, продуцировать нечто новое, непредусмотренное сложившимся ходом вещей.

Когда в организации используется коучинг, действует коучинг-культура, то это создает мощную основу для процессов индивидуации сотрудников компании, роста ее кадрового потенциала и, как следствие, конкурентоспособности в целом.

СПИСОК ЛИТЕРАТУРЫ

1. *Аветисов А.* Альфа-коучинг. -М., 2008.
2. *Одинцова О.Н.* Культура гражданского общества: концептуальные основы и стратегии преодоления отчуждения. Диссертация на соискание ученой степени кандидате философских наук. –Ростов н/Д, 2005.

А.А. Яковенко, Е.П. Косарева

ПЛАНИРОВАНИЕ КАК МЕХАНИЗМ РЕАЛИЗАЦИИ ЦЕЛЕЙ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ СОВРЕМЕННОГО ОБЩЕСТВА

Северо-кавказский филиал ордена трудового красного знамени федерального государственного бюджетного образовательного учреждения высшего образования «московский технический университет связи и информатики», Ростов-на-Дону, Россия.

Ключевые слова: планирование, цель, деятельность, система, общество, механизм, развитие, согласование, реализация.

В данной статье показаны цели социально-экономического развития общества и планирование как возможный механизм их согласования и реализации в современных условиях.

A.A. Yakovenko, E.P. Kosareva

PLANNING AS A MECHANISM OF IMPLEMENTATION OF SOCIAL AND ECONOMIC DEVELOPMENT GOALS OF THE CONTEMPORARY SOCIETY

North-Caucasian Branch of the Order of the Red Banner of Labor of the Federal State Budget Educational Institution of Higher Education "Moscow Technical University of Communication and Informatics", Rostov-on-Don, Russia

Keywords: planning, goal, activity, system, society, mechanism, development, coordination, realization.

There are shown the aims of the social and economic development of the society and the planning as a possible mechanism of their coordination and realization in the modern conditions.

В современном российском обществе не выработан эффективный механизм координации, согласования и реализации целей социально-экономического развития общества, а реализация этих целей позволила бы обеспечить повышение уровня жизни населения. Наиболее приемлемым в такой ситуации, исходя из опыта западных стран, является государственное планирование. Поэтому формирование такой системы планирования связано с необходимостью согласования целей различных слоев общества и сфер деятельности в условиях новых экономических отношений в России.

Прошедшие десятилетия, характеризовавшиеся кардинальными преобразованиями в экономике России, показали, что необходимо сделать не только выбор курса, в направлении которого должно продвигаться наше общество, но и определить цели социально-экономического развития страны, реализация которых, обеспечив рост экономики, позволила бы повысить уровень жизни населения.

Сложившаяся ситуация ведет к необходимости определения целей социально-экономического развития нашей страны. В настоящее время у нас нет ясности как в постановке таких целей, так и в определении основной цели социально-экономического развития страны. То есть даже после осуществленных в России преобразований, в стране нет еще четкого объяснения того, какая система у нас создается и какие цели социально-экономические развития при этом ставятся. «Но может ли общество успешно развиваться, отчетливо не представляя себе, куда оно идет и какие стратегические цели преследует, каковы ожидаемые результаты и цена их достижения? Безусловно, что эти вопросы особенно остро встают тогда, когда общество вступает на этап перелома, смены траектории общественно-экономического развития. Другими словами, попадает как раз в ту ситуацию, в какой ныне пребывает российское общество» [14, с. 410-411].

Поэтому для определения целей социально-экономического развития, следует остановиться на характеристике самого понятия. Хорошо известно, что естественной потребностью человека является постановка целей, которые позволяют ему определить свое будущее. Отсюда следует, что правильно поставленная цель ведет к достижению желаемого результата, а неправильно поставленная цель искажает суть процесса и придает ему иное направление движения, которое может привести к достижению цели в

достаточно отдаленной перспективе или вообще не дать результата. И поэтому «хозяйствование, не подчиненное определенной общественной цели, означало бы стихийность развития» [3, с.17].

Человек, реализуя свою хозяйственную деятельность, может ставить цели исходя из тех целей, которые ставит перед собой общество, так как человек, живя в данном обществе, подчиняется его законам и порядкам. Следовательно, формулировка цели социально-экономического развития общества дает возможность определиться со своими целями и направлением развития, как хозяйствующим субъектам, так и каждому человеку.

Исходя из того, что человек наделен сознанием, его действия предопределены целеполаганием. И «чем более люди отдаляются от животных, тем более их воздействие на природу принимает характер преднамеренных, планомерных действий, направленных на достижение определенных, заранее известных целей»,[8,с.494] которые выражают идеальное представление желаемого состояния. Поэтому целеполагание как мыслительный процесс является элементом планирования, которое должно характеризовать будущее состояние объекта или процесса.

Планируя свою деятельность, каждый человек в любой сфере ставит перед собой определенные цели с намерением получить оптимальный результат.

«В конечном счете, для человека есть всего одна цель: достижение наибольшего удовлетворения. Сюда включено удовлетворение всех видов человеческих желаний и потребностей независимо от их природы, материальной или нематериальной (духовной)…» [9, с.85]. При этом следует подчеркнуть, что удовлетворение потребностей человека всегда субъективно.

И поэтому, начиная любую деятельность, человек планирует получение желаемого именно им результата, то есть он осуществляет свои действия осознанно. И это, как известно, составляет отличительную черту развития общества, где действуют люди, наделенные волей и сознанием.

Осознанное осуществление деятельности проявляется и в экономической сфере, где для получения желаемого результата человеку необходимо затрачивать определенные трудовые усилия, а труд «всегда носит осознанный, целенаправленный характер, следовательно, включает в себя момент планомерности» [12, с. 23]. В связи с этим можно вспомнить хорошо известное высказывание К.Маркса о том, что «самый плохой архитектор от наилучшей пчелы с самого начала отличается тем, что, прежде чем строить ячейку из воска, он уже построил ее в своей голове» [8, с.189].

Известно, что, целеполагание включает в себя не только определение цели, но и обоснование средств и методов ее достижения. И поскольку существует множество способов достижения поставленной цели, то необходим выбор наилучшего варианта ее реализации.

Для выбора наиболее рационального с точки зрения определенных критериев варианта достижения цели, то есть для оптимальной реализации этой цели, необходимо задействовать планирование, которое могло бы обеспечить согласование, координацию действий для достижения результатов на основе рационального использования имеющихся ресурсов.

Деятельность каждого хозяйствующего субъекта связана с постановкой конкретных целей, которые могут быть объединены в систему с определенным ранжированием, то есть могут выделяться цели разного порядка, которые, в свою очередь,

можно разделить на ряд видов по определенному признаку. Например, масштаб поставленных целей зависит, в первую очередь, от уровня хозяйствования.

Так, для развития любой страны особое значение имеют цели социально-экономического характера, позволяющие объединять усилия всего общества для достижения общенациональных целей. Однако это достаточно сложная задача, решение которой должно обеспечить государство.

Но прежде чем ставить вопрос о достижении целей социально-экономического развития общества, их надо поставить, а у нас до сих пор нет ясности в формулировке таких целей.

Отсутствие же четко сформулированных целей социально-экономического развития и долговременных ориентиров не позволяет государству, государственной власти сконцентрировать и направить все усилия общества на решение тех проблем, от которых зависит будущее страны. Поэтому важнейшей функцией государства является определение цели социально-экономического развития нашего общества, а отсутствие «внятных целей развития или их неправильный выбор могут повлечь за собой тяжелые последствия для всего общества…» [5, с. 11].

В сфере экономики в полной мере проявляется положение о том, что «в силу общности целей люди способны жить вместе» [9, с.85]. В этой сфере без взаимодействия субъекты хозяйствования не могут решать общенациональные задачи и реализовывать цели социально-экономического развития. Несмотря на то, что цели могут существенно различаться, их можно объединить, как для отдельных групп, так и для общества в целом. Хотя, реальная жизнь показывает, что у каждого члена общества, каждого хозяйствующего субъекта имеется собственное представление об общественной цели и общественной выгоде. Поэтому совместная деятельность субъектов в обществе возможна на условиях компромисса. «И такой компромисс определяет и проводит в жизнь только государственная власть» [1, с.144].

Исторический опыт свидетельствует о том, что «олицетворяемый государством жесткий административный централизм в определенных условиях оказывается единственно эффективной стратегией, способной в наибольшей степени мобилизовать силы общества на решение его главной в данных условиях задачи» [10, с. 35].

Так как цели социально-экономического развития общества могут быть разного порядка, то между ними могут существовать противоречия, характер причин которых может быть, как объективным, так и субъективным. Если к объективным причинам следует отнести, например, состояние экономики в отдельном регионе или в стране в целом, то к субъективным – неправильную постановку целей социально-экономического развития общества, неточную последовательность осуществления этих целей, а также принятие решений об их реализации.

Эти противоречия проявляются на разных уровнях, в том числе на уровне отдельного хозяйствующего субъекта. Они могут возникать между отдельными субъектами, между различными группами субъектов, между отдельным субъектом и группой субъектов, между отдельным субъектом и обществом, между отдельной группой субъектов и обществом в целом. Здесь можно выделить еще один важный момент, связанный с наличием глубоких противоречий между целями, связанными с решением социально-экономических задач в обществе, и «повседневной управленческой практикой, имеющей весьма относительную связь как с декларируемыми целями, так и реальными

потребностями в развитии экономики и социальной сферы» [6, с.4]. Основной причиной такого положения дел является несовершенство методологии государственного целеполагания, а также отсутствие механизма ранжирования целей и выделения главной цели. Видимо это и является причиной того, что в настоящее время не сформулирована основная цель социально-экономического развития общества.

Противоречия целей выступают источником движения и развития экономических отношений в обществе. Поэтому необходимо не устранение противоречий целей социально-экономического развития общества, а их разрешение. А это, в свою очередь, ведет к возникновению новых противоречий, но уже на другом уровне, так как разрешение противоречий целей социально-экономического развития общества осуществляется в ходе хозяйственной деятельности субъектов. Поэтому сами цели выступают стимулом социально-экономического развития общества.

Следовательно, противоречивость целей социально-экономического развития общества предполагает постоянный поиск и обновление механизма их координации и реализации.

Таким механизмом может быть планирование, осуществляемое на государственном уровне, которое будет способствовать целенаправленному преобразованию жизни общества в целом. Это связано с тем, что хозяйственная деятельность, особенно, в условиях современного сложно организованного производства, не может обойтись без соответствующих планов. При анализе современного хозяйства, как отмечал Р.Барр, следует исходить из того факта, что: «…люди, участвующие в экономической деятельности, руководствуются планами, которые они составляют и исполняют» [2, с.175-176].

Присутствие в современном обществе элемента стихийности приводит к тому, что «трудно направить развитие экономики на достижение общенациональных целей (укрепление геополитического положения страны в мире, обеспечение научно-технического, социально-экономического, культурного, духовного и нравственного прогресса общества, достойной жизни граждан)» [4, с.17]. Именно поэтому большинство экономически развитых стран мира широко используют систему государственного регулирования и планирования.

В целом такая система в рассматриваемых странах сформирована в виде пирамидальной взаимосвязанной системы. Долгосрочное прогнозирование и регулирование представляет собой необходимый элемент экономической политики, ориентированной на обеспечение структурной трансформации экономики в соответствии с новейшими мировыми тенденциями. В рамках долгосрочной структурной регулирующей деятельности государства осуществляется разработка и реализация среднесрочных программ развития. В свою очередь, в рамках среднесрочных программ осуществляется краткосрочное государственное планирование и регулирование экономики и социальной сферы.

Планирование в том или ином виде осуществляется во многих странах, в частности, во Франции, Китае, Японии, Южной Корее, США и других странах. Практика использования планирования в разных странах мира доказала его эффективность, поэтому можно согласиться с мнением западных ученых о том, что «недальновидно и преждевременно списывать планирование как устаревшее» [15, с.134].

Таким образом, опыт западных стран свидетельствует о необходимости осуществления планирования как механизма реализации целей социально-экономического развития общества.

Решение масштабных общенациональных задач в настоящее время возможно лишь при использовании методов государственного регулирования и планирования. Однако здесь есть определенные сложности, которые связаны с тем, что в нашей стране планирование отождествляется с социализмом, а поэтому, как инструмент регулирования, сразу отвергается большинством населения. Планирование рассматривается в данном случае лишь как централизованно-директивное и в качестве аргументов против планирования вообще используются недостатки плановой системы.

Формирование системы планирования, соответствующей нашим изменившимся условиям «позволит эффективно достигать приоритетных целей развития экономики России» [13, с.38] и тем самым способствовать повышению качества и уровня жизни населения нашей страны.

СПИСОК ЛИТЕРАТУРЫ

1. *Алле М.* Условия эффективности в экономике. Пер. с фр. -М.: НИЦ «Наука для общества», 1998.
2. *Барр Р.* Политическая экономия. -М.: Международные отношения, 1995. Т.1.
3. *Игнатовский П.* Отечественный опыт планирования убеждает…// Экономист. -2007. -№ 7.
4. *Клоцвог Ф.* Ключевые подходы к регулированию экономики// Экономист. -2006. -№ 11.
5. Концепция стратегического развития России до 2010 года. -М.: Издательство ИСЭПН, 2001.
6. *Махотаева Ю.М.* Целеполагание в управлении региональными социально-экономическими системами. -Псков: Издательство ППИ, 2006.
7. *Маркс К., Энгельс Ф.* Соч. Т.20.
8. *Маркс К., Энгельс Ф.* Соч. Т.23.
9. *Мизес Людвиг фон.* Бюрократия. Запланированный хаос. Антикапиталистическая ментальность: Пер. с нем. -М.: Дело, 1993.
10. *Папава В.Г., Беридзе Т.А.* Очерки политической экономии посткоммунистического капитализма (опыт Грузии). -М., 2005.
11. Переходная экономика: теоретические аспекты, российские проблемы, мировой опыт/ Отв. ред. В.А.Мартынов, В.С.Автономов, И.М.Осадчая. -М.: ЗАО «Издательство «Экономика», 2004.
12. *Пешехонов В.А.* Планомерность и стоимость в социалистическом обществе. -Л.: Издательство ЛГУ, 1971.
13. *Попов А.* Планирование и формы собственности //Экономист. -2007. -№6.
14. *Рязанов В.Т.* Экономическое развитие России. Реформы и российское хозяйство в XIX-XX вв. -СПб. «Наука», 1998.
15. *Холланд С.* Планирование и смешанная экономика// Вопросы экономики. -1993. -№ 1.

А.А. Яковенко А.А. Пятина

ИННОВАЦИИ И РИСКИ В ОТРАСЛИ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

Ключевые слова: инновации, разработки, риск, финансы, ресурсы, производство.

В данной статье раскрываются главные аспекты в разработке инноваций. Рассматриваются основные пути развития инноваций в тенденции развития рисков.

A.A. Yakovenko, A.A. Pyatina

INNOVATIONS AND RISK IN THE COMMUNICATIONS INDUSTRY

North-Caucasian Branch of the Order of the Red Banner of Labor of the Federal State Budget Educational Institution of Higher Education "Moscow Technical University of Communication and Informatics", Rostov-on-Don, Russia

Keywords: innovation, development, risk, finance, resources, production.

This article reveals the main aspects in the development of innovation. Discusses the basic ways of promoting innovation in the development trends of risks

За последние годы термин «инновации» стал широко использоваться в политическом и научном обороте. Причем зачастую современные политики, включая высших государственных деятелей, пытаются представить инновационную деятельность как некоторое новшество, являющееся продуктом современной стадии существования российской государственности. Делается это либо из-за незнания или с целью дискредитации истории становления, существования и развития советского периода страны с названием «СССР». Более чем за семидесятилетнюю историю осуществлялась целенаправленная политика и реальные действия государства, научно-технической и производственной общественности по разработке и реализации программ научно-технического прогресса во всех сферах жизнедеятельности общества. Рационализаторские предложения и изобретения, огромный объем научно-исследовательских и опытно-конструкторских работ, глобальные исследования ученых с мировым именем, практические разработки многочисленных научных центров, конструкторско-технологических подразделений производств создавали значимый потенциал страны и обеспечивали ей передовые позиции на мировом уровне. Советское общество, жившее многие десятилетия в условиях планово-директивной, распределительной системы, во многом было перспективно предсказуемо и текущее гарантированно защищено.

К сожалению, за чуть более десятилетний период псевдодемократических преобразований выделение ресурсов на эти цели резко сократилось. Значительный объем

научно-производственного базиса разрушен и уничтожен. Россия скатилась по этим показателям в мировом исчислении до уровня развивающихся стран. В списке ведущих мировых компаний одна из самых значимых в России «Газпром» занимает 144 место с долей НИОКР в выручке 0,67 процента и отрицательно растущей динамикой за последние годы.

Современный период формирования и становления рыночных отношений в России сопровождается большим количеством неясных и непредвиденных ситуаций. Лишь изредка проявляются те или иные примеры инновационных решений и результатов, которые чаще всего базируются на научно-технических разработках былых времен. Нынешнее состояние сопровождается разнообразными опасностями, неожиданно возникающими осложнениями, когда риски и связанные с ними операционные издержки растут не по дням, а по часам. Значительная часть общества реально представляет, что без принятия радикальных действий по всему фронту научно-технического прогресса не только будет сдерживаться общее социально-экономическое развитие, но и приведет Россию к полной деградации.

При осуществлении любого вида хозяйственной деятельности всегда возникает опасность рисков, объем которых обусловлен спецификой конкретных условий. Риски представляют собой совокупность проблем, возникающих из-за несоответствия между действиями организации или компании с теоретическими представлениями о возможно достижимых целях или планируемых результатах. Их можно виртуально представить еще на стадии разработки стратегического плана и необходимых для его реализации краткосрочных оперативных, реалистических действий.

Управление риском постепенно становиться составной частью общей системы хозяйствования. Угрозам могут быть подвержены такие самые важные активы, как земля и оборудование, технология и финансовые структуры, поставщики или клиенты, служащие, саморепутация как достояние организации.

Современные проблемы и тенденции развития риск - менеджмента в последнее время всё больше привлекают внимание отечественных исследователей и предпринимателей. Как и их западные коллеги, они сталкиваются с многочисленными рисками, связанными с рыночными факторами, как внутри страны, так и во внешней сфере.

Риск всегда является неотъемлемой частью управленческой деятельности, выбора форм экономического поведения и тем более в сфере инновационной деятельности. И даже тогда, когда производственные отношения отработаны годами, достаточно стабильны и не предвещают каких-либо осложнений, неожиданный субъективный фактор, зависящий только от одного человека или техническая случайность, могут привести к непредсказуемым последствиям. Что касается нового дела, то риск выступает одним из решающих факторов скорости, качества достижения цели, возможного провала и банкротства. Поэтому величайшей способностью любого менеджера и предпринимателя должно быть умение распознать зыбкую грань между разумной предприимчивостью и безрассудством.

Известны два взгляда на сущность риска:

– это возможная неудача, материальные или финансовые потери, которые могут наступать в результате реализации конкретных решений;

– когда риск отождествляют с предполагаемой удачей, благоприятным исходом, извлечением прибыли или доходом.

Знание подходов к проблемам риска и его оценки практически необходимо при разработке управленческих решений. Риск может возникнуть на стадиях изучения, прогнозирования, при предпроектных проработках, а также может иметь место риск действий, связанный с управлением объектом. Риск-менеджмент должен стать неотъемлемой частью каждого преуспевающего предприятия.

Все риски можно также сгруппировать по следующим категориям.

Организационно-правовые – это риски, связанные с ошибками менеджмента компании, её сотрудников, проблемами системы внутреннего контроля, плохо разработанными правилами работ, то есть риски, связанные с внутренней организацией работы компании.

Правовой риск – риск того, что соглашение между участниками окажется невозможно выполнить по действующему законодательству или же, что соглашение окажется не надлежащим образом оформленным.

Производственно-технологические – риски из-за несовершенства технологи производства нанесения ущерба окружающей среде (экологический риск), возможность возникновения аварий, пожаров, поломок, нарушения условий функционирования объекта вследствие ошибок при проектировании и монтаже, выполнение строительных работ и пр.

Ресурсные – это риски, связанные с фундаментальными (ресурсными) факторами осуществления бизнеса, конкурентоспособности предприятия и его продукции, реализация которых может привести к отсутствию ожидаемой стабильности или к существенному ухудшению конкурентной позиции предприятия на рынке.

Финансовые – риски, которые возникают в процессе отношений предприятия с финансовыми институтами (банками, инвестиционными, страховыми компаниями, биржами и др.). Причинами финансового риска чаще всего являются инфляционные факторы, изменение учетных ставок банка, курсов валют, снижение стоимости ценных бумаг и др.

Коммерческие – это риски, возникающие в процессе реализации товаров и услуг. Основными причинами коммерческого риска являются: колебания рынков, снижение объемов реализации товара, повышение закупочной цены на исходные компоненты, непредвиденное снижение объемов закупок товаров по сравнению с намеченным, утрата товара, потери его качества в процессе обращения, повышение издержек обращения.

Конкурентного взаимодействия на рынке. Под риском в конкуренции (или конкурентным риском) понимается состояние относительной неопределенности, присущее конкурентным действиям, результативность которых не представляется очевидной и имеет вероятностный характер. Действуя в состоянии относительной неопределенности, субъекты бизнеса вынуждены рисковать, ибо они не уверены в непременно благоприятном для них исходе соперничества.

Эти и многие другие аспекты реальной жизни всегда сопровождают сложные этапы инновационной деятельности и выступают в качестве разнообразных рисков. Представив обобщенно примерную классификацию различных критерий рисков, возникает необходимость раскрыть, хотя бы в общих чертах, опасности, которые они за собой несут.

Можно много говорить о несовершенстве нормативно-правовой базы, определяющей разнообразные аспекты инновационной деятельности. В базовом

законодательстве следует четко регламентировать уровни инновационной деятельности от хозяйствующего субъекта, предпринимательской структуры до субъектно-регионального и федерального. При этом следует четко определить систему участия ресурсного обеспечения, формы государственного участия и регулирования.

Любая предпринимательская и управленческая деятельность строится на основе целеполагания и формирования организационных структур, в рамках которых идет разработка и реализация инновационных программ. Поэтому одним из важнейших аспектов успеха является выбор её оптимальной структуры, кадровой иерархии и системы управления. С одной стороны, стабильный, устоявшийся коллектив, налаженная система взаимодействия дают надежды на успешную реализацию любого нового замысла. С другой стороны, как при положительных, так и отрицательных результатах даже в благополучных коллективах развиваются и укрепляются консервативные позиции стабильности, желание «ничего не менять». Поэтому кадровому менеджменту самое главное внимание при разработке инновационных программ следует уделять прогнозированию адаптационного восприятия сотрудниками планируемых новаций для реальной практики. И если действующий состав не в состоянии самостоятельно перестроиться на инновационный лад, то надо, либо насильственно перестраивать его мышление, либо подбирать новые кадры.

Не менее важными являются риски в сфере производственно-технологической деятельности. Здесь всегда имеют место классические противоречия между созидательными структурами в образе конструкторско-дизайнерских и технологических структур. Одни стремятся к разработке и созданию образцов новых товаров и услуг, соответствующих самым изысканным запросам потребителей, другим приоритетам на конкурентном рынке. Другие, практически всегда противоборствуют этому из-за невозможности обеспечить технологически-производственные условия реализации новых прогрессивных замыслов разработчиков.

Разработка и реализация инновационных идей всегда влечет за собой поиск и использование новых ресурсных возможностей. Именно производители тех или иных товаров, услуг вызывают необходимость появления новых материалов, оборудования, технологий. При нынешней отсталости и запущенности производственного потенциала в России возникает острая необходимость возрождения, а точнее создания новых видов оборудования, инструментов, соответствующих самым современным требованиям, либо их интенсивной закупки за рубежом. Но последний вариант упирается в непреодолимые таможенные пошлины и барьеры, о которых все говорят, но никто ничего не предпринимает по их разрешению. Поэтому производственно-технологические возможности любого хозяйствующего субъекта являются сдерживающим фактором.

При разработке и реализации инновационных программ особого внимания заслуживает отношение к капиталу инвесторов, предназначенному для финансирования новых растущих или борющихся за место на рынке предприятий и фирм. Здесь любые решения сопряжены с высокой или относительно высокой степенью риска формирования портфеля долгосрочных инноваций, вложениями в рискованные ценные бумаги или предприятия.

Особенно ответственными должно быть отношение к венчурному капиталу, который формируется за счет прямых частных инвестиций обычно предоставляется внешними инвесторами для формирования новых или растущих компаний, преодоления

возможного банкротства или для реинженеринговых преобразований ключевых бизнес-проектов. Следует обязательно учитывать, что венчурный капитал это, как правило, рискованные инвестиции, обладающие потенциальной доходностью выше среднего уровня. При этом важно учитывать, что обычно разработчики реально рассчитывают на соответствующий объем ресурсов. Поэтому они должны иметь базовый план, целевой, ориентированный на достижение важных промежуточных результатов, и план, сопряженный с возможными рисками и механизмами их преодоления.

В заключении следует сказать еще об одном важном обстоятельстве – рисках связанных с востребованностью инноваций и их рыночной конкурентоспособностью. Во все времена и в большинстве стран «паровозиками прогресса» выступают определенные ключевые отрасли экономики. Если в стране значительный приоритет отводится военно-промышленному комплексу и его конкурентоспособности на мировом рынке, то разработка и реализация инновационных программ вызовет необходимость инновационных преобразований во многих смежных сферах и производствах, поставляющих основные материалы, компоненты, комплектующие изделия. Если приоритет отдается сельскохозяйственному производству, продовольственной безопасности страны, то качественное развитие агропромышленного комплекса будет возможно только тогда, когда прогрессивно и целенаправленно будут работать на достижение собственных целей десятки отраслей и прежде всего агрохимический комплекс, в целом транспортное и сельскохозяйственное машиностроение, предприятия производящие и поставляющие горюче-смазочные материалы, технологическое оборудование для переработки сельхозсырья в продукты питания и многие другие отрасли. При этом, как бы ни отрицали этот принцип либералы, в масштабах государства должна существовать долгосрочная система целеполагания, государственного регулирования в рамках цивилизованной мировой практики, обеспечения страховых гарантий и много другого, что обеспечит инновационность преобразований. Декларации о том, что «рынок сам себя сформирует и обеспечит эффективное функционирование всей российской социально-экономической системы», оказались несостоятельными.

Важнейшим качеством для менеджмента любого уровня является постоянный мониторинг ситуации, анализ происходящего и корректирующее воздействие с целью достижения планируемых целей или результатов. При этом следует постоянно помнить, что любое управление граничит с риском.

СПИСОК ЛИТЕРАТУРЫ

1. *Агафонова И.П.* Риск как объект управления при реализации инновационного проекта// Экономическое преобразование в России: проблемы и перспективы. Межвузовский сборник научных трудов. -2002. -№ 3.
2. *Балдин К.В., Воробьев С.Н.* Риск-менеджмент: Учебное пособие. -М.: Гардарики, 2005.
3. *Иванченко Л.А.* Основы успеха: теория и практика менеджмента. -М.: Мысль, 2003.
4. *Иванченко Л.А. и др.* Менеджмент в условиях инвестиционной и инновационной активности. –Ростов н/Д: Росиздат, 2008.
5. *Рыхтикова Н.А.* Анализ и управление рисками организации: учебное пособие. -М.: ФОРУМ, ИНФРА-М, 2008.

6. *Черкасов В.В.* Проблемы риска в управленческой деятельности: Монография. -М.: Рефл-бук, Киев: Валер, 2003.
7. *Уколов В.Ф.* Инновационный менеджмент в государственной сфере и бизнесе. –М: ЗАО «Издательство экономика», 2009.
8. *Черкасова В.А., Батенкова А.А.* Влияние стратегических рисков на финансовые результаты компании//Корпоративные финансы: электронный научный журнал. -2007. -№ 3.
9. www.ecsocman.edu.ru

А.А. Яковенко, О.О. Шадрунова

СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ БЕДНОСТИ И СОЦИАЛЬНОГО НЕРАВЕНСТВА В РОССИЙСКОМ ОБЩЕСТВЕ

Северо-Кавказский филиал Московского Технического Университета Связи и Информатики,
г. Ростов-на-Дону, Россия.

Ключевые слова: Бедность, безработица, ресурсы, преступность, потребность, поведение, мотивация.

Описана проблема формирования безработицы в стране и пути решения. Раскрывается суть и причины развития бедности и социального неравенства в Российском обществе, а так же последствия.

A.A.Yakovenko , O.O. Shadrunova

STATISTICAL STUDY OF POVERTY AND SOCIAL INEQUALITY IN THE RUSSIAN SOCIETY

North-Caucasian Branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia.

Keywords: Poverty, unemployment, resources, crime, need, behavior, motivation.

The article describes the problem of formation of unemployment in the country and a way of the decision is described. The essence and causes of the development of poverty and social inequality in Russian society, as well as the consequences are revealed

«Бедность порождает бунт и преступления»
Аристотель

Бедность – фундаментальная глобальная проблема, стоящая перед мировым сообществом. Она оказывает пагубное влияние на различные аспекты общественной жизни и ее организацию. То обстоятельство, что сегодня нищета, бедность, отсталость характерны прежде всего для слаборазвитых стран мира, не делает проблему менее актуальной по отношению к другим государствам. Неспособность большинства беднейших стран вырваться из нищеты собственными силами сделала проблему бедности общепланетарной, поскольку на данный момент более 1,5 млрд. людей живут за чертой бедности. Об этом свидетельствуют материалы ООН, доклады Всемирного банка, других международных организаций, повестки дня саммитов «восьмерки» и «двадцатки». Важнейшей инициативой на мировом уровне стал саммит ООН в Нью-Йорке, сформулировавший в 2000 году «Цели развития тысячелетия». Именно тогда первое место в списке задач, которые человечество должно решить к 2015 году, заняло сокращение в два раза числа нищих и голодающих людей в мире по сравнению с 1990 годом [1].

Историческая ретроспектива свидетельствует о снижении государственного участия в регулировании социально-экономических отношений, а правовые и моральные ограничения все в большей степени носят относительный характер, тогда как ничем не контролируемые рыночные силы, углубляя социальное неравенство, увеличивают разрыв между самыми богатыми и самыми бедными. Такую тенденцию сегодня можно наблюдать как в мире в целом, так и внутри отдельных обществ. Бедность сказывается на уровне и облике правового порядка, сопряжена с резким расслоением или практически социальной поляризацией населения по уровню доходов, о чем свидетельствуют данные Всемирного банка, так, например, средние доходы в 20-ти наиболее богатых странах мира в 37 раз превышают средние доходы в 20 беднейших и за последние 40 лет этот разрыв удвоился (табл.) [2].

Степень социально-экономического расслоения и бедность населения

	Годы	Доля доходов (потребительских расходов), приходящаяся на каждую из 20-процентных групп населения					Коэффициент Джини	Коэффициент фондов (в разах)	Годы	Уровень бедности
		I	II	III	IV	V				
Россия[2)]	2008	5,1	9,8	14,8	22,5	47,8	42,2	16,8	2008	13,4
	2009	5,1	9,8	14,8	22,5	47,8	42,2	16,7	2009	13,2
США[2)]	2000	5,4	10,7	15,7	22,4	45,8	40,8	15,9	2007	12,5
Мексика[3)]	2008	3,8	8,1	12,4	19,2	56,4	51,6	34,4	2004	47,0
Китай[2)]	2005	5,7	9,8	14,7	22,0	47,8	41,5	13,1	2004	2,8

Проблема бедности в различных странах и регионах мира имеет свои особенности. В Восточной Азии количество людей, живущих менее чем на 1 долл. В день сокращается, а в странах Африки в государствах Восточной Европы и средней Азии оно растет.

Существенные различия в распространении бедности отмечаются также внутри стран. Это можно наблюдать и в России. Большинство исследователей данной проблематики считают, что следует учитывать уровень экономического развития страны: какая экономика, такие и доходы. В 2003 году доходы населения составляли в России в среднедушевом выражении 4 690 долл., то есть 95 % от среднемирового уровня. Личные доходы в расчете на душу населения в России равнялись 17,9 % от уровня США, 28,8 % от уровня Германии, 29,7 % от уровня Японии и 211,7 % от уровня Китая. Для России, вполне естественно, что 70 - 80% населения живут исключительно от зарплаты до зарплаты. Некоторые эксперты считают, что в любом случае действует известный оптимум Парето 20/80, согласно которому меньшая часть усилий и меньшая часть людей дает большую часть результатов. В частности, 20% клиентов дают 80% выручки, 20% сотрудников обеспечивают 80% дела, 20% людей выпивают 80% пива в мире и т.д. Соответственно, труд 10 - 20% наиболее динамичных россиян имеет критически важное, можно сказать, решающее значение для нашей экономики" [1]. Некоторые специалисты берут на себя смелость утверждать, что существующий в стране уровень социального неравенства несет в себе положительный заряд, обеспечивая более сильные мотивации для труда, необходимое стимулирование деловой и социальной активности населения [2].

Возникает вопрос: «Почему в такой богатой природными ресурсами стране так много бедных?» Основная проблема заключается, по всей видимости, не в том, что у нашей страны не хватает ресурсов для того, чтобы обеспечить каждому человеку право на достойную жизнь и возможность получения необходимых для этого доходов. Главные препятствия, как полагают эксперты, кроются в неумении, иногда в нежелании, этими богатейшими ресурсами рационально распоряжаться [3].

Когда исследователь исходит из того, что 20% крепко стоящих на ногах россиян (почти 29 млн. человек) - это хороший показатель, свидетельствующий о позитивной социальной динамике, но при этом не принимает в расчет житейские проблемы остальной части населения, вынужденной ежемесячно сводить концы с концами.

Глубокое расслоение по уровню доходов вовсе не усилило трудовую мотивацию современного русского человека. Наоборот, за годы рыночных реформ эта мотивация в значительной степени ослабла. Ощутимый и очевидный разрыв в доходах населения, который наблюдается в российском обществе, все реже выступает в качестве стимула позитивной деловой и социальной активности населения. Никто, конечно же, не хочет жить в бедности, тем более в нищете. Но для 80% россиян "лифт" восходящей социальной мобильности прочно застрял на "нижних этажах". Вырваться из цепких "объятий" нужды без поддержки государственных и социальных институтов удается не многим. К сожалению, в российской общественной жизни чаще срабатывает правило "социальной воронки" - больные рожают больных, бедные воспроизводят бедных. Из этой "воронки быстро не выберешься, потребуется смена не одного поколения" [5].

Масштаб и глубина социального неравенства в современной России выступают в качестве факторов, которые способны генерировать в общественном, групповом и индивидуальном сознании крайне негативные чувства и настроения. Сегодня сознание тех, кто не выиграл от реформ или в результате преобразований вообще оказался отброшенным на обочину жизни, наряду с разочарованием, апатией и пессимизмом нередко переполняется озлобленностью и ненавистью. В конечном итоге этот

эмоциональный негатив находит свой выход в различных моделях агрессивного, зачастую асоциального, противоправного и даже преступного, поведения [13].

Границей социально-правовой стабильности принято считать ситуацию, когда разрыв в доходах 10% наиболее и 10% наименее обеспеченного населения составляет не более 10 раз [2]. Это своего рода "критический предел". Если децильный коэффициент превышает указанное значение (в России децильный коэффициент – 16,8 раз), то это свидетельствует о нарастании социально-правовой напряженности в обществе, возникновении предпосылок для развития опасных тенденций, включая рост преступности (в самых различных ее проявлениях: уличной, ситуативной, насильственной, детской), пьянства, наркомании, проституции.

Практически во всех российских регионах этот критический показатель давно уже превышен, а в некоторых субъектах Федерации имеет место его многократное "перекрытие". Так, по данным Росстата, децильный коэффициент в Москве в первом квартале 2010 г. достигал отметки 42,0; согласно экспертным оценкам, он давно "зашкаливает" за 50 [9]. Стоит ли после этого удивляться росту российской преступности? По результатам исследований специалистами РАН в 2006 г. уровень преступности в России достиг наивысшей отметки, тогда было зарегистрировано 2706 преступлений на 100 тысяч человек постоянного населения, в последние три года данный показатель понемногу снижается из-за сокращения численности населения.

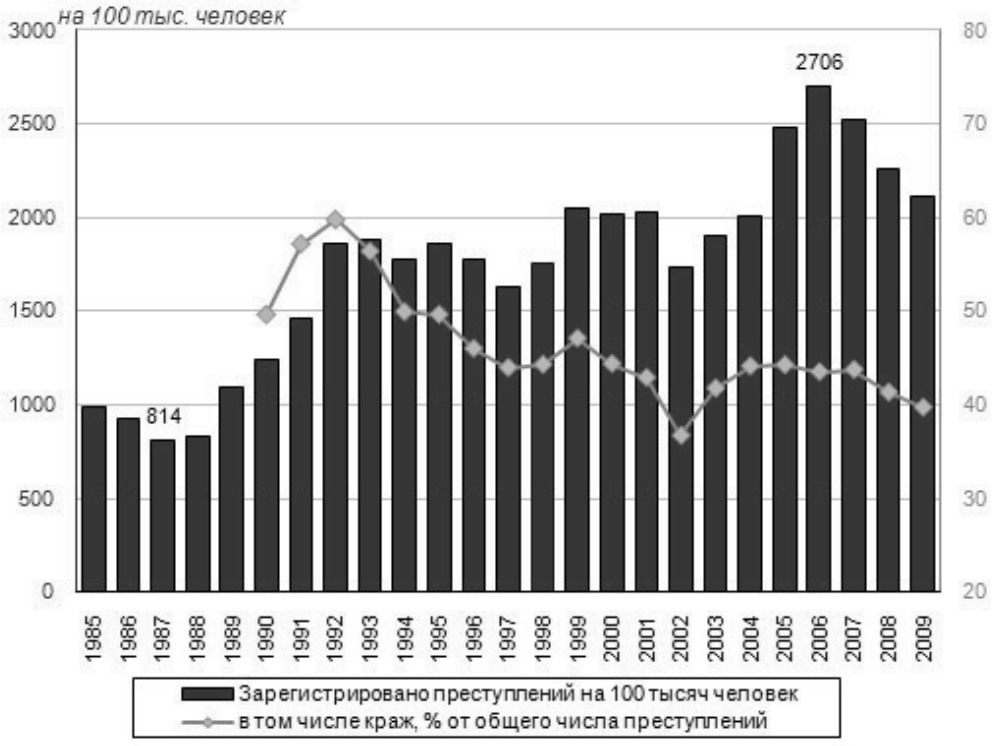


Рис. 1. Общий уровень преступности в России (число зарегистрированных преступлений на 100 тысяч человек постоянного населения) и доля краж в общем числе зарегистрированных преступлений (%), 1985-2009 годы

Наиболее высокий уровень преступности в 2009 году зарегистрирован в Пермском крае (3262 зарегистрированных преступлений на 100 тысяч постоянного населения), Иркутской области (3222), Республике Бурятия (3147), Хабаровском крае (3142).

Наиболее низкие значения - менее 500 на 100 тысяч человек - отмечаются в республиках Чечне, Ингушетии, Дагестане. Всего в 5 регионах-субъектах Российской Федерации было зарегистрировано менее 1000 преступлений в расчете на 100 тысяч человек, еще в 10 - от 1000 до 1500, а всего в 48 регионах ниже, чем в среднем по России (2110) [10].

Другим аспектом проблемы глубокого социального неравенства, который заслуживает особого внимания при рассмотрении вопросов, касается текущего состояния и тенденций развития правового порядка. "Если мы проследим историю революций в мире, а в особенности у нас в России, - писал академик Д.С. Львов, - то увидим, что революции происходили не там, где росла абсолютная величина бедности, а там, где соотношение между богатыми и бедными достигало предельных отметок. Нет другого такого параметра, который бы более точно указывал на эту опасность. Мы сегодня особенно близки к этому неблагополучному показателю, поскольку перед нами простирается социально-экономическое поле, где нет единой в социально-экономическом отношении страны.

Многое в суждениях известного российского экономиста представляется рационально выверенным. Верно, что наличие такой глубокой социальной дифференциации и по доходам, и по территории - это предвестник очень тревожных событий. Действительно, российский социум настолько неоднороден, что он становится взрывоопасным. В нем нарастает вероятность возникновения чрезвычайных положений, трудноразрешимых конфликтов, локальных беспорядков. Однако едва ли в современных российских условиях бедность (учитывая даже ее критические значения) способна выступить в качестве катализатора, приближающего момент, хотя бы отдаленно напоминающий революционную ситуацию [13].

Влияние бедности на правовую жизнь в современных социумах носит амбивалентный характер. С одной стороны, российская бедность в своих критических значениях (учитывая ее масштабы, запредельные показатели социального неравенства и др.) представляет серьезную угрозу для режима законности и задуманной законодателем (идеальной) модели правопорядка. Крайне бедственное положение людей в совокупности с другими негативными факторами зачастую провоцирует рост противоправного (в том числе преступного) поведения, тем самым разрушая идеальный образ правового порядка, который должен выстраиваться на основе прочного режима законности. Но это лишь видимая грань проблемы.

С другой стороны, та же бедность одновременно выступает как скрепа, по сути дела, "цементируя", пусть и не очень справедливый, далеко неэффективный, не слишком гармоничный, но реально существующий правовой порядок. Эта сторона проблемы не столь заметна, может быть, поэтому она зачастую упускается из виду многими исследователями. Между тем достоверность второй части тезиса не вызывает сомнений, если взглянуть на проблему через призму потребностей и интересов, которые во многом определяют поведенческую мотивацию социальных субъектов (пирамида А. Маслоу), то в структуре "пирамиды" выделяются потребности социального характера: в безопасности (включая свободу от страха и тревоги, осознание состояние защищенности, действенности порядка и закона); в принадлежности и любви; в признании; в самоактуализации. Потребности располагаются в строгом иерархическом порядке. Пока не удовлетворена потребность более низкого плана, остальные потребности могут даже не ощущаться человеком. Неудовлетворенная потребность обладает колоссальной энергией,

детерминируя поведение индивида. В то же время потребность, которая удовлетворена, может не играть никакой роли в текущей динамике его поведения.

Самыми насущными и мощными из всех потребностей являются потребности физиологические. "Если человеку нечего есть и если ему при этом не хватает любви и уважения, то все-таки в первую очередь он будет стремиться утолить свой физический голод, а не эмоциональный, - справедливо утверждал А. Маслоу. - Желание писать стихи, приобрести автомобиль, интерес к родной истории, страсть к желтым ботинкам - все эти интересы и желания либо блекнут, либо пропадают вовсе. Человека, чувствующего смертельный голод, не интересует ничего, кроме еды. Он мечтает только о еде, он вспоминает только еду..." [11].

Действительно, человек, живущий в условиях крайней нужды, движим прежде всего потребностями физиологического уровня. Это своего рода аксиома общественной жизни (теперь, к сожалению, и российской). Более высокий уровень социальных потребностей, включая идеи торжества законности, правопорядка, социальной справедливости, такого человека либо просто не волнует, либо на участие в решении этих проблем у него не остается ни физических, ни духовных сил. Нет ничего удивительного, что сегодня значительная часть россиян, оказавшись у порога бедности, демонстрируют социально-правовую индифферентность, что в конечном итоге служит укреплению существующего "порядка" вещей.

Для социального и правового порядков наличие большой армии бедняков, широкая известность бедственности их положения являются важными "уравновешивающими" факторами. В современных обществах бедность в своих критических значениях генерирует социально-правовую пассивность тех, кому есть что терять. Один только вид бедных, как отмечает известный западный социолог З. Бауман, держит обеспеченных в состоянии страха и покорности, ограничивая их воображение и связывая руки. Им не хватает отваги, чтобы вообразить иной мир, они становятся слишком осмотрительными, чтобы попытаться реформировать этот мир [13]. Между тем для изменения существующего несправедливого порядка требуются проявление элементарной солидарности, стремление и желание реализовать общие интересы. Однако солидарность в современном российском социуме - дефицит, в лучшем случае она срабатывает по линии "свой - чужой". Разобщенность, пожалуй, сегодня в большей степени определяет характер социальных связей в нашем обществе.

Изложенное выше свидетельствует, что бедность, учитывая ее критические показатели, есть серьезный барьер на пути становления эффективного правового порядка в современной России. Вот почему ее ликвидация - это одна из ключевых проблем, стоящих сегодня перед Российским государством и обществом. Ее успешное решение требует активных, системных, согласованных действий государственных и общественных институтов. Социально-экономическая политика Российского государства должна быть в большей степени ориентирована на поддержание доступного и достойного уровня жизни членов общества, уменьшение в нем остроты и социальной напряженности, предотвращение социальных расколов и конфликтов.

Социальные институты, которые претендуют на то, чтобы гордо называться гражданским обществом, не должны оставаться в стороне от этой масштабной задачи. Их усилия должны быть направлены на то, чтобы воспрепятствовать воспроизводству в

общественной жизни противоправных моделей поведения, социально-правовой пассивности и индифферентности, неуверенности и разобщенности российских граждан.

Не менее сложные задачи стоят и перед представителями научного сообщества, от которых государство и социум ждут рационально выверенных рекомендаций по исправлению кризисной ситуации в социально-правовой сфере, а не всевозможных спекуляций по этому поводу. Пока масштабы и уровень бедности в нашей стране будут оставаться на прежнем уровне, до тех пор надежды на обеспечение устойчивого и прогрессивного развития обновленной России останутся недостижимыми.

СПИСОК ЛИТЕРАТУРЫ

1. *Бауман З.* Индивидуализированное общество. -М., 2005. С. 147.
2. Деньги к деньгам // Российская газета. 2008. 13 августа. Краткий анализ состояния преступности. 20.02.2010. - Министерство внутренних дел Российской Федерации. - www.mvd.ru Главная / Статистика / Статистика за 2009 год / Состояние преступности в Российской Федерации за декабрь 2009 года / Краткий анализ состояния преступности
3. *Львов Д.С.* Будущее Запада в будущем России // Русский журнал. 2007. N 6. С. 45.
4. *Мамут Л.С.* Социальное государство с точки зрения права // Государство и право. - 2001. -№ 7. С. 7 - 8.
5. *Маслоу А.* Мотивация и личность. СПб. 1999. С. 79 - 80.
6. *Петров Н.П.* Бедность как глобальная проблема: взаимозависимость стала причиной взаимной уязвимости// http://www.ng.ru/scenario/2010-11-23/12_dno.html
7. *Пятенко С.В.* Расслоение: играем на своем уровне // Ведомости. 2007.
8. *Римашевская Н.М.* Качество человеческого потенциала в России // Возвращение Питирима Сорокина. Материалы Международного научного симпозиума, посвященного 110-летию со дня рождения П.А. Сорокина. М., 2000. С. 283 - 284.
9. *Сауляк О.П.* Государство и общественные институты как субъекты обеспечения правопорядка в современной России / Актуальные проблемы современного российского государствоведения: сб. научных трудов. Вып.2, 2009 / Под общ. Ред. С.Н. Бабурина. – М.: Изд-во РТГЭУ, 2009.
10. *Сауляк О.П.* Социально-экономическая поляризация в современной России как детерминанта законности и правопорядка // Кавказские научные записки. -2009.
11. *Сауляк О.П.* Сущность правопорядка: теоретико-методологическое исследование// http://dibase.ru/article/12042010_saulyakop/4
12. Социальное положение и уровень жизни населения России – 2010// Стат. Сборник. -М., Росстат 2011.
13. *Щербакова Е.* Преступность в России сокращается третий год подряд //http://www.demoscope.ru/weekly/2010/0413/barom01.php

КРАТКИЕ СВЕДЕНИЯ ОБ АВТОРАХ

1. **Абрамов Иван Сергеевич**, студент 3 курса. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
2. **Абрамова Надежда Игоревна**, преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ» (Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий)
3. **Акулин Павел Петрович**, студент. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
4. **Алтунин Федор Александрович**, магистрант. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
5. **Аль Ясири Джамаль Хамид Абдул Адим**, студент 2 года магистратуры. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
6. **Амирсаидов Улугбек Бабурович**, к.т.н., доцент. Ташкентский университет информационных технологий
7. **Артеменкова Анжелика Сергеевна**, студент 5-го курса. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
8. **Артынов Константин Артурович**, студент курс 4, ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
9. **Астрецов Дмитрий Вячеславович**, профессор кафедры ОПДТС, к.т.н., профессор. Уральский технический институт связи и информатики (филиал), г. Екатеринбург, Россия
10. **Бабаян Армен Хачикович**, Технологический институт (филиал) Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ) в г. Азове
11. **Бабычев Алексей Михайлович**, студент магистратуры. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
12. **Бадыштова Кристина Дмитриевна**, студентка ДВ-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

13. **Баженов Михаил Константинович**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
14. **Баранов Сергей Анатольевич**, к.т.н., доцент кафедры ОПДТС. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
15. **Бармина Екатерина Вадимовна**, студент магистратуры. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
16. **Батенков Кирилл Александрович**, доцент. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
17. **Белянчикова Мария Павловна**, аспирант кафедры экономики связи. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
18. **Безруков Игорь Михайлович**, студент 1-го курса магистратуры, группа М61601. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
19. **Безуглый Юрий Андреевич**, курсант. Военная академия связи им. Маршала Советского Союза С.М. Буденного.
20. **Безумнов Данил Николаевич**, ассистент кафедры ИСУиА. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
21. **Белан Надежда Викторовна**, магистрант. ФГАОУ ВПО Северо-Кавказский федеральный университет
22. **Беленькая Марина Наумовна**, доцент. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
23. **Бикбулатова Наталья Генриховна,** старший преподаватель кафедры ИСТ. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
24. **Бинеев Энвер Абдулхакович**, к.х.н., профессор кафедры ОНП, профессор. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
25. **Боковеев Денис Сергеевич,** студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)

26. **Болдырихин Николай Вячеславович**, доцент кафедры СССК, к.т.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
27. **Борисенко Николай Павлович,** к.т.н., профессор, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
28. **Борисов Борис Петрович**, доцент, к.т.н, доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
29. **Бородин Алексей Викторович**, к.физ.-мат.н., доцент кафедры ОНП. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
30. **Боярчук Андрей Эдуардович**, профессор кафедры, к.т.н., профессор. г. Ростов-на-Дону. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
31. **Бражуненко Павел Сергеевич**, студент 2-ого курса магистратуры. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
32. **Брежный Игорь Андреевич**, магистрант, студент группы ВМВТ11, Специализация: Методы и системы принятия решений, Специальность: Информатика и вычислительная техника, Кафедра: "Кибербезопасность информационных систем". Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
33. **Будылдина Надежда Вениаминовна**, заместитель заведующего кафедрой ОПД ТС, доцент, к.т.н. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
34. **Букрина Екатерина Владимировна**, к.э.н., доцент кафедры Многоканальной электрической связи. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
35. **Бурдюг Владислав Владимирович**, курсант. Военный учебно-научный центр ВВС «Военно-воздушная академия им. профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
36. **Быстров Сергей Александрович**, старший преподаватель кафедры ОПД ТС. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
37. **Варакосов Дмитрий Викторович**, курсант 206 учебной группы. Уральский юридический институт МВД России

38. **Васинев Дмитрий Александрович**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
39. **Вернигорова Наталья Александровна**, студентка гр. ДЭ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
40. **Вершенник Алексей Васильевич**, преподаватель кафедры Безопасности инфокоммуникационных систем специального назначения. Военная академия связи им. Маршала Советского Союза С.М. Буденного
41. **Водовозов Илья Витальевич**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
42. **Волгарев Евгений Алексеевич**, аспирант 3 курса кафедры ВМиФ. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
43. **Галкин Алексей Сергеевич**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
44. **Галухин Михаил Александрович**, студент гр.ДЭ-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
45. **Гатилова Елена Александровна**, студент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
46. **Герасименко Виктор Евгеньевич**, 2 курс магистратуры физфака. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
47. **Гизатуллин Марат Галимянович**, доцент кафедры информационного обеспечения органов внутренних дел, кандидат технических наук, доцент. Уральский юридический институт МВД России
48. **Гирин Иван Сергеевич**, студент группы ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
49. **Глушак Елена Владимировна**, доцент кафедры АЭС ПГУТИ. ФГБОУ ВО Поволжский государственный университет телекоммуникаций и информатики
50. **Гниломёдов Ефим Иванович**, доцент кафедры МЭС. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

51. **Говор Светлана Александровна**, аспирант. Московский государственный технический университет им. Н.Э. Баумана
52. **Головина Ирина Витальевна**, доцент кафедры ЭиУ, доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
53. **Головской Василий Андреевич**, старший научный сотрудник отдела научно-исследовательской работы и инновационного развития, к.т.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
54. **Гончаров Артём Александрович**, студент группы ДЭ-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
55. **Гончарова Оксана Владимировна**, к.э.н., доцент кафедры ЭиУ, заместитель декана по ВР. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
56. **Горохова Екатерина Александровна**, магистрант. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
57. **Горшенин Николай Олегович**, студент. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
58. **Грабовый Кирилл Дмитриевич**, студент группы ДВ-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
59. **Григорьев Илья Дмитриевич**, магистрант. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
60. **Давыдов Роман Вадимович**, магистрант. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
61. **Данилова Наталья Викторовна**, доцент, к.ф.-м.н., доцент. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
62. **Данилов Виктор Александрович**, профессор, д.т.н., профессор. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального

государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

63. **Данилова Людмила Викторовна**, доцент, к.ф.-м.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный университет путей сообщения» (ФГБОУ ВО «Ростовский государственный университет путей сообщения» ФГБОУ ВО РГУПС, РГУПС)
64. **Данилова Анастасия Михайловна**, магистрант 2-го курса. Ташкентский университет информационных технологий
65. **Денисов Владислав Юрьевич**, магистр. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
66. **Денисов Дмитрий Вадимович,** к.т.н., доцент кафедры ОПДТС. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
67. **Дерканосов Максим Александрович**, студент группы ДВ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
68. **Деркачев Игорь Сергеевич**, младший научный сотрудник, к.т.н. Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия
69. **Детко Герман Валерьевич**. Мастер по обслуживанию абонентов. Крыловский ЛТЦ Краснодарского края ПАО «Ростелеком»
70. **Демидов Дмитрий Евгеньевич**, бакалавр гр.Э-45Б. Уральский технический институт связи и информатики (филиал СибГУТИ)
71. **Докучаев Сергей Аркадьевич**, ст. преподаватель. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
72. **Долинер Леонид Исаевич**, профессор кафедры ИСТ, д.п.н., профессор. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
73. **Доткулова Анастасия Сергеевна**, ассистент. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
74. **Евдакова Лилия Николаевна**, зав. кафедрой экономики связи, к.э.н., доцент. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

75. **Евстафьев Вячеслав Владимирович**, доцент кафедры, к.т.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
76. **Елисеев Александр Вячеславович**, профессор кафедры «Радиоэлектроника», д.т.н., доцент. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
77. **Елфимов Михаил Андреевич**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
78. **Енгибарян Ирина Алешаевна**, к.т.н., доцент кафедры МТС. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
79. **Ермолаев Андрей Владимирович**, студент курс 4, ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
80. **Ершов Валерий Васильевич**, доцент кафедры «Сети связи и системы коммутации», к.т.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
81. **Жабинский Юрий Вячеславович**, доцент кафедры СПОИ, к.т.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
82. **Жук Арсений Сергеевич**, начальник учебно-методического отдела. НЧОУ ВО «Кубанский институт информзащиты»
83. **Жуковский Александр Георгиевич**, заместитель директора по УВР,, д.п.н., к.т.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
84. **Зайченко Дмитрий Сергеевич**, бакалавр. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
85. **Зверев Алексей Петрович**, к.т.н., доцент кафедры инфокоммуникационных технологий и систем связи, доцент. Академия гражданской защиты МЧС России
86. **Зеленский Сергей Валентинович**. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»

87. **Зубарев Игорь Александрович**, доцент, к.п.н., полковник внутренней службы. Уральский институт Государственной противопожарной службы МЧС России, г. Екатеринбург, Россия
88. **Зуйков Алексей Петрович**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
89. **Игначкова Екатерина Валерьевна**, студент группы ДВ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
90. **Иевлев Олег Павлович**, декан факультета ИТ, к.т.н., доцент. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
91. **Ильиных Нина Иосифовна**, к.ф.-м.н, доцент кафедры ВМиФ. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
92. **Ишдавлетова Эмине Талгатовна**, старший преподаватель. Ташкентский университет информационных технологий
93. **Калиенко Иван Викторович**, доцент кафедры «Радиоэлектроника», к.т.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
94. **Каличак Максим Геннадьевич**, студент. ГОУВПО «Донецкий национальный технический университет»
95. **Кальфа Александр Алексеевич**, д.ф.-м.н., проф. каф. МСиУС. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
96. **Карасев Иван Валентинович**, студент. ФГАОУ ВПО Северо-Кавказский федеральный университет
97. **Караченцев Вадим Григорьевич,** Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
98. **Каримова Венера Аркиновна**, кафедра «Информационные технологии», к.т.н., доцент. Ташкентский университет информационных технологий
99. **Карпов Евгений Анатольевич**, начальник НТЦ 3 «Инновационные разработки» АО ВНИИ «Градиент»
100. **Кашуба Константин Алексеевич**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
101. **Киреев Максим Олегович**, студент 4-го курса гр. ИКТр-33. Поволжский государственный университет телекоммуникаций и информатики

102. **Кириленко Николай Евгеньевич**, студент 2го курса магистратуры. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
103. **Кирхеев Артем Геннадьевич**, заместитель командира взвода. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко
104. **Клевакин Максим Александрович**, студент магистратуры. Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге
105. **Кносаль Вячеслав Михайлович**, магистрант. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
106. **Кобак Валерий Григорьевич**, профессор, д.т.н. доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
107. **Коломиец Елена Анатольевна**, студент группы ДС-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
108. **Колосков Алексей Владимирович**, студент ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
109. **Коновалов Игорь Сергеевич**, аспирант. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
110. **Коновалов Степан Валерьевич**, магистрант 2 курса. Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге
111. **Конева Светлана Ивановна**, старший преподаватель. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
112. **Конкин Борис Борисович**, заведующий кафедрой ОНП, к.т.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
113. **Коньшина Надежда Александровна**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)

114. **Королев Дмитрий Эдуардович**, Уральский технический институт связи и информатики (филиал), г. Екатеринбург, Россия
115. **Корчемкина Мария Николаевна**, курсант. Военная академия связи им. Маршала Советского Союза С.М. Буденного
116. **Коршун Анна Михайловна**, доцент кафедры СПОИ СКФ МТУСИ, к.г.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
117. **Косарева Екатерина Павловна**, студент гр.ДЭ-21. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
118. **Костецкая Галина Сергеевна**, доцент, к.ф.-.м.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
119. **Костюченко Джанета Владимировна**, старший преподаватель кафедры ОНП. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
120. **Красников Степан Олегович**, аспирант. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
121. **Краснопеев Сергей Михайлович**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
122. **Кривошей Н.И.**, аспирант. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
123. **Кильдишов Роман Михайлович**, Ведущий специалист КЦ Теле2-Ростов.
124. **Куанышев Валерий Таукенович**, доцент кафедры «Мультимедиа и мобильных систем», к.ф.-м.н. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «СибГУТИ», г. Екатеринбург, Россия
125. **Кудряшова Анастасия Юрьевна**, магистр 2 курса. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
126. **Кузнецов Сергей Иванович**, доцент кафедры Безопасности инфокоммуникационных систем специального назначения, кандидат технических наук, доцент. Военная академия связи им. Маршала Советского Союза С.М. Буденного
127. **Куликов Михаил Алексеевич**, курсант, рядовой. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»

128. **Куприянов Никита Алексеевич**, курсант. Военная академия связи им. Маршала Советского Союза С.М. Буденного
129. **Кусайкин Дмитрий Вячеславович**, доцент кафедры МЭС, к.т.н. Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге
130. **Ланко Дмитрий Александрович,** системный администратор ООО «Вилмари».
131. **Лаухин Александр Вячеславович**, 2 курс магистратуры физфака. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
132. **Лобзенко Павел Владимирович**, доцент кафедры СПОИ, к.т.н, Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
133. **Лукиенко Максим Алексеевич**, студент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
134. **Луганская Людмила Алексеевна**, сотрудник. ФГАОУ ВПО Северо-Кавказский федеральный университет
135. **Львов Владимир Леонтьевич**, старший преподаватель кафедры СПОИ. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
136. **Львов Кирилл Владимирович**, студент. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
137. **Максимов Денис Андреевич**, Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
138. **Малкова Ирина Андреевна**, аспирант 3 курса кафедры ВМиФ. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
139. **Манин Александр Анатольевич**, к.т.н., директор Северо-Кавказского филиала Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», доцент
140. **Маркин Дмитрий Олегович**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»

141. **Михайленко Юлиана Евгеньевна**, студент группы ВМ-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
142. **Мищук Евгений Михайлович**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
143. **Молоковский Игорь Алексеевич**, доцент кафедры АТ, к.т.н., доцент. ГОУВПО «Донецкий национальный технический университет»
144. **Момот Александр Иванович**, заведующий кафедрой ЭиУ, д.э.н., профессор. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
145. **Момот Роман Александрович,** студент 3-го курса. ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)»
146. **Мосева Марина Сергеевна**, ассистент. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
147. **Мухитдинова Муаззам Лутфулла** кизи, магистрант 1-го курса. Ташкентский университет информационных технологий
148. **Невельский Владислав Сергеевич**, магистрант. Уральский технический институт связи и информатики (филиал),г. Екатеринбург, Россия
149. **Новикова Ирина Анатольевна**, магистрант кафедры экономики связи. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
150. **Овсянников Сергей Николаевич**, аспирант. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
151. **Овчинников Дмитрий Александрович**, аспирант. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
152. **Опарин Алексей Юрьевич**, начальник отдела научно-исследовательской работы и инновационного развития, действительный член (академик) Международной академии наук экологии и безопасности жизнедеятельности, к.ф.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
153. **Орлов Владимир Георгиевич**, начальник научного отдела ИВД, к.т.н., доцент. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
154. **Павлова Анастасия Викторовна**, студентка 3-го курса. Федеральное государственное бюджетное образовательное учреждение высшего

профессионального образования «Донской государственный технический университет» (ДГТУ)

155. **Папаев Анатолий Борисович**, старший преподаватель кафедры «Мультимедиа и мобильных систем». Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «СибГУТИ», г. Екатеринбург, Россия
156. **Пащенко Ксения Владимировна**, студентка 3-го курса. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
157. **Пешкевич А.А.**, аспирант. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
158. **Полков Анатолий Анатольевич**, к.т.н., доцент, сотрудник, руководитель. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
159. **Полякова Марианна Витальевна**, аспирант. Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный университет путей сообщения» (ФГБОУ ВО «Ростовский государственный университет путей сообщения» ФГБОУ ВО РГУПС, РГУПС)
160. **Попова Анжелика Вячеславовна**, курсант. Военная академия связи им. Маршала Советского Союза С.М. Буденного
161. **Поркшеян Виталий Маркосович**, декан факультета «Информатика и вычислительная техника», к.т.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
162. **Портнов Эдуард Львович**, профессор, д.т.н., профессор. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
163. **Прыгунов Александр Германович**, доцент кафедры «Радиоэлектроника», к.т.н., доцент. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
164. **Пташинский Михаил Андреевич** студент 5-го курса. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
165. **Птицын Герман Александрович**, доцент кафедры ИСУиА МТУСИ, к.т.н., доцент. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
166. **Пузанов Алексей Станиславович**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
167. **Путилин Николай Витальевич**, заместитель начальника. Научно-технический отдел (дислокация г. Ростов-на-Дону) Федерального казенного учреждения

«Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации

168. **Пятина Анна Алексеевна**, студент гр.ДЭ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
169. **Рахимьянов Александр Вячеславович**, студент ВМ-51. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
170. **Ремез Ирина Геннадьевна**, старший преподаватель кафедры менеджмента связи. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
171. **Решетникова Ирина Витальевна**, доцент кафедры СССК, к.т.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
172. **Решетникова Ксения Алексеевна**, студент ДС-31. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
173. **Ролдугина К.А.**, студентка 4 курса. Ташкентский университет информационных технологий
174. **Ротова Елена Георгиевна** студент 5-го курса СКФ МТУСИ. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
175. **Руденко Николай Валерьевич**, доцент кафедры «Радиоэлектроника», к.т.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
176. **Руднев Алексей Николаевич**, к.т.н., доцент кафедры ИБ. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
177. **Рыбалко Игорь Петрович**, доцент кафедры СССК, к.т.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
178. **Самков Михаил Сергеевич**, Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

179. **Санников Артем Андреевич**, магистрант группы МИТЕ-61 кафедры «Мультимедиа и мобильных систем». Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «СибГУТИ», г. Екатеринбург, Россия
180. **Санникова Ксения Андреевна**. Уральский технический институт связи и информатики (филиал),г. Екатеринбург, Россия
181. **Сафарьян Ольга Александровна**, доцент, кандидат технических наук. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
182. **Сафронов Александр Игоревич**, инженер, Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
183. **Свирщ Елена Александровна,** ст. преподаватель. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
184. **Семенец Вячеслав Олегович**, аспирант. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
185. **Семиряд Никита Юрьевич**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
186. **Сидняев Николай Иванович**, заведующий кафедрой "Высшая математика" (ФН-1), д.т.н., профессор. Московский государственный технический университет им. Н.Э. Баумана
187. **Сидорина Татьяна Викторовна**, доцент кафедры: «Экономическая безопасность», учет и право, к.э.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
188. **Сильченко Владислав Витальевич**. Электромеханик ЛТЦ Руднянского р-на МЦТЭТ г. Камышин Волгоградского филиала ПАО Ростелеком
189. **Синева Ирина Сергеевна**, доцент, к.ф.-м.н., доцент. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
190. **Ситьков Иван Алексеевич**, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
191. **Скоробогатова Елена Анатольевна**, ст.преподаватель,кафедры экономики связи. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
192. **Смоляков Виктор Николаевич**, доцент кафедры СПОИ СКФ МТУСИ, ктн, доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения

высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия

193. **Совенко Дмитрий Сергеевич**, курсант, рядовой. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
194. **Соколов Сергей Викторович**, зав. Кафедрой СПОИ, д.т.н., профессор. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи
195. **Соколова Ольга Ивановна**, профессор, д.п.н., профессор. Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный университет путей сообщения» (ФГБОУ ВО «Ростовский государственный университет путей сообщения» ФГБОУ ВО РГУПС, РГУПС)
196. **Сосновский Иван Александрович**, декан заочного факультета, к.т.н. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
197. **Степская Ирина Алексеевна,** студент 5-го курса. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
198. **Стремоухов Михаил Владимирович,** сотрудник, к.т.н. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
199. **Сулименко Илья Юрьевич**, студент курс 4, ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
200. **Сумарокова Ольга Владимировна**, студент 4-го курса гр. ИКТр-33. ФГБОУ ВО Поволжский государственный университет телекоммуникаций и информатики
201. **Сухоев Алексей Павлович**, студент магистратуры. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
202. **Сухоева Ксения Сергеевна,** Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
203. **Сухорукова Елена Валерьевна**, старший преподаватель кафедры Безопасности инфокоммуникационных систем специального назначения. Военная академия связи им. Маршала Советского Союза С.М. Буденного
204. **Табунщикова Полина Михайловна**, Студент 1 курса, группа ДИ-11. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального

государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

205. **Таов Инал Нарзанович**, студент группы ДС-41. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
206. **Тарасов Евгений Сергеевич**, старший преподаватель. Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ) Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге (УрТИСИ СибГУТИ)
207. **Тесля Сергей Петрович**, старший преподаватель кафедры Безопасности инфокоммуникационных систем специального назначения. Военная академия связи им. Маршала Советского Союза С.М. Буденного
208. **Тимирбулатова Тамара Эдуардовна**, студент. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
209. **Тищенко Евгений Николаевич**, заведующий кафедрой информационных технологий и защиты информации, д.э.н., доцент. РГЭУ (РИНХ), г. Ростов-на-Дону
210. **Тлекова Элфира Равилевна**, студентка 4 курса кафедры «Связь». Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный технический университет»
211. **Трофименко Владимир Николаевич**, доцент каф. "Радиоэлектроника", к.т.н., доцент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
212. **Трофлянин Владимир Вадимович**, магистр 2 курса. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» 20.18.16.22.10
213. **Трухин Михаил Павлович**, к.т.н, доцент кафедры ОПД ТС. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
214. **Тураев Фаррух Икрамович**, иностранный обучающийся 306 И учебной группы. Уральский юридический институт МВД России
215. **Турсунов Шерзод Абдукодирович**, заведующий кафедрой «Менеджмент и маркетинг». Ташкентский университет информационных технологий.
216. **Тютюнникова Алина Игорьевна**, Студентка ДГТУ 1 курса магистратуры направление 09.04.01 «Информатика и вычислительная техника» («Методы и системы принятия решений»). Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)

217. **Уколова Светлана Александровна**, ст.преподаватель кафедры ЭиУ, к.э.н. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
218. **Уманов А.А.**, студент аспирантуры обучающийся по направлению 09.04.01 «Информатика и вычислительная техника». Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
219. **Усманова Наргиза Бахтиербековна**, к.т.н., доцент кафедры «Сети и системы передачи данных». Ташкентский Университет Информационных Технологий (ТУИТ) имени Аль Хорезми
220. **Усынин Марат Геннадьевич**, студент группы ДЗ-41. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
221. **Фатхи Владимир Ахатович**, заведующий кафедрой «Вычислительные системы и информационная безопасность», д.т.н., профессор, почетный работник высшего профессионального образования, заслуженный работник высшей школы РФ, академик Академии военных наук. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
222. **Фатхулин Тимур Джалилевич**, ассистент, аспирант. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
223. **Федотов Виталий Викторович**, руководитель направления ГСП КиГС, соискатель ученой степени кандидата экономических наук. Ростовский филиал. ПАО «Ростелеком»
224. Федотов Владислав Евгениевич, студент. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Донской государственный технический университет» (ДГТУ)
225. **Федотова Полина Чан Ен**, студент магистратуры. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
226. **Филиппов Андрей Павлович**, студент магистратуры. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
227. **Харченко Виктор Викторович**, заместитель начальника кафедры ВУНЦ ВВС «ВВА», к.т.н., доцент. Военный учебно-научный центр ВВС «Военно-воздушная академия им. профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
228. **Хурматов Роман Ильдарович,** Уральский технический институт связи и информатики (филиал),г. Екатеринбург, Россия

229. **Хушмуродов Комронбек Шамсидинович**, студент магистратуры. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
230. **Цибульский Евгений Александрович**, студент группы ДС-41. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
231. **Цыганов Александр Михайлович**, курсант, рядовой. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
232. **Черемных Вадим Геннадьевич**, магистрант. Уральский технический институт связи и информатики (филиал), г. Екатеринбург, Россия
233. **Чернышев Виталий Васильевич**. Печатник типографии «Lucky Pack», студент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия
234. Черпаченко Станислав Игоревич, студент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», Ростов-на-Дону, Россия
235. **Шадрин Андрей Анатольевич**, аспирант. Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)
236. **Шадрунова Ольга Олеговна**, студент гр.ДЭ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
237. **Шаповалов Александр Михайлович**, студент группы ДЭ-21. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
238. **Шаравова Ольга Ивановна**, доцент кафедры экономики связи, к.э.н., доцент. Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
239. **Швачко Олег Викторович**, научный сотрудник, к.ф.-м.н. Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации, г. Ростов-на-Дону, Россия
240. **Шестаков Иван Игоревич**, старший преподаватель кафедры МЭС. Федеральное агентство связи Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

241. **Шпилько Антон Сергеевич**, студент ДС-41. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
242. **Щербань Игорь Васильевич**, профессор кафедры, д.т.н., доцент. Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет, ФГАОУ «ЮФУ», ЮФУ)
243. **Юркин Андрей Анатольевич**, сотрудник. Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия ФСО России»
244. **Юхнов Василий Иванович**, заведующий кафедрой МТС, к.т.н., доцент. Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
245. **Явтушенко Павел Владимирович**, студент ДИ-11. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
246. **Яковенко Анатолий Алексеевич**, профессор кафедры ЭиУ, к.э.н., профессор. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
247. **Яковлев Дмитрий Александрович**, аспирант. Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»
248. **Янкина Ангелина Игоревна**, студент. Группы ДЗ-31. Северо-Кавказский филиал Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

АВТОРСКИЙ УКАЗАТЕЛЬ

Часть I

Акулин П.П. 19
Алтунин Ф.А. 22, 244
Аль Ясири Д.Х. 26
Амирсаидов У.Б. 33
Артынов К.А. 204
Астрецов Д.В. 511
Бабычев А.М. 42
Бадыштова К.Д. 235
Баженов М.К. 195
Баранов С.А. 338
Бармина Е.В. 48
Батенков К.А. 225, 352
Безруков И.М. 57
Безумнов Д.Н. 348
Беленькая М.Н. 472
Бикбулатова Н.Г. 477
Боковеев Д.С. 206
Болдырихин Н.В. 19, 22, 69, 244, 266, 327, 396
Борисов Б.П. 497
Бородин А.В. 72
Бражуненко П.С. 76
Брежный И.А. 83
Будылдина Н.В. 42
Букрина Е.В. 86
Бурдюг В.В. 501
Буренин А.Н. 91
Волгарев Е.А. 229
Волков В.С. 97
Герасименко В.Е. 108
Гирин И.С. 69
Глушак Е.В. 232
Горохова Е.А. 113
Горшенин Н.О. 121
Грабовый К.Д. 121
Григорьев И.Д. 128, 132
Давыдов Р.В. 22, 244
Данилов В.А. 138, 144, 147
Данилова Л.В. 147
Денисов Д.В. 152, 161, 175
Дерканосов М.А. 212
Детко Г.В. 414
Евстафьев В.В. 179, 195
Езин А.Н. 530
Елисеев А.В. 186
Елфимов М.А. 195, 291
Енгибарян И.А. 199
Ермолаев А.В. 199, 204
Ершов В.В. 206, 291
Жабинский Ю.В. 138
Жуковский А.Г. 251, 256, 261
Жуковский Д.А. 247
Зайченко Д.С. 400
Зверев А.П. 212, 219
Зеленский С.В. 225
Зубарев И.А. 296
Зуйков А.П. 179
Игначкова Е.В. 323
Иевлев О.П. 76
Ильиных Н.И. 48, 229, 437
Кабакова В.Г. 272
Каличак М.Г. 333
Кальфа А.А. 132
Караченцев В.Г 375
Карпов Е.А. 108
Кашуба К.А. 179
Киреев М.О. 232
Кириленко Н.Е. 235
Клевакин М.А. 237, 301
Кносаль В.М. 22, 244
Кобак В.Г. 247, 251, 256, 261, 280
Колосков А.В. 266
Конева С.И. 268, 272, 276
Коновалов И.С. 280
Коновалов С.В. 301
Константинова Я.Б. 286
Коньшина Н.А. 195, 291
Коробенко С.В. 327
Королев Д.Э. 152
Красников С.О. 235
Кривошей Н.И. 247
Куанышев В.Т. 296
Кузьменко А.С. 276
Кусайкин Д.В. 237, 301, 307
Ланко Д.А. 420
Лаухин А.В. 108
Легков К.Е. 91
Лобзенко П.В. 318, 364, 518
Лукиенко М.А. 318
Львов В.Л. 144, 323
Львов К.В. 323
Максимов Д.А. 161
Малкова И.А. 229
Манин А.А. 251, 327, 445

Михайленко Ю.Е. 268
Мищук Е.М.....291
Молоковский И.А. 333
Невельский В.С. 511
Овсянников С.Н. 186
Овчинников Д.А.....338
Опарин А.Ю. 527, 539
Оркин В.В. 91
Орлов В.Г.....128
Папаев А.Б. 296
Пешкевич А.А. 251
Полякова М.В. 430
Поркшеян В.М. 256, 261
Портнов Э.Л. 343
Прыгунов А.Г. 186
Птицын Г.А. 348
Пузанов А.С. 352
Рахимьянов А.В. 364
Ревякина Е.А. 83
Ремез И.Г. 370
Решетникова И.В. 204
Решетникова К.А. 206
Руденко Н.В.....179, 195, 206, 291
Рыбалко И.П. 69, 212, 219, 375
Санникова К.А. 152, 161
Сафарьян О.А. 19, 199
Сафронов А.И. 378
Светличная Н.О.....286
Семенец В.О. 392
Семиряд Н.Ю. 396
Синева И.С. 400
Ситьков И.А. 179
Смоляков В.Н. 414, 425
Соколов С.В. 430
Соколова О.И. 430
Соловаров И.В.....523
Сосновский И.А. 69, 327
Стремоухов М.В. 352
Сулименко И.Ю. 204
Сумарокова О.В. 435
Сухоев А.П. 437
Сухоева К.С. 161
Таов И.Н. 445
Тарасов Е.С. 448
Тимирбулатова Т.Э. 291
Тлекова Э.Р. 460
Трофлянин В.В. 132, 472
Трухин М.П. 392, 506, 523
Тютюнникова А.И. 199
Уколов Е.М. 83
Уманов А.А. 477
Усик А.С. 138
Усманова Н.Б. 485
Фатхи В.А. 280
Фатхулин Т.Д. 343
Федоров Д.С. 490
Федотов В.А. 195
Федотов В.В. 497
Филиппов Ф.П. 48
Харченко В.В. 501
Хурматов Р.И. 307
Хушмуродов К.Ш. 506
Цибульский Е.А. 375
Чащин В.С. 175
Черемных В.Г. 511
Чернышев В.В. 425
Черпаченко Г.Н. 518
Шадрин А.А. 523
Шаповалов А.М. 527
Шимельфених К.А. 97
Шпилько А.С. 266
Щербань И.В. 121, 235
Юферев М.В. 530
Юхнов В.И. 490
Явтушенко П.В. 539

Абрамов И.С. 299
Абрамова Н.И. 299
Артеменкова А.С. 189
Бабаян А.Х. 196
Безуглов Д.А. 199
Безуглый Ю.А. 19, 24
Белан Н.В. 28
Белянчикова М.П. 387
Бикбулатова Н.Г. 281
Бинеев Э.А. 208
Борисенко Н.П. 34
Борисов Б.П. 38
Боярчук А.Э. 42, 210
Будылдина Н.В. 383
Быстров С.А. 216
Варакосов Д.В. 71
Васинев Д.А. 224
Вернигорова Н.А. 220
Вершенник А.В. 19, 24, 48, 53, 124
Водовозов И.В. 224
Галкин А.С. 60
Галухин М.А. 394
Гатилова Е.А. 376
Гизатуллин М.Г. 71, 227
Гирин И.С. 76
Гниломёдов Е.И. 241
Говор С.А. 145
Головина И.В. 220
Головской В.А. 81, 90, 103, 140
Гончаров А.А. 78
Гончарова О.В. 78, 248
Данилова А.М. 250
Данилова Н.В. 255
Демидов Д.Е. 257
Денисенко Ю.Н. 264
Денисов В.Ю. 270
Деркачев И.С. 179
Докучаев С.А. 275, 278
Долинер Л.И. 281
Доткулова А.С. 286
Евдакова Л.Н. 257, 293
Жук А.С. 81, 90
Ишдавлетова Э.Т. 97
Калиенко И.В. 299
Карасев И.В. 28
Каримова В.А. 329
Кильдишов Р.М. 155
Кирхеев А.Г. 103
Коломиец Е.А. 308
Конкин Б.Б. 313
Корчемкина М.Н. 48, 53
Коршун А.М. 308
Косарева Е.П. 400
Костецкая Г.С. 275, 278
Костюченко Д.В. 318
Краснопеев С.М. 106
Крутов В.А. 140
Куанышев В.Т. 350
Кудряшова А.Ю. 114
Кузин А.П. 199
Кузнецов С.И. 124
Куликов М.А. 34
Куприянов Н.А. 48, 53
Лисицин В.Г. 321
Лобзенко П.В. 196
Луганская Л.А. 28
Маркин Д.О. 60
Момот А.И. 189, 340, 345, 367
Момот Р.А. 325
Мосева М.С 286
Мухитдинова М.Л. 329
Новикова И.А. 387
Олейникова Ю.А. 264
Опарин А.Ю. 167, 248
Павлова А.В. 372
Пащенко К.В. 372
Погорелов В.А. 334
Полков А.А. 132, 135
Попова А.В. 19, 24
Пташинский М.А. 340
Путилин Н.В. 140
Пятина А.А. 406
Ролдугина К.А. 97
Ротова Е.Г. 345
Руднев А.Н. 114
Санников А.А. 350
Светличная Н.О. 275
Свирщ Е.А. 353
Семилеткин А.О. 334
Сидняев Н.И. 145
Сидорина Т.В. 357
Сильченко В.В. 161
Синева И.С. 183, 270
Скоробогатова Е.А. 363
Смоляков В.Н. 155, 161
Совенко А.С. 132
Совенко Д.С. 135
Сосновский И.А. 76
Стаценко Е.А. 76
Степская И.А. 367

Сухорукова Е.В. 19, 24, 48, 53, 124
Табунщикова П.М. 318
Тесля С.П. 124
Тищенко Е.Н. 379
Трофименко В.Н. 372
Тураев Ф.И. 227
Турсунов Ш.А. 250
Уколова С.А. 367
Устименко Д.Л. 376
Усынин М.Г. 167
Федотов В.В. 379
Федотова П.Ч.Е. 383
Цыганов А.М. 34
Чикалов А.Н. 175
Шадрунова О.О. 411
Шаравова О.И. 387
Швачко О.В. 179
Швидченко С.А. 199, 334
Шевчук П.С. 42, 210
Шестаков И.И. 241
Юркин А.А. 106
Юхнов В.И. 42, 210
Яковенко А.А. 379, 394, 400, 406, 411
Яковлев Д.А. 183
Янкина А.И. 38, 175