ISSN 2221-7975

ТРУДЫ

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

РОСТОВ-НА-ДОНУ
2021

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

Подготовлены по результатам
XIV
Международной научно-практической конференции
«ИНФОКОМ 2021»

Ростов-на-Дону
2021

УДК 621.396.1

ББК 32

Т 78

Т 78 Труды Северо-Кавказского филиала Московского технического университета связи и информатики - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2021, 421с.

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 XIV-ой Международной научно-практической конференции «ИНФОКОМ 2021». 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.

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: Решетникова И.В., Головенко М.В.

Подписано в печать __.__.2021
Формат 60x84/8. Печать офсетная. Тираж 50 экз.
Полиграфический центр «Университет» СКФ МТУСИ,
Ростов-на-Дону, 344002, ул. Серафимовича, 62

СОДЕРЖАНИЕ

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИЙ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБРАЗОВАНИЯ, ЭКОНОМИКИ И МЕНЕДЖМЕНТА

STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

CONTENTS

STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

INFORMATION SECURITY

INFORMATION AND COMMUNICATION TECHNOLOGY IN EDUCATION, ECONOMICS AND MANAGEMENT

STATE AND PROSPECTS OF INFOCOMMUNICATION DEVELOPMENT

А.А. Манин[1], С.В. Соколов[1], О.И. Соколова[2]

ОБ ОДНОМ ПОДХОДЕ К ТЕРМИНАЛЬНОЙ НЕЛИНЕЙНОЙ ФИЛЬТРАЦИИ ПРОЦЕССОВ НА КОНЕЧНОМ ВРЕМЕННОМ ИНТЕРВАЛЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
ФГБОУ ВО «Ростовский государственный университет путей сообщения»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: терминальный критерий, конечный интервал наблюдения, стохастические нелинейные динамические системы, двухточечная краевая задача, инвариантное погружение.

В статье рассмотрена задача оценки стохастических процессов, наблюдаемых на конечном временном интервале, которая на сегодняшний день решается только для наборов данных в виде временных рядов с использованием ограниченного числа методов статистического вариационного или спектрального анализа, а также различных модификаций методов регрессии. Используются при этом параметрические критерии, зависящие от параметров плотности распределения, а не от самой плотности, что резко ограничивает возможности повышения точности оценивания нелинейных стохастических процессов. В связи с этим, для высокоточной оценки стохастических процессов на конечном интервале времени наблюдения предлагается подход, обеспечивающий как оптимальное оценивание по критерию, зависящему от апостериорной плотности распределения, так и учитывающий динамическую нелинейную структуру процесса и финитность интервала наблюдения. Численный пример иллюстрирует эффективность разработанного подхода.

A.A. Manin[1], S.V. Sokolov[1], O.I. Sokolova[2]

ON ONE APPROACH TO TERMINAL NONLINEAR FILTRATION OF PROCESSES AT A FINITE TIME INTERVAL

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Rostov State Transport University, Rostov-on-Don, Russia[2]

Keywords: terminal criterion, finite observation interval, stochastic nonlinear dynamical systems, two-point boundary value problem, invariant immersion.

The article considers the problem of estimating stochastic processes, observed over a finite time interval, which is currently solved only for data sets in the form of time series using a limited number of methods of statistical variational or spectral analysis, as well as various modifications of regression methods. In this case, parametric criteria are used that depend on the parameters of the distribution density, and not on the density itself, which sharply limits the possibilities of

improving the accuracy of estimating nonlinear stochastic processes. In this regard, for a high-precision estimation of stochastic processes at a finite observation time interval, an approach is proposed that provides both optimal estimation by a criterion depending on the a posteriori distribution density and taking into account the dynamic nonlinear structure of the process and the finiteness of the observation interval. A numerical example illustrates the effectiveness of the developed approach.

Введение. Задача высокоточной оценки экспериментальных данных, продуцируемых стохастическими нелинейными динамическими системами и полученных на конечном временном интервале наблюдения в условиях действия случайных помех измерения, оказывается чрезвычайно актуальной для широкого спектра научно-технических исследований: астрономии [1, 2], сейсмологии [3, 4], зондировании Земли [5-7], спутниковой навигации [8, 9], геодезии [10] и т.д. На сегодняшний день эта задача решается только для наборов данных в виде временных рядов с использованием достаточно ограниченного числа методов статистического вариационного анализа [11-13], интервального анализа [14], различных модификаций методов регрессии [15, 16] и локальной аппроксимации [17, 18]. При этом для обработки стохастических данных привлекаются параметрические критерии, зависящие от отдельных параметров вероятностного распределения наблюдаемого процесса, а не его функции, что существенно ограничивает возможности повышения точности обработки информации.

Цель исследования - разработка универсального подхода, который обеспечивал бы оптимальное оценивание по критерию, зависящему от апостериорной плотности распределения процесса, и одновременно учитывал динамическую нелинейную структуру процесса и финитность интервала наблюдения.

Задача исследования. Пусть N–мерный марковский процесс ξ_t описывается в общем случае системой нелинейных стохастических дифференциальных уравнений в симметризованной форме:

$$\dot{\xi}_t = f(\xi,t) + f_0(\xi,t)n_t, \qquad \xi(0) = \xi_0 , \tag{1}$$

где f, f_0 – известные нелинейные векторная и матричная функции размерности, соответственно, N и $N*M$,

n_t – центрированный векторный белый гауссовский шум (БГШ) объекта размерности M с известной интенсивностью $D_n(t)$, и измеряется с помощью нелинейного наблюдателя вида:

$$z = h(\xi,t) + W_t , \tag{2}$$

где z – выходной сигнал наблюдателя (вектор измерений) размерности K,

h – известная нелинейная вектор-функция размерности K,

W_t – центрированный векторный БГШ измерения размерности K с известной интенсивностью $D_W(t)$.

Для данного процесса требуется построить оценку $\hat{\xi}_t$, обеспечивающую максимум апостериорной вероятности невыхода ошибки оценивания $\sigma = \xi - \hat{\xi}$ за границы N–мерной области $[A,B]$ в течение известного интервала времени $[t_0,T]$.

Оценку $\hat{\xi}_t$ будем искать в виде дифференциальной системы

$$\dot{\hat{\xi}} = U(\hat{\xi},z,t) , \tag{3}$$

где $U(\hat{\xi},z,t)$ - искомая нелинейная векторная функция размерности N, удовлетворяющая заданным условиям оптимальности.

При формировании критерия, минимизация которого обеспечивает выполнение поставленной задачи, учтем также возможность обеспечения заданной формы Ф правой

части уравнения (3) (при последующем решении оптимизационной задачи - минимума отклонения от нее) – например, *f*. Дополнительное введение подобного ограничения, ориентированного на известный вид уравнения (1) процесса $\hat{\xi}_t$, не влияет, как показано далее, на общий ход решения задачи, но может повысить точность оценивания за счет приближения формы (3) к истинной структуре процесса (1).

Так как апостериорная вероятность существования ошибки σ в *N*–мерной области [*A*,*B*] равна $\int_A^B \rho(\sigma,t)d\sigma$, где ρ(…) – апостериорная плотность вероятности (АПВ) ошибки σ_t, то с учетом положительной определенности ρ(σ,*t*)∀σ, *t* искомый функционал *J*, минимизация которого обеспечивает максимум апостериорной вероятности существования ошибки σ_t в области [*A*,*B*] в течение интервала времени [t_0,*T*] наряду с требованием заданной формы правой части (3), может быть представлен в следующем виде:

$$J = -\int_{t_0}^{T}\int_{A}^{B} \rho(\sigma,t)\, d\sigma dt + \int_{t_0}^{T} [U(\hat{\xi},z,t) - \Phi(\hat{\xi},z,t)]^T [U(\hat{\xi},z,t) - \Phi(\hat{\xi},z,t)]\, dt \quad (4)$$

В выражение (4) входит неизвестная функция АПВ ρ(σ,*t*), для дальнейшего определения которой произведем следующие построения.

Из определения ошибки $\sigma = \xi - \hat{\xi}$ и уравнений (1), (3) вытекает стохастическая дифференциальная система, описывающая текущее изменение вектора σ_t:

$$\dot{\sigma}_t = f\left(\sigma + \hat{\xi}, t\right) + f_0\left(\sigma + \hat{\xi}, t\right) n_t - U\left(\hat{\xi}, z, t\right). \quad (5)$$

Для построения АПВ ρ(σ,*t*) необходимо предварительное формирование уравнения наблюдателя вектора σ_t, которое может быть получено подстановкой $\xi = \hat{\xi} + \sigma$ в уравнение (2):

$$z = h\left(\sigma + \hat{\xi}, t\right) + W_t, \quad (6)$$

после чего применение известных результатов теории оптимальной фильтрации к системе уравнений (5, 6) позволяет задать функцию ρ(σ, *t*) в форме интегро-дифференциального уравнения Стратоновича [19]. Так как аналитических методов решения данного уравнения в общем случае не существует, а использование известных конечно-разностных (сеточно-узловых) методов решения ввиду значительных вычислительных затрат для организации процесса оценивания в реальном времени не представляется возможным, то в процессе последующего синтеза оценки, оптимальной по критерию (4), будем использовать параметрическое представление АПВ ρ(σ, *t*), аппроксимируя ее далее гауссовской функцией.

В этом случае уравнение оценки $\hat{\sigma}$ вектора σ_t имеет традиционный вид расширенного фильтра Калмана:

$$\dot{\hat{\sigma}} = f\left(\hat{\sigma} + \hat{\xi}, t\right) - U(\hat{\xi}, z, t) + K\left(\hat{\sigma} + \hat{\xi}, t\right)\left[z - h\left(\hat{\sigma} + \hat{\xi}, t\right)\right], \quad (7)$$

$$K\left(\hat{\sigma} + \hat{\xi}, t\right) = R\frac{\partial h^T\left(\hat{\sigma} + \hat{\xi}, t\right)}{\partial \hat{\sigma}} D_W^{-1},$$

$$\dot{R}\left(\hat{\sigma}+\hat{\xi},t\right)=\frac{\partial f\left(\hat{\sigma}+\hat{\xi},t\right)}{\partial\hat{\sigma}}R\left(\hat{\sigma}+\hat{\xi},t\right)+R\left(\hat{\sigma}+\hat{\xi},t\right)\frac{\partial f^{T}\left(\hat{\sigma}+\hat{\xi},t\right)}{\partial\hat{\sigma}}+$$
$$+f_0\left(\hat{\sigma}+\hat{\xi},t\right)D_n\ f_0^{T}\left(\hat{\sigma}+\hat{\xi},t\right)-K\left(\hat{\sigma}+\hat{\xi},t\right)D_W K^{T}\left(\hat{\sigma}+\hat{\xi},t\right),$$

где $R\left(\hat{\sigma}+\hat{\xi},t\right)$ - апостериорная ковариационная матрица,

$$\hat{\sigma}_0=M\left(\sigma_0\right),\ R_0=M\left\{\left(\sigma_0\ -\hat{\sigma}_0\right)\left(\sigma_0\ -\hat{\sigma}_0\right)^{T}\right\}.$$

Т.к. в классе распределений с ограниченными квадратами гауссовское распределение с информационной точки зрения является «наихудшим» [19, 20], то оценка $\hat{\sigma}$ (7) является в данном случае оптимальной по минимаксному критерию, обеспечивая максимальную точность оценивания при минимуме информации о наблюдаемом процессе.

Соответственно, функционал (4) принимает вид:

$$J=\int_{t_0}^{T}\Psi(\hat{\sigma},R)\,dt+\int_{t_0}^{T}[U(\hat{\xi},z,t)-\Phi(\hat{\xi},z,t)]^{T}[U(\hat{\xi},z,t)-\Phi(\hat{\xi},z,t)]\,dt,\qquad(8)$$

$$\Psi(\hat{\sigma},R)=-\int_{A}^{B}G(\sigma,\hat{\sigma},R)\ d\sigma,\quad G(\sigma,\hat{\sigma},R)=\frac{\exp\{-\frac{1}{2}(\sigma-\hat{\sigma})^{T}R^{-1}(\sigma-\hat{\sigma})\}}{(2\pi)^{\frac{N}{2}}\det^{\frac{1}{2}}R}.$$

Опираясь на формулировку критерия (8), перейдем далее непосредственно к построению оптимальной оценки процесса $\hat{\xi}_t$, т.е. к определению искомой функции $U(\hat{\xi},z,t)$.

Методы и результаты исследования. Минимизация функционала (8) по *U* осуществляется при ограничениях на переменные, задаваемых совокупностью приведенных выше уравнений (3), (7):

$$\dot{\hat{\xi}}=U(\hat{\xi},z,t)$$
$$\dot{\hat{\sigma}}=f\left(\hat{\sigma}+\hat{\xi},t\right)-U(\hat{\xi},z,t)+K\left(\hat{\sigma}+\hat{\xi},t\right)\left[z-h\left(\hat{\sigma}+\hat{\xi},t\right)\right]$$
$$\dot{R}^{(V)}=[E\otimes\frac{\partial f\left(\hat{\sigma}+\hat{\xi},t\right)}{\partial\hat{\sigma}}+\frac{\partial f\left(\hat{\sigma}+\hat{\xi},t\right)}{\partial\hat{\sigma}}\otimes E]R^{(V)}+$$
$$+[f_0\left(\hat{\sigma}+\hat{\xi},t\right)\otimes f_0\left(\hat{\sigma}+\hat{\xi},t\right)]D_n{}^{(V)}-[K\left(\hat{\sigma}+\hat{\xi},t\right)\otimes K\left(\hat{\sigma}+\hat{\xi},t\right)]D_W{}^{(V)}\qquad(9)$$

где для возможности представления системы ограничений (9) в векторном виде матричное уравнение апостериорной ковариационной матрицы *R* было преобразовано в векторное с использованием правил, приведенных в [20,21] и введенного там же определения вектора-трансформанта $A^{(V)}$:

$A^{(V)}$ - вектор, сформированный из элементов A_{ij} матрицы *A* размерности $m^{*}n$:

$$A^{(V)}=\left|A_{11}A_{21}...A_{m1}A_{12}A_{22}...A_{m2}...A_{1n}A_{2n}...A_{mn}\right|^{T},$$

$\otimes$ - символ кронекеровского произведения, *E* - единичная матрица.

Для упрощения записи системы (9) перепишем ее в виде:

$$\dot{Y} = \Theta_*\left(Y, z, t\right) + E_* \cdot U(Y, z, t), \qquad (10)$$

где

$$Y = \begin{vmatrix} \hat{\xi} \\ \hat{\sigma} \\ R^{(V)} \end{vmatrix}, \quad \Theta_*\left(Y, z, t\right) = \begin{vmatrix} 0 \\ \Theta\left(\hat{\sigma} + \hat{\xi}, R, z, t\right) \\ \Theta_1\left(\hat{\sigma} + \hat{\xi}, R, t\right) \end{vmatrix}, \quad E_* = \begin{vmatrix} E \\ -E \\ 0 \end{vmatrix},$$

$$\Theta\left(\hat{\sigma} + \hat{\xi}, R, z, t\right) = f\left(\hat{\sigma} + \hat{\xi}, t\right) + K\left(\hat{\sigma} + \hat{\xi}, t\right)\left[z - h\left(\hat{\sigma} + \hat{\xi}, t\right)\right],$$

$$\Theta_1\left(\hat{\sigma} + \hat{\xi}, R, t\right) = (E \otimes \frac{\partial f\left(\hat{\sigma} + \hat{\xi}, t\right)}{\partial \hat{\sigma}} + \frac{\partial f\left(\hat{\sigma} + \hat{\xi}, t\right)}{\partial \hat{\sigma}} \otimes E) R^{(V)} +$$

$$+[f_0\left(\hat{\sigma} + \hat{\xi}, t\right) \otimes f_0\left(\hat{\sigma} + \hat{\xi}, t\right)] D_n{}^{(V)} - [K\left(\hat{\sigma} + \hat{\xi}, t\right) \otimes K\left(\hat{\sigma} + \hat{\xi}, t\right)] D_W{}^{(V)}.$$

Для решения задачи минимизации функционала (8) при ограничениях (10) составим гамильтониан:

$$H = -\int_A^B G(\sigma, Y)\, d\sigma + [U(Y, z, t) - \Phi(Y, z, t)]^T [U(Y, z, t) - \Phi(Y, z, t)] + \Psi^T \{\Theta_*\left(Y, z, t\right) + E_* \cdot U(Y, z, t)\},$$

где Ψ - вектор сопряженных переменных.

Из условия оптимума гамильтониана

$$\frac{\partial H}{\partial U} = 2[U(Y, z, t) - \Phi(Y, z, t)]^T + \Psi^T \cdot E_* = 0$$

определяется вид искомого оптимального вектора *U*:

$$U(Y, z, t) = -\frac{1}{2} E_*{}^T \cdot \Psi + \Phi(Y, z, t)\,.$$

Соответственно, вектор сопряженных переменных определяется из условия

$$\dot{\Psi} = \frac{\partial H^T}{\partial Y}$$

и удовлетворяет следующей системе уравнений:

$$\dot{\Psi} = -\left| 0 : \int_A^B \frac{\partial G(\sigma, Y)}{\partial \hat{\sigma}} d\sigma : \int_A^B \frac{\partial G(\sigma, Y)}{\partial R^{(V)}} d\sigma \right|^T - 2 \frac{\partial \Phi(Y, z, t)}{\partial Y}^T [U(Y, z, t) - \Phi(Y, z, t)] + \frac{\partial \Theta_*\left(Y, z, t\right)}{\partial Y}^T \Psi,$$

$$\Psi(T) = 0,$$

где

$$\frac{\partial G(\sigma,Y)}{\partial Y}=\left|0:\frac{\partial G(\sigma,Y)}{\partial\hat{\sigma}}:\frac{\partial G(\sigma,Y)}{\partial R^{(V)}}\right|,$$

$$\frac{\partial G(\sigma,Y)}{\partial\hat{\sigma}}=\frac{\exp\left\{-\frac{1}{2}\left(\sigma-\hat{\sigma}\right)^T R^{-1}\left(\sigma-\hat{\sigma}\right)\right\}}{(2\pi)^{\frac{N}{2}}\det^{\frac{1}{2}}R}\left(\sigma-\hat{\sigma}\right)^T R^{-1}=G(\sigma,Y)\left(\sigma-\hat{\sigma}\right)^T R^{-1},$$

$$\frac{\partial G(\sigma,Y)}{\partial R^{(V)}}=\frac{\exp\left\{-\frac{1}{2}\left(\sigma-\hat{\sigma}\right)^T R^{-1}\left(\sigma-\hat{\sigma}\right)\right\}}{2(2\pi)^{\frac{N}{2}}\det^{\frac{1}{2}}R}\left[\left(\sigma-\hat{\sigma}\right)^T R^{-1}\left(E_N\otimes\left\{E_N^{(V)}\right\}^T\hat{\otimes}R^{-1}\left(\sigma-\hat{\sigma}\right)-\frac{1}{\det R}\left\{R_A^{(V)}\right\}^T\right]=$$

$$=G(\sigma,Y)\frac{1}{2}\left[\left(\sigma-\hat{\sigma}\right)^T R^{-1}\left(E_N\otimes\left\{E_N^{(V)}\right\}^T\hat{\otimes}R^{-1}\left(\sigma-\hat{\sigma}\right)-\frac{1}{\det R}\left\{R_A^{(V)}\right\}^T\right].$$

Таким образом, система сопряженных уравнений принимает вид:

$$\dot{Y}=\Theta_*(Y,z,t)+E_*\cdot(\Phi(Y,z,t)-\frac{1}{2}{E_*}^T\cdot\Psi)\quad(11)$$

$$\dot{\Psi}=-\int_A^B\frac{\partial G(\sigma,Y)}{\partial Y}^T d\sigma+[\frac{\partial\Phi(Y,z,t)}{\partial Y}^T\cdot{E_*}^T+\frac{\partial\Theta_*(Y,z,t)}{\partial Y}^T]\cdot\Psi$$

$$Y(0)=Y_0,\Psi(T)=0$$

а при отсутствии ограничений на форму вектора *U*, соответственно:

$$\dot{Y}=\Theta_*(Y,z,t)-\frac{1}{2}E_*\cdot{E_*}^T\cdot\Psi$$

$$\dot{\Psi}=-\int_A^B\frac{\partial G(\sigma,Y)}{\partial Y}^T d\sigma+\frac{\partial\Theta_*(Y,z,t)}{\partial Y}^T\cdot\Psi$$

$$Y(0)=Y_0,\Psi(T)=0$$

Решение системы полностью исчерпывает поставленную задачу, позволяя построить искомую оценку $\hat{\xi}_t$ процесса ξ_t, оптимальную по терминальному критерию (8). Тем не менее, учитывая известные вычислительные трудности, возникающие при решении двухточечной краевой задачи (11) и резко возрастающие с ростом размерности вектора ξ_t, рассмотрим также существенно менее затратное субоптимальное решение поставленной задачи, используя для приближенного решения системы (11) метод инвариантного погружения [22, 23]. В этом случае уравнения субоптимальной оценки принимают вид:

$$\hat{\dot{Y}}=\Theta_*(\hat{Y},z,t)+E_*\cdot\Phi(\hat{Y},z,t)-D\cdot\int_A^B\frac{\partial G(\sigma,\hat{Y})}{\partial\hat{Y}}^T d\sigma$$

$$\dot{D}=(E_*\cdot\frac{\partial\Phi(Y,z,t)}{\partial Y}+\frac{\partial\Theta_*(Y,z,t)}{\partial Y})D-$$

$$-D\cdot(\frac{\partial\Phi(Y,z,t)}{\partial Y}^T\cdot{E_*}^T+\frac{\partial\Theta_*(Y,z,t)}{\partial Y}^T)+\frac{1}{2}E_*\cdot{E_*}^T-D\cdot\int_A^B\frac{\partial}{\partial\hat{Y}}[\frac{\partial G(\sigma,\hat{Y})}{\partial\hat{Y}}^T]d\sigma\cdot D$$

а при отсутствии ограничений на форму вектора *U* (Ф=0):

$$\hat{\dot{Y}}=\Theta_*\left(\hat{Y},z,t\right)-D\cdot\int_A^B\frac{\partial G(\sigma,\hat{Y})}{\partial\hat{Y}}^T d\sigma$$

$$\dot{D}=\frac{\partial\Theta_*\left(Y,z,t\right)}{\partial Y}D-D\cdot\frac{\partial\Theta_*\left(Y,z,t\right)}{\partial Y}^T+\frac{1}{2}E_*\cdot{E_*}^T-D\cdot\int_A^B\frac{\partial}{\partial\hat{Y}}[\frac{\partial G(\sigma,\hat{Y})}{\partial\hat{Y}}^T]d\sigma\cdot D\quad(12)$$

Для оценки эффективности предложенного подхода рассмотрим следующий пример.

Обсуждение результатов. Для стохастического процесса, описываемого нелинейным дифференциальным уравнением

$$\dot{\xi}_t = \cos^2 \xi_t^2 + n_t,$$

где n_t – центрированный БГШ с интенсивностью $D_n(t)$,
и наблюдаемого на временном интервале [0,500] с, уравнение измерителя имеет вид:

$$z = \exp(-\xi_t^2) + W_t,$$

где W_t – центрированный БГШ с интенсивностью $D_W(t)$.

Интегрирование уравнения объекта осуществлялось методом Рунге-Кутты 4-го порядка с шагом 0.01 с. Шумы объекта и измерителя моделировались случайными гауссовскими последовательностями с единичными с.к.о.

Обработка измерений z производилась с использованием метода наименьших квадратов (МНК) и уравнения кубической регрессии, расширенного фильтра Калмана и предложенного подхода, реализованного путем интегрирования уравнений (12).

Анализ результатов моделирования показал, что при использовании МНК и расширенного фильтра Калмана наблюдается существенный тренд ошибок оценивания, причем, с тенденцией к дальнейшему увеличению.

В то же время при обработке данных алгоритмом (12) тренд практически отсутствует, а ошибка оценивания в конце интервала измерения оказалась на два порядка меньше ошибки МНК и на порядок меньше ошибки расширенного фильтра Калмана.

Заключение. Выявленные в результате исследования преимущества рассмотренного подхода: возможность оптимального оценивания по критерию, зависящему от наиболее информативной характеристики наблюдаемого процесса – апостериорной плотности распределения, и учета его динамической нелинейной структуры наряду с финитностью интервала наблюдения, в совокупности со сравнительным анализом приведенных ошибок позволяют сделать вывод о возможности его эффективного использования при обработке нелинейных стохастических процессов, наблюдаемых на конечном интервале времени.

СПИСОК ЛИТЕРАТУРЫ

1. *Lohman A.W., Weigelt G., Wiruitzer B.* Speckle masking in astronomy: triple correlation theory and applications // Applied Optics. -1983, vol. 22, p. 4028-4037.
2. *Jenkin A.B.* DEBRIS: A Computer Program for Debris Cloud Modeling. Paper No. IAA.6.3-93-746 // 44th Congress of the International Austronautical Federation. -Graz, Austria, 1993.
3. *Василенко В.Ф., Прытков А.С.* Моделирование взаимодействия литосферных плит на о.Сахалин по данным GPS наблюдений // Тихоокеанская геология. -2012, т. 31, №1, с. 42-48.
4. *Любушин А.А.* Анализ данных систем геофизического и экологического мониторинга. М.: Наука, 2007.
5. *Totsky A.V., Gorbunenko B.F.* Investigations of the synthetic aperture radar images formed by processing of bispectral data // International Journal of Electronics and Communications. -1999, vol. 53, №3, p. 146-150.
6. *Савиных В.П., Цветков В.Я.* Геоинформационный анализ данных дистанционного зондирования. М.: Картгеоцентр – Геодезиздат, 2001.
7. *Чандра А.М., Гош С.К.* Дистанционное зондирование и географические информационные системы. -М.: Техносфера, 2008.
8. *Аншаков Г.П., Голяков А.Д., Петрищев В.Ф., Фурсов В.А.* Автономная навигация космических аппаратов. -Самара: Изд-во ГНПРКЦ «ЦСКБ-Прогресс», 2011.

9. *Gurevich G., Wertz J.R.* Autonomous On-board Orbit Control Flight Results and Applications // AIAApaper 2000-5226. -Long Beach, CA, 2000, p. 19-21.
10. *Спиридонов А.И.* Основы геодезической метрологии. -М.: Картгеоцентр - Геодезиздат. 2003.
11. *Бокс Дж., Дженкинс Г.* Анализ временных рядов прогноз и управление. -М.: СИНТЕГ, 2002.
12. *Симчера В.М.* Методы многомерного анализа статистических данных. -М.: Финансы и статистика, 2008.
13. *Кулаичев А.П.* Методы и средства комплексного анализа данных. -М.: Форум, 2018.
14. *Кумков С.И., Жолен Л.* Сравнение методов интервального анализа и статистических методов в задаче оценивания экспериментальных данных с неопределенностью // Измерительная техника. -2019, № 2, с. 13-17.
15. *Бриллинджер Д.* Временные ряды. Обработка данных и теория. -М.: Мир, 1980.
16. *Рудой Г.И.* Модификация функционала качества в задачах нелинейной регрессии для учета гетероскедастичных погрешностей измеряемых данных. // Информатика и ее применения. -2017, т. 11, № 2, с. 74-84.
17. *Миркин Б.Г.* Введение в анализ данных. -Люберцы: Юрайт, 2016.
18. *Афанасьев В.Н., Лебедева Т.В.* Моделирование и прогнозирование временных рядов. -М.: Финансы и статистика, 2009.
19. *Тихонов В. И., Харисов В. Н.* Статистический анализ и синтез радиотехнических устройств и систем. -М.: Радио и связь, 1991.
20. *Соколов С.В., Ковалев С.М., Кучеренко П.А., Смирнов Ю.А.* Методы идентификации нечетких и стохастических систем. -М: Физматлит, 2018.
21. *Чернов А.А., Ястребов В.Д.* Метод оценки возмущений в алгоритмах решения навигационных задач // Космические исследования. -1984, т. 22, № 3.
22. *Первачев С. В., Перов А. И.* Адаптивная фильтрация сообщений. -М.: Радио и связь, 1991.
23. *Сейдж Э., Мелс Дж.* Теория оценивания и ее применение в связи и управлении. -М.: Связь, 1976.

С.В. Соколов[1], О.И. Соколова[2]
Сун Чжили[3], Тун Юйлинь[3], Хасытеэр Нуерланьиеке[3], Чжан Цзяньцун[3]

СИНТЕЗ АЛГОРИТМОВ РОБАСТНОЙ ФИЛЬТРАЦИИ ПАРАМЕТРОВ СОСТОЯНИЯ НЕЛИНЕЙНЫХ СТОХАСТИЧЕСКИХ СИСТЕМ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
ФГБОУ ВО «Ростовский государственный университет путей сообщения»,
г. Ростов-на-Дону, Россия[2]
ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова», Воронеж, Россия [3]

Ключевые слова: критерий робастности, вероятностные характеристики помех измерений, алгоритмы робастной фильтрации.

В статье на основе введенного нового критерия робастности рассмотрен подход к синтезу оптимальных алгоритмов робастной фильтрации, обеспечивающих устойчивость

процесса оценки состояния нелинейной стохастической системы при различных классах неопределенных помех измерения и шумов объекта. Простота и низкая вычислительная сложность полученных алгоритмов обеспечивают возможность их широкого применения в системах инфокоммуникаций, управления, навигации и пр.

S.V. Sokolov[1], O.I. Sokolova[2]
Song Czhili[3], Tong Yulin[3], Hasyteer Nuerlanyieke[3], Zhang Jianzong[3]

SYNTHESIS OF ALGORITHMS FOR ROBUST FILTERING OF STATE PARAMETERS OF NONLINEAR STOCHASTIC SYSTEMS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Rostov State Transport University, Rostov-on-Don, Russia[2]
Voronezh State University of Forestry and Technologies Named after G.F. Morozov[3]

Keywords: robustness criterion, probabilistic characteristics of measurement interference, robust filtering algorithms.

Based on the introduced new robustness criterion, the article considers an approach to the synthesis of optimal robust filtering algorithms that ensure the stability of the process of assessing the state of a nonlinear stochastic system for various classes of undefined measurement interference and object noise. The simplicity and low computational complexity of the algorithms obtained make it possible for them to be widely used in information communication systems, management, navigation, etc.

Введение. Практическое использование подавляющего большинства современных методов фильтрации ограничено необходимостью точного априорного знания параметров системы и вероятностных характеристик как ее шумов, так и помех измерений. Отсутствие во многих практических приложениях подобной точной информации приводит к необходимости разработки новых подходов, свободных от таких ограничений и обеспечивающих устойчивый характер процесса фильтрации. Такие фильтры получили название робастных. В то же время существующие алгоритмы робастной фильтрации весьма далеки от полного решения задачи робастной фильтрации: большинство алгоритмов построено только на основе или квадратичного, или модульного критериев; значительная часть робастных фильтров ориентирована только на обеспечение устойчивой работы фильтра Калмана или на оценку линейных объектов, что резко сужает области их применения.

При оценке состояния стохастических динамических систем по зашумленным измерениям наиболее мощным и универсальным аппаратом на сегодняшний день является теория стохастической фильтрации [1-4]. Но эффективное использование подавляющего большинства методов фильтрации ограничено необходимостью точного априорного знания параметров системы и вероятностных характеристик как ее шумов, так и помех измерений. Очевидно, что во многих практических приложениях получить подобную точную информацию не представляется возможным. Это обстоятельство, в свою очередь, требует разработки новых подходов, свободных от данного ограничения и обеспечивающих устойчивое изменение ошибки фильтрации в заданных пределах. Такие фильтры получили название робастных и заняли свою нишу в общем ряду методов стохастической оценки [5-12]. В первоначальном варианте [5,7-9] под робастностью понималась нечувствительность алгоритма оценивания к малым отклонениям вероятностных характеристик помех измерителей от их априорных моделей (в частности, к аномальным отклонениям относительно гауссовского распределения). С развитием данного направления трактовка

робастности алгоритмов фильтрации несколько расширилась. Среди наиболее интересных решений робастной фильтрации можно отметить:

- фильтр Särkkä – Nummenmaa, который позволяет находить не только оценки вектора состояния, но и оценку ковариационной матрицы шума измерений [7],
- фильтр Izanloo – Fakoorian – Yazdi – Simon [11], основанный на критерии максимальной коррентропии и методе взвешенных наименьших квадратов и уменьшающий влияние аномальных наблюдений,
- робастные фильтры в неопределенных системах при известных ковариациях случайных факторов, построенные на основе методов H2-, H∞- и смешанной H2/H∞-оптимизации [12-14],
- фильтры с неопределенными ковариационными матрицами случайных факторов [15–19],

а также фильтры по критерию минимума суммы модулей, формирующие оптимальную оценку в случае, когда помеха измерения распределена по закону Лапласа, что делает оценку менее чувствительной к “выбросам” в измерениях [20,21].

Анализ вышеперечисленных, а также им аналогичных, схем робастной фильтрации позволяет сделать следующие выводы:

- подавляющее большинство алгоритмов построено только на основе или квадратичного, или модульного критериев;
- значительная часть робастных фильтров ориентирована только на обеспечение устойчивой работы фильтра Калмана (как правило, дискретного), причем, за счет реализации дополнительных вычислительных схем, увеличивающих объем вычислительных затрат на фильтрацию;
- б*о*льшая часть работ по робастной фильтрации посвящена исследованию линейных объектов, что резко сужает области их применения.

Цель исследования - дальнейшее развитие методов робастной фильтрации как с точки зрения расширения их функциональных возможностей с целью формирования оптимальных минимаксных оценок состояния в предположении более широкого спектра допущений о характере распределений помех измерений и шумов объекта, так и сокращения вычислительных затрат на реализацию алгоритма оценки.

В связи с этим рассмотрим следующий подход к решению задачи синтеза алгоритмов робастной фильтрации.

Задача исследования. Пусть объект, вектор состояния которого *x* подлежит оцениванию, описывается стохастическим дифференциальным уравнением вида:

$$\dot{x} = f(x,t) + f_0(x,t)W_t, \tag{1}$$

где $f(x,t), f_0(x,t)$ – известные векторная и матричная функции размерности, соответственно, *N* и *N*M*,

W_t – вектор-шум объекта размерности *M* с функцией распределения, принадлежащей классу распределений с ограниченными средними квадратами [22],

и измеряется нелинейным наблюдателем

$$z = h(x,t) + V_t, \tag{2}$$

где *z* – вектор измерений размерности *K*,

$h(x,t)$ – известная вектор-функция размерности *K*,

V_t – вектор помехи измерения размерности *K* с функцией распределения, определенной в некотором известном классе распределений [22].

В практических приложениях в качестве основных классов распределений рассматриваются, как правило, распределения [22]:

- с плотностью ρ, непрерывной в нуле ($\rho(0) \geq a \succ 0$),
- распределения с ограниченными средними квадратами ($\int_{-\infty}^{\infty} x^2 \rho(x) dx \prec \infty$),
- «засоренные» распределения ($\rho(x) = (1-\varepsilon)\rho_0(x) + \varepsilon\rho_1(x),\ 0 \leq \varepsilon \leq 1$),
- существующие на ограниченном интервале аргумента ($\int_a^a \rho(x) dx = 1$) и некоторые др.

Т.к. в рассматриваемом случае для помехи измерения известен только класс распределения, но не его вид, то оценку $\hat{x}$ вектора состояния *x* будем искать как оценку, гарантирующую наилучшую точность оценивания в минимаксном смысле (т.е. минимальные ошибки в наиболее неблагоприятной ситуации, определяемой заданным классом распределения). В традиционной постановке [5,7,8,22] данная задача решается как задача определения оценки $\hat{x}$ из условия минимизации функционала $\int_{t_0}^{t} F[z - h(\hat{x}, t)] dt$, где функция *F* определяется выбранным (наиболее неблагоприятным) классом распределения помехи измерения. При подобной оптимизации приведенного функционала по вектору $\hat{x}$, не учитывающей *apriori* известную стохастическую динамику вектора состояния *x*, возникают существенные вычислительные сложности, связанные с поиском глобального минимума многомерной нелинейной случайной функции в реальном времени. Очевидно, что такой подход, несмотря на его «классическую» робастность и универсальность применения, при практической реализации в реальных системах может существенно проигрывать по вычислительным затратам и точности алгоритмам робастной фильтрации, реализуемым в дифференциальной (или рекуррентной) форме, даже при более ограниченной области применения последних. В связи с этим возникает задача разработки такого подхода к синтезу алгоритмов робастной оценки, который обеспечивал бы как универсальность его использования для всех известных классов неблагоприятных распределений помех измерения, так и практически доступный уровень вычислительных затрат за счет реализации алгоритмов в дифференциальной форме. Рассмотрим далее возможность решения данной задачи в подобной постановке.

Методы и результаты исследований. Исходя из вида уравнения (1), описывающего динамику стохастического вектора состояния *x*, искомую оценку $\hat{x}$ вектора *x* будем искать в следующей дифференциальной форме:

$$\dot{\hat{x}} = f(\hat{x}, t) + f_0(\hat{x}, t) u(\hat{x}, z, t), \qquad (3)$$

где $u(\hat{x}, z, t)$ – вектор-функция, определяемая из условия обеспечения робастности оценки (3), т.е. минимальности ошибок оценивания при наиболее неблагоприятном классе распределения помехи измерения.

В качестве исходной формы минимизируемого функционала, гарантирующего наилучшую точность оценивания в минимаксном смысле, предварительно рассмотрим классический функционал $\int_{t_0}^{t} F[z - h(\hat{x}, t)] dt$. Анализ всех известных видов его подынтегральной функции *F* показывает [5,7,22], что данная функция является неотрицательно определенной для всей области определения аргумента. Это обстоятельство позволяет перейти от минимизации данного функционала к минимизации

функции $F[z-h(\hat{x},t)]$ и с учетом принадлежности функции распределения шума объекта классу распределений с ограниченными средними квадратами, для которого функция *F* является квадратичной [5,22], окончательно сформировать минимаксный критерий оптимальности *J* в виде:

$$J = F[z-h(\hat{x},t)] + \int_{t_0}^{t} u(\hat{x},z,t)^T u(\hat{x},z,t)dt \qquad (4)$$

Для последующего определения искомой функции $u(\hat{x},z,t)$ используем тот известный факт, что при неотрицательно определенной критериальной функции для обеспечения ее минимального значения в каждый момент времени достаточно, чтобы производная ее по времени, взятая с обратным знаком, имела максимум [3]. Это позволяет для рассматриваемого случая получить исходное условие для определения вектора $u(\hat{x},z,t)$:

$$\max_u(-\dot{J}) = \max_u\{-\frac{dF[z-h(\hat{x},t)]}{dz}[\dot{z}-\frac{\partial h(\hat{x},t)}{\partial \hat{x}}\dot{\hat{x}}-\frac{\partial h(\hat{x},t)}{\partial t}]-u(\hat{x},z,t)^T u(\hat{x},z,t)\}$$

С учетом уравнения оценки (3) данное условие трансформируется к виду:

$$\max_u(-\dot{J}) = \max_u\{-\frac{dF[z-h(\hat{x},t)]}{dz}[\dot{z}-\frac{\partial h(\hat{x},t)}{\partial \hat{x}}(f(\hat{x},t)+f_0(\hat{x},t)u(\hat{x},z,t))-\frac{\partial h(\hat{x},t)}{\partial t}]-u(\hat{x},z,t)^T u(\hat{x},z,t)\}$$

Вводя, следуя [22], обозначение $\frac{dF[z-h(\hat{x},t)]}{dz} = \psi[z-h(\hat{x},t)]$ (где виды функций ψ для основных классов распределений приведены в [22]), из последнего условия имеем уравнение

$$\psi[z-h(\hat{x},t)]\frac{\partial h(\hat{x},t)}{\partial \hat{x}} f_0(\hat{x},t) - 2u^T(\hat{x},z,t) = 0,$$

позволяющее сразу определить искомую вектор-функцию $u(\hat{x},z,t)$:

$$u(\hat{x},z,t) = \frac{1}{2} f_0{}^T(\hat{x},t)\frac{\partial h^T(\hat{x},t)}{\partial \hat{x}}\psi^T[z-h(\hat{x},t)] \qquad (5)$$

С учетом (5) уравнение робастной оценки (3) окончательно принимает вид:

$$\dot{\hat{x}} = f(\hat{x},t) + \frac{1}{2} f_0(\hat{x},t) f_0{}^T(\hat{x},t)\frac{\partial h^T(\hat{x},t)}{\partial \hat{x}}\psi^T[z-h(\hat{x},t)] \qquad (6)$$

Для оценки возможности использования предложенного подхода рассмотрим следующий пример.

Обсуждение результатов. Рассмотрим возможность робастного решения задачи помехоустойчивого позиционирования беспилотного автомобиля (БА), навигационная система которого построена на основе комплексирования хронометрического одометра и спутниковой навигационной системы (СНС). В качестве модели выходного сигнала хронометрического одометра Z_{XO} используем далее традиционную модель с аддитивным шумом W_t:

$$Z_{XO} = V + W_t, \qquad (7)$$

где *V* – модуль скорости БА,

а в качестве модели сигнала спутниковых измерений - модель кодовых измерений псевдодальности Z_{CHC}, записанных в географической системе координат (СК)[23]:

$$Z_{CHC} = \sqrt{(\xi_c-(\mathrm{r}+H)\cos\varphi\sin\lambda)^2+(\eta_c-(\mathrm{r}+H)\sin\varphi)^2+(\zeta_c-(\mathrm{r}+H)\cos\varphi\cos\lambda)^2} + V_t =$$
$$= h(\varphi,\lambda,t) + V_t, \qquad (8)$$

где ξ_c, η_c, ζ_c – известные координаты спутника в геоцентрической СК,

H - текущая высота БА, *r* – радиус Земли, φ, λ – географические широта и долгота БА.

При этом полагаем, что функция распределения шума хронометрического одометра W_t принадлежит классу распределений с ограниченными средними квадратами (что определяется результатами длительной эксплуатации данных измерителей), а функция распределения помехи кодовых измерений псевдодальности V_t – классу распределений, непрерывных в нуле, что, в свою очередь, вытекает из существенной неопределенности вероятностного характера помех СНС, обусловленной их зависимостью от множества непрогнозируемых неравномощных факторов: состояния атмосферы, рельефа местности, особенностей городской застройки, инструментальных погрешностей передатчика спутника и приемника объекта, особенностей городской застройки и ошибок многолучевости и пр. При моделировании движения БА полагаем, что БА движется из точки с координатами $\varphi_0 = 0{,}78$ рад, $\lambda_0 = 0{,}29$ рад, в течение интервала времени [0; 1000 сек] с постоянной скоростью $V = 22$ м/с по локсодромической траектории с азимутальным углом *A*=0,19 рад по поверхности Земли на высоте *H*=250м.

При решении задачи измерения навигационных параметров объекта, движущегося по локсодромии, используемые уравнения движения его центра масс имеют вид [23,24,25]:

$$\dot{\varphi} = \frac{V_y}{r+H}, \tag{9}$$

$$\lambda(\varphi) = \lambda_0 + tgA \cdot \ln\left(\frac{\xi(\varphi)}{\xi(\varphi_0)}\right), \qquad \xi(\varphi) = \left| tg\left(\frac{\varphi}{2} + \frac{\pi}{4}\right)\right|,$$

где λ_0 – начальное значение долготы участка траектории с постоянным известным курсовым углом *A*, φ_0 – начальное значение его широты,

V_y – проекция скорости БА на соответствующую ось *Oy* географической системы координат.

При движении по локсодромической траектории с азимутальным углом *A* проекция скорости БА на ось географической СК *Oy* равна:

$$V_y = V \cdot \cos A,$$

что позволяет записать, с учетом (7), (9) и следуя (1), уравнения движения БА в исходной для последующего оценивания навигационных параметров форме:

$$\dot{\varphi} = \frac{(Z_{XO} - W_t)cosA}{r+H} = \frac{Z_{XO}}{r+H} - \frac{1}{r+H} W_t, \tag{10}$$

совместно с уравнением наблюдателя его параметров движения

$$Z_{CHC} = h(\varphi, t) + V_t, \tag{11}$$

где

$$h(\varphi,t) = \sqrt{(\xi_c - (r+H)\cos\varphi\sin\lambda(\varphi))^2 + (\eta_c - (r+H)\sin\varphi)^2 + (\zeta_c - (r+H)\cos\varphi\cos\lambda(\varphi))^2}$$

$$\lambda(\varphi) = \lambda_0 + tgA \cdot \ln\left(\frac{\xi(\varphi)}{\xi(\varphi_0)}\right), \qquad \xi(\varphi) = \left| tg\left(\frac{\varphi}{2} + \frac{\pi}{4}\right)\right|.$$

Исходя из уравнения движения БА (10) и уравнения его наблюдателя (11), уравнение робастного фильтра в соответствии с полученным выше уравнением оценки (6) запишем в виде

$$\dot{\hat{\varphi}} = \frac{Z_{XO}}{r+H} + \frac{a}{2(r+H)^2}\frac{dh(\hat{\varphi},t)}{d\hat{\varphi}}\,\mathrm{sgn}[Z_{CHC} - h(\hat{\varphi},t)], \qquad (12)$$

т.к. функция ψ, исходя из класса распределений помехи кодовых измерений V_t (распределений, непрерывных в нуле), в данном случае имеет вид:

$$\psi[Z_{CHC} - h(\hat{\varphi},t)] = \mathrm{sgn}[Z_{CHC} - h(\hat{\varphi},t)] = \begin{cases} a, Z_{CHC} - h(\hat{\varphi},t) \geq 0, \\ -a, Z_{CHC} - h(\hat{\varphi},t) \prec 0 \end{cases}$$

Оценка второго навигационного параметра - долготы БА $\hat{\lambda}$, осуществляется на основании полученной оценки широты $\hat{\varphi}$ в соответствии с приведенной выше функциональной зависимостью: $\hat{\lambda}\,(\hat{\varphi}) = \hat{\lambda}_0 + tgA \cdot \ln(\frac{\xi(\hat{\varphi})}{\xi(\hat{\varphi}_0)})$.

При численном моделировании процесса оценивания в качестве распределения шума W_t использовалось распределение Лапласа с нулевым матожиданием и дисперсией $(0{,}25\ \text{м/с})^2$, а в качестве распределения шума V_t – стандартное распределение Коши (в связи с чем параметр a в алгоритме (12) был выбран равным 0,24). Для оценки эффективности предложенного подхода оценивание навигационных параметров БА производилось с использованием следующих алгоритмов:

- алгоритма (12), реализованного с использованием метода Рунге-Кутты 4-го порядка с шагом 0,01с;
- классического робастного алгоритма, определяющего оценку $\hat{x}$ из условия минимизации функционала $\int_{t_0}^{t} F[z - h(\hat{x},t)]dt$, в рассматриваемом случае - функционала $\int_{t_0}^{t} |Z - h(\hat{x},t)|dt$;
- расширенного фильтра Калмана, также реализованного методом Рунге-Кутты 4-го порядка с шагом 0,01 с, для которого дисперсии центрированных шумов хронометрического одометра и кодовых измерений были выбраны, соответственно, равными $(0{,}3\ \text{м/с})^2$ и $(2\ \text{м})^2$.

Анализ результатов моделирования показал, что по сравнению с расширенным фильтром Калмана, процесс оценивания в котором оказался существенно неустойчивым, предложенный алгоритм и классический робастный алгоритм обеспечивают устойчивость процесса фильтрации. При этом предложенный алгоритм оказался, во-первых, точнее классического, а во-вторых, значительно менее затратным по объему вычислений. Это обусловлено тем, что, несмотря на определенную сложность функции h, алгоритм (12) был реализован в реальном масштабе времени, в то время как классический робастный алгоритм на каждом временном шаге требовал решения оптимизационной задачи с размерностью, увеличивающейся с каждым шагом.

Заключение. Таким образом, полученные результаты позволяют сделать вывод о возможности эффективного применения предложенного подхода при оценке состояния стохастических динамических систем в условиях неопределенности вероятностных характеристик их шумов.

СПИСОК ЛИТЕРАТУРЫ

1. *Тихонов В.И., Харисов В.Н.* Статистический анализ и синтез радиотехнических устройств и систем. -М.: Радио и связь, 2004.
2. *Пугачев В.С., Синицын И.Н.* Стохастические дифференциальные системы: Анализ и

фильтрация. -М. : Наука, 1990.
3. *Казаков И.Е.* Статистическая теория систем управления в пространстве состояний. -М.: Наука, 1975.
4. *Сейдж Э., Мелс Дж.* Теория оценивания и ее применение в связи и управлении. -М.: Связь, 1976.
5. *Huber P. J., Ronchetti E.M.* Robust statistics. -New Jersey: John Wiley Sons, 2009.
6. *Maronna R.A., Martin D.R., Yohai V.J.* Robust statistics. Theory and methods. -England: John Wiley Sons, 2006.
7. *Цыпкин Я.З., Поляк Б.Т.* Огрубленный метод максимального правдоподобия // Динамика систем. Математические методы теории колебаний. -Горький. 1977, № 12.
8. *Хьюбер П.* Дж. Робастность в статистике / Пер. с англ. под ред. Я.З.Цыпкина. – -М.: Мир, 1984.
9. Устойчивые статистические методы оценки данных / Под ред. Р.Л. Лонера. -М.: Машиностроение, 1984.
10. *Särkkä S., Nummenmaa A*. Recursive noise adaptive Kalman filtering by variational Bayesian approximations // IEEE Transactions on Automatic control. 2009. Vol. 54, p. 596-600.
11. *Izanloo R., Fakoorian S.A., Yazdi H.S., Simon D*. Kalman filtering based on the maximum correntropy criterion in the presence of non- Gaussian noise // Annual Conference on Information Science and Systems (CISS), Princeton, USA: proccedings. -2016, p. 500-505.
12. *Gao H., Lam J., Wang C*. Induced l2 and generalized H∞ filtering for systems with repeated scalar nonlinearities // IEEE Transact. Signal Proc. -2005, v. 53, № 11, p. 4215-4226.
13. *Gao H., Lam J., Wang C*. New approach to mixed H2/H∞ filtering for polytopic discrete-time systems // IEEE Transact. Signal Proc. -2005, v. 53, № 8, p. 3183-3192.
14. *Gao H., Lam J., Wang C*. Robust H∞ filtering for discrete stochastic time-delay systems with nonlinear disturbances // Nonlinear Dynam. Syst. Theory. -2004, v. 4, № 3, p. 285-301.
15. 15.*Poor H.V., Looze D.P*. Minimax State Estimation for Linear Stochastic Systems with Noise Uncertainty // IEEE Trans. Automat. Control. -1981, v. 26, p. 902-906.
16. *Sayed A.H.* A Framework for State-space Estimation with Uncertain Models // IEEE Trans. Automat. Control. -2001, v. 46, p. 998-1013.
17. *Calafiore G., El Ghaoui L*. Minimum Variance Estimation with Uncertain Statistical Model // Proc. IEEE CDC. -2001, p. 3497-3499.
18. *Bitar E., Baeyens E., Packard A., et al*. Linear Minimax Estimation for Random Vectors with Parametric Uncertainty // Proc. Amer. Control Conf. -2010, p. 590-592.
19. *Коган М.М.* Робастное оценивание и фильтрация в неопределенных линейных системах при неизвестных ковариациях // Автоматика и телемеханика. -2015, № 10, с. 50-66.
20. *Samuel Kotz, Tomasz J. Kozubowski, Krzysztof Podgorski.* The Laplace Distribution and Generalizations, -2001, Springer.
21. *Миллер Б.М., Колосов К.С.* Робастное оценивание на основе метода наименьших модулей и фильтра Калмана // Автоматика и телемеханика. -2020, №11, с.72-92.
22. Справочник по теории автоматического управления / Под ред. Красовского А.А. -М.: Наука. Гл. ред. физ. -мат. лит. 1987.
23. *Розенберг И.Н., Соколов С.В. ,Уманский В.И., Погорелов В.А.* Теоретические основы тесной интеграции инерциально-спутниковых навигационных систем. -М.: Физматлит, 2018.
24. *Дмитриев В.И.* Навигация и лоция. -М.: Моркнига, 2009.
25. *Соколов С.В.* Аналитические модели пространственных траекторий для решения задач навигации // Прикладная математика и механика. 2015. Т.79. №1. С.24-30

Г.С. Домбаян[1], О.В. Куликова[1], В.П. Шпаковский[2]

РАСПОЗНАВАНИЕ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ АЛГОРИТМОВ, ОСНОВАННЫХ НА НЕЧЕТКИХ НЕЙРОННЫХ СЕТЯХ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»
Ростов-на-Дону, Россия[1]
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный университет путей сообщения»
Ростов-на-Дону, Россия[2]

Ключевые слова: изображение, графический образ, алгоритм, модель, нечеткая логика, нейронные сети.

В статье будет подробно раскрыта сущность нечетких нейронных сетей; исследованы модели и алгоритмы распознавания изображений на основе нечетких нейронных сетей.

G.S. Dombayan[1], O.V. Kulikova[1], V.P. Shpakovskiy[2]

IMAGE RECOGNITION USING ALGORITHMS BASED ON FUZZY NEURAL NETWORKS

Federal State Budgetary Educational Institution of Higher Education «Don State Technical University» Rostov-on-Don, Russia[1]
Federal State Budgetary Educational Institution of Higher Education «Rostov State Transport University» Rostov-on-Don, Russia[2]

Keywords: image, graphic image, algorithm, model, fuzzy logic, neural networks.

The article will reveal in detail the essence of neural networks; explore models and algorithms for image recognition based on fuzzy neural networks.

За последние несколько лет произошел большой и энергичный рост в развитии научных и прикладных исследований, направленных на синтез нечеткой логики с нейронными сетями. Нечеткая нейронная сеть или нейро-нечеткая система является системой из области искусственного интеллекта, которая находит параметры нечетких систем, т.е. нечетких множеств за счет использования методов аппроксимации нейронных сетей. При применении этих двух концепций вместе пропадают недостатки, которые могут возникать при использовании их порознь. [1]

Нейронные сети имеют огромное преимущество перед традиционными статистическими методами.Одним из таких преимуществ является то, что нейронные сети способны оперировать дополнительной информацией, такой как высота и наклон предмета.

Нейронные сети целесообразно применять только в том случае, если проблема выражена достаточным количеством наблюдаемых примеров. Эти наблюдения используются для обучения нейронной сети. С одной стороны, никаких предварительных знаний о проблеме не требуется. Однако нелегко извлечь понятные правила из структуры нейронной сети.

Модели, основанные на нечетких нейронных сетях – это такие модели, которые являются объединением теории нечетких множеств, как механизма представления знаний и искусственного интеллекта. Главной особенностью этих моделей является прозрачность, поскольку набор нечетких правил могут быть извлечены из структуры сети после обучения.

Кроме того, данные модели имеют топологию нейронной сети, что позволяет использовать большое разнообразие существующих алгоритмов машинного обучения для идентификации структуры и оценки параметров. Нечеткие нейронные сети используются для решения различных задач, таких, как прогнозирование, распознавание и классификация. [2]

Нейро-нечёткие системы в исследовательской сфере нечёткого моделирования разделены на две зоны:

1. Лингвистическое нечёткое моделирование, которое ориентировано на интерпретируемость;
2. Точное нечёткое моделирование, которое ориентировано на точность.

Каждая такая нейронная сеть должна быть обучена и обладать знаниями. Если знание является неполным, неправильным или противоречивым, то нейро-нечеткая система должна быть готова и к этому. Поскольку формального подхода к такого рода задач нет, то настройка выполняется эвристическими методами. Это обычно занимает очень много времени и не исключает наличие ошибок. [3]

Рассмотрим структуру нейронных сетей. Каждая сеть состоит из нейронов. Нейрон – это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше. Они делятся на три основных типа: входной, скрытый и выходной. Нейроны оперируют числами в диапазоне [0,1] или [-1,1]. [4]

Также, следует упомянуть такое понятие в теории нейронных сетей, как синапс. Синапс представляет собой связь между двумя нейронами. У синапсов имеется один параметр – вес. Благодаря ему, входная информация изменяется, когда передается от одного нейрона к другому.

Обучение нейросети выполняется в два этапа. На первом этапе определяются нечеткие множества для каждого входного нейрона, выбор подходящего числа нейронов и определение структуры. Наиболее часто используемые методы определения структуры – кластеризация и эволюционная оптимизация. Как только структура сети определена, наступает второй этап – оцениваются свободные параметры.

Что касается оптимизации структуры сети, то на этом этапе могут возникнуть сложности. Эволюционная оптимизация требует очень больших вычислительных мощностей, по сравнению с кластеризацией. Тем не менее, нечеткие правила обычно не могут быть извлечены из результирующей сети, поскольку нечеткие множества, генерируемые кластеризацией, обычно трудно интерпретировать. [5]

Существует три основных метода распознавания образов:

- Статистический – определяет, чему принадлежит конкретный фрагмент изображения. Эта модель использует контролируемое машинное обучение.
- Синтаксический/Структурный – используется, чтобы определить более сложные отношения между элементами. Эта модель использует машинное обучение под наблюдением.
- Сопоставление с шаблоном – для сопоставления свойств объекта с предопределенным шаблоном и идентификации объекта. Одним из применений такой модели является проверка на плагиат [6].

Выделяют исследовательский алгоритм распознавания образов, который используется для распознавания общности данных, при этом необходимо собрать все характеристики изучаемого объекта, и описательный алгоритм распознавания образов, используемый для классификации общих черт определенным образом.

Комбинация этих двух элементов используется для извлечения информации из данных, включая использование в аналитике. Анализ общих факторов и их взаимосвязи раскрывает детали в предмете, которые могут иметь решающее значение для его понимания.

Алгоритм состоит из следующих этапов:

1. Данные собираются из источников.
2. Данные очищаются от лишнего.
3. Информация проверяется на наличие соответствующих признаковили общих элементов.
4. Эти элементы впоследствии сгруппированы в определенные сегменты.
5. Сегменты анализируются для понимания наборов данных.
6. Извлеченные данные внедряются в другие операции [7].

При решении конкретных задач, важно учитывать, какие данные есть, чтобы избежать избыточности в описании графического образа. В данной статье были рассмотрены различия нейронной сети и нечеткой нейронной сети, основные методы и алгоритмы распознавания образов.

СПИСОК ЛИТЕРАТУРЫ

1. Buckley, J. J. and Hayashi, Y. (1994). Fuzzy neural networks: A survey, Fuzzy Sets and Systems. Pp. 78-82.
2. W. Caminhas, H. Tavares, F. Gomide, and W. Pedrycz, “Fuzzy sets based neural networks: Structure, learning and applications,” Journal of Advanced Computational Intelligence, vol. 3, no.3, 1999, pp. 151-157.
3. A. E. Gobi and W. Pedrycz, "Logic minimization as an efficient means of fuzzy structure discovery," IEEE Transactions on Fuzzy Systems, vol. 16, no. 3, pp. 553- 566, JUN 2008.
4. Buckley, J. J. and Hayashi, Y. (1995). Neural networks for fuzzy systems, Fuzzy Sets and Systems. p. 265.
5. Nauck, D. and Kruse, R. (1997). Function Approximation by NEFPROX, in Proc. Second European Workshop on Fuzzy Decision Analysis and Neural Networks for Management. pp. 254-257.
6. Bezdek, J. C., Tsao, E. C.-K. and Pal, N. R. (1992). Fuzzy Kohonen Clustering Networks. p.129.
7. Kosko, B. (1992). Neural Networks and Fuzzy Systems. A Dynamical Systems Approach to Machine Intelligence. pp. 67-76.

А.В. Бородин, А.А. Бородина

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ПИРОЭЛЕКТРИЧЕСКИХ МАТЕРИАЛОВ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: пироэлектрический эффект, поляризованность, пироэлектрические приемники, сегнетоэлектрики.

В статье перечислены особенности пироэлектрических материалов. В пироэлектриках тепловая энергия может непосредственно превращаться в электрическую за счет пироэлектрического эффекта, то есть за счет изменения собственной поляризации пироэлектриков при изменении температуры. Поиск новых пироэлектриков связан с

улучшением качества материалов, предназначенных для создания высокочувствительных и малоинерционных пироэлектрических приемников излучения, пировидиконов и других пироэлектрических устройств. Рассмотрены наиболее перспективные направления применения пироэлектрических материалов.

A.V. Borodin, A.A. Borodina

PROSPECTIVE DIRECTIONS OF USING PYROELECTRIC MATERIALS

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

Keywords: pyroelectric effect, polarization, pyroelectric receivers, ferroelectrics.

The article considers the features of pyroelectric materials. Thermal energy in pyroelectrics can be directly converted into electrical energy due to the pyroelectric effect, that is due to the changing intrinsic polarization of pyroelectrics when the temperature changes. A search for new pyroelectrics is associated with improving the quality of materials intended for creating highly sensitive and low-inertia pyroelectric radiation detectors, pyrovidicons and other pyroelectric devices. The article examines the most promising areas of application of pyroelectric materials.

В некоторых диэлектриках электрическая поляризация может длительно существовать в отсутствие приложенного извне электрического поля. Это поляризованное состояние может быть как стабильным и весьма устойчивым к внешним воздействиям, так и существовать в виде метастабильного состояния, которое может быть нарушено. В первом случае поляризация называется «спонтанной», а во втором случае – «остаточной». В спонтанно поляризованных диэлектриках тепловая энергия может непосредственно превращаться в электрическую энергию за счет пироэлектрического эффекта, т. е. за счет изменения собственной поляризации диэлектриков при нагревании и охлаждении. Таким образом, пироэлектрик, как и пьезоэлектрик, представляет собой твердотельный преобразователь энергии. Только пьезоэлектрик является электромеханическим преобразователем, а пироэлектрик представляет собой теплоэлектрический преобразователь. Такое превращение энергии в твердом теле возможно только в том случае, когда диэлектрик (кристалл, поликристалл или полимер) электрически поляризован. Однако эта поляризация в отсутствие внешних воздействий заметным образом не проявляется. Дело в том, что при неизменной температуре спонтанная поляризация обычно полностью скомпенсирована электрическими зарядами, оседающими на поверхности полярного диэлектрика или на электродах. Собственная поляризация пироэлектрика проявляется только при динамическом изменении внешних условий. Изменение механических напряжений приводит к пьезоэлектрической поляризации полярного диэлектрика. Пироэлектрическая поляризация проявляется при изменении температуры полярного вещества. Поиск новых пироэлектриков теснейшим образом связан с улучшением качества материалов, предназначенных для создания высокочувствительных и малоинерционных пироэлектрических приемников излучения, пировидиконов и других пироэлектрических устройств.

Основной характеристикой пироэлектрического кристалла, непосредственно определяемой в эксперименте, является тензор первого ранга – вектор пироэлектрических коэффициентов (измеряется не сама спонтанная поляризация, а ее изменение с температурой). Обнаружить пироэлектрические свойства кристалла позволяет изменение его температуры, приводящее к возникновению поверхностного заряда на гранях образца, перпендикулярных к особенной полярной оси. Описанное явление и носит название

пироэлектрического эффекта. Пироэлетрики обладают поляризованностью, которая изменяет свою величину *Ps* с изменением температуры образца. При тепловом равновесии связанные заряды экранируются свободными зарядами, накапливающимися на электродах или в поверхностных слоях. Экранирование нарушается при изменении температуры, и возникает электрический ток.

При отсутствии внешнего электрического поля, а также при отсутствии механических воздействий изменение поляризованности с температурой возможно только в кристаллах, где поляризованность существует спонтанно. Так, вблизи температуры 300 К, спонтанная поляризованность специально синтезированных кристаллов – пироэлектриков равна: в ниобате лития *Ps* = 100 мкКл/см^2, в сульфате лития *Ps* = 6 мкКл/см^2, в виннокислом калии *Ps* = 80 мкКл/см^2. В природном кристалле турмалина спонтанная поляризованность равна 17 мкКл/см^2.

Все сегнетоэлектрики потенциально являются пироэлектриками, так как они спонтанно поляризованы. Сегнетоэлектрики обладают довольно большими значениями пироэлектрического коэффициента. В тоже время, спонтанная поляризация у сегнетоэлектриков наблюдается только в определенном диапазоне температур, ограниченном температурой сегнетоэлектрического фазового перехода – температурой Кюри T_K. При повышении температуры спонтанная поляризация уменьшается и исчезает в точке фазового перехода T_K. Для того, чтобы сегнетоэлектрический кристалл приобрел высокие пироэлектрические свойства, необходимо сделать его поляризацию однородной, а сам кристалл – монодоменным. Монодоменизацию сегнетоэлектриков можно осуществить разными способами. Например, для достижения монодоменного состояния в сегнетоэлектрическую матрицу вводят полярные дефекты (примеси), создающие внутреннее смещающее поле, постоянно поляризующее кристалл. В сегнетоэлектриках с высокой температурой Кюри (ниобат лития $LiNbO_3$, T_C = 1000 °C; танталат лития $LiTaO_3$, T_C = 665 °C и др.) монодоменное состояние может быть получено охлаждением кристалла в электрическом поле через точку Кюри до комнатной температуры. Монодоменное состояние также можно формировать непосредственно в процессе выращивания кристаллов. На практике широко используются керамические сегнетоэлектрики на основе твердых растворов титаната свинца и цирконата свинца - $PbTiO_3$–$PbZrO_3$ (ЦТС) с различными добавками. Керамические образцы, охлажденные в электрическом поле с прохождением точки Кюри, сохраняют довольно высокую остаточную электрическую поляризацию, что позволяет их эффективно использовать в качестве пироэлементов [1].

Так в [2] для поликристаллических составов типа ЦТС, синтезированных в области морфотропного фазового перехода, исследованы температурные изменения пироэлектрического коэффициента в динамическом режиме измерения в зависимости от режима поляризации. Предварительную поляризацию образцов проводили в двух режимах: в сегнетоэлектрической фазе ($T_п$ = 160ºC), в электрическом поле $E_п = 4\times10^6$ В/м при выдержке 30 мин с последующим охлаждением до комнатной температуры («высоковольтная» поляризация); с переходом через точку Кюри ($T_к$) в электрическом поле $E_п = (4\text{-}5)\times10^5$ В/м в процессе охлаждения до комнатной температуры от $T_{max} \approx (350\text{-}400)$ºC («низкоковольтная» поляризация). В процессе эксперимента были выявлены температурные интервалы термодинамической нестабильности доменных и фазовых структур после «высоковольтной» поляризации. У образцов, претерпевающих фазовый переход в сегнетоэлектрическое состояние в электрическое поле, обнаружена повышенная термическая стабильность доменных структур.

Кроме того, важную в практическом отношении группу пироматериалов составляют полярные пленочные полимеры типа поливинилфторида и поливинилиденфторида. Поскольку при увеличении толщины материала пироэлектрические свойства ухудшаются, оптимальной формой существования таких пироэлектриков является пленка. Для

получения устойчивого полярного состояния пленки этих соединений раскатываются до 5 – 15 мкм. После специальной обработки (механическое растяжение, охлаждение в электрическом поле) такие полимерные пленки приобретают спонтанную поляризацию и пироэлектрический эффект.

Пироэлектрики можно применять для детектирования любого излучения, которое вызывает изменение температуры кристалла, от рентгеновского до микроволнового, и даже для детектирования элементарных частиц. К тому же они имеют следующие полезные характеристики: работают при комнатной температуре (или при любой другой удобной температуре). Обладают простой конструкцией, просты в эксплуатации и к ним не нужно прикладывать внешнее смещающее поле. Однако в отличие от других тепловых приемников пироэлектрический токовый отклик зависит от скорости изменения температуры, а не от самой температуры. По этой причине максимальный отклик получается при временах, меньших времени термической релаксации элемента, поэтому пироэлектрики по своему существу являются значительно более высокочастотными приборами, чем другие тепловые приемники [3].

Перспективно применение пироэлектрических приемников в области частот инфракрасного (ИК) диапазона. Они практически решают проблему детектирования потоков тепловой энергии малой мощности; измерения формы и мощности коротких (10^{-5} - 10^{-11}с) импульсов лазерного излучения; чувствительного контактного и бесконтактного измерения температуры (чувствительность пироэлектрических термометров достигает 10^{-6} К) [4]. Пириконы применяются в различных областях: в системах охранной и пожарной сигнализации, при дистанционных измерениях температуры, космических исследованиях, в лазерной измерительной аппаратуре, военной технике, в медицине и др. Пироэлектрические приемники самой различной формы и размеров технологичны и сравнительно недороги. Низкая теплопроводность пироэлектрических кристаллов позволяет создавать многоэлементные структуры с низкими перекрестными тепловыми помехами между отдельными элементами чувствительного слоя.

В настоящее время широко обсуждается возможность применения пироэлектриков для прямого преобразования тепловой энергии в электрическую: переменный поток тепловой энергии вызывает переменный ток во внешней цепи пироэлектрического элемента. Хотя КПД подобного устройства уступает имеющимся способам преобразования энергии, для некоторых специальных применений данный способ преобразования является конкурентоспособным. Например, был разработан новый способ эффективного преобразования тепла, которое выделяется в проводах, в электрический ток. Для этого предложено использовать пленку из материала, который на треть состоит из титаната свинца, а на две трети — из смешанного ниобата свинца и магния. Этот материал обладает свойствами сегнетоэлектрического релаксора, то есть при определенной температуре может переходить в поляризованное состояние, при этом такой переход происходит не скачком, а сильно растягивается по температуре. За счет этого материал можно использовать как пироэлектрик, то есть при нагревании в нем происходит разделение зарядов и возникает разность потенциалов. При этом используется для преобразования тепла не объемный материал, а пленка толщиной всего 150 нанометров, что дает возможность для применения подхода в широком диапазоне температурных колебаний и электрических напряжений.

СПИСОК ЛИТЕРАТУРЫ

1. *Бородин А.В., Захаров Ю.Н., Резниченко Л.А*. Влияние полей объемных зарядов на пироэффект в сегнетокерамике $(1-x)NaNbO_3–xKNbO_3$. Сборник трудов

Международного симпозиума «Порядок, беспорядок и свойства оксидов», (“ODPO-2002”), Сочи, 2002г., с.41-42.
2. *Захаров Ю.Н., Бородин А.В., Бородин В.З.* Пироэлектрические свойства сегнетокерамики типа ЦТС в области морфотропного фазового перехода. - Известия РАН. Серия физическая. т.71, номер 5, 2007г., с.709 -710.
3. *Бородин А.В.* Пироэлектрический эффект и его применение. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2016. № 1. С. 57-60.
4. *Бородин А.В.* Преимущества использования пироэлектрических приемников. «Фундаментальные проблемы радиоэлектронного приборостроения», 2016 т.16 №4 с.19-21.

А.И. Сакалова[1], В.В. Ершов[1], Н.В. Руденко[2], Д.А.Жукова[2]

ЭЛЕКТРОСНАБЖЕНИЕ ОБЪЕКТОВ СВЯЗИ В РЕГИОНАХ С ДОСТАТОЧНЫМ РЕСУРСОМ ВЕТРОВОЙ ЭНЕРГИИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: автономное электроснабжение объектов мобильной связи, возобновляемые источники энергии, вертикальные ветроэнергетические установки, гибридная ветро-дизельная энергетическая установка.

В статье решается задача надёжного и экономичного электроснабжения объектов связи в регионах централизованного и децентрализованного электроснабжения. В регионах с достаточным ресурсом ветровой энергии предложено в качестве основных, резервных и автономных источников электроэнергии использовать ветроустановки. Проведен анализ технических характеристик и сделан выбор в пользу ветроустановок с вертикальной осью вращения в качестве первичных источников для объектов связи. Предложены структуры и разработаны алгоритмы работы схем электроснабжения для объектов связи в зонах централизованного и децентрализованного электроснабжения. Показано, что предлагаемые структуры позволяют экономить потребляемую от государственной сети электроэнергию за счет использования энергии ветра.

A.I. Sakalova[1], V.V. Ershov[1], N.V. Rudenko[2], D.A. Zhukova[2]

ELECTRICITY SUPPLY OF COMMUNICATION OBJECTS IN REGIONS WITH SUFFICIENT RESOURCE OF WIND ENERGY

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia
Federal State Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia[2]

Key words: autonomous power supply of mobile communication facilities, renewable energy sources, vertical wind power plants, hybrid wind-diesel power plant.

The article solves the problem of reliable and economical power supply of communication facilities in the regions of centralized and decentralized power supply. In regions with a sufficient resource of wind energy, it is proposed to use wind turbines as the main, reserve and autonomous sources of electricity. The analysis of technical characteristics is carried out and a choice is made in favor of wind turbines with a vertical axis of rotation as primary sources for communication objects. Structures are proposed and algorithms for the operation of power supply schemes for communication facilities in the zones of centralized and decentralized power supply are developed. It is shown that the proposed structures allow saving energy consumed from the state grid through the use of wind energy.

Введение. Надежное, качественное и экономически обоснованное обеспечение потребностей внутреннего рынка страны в энергоносителях, энергии и сырье на принципах энергосбережения и энергоэффективности является целью государственной программы Российской Федерации "Развитие энергетики" [1]. Достижение этой цели в плане бесперебойного электроснабжения регионов РФ обеспечивает рост и укрепление экономики государства.

В рамках действующей государственной системы централизованного электроснабжения механизм обеспечения электроэнергией регионов на территории РФ представляется достаточно неоднородным. Одни из них находятся в зоне непосредственной близости от этой системы, другие - на значительных расстояниях, для третьих получение электроэнергии от этой системы невозможно по различным причинам. В зоне децентрализованного электроснабжения находится более 50% территории России. На ней проживает около 20 млн человек [2, 3]. Главными элементами для коммуникации населения в этих регионах являются базовые станции (БС) системы сотовой связи. Их надежное функционирование обеспечивается автономными системами электроснабжения (АСЭ).

Известно [4-6], что в качестве первичных источников электрической энергии на таких станциях широкое применение в настоящее время находят устройства на основе возобновляемых источников электроэнергии (ВИЭ), использующих энергию солнца и ветра в сочетании с накопителем энергии в виде аккумуляторной батареи (АКБ) и резервным источником на базе дизель-электрической установки (ДЭУ).

Значительные территории в зонах централизованного и децентрализованного электроснабжения характеризуются преобладающими потенциалами энергии ветра над энергией солнца. К регионам с достаточно высоким ресурсом ветровой энергии (более 5 м/с) относятся районы Севера, Заполярье, районы Дальнего Востока, Калининградская, Ленинградская, Архангельская, Мурманская, Новосибирская, Магаданская, Камчатская области [4-6]. Поэтому для этих регионов актуальной является проблема надежного и экономичного электроснабжения объектов связи на базе ветроэнергетических установок (ВЭУ). В этой связи обоснование и разработка систем электроснабжения (СЭ) для объектов связи в регионах с достаточным ресурсом ветровой энергии является актуальной научно-технической задачей.

Результаты исследований. Для решения этой задачи требуется рассмотрение следующих вопросов:

- выбор и обоснование ВЭУ для регионов с достаточным ресурсом ветровой энергии;
- разработка структур СЭ как для объектов связи в регионах централизованного электроснабжения, так и вне зон централизованного электроснабжения;

Выбор и обоснование ВЭУ для регионов с достаточным ресурсом ветровой энергии. Применительно к объектам связи в указанных регионах наиболее целесообразно применение ВЭУ с вертикальной осью вращения. По сравнению с горизонтальными эти ВЭУ обладают следующими достоинствами [7 - 12]:

- пониженная начальная скорость вращения (от 1,3 м/с);
- не создает вибрацию на грунт;
- не требует установки высоких мачт;
- экологичны (уровень шума не превышает 35 дБ);
- не требуется система ориентации на ветер;
- используют энергию не только горизонтальных, но и восходящих потоков ветра.

Применение в этих регионах в качестве ВЭУ солнечных батарей нецелесообразно. Это обусловлено их большой площадью и усложнением в этой связи процесса эксплуатации в условиях сильных ветров и снежных заносов. Таким образом, СЭ для объектов регионов с достаточным ресурсом ветровой энергии целесообразно строить на базе ВЭУ с вертикальной осью вращения.

Вариант построения структуры системы электроснабжения базовой станции сотовой связи. Для регионов с достаточным ресурсом ветровой энергии и продолжительным зимним периодом наиболее целесообразно применение ВЭУ. Источниками питания в этом случае являются: районная централизованная энергосистема и ВЭУ. Схема СЭ БС представлена на рисунке 1. Алгоритм работы системы состоит в следующем. При текущем значении требуемой электрической мощности $P_{\Sigma.ТР.}$, меньшем суммарной мощности, вырабатываемой ВЭУ $P_{ВЭУ}$ приемники обеспечиваются электроэнергией от ВЭУ. Потребление электроэнергии от централизованной энергосистемы отсутствует, а значит, имеет место экономия средств компании на оплату за потребляемую энергию. При текущем значении требуемой электрической мощности $P_{\Sigma.ТР.}$, большем суммарной мощности, вырабатываемой ВЭУ $P_{ВЭУ}$ приемники обеспечиваются электроэнергией от централизованной энергосистемы и ВЭУ. Описанный алгоритм реализуется схемой, представленной на рисунке 1.

При $P_{\Sigma.ТР.}$, меньшем суммарной мощности, вырабатываемой ВЭУ $P_{ВЭУ}$ электроэнергия напряжением 0,38 кВ с выхода ВЭУ через коммутаторы К2, К1, распределительный щит ЩР1 подается к приемникам БС. Текущее значение требуемой мощности контролируется датчиком потребляемой мощности ДПМ. В случае понижения скоростного напора воздуха и уменьшения по этой причине вырабатываемой электрической мощности по команде от системы управления коммутатор К2 переключает выход ВЭУ на выпрямитель В1.

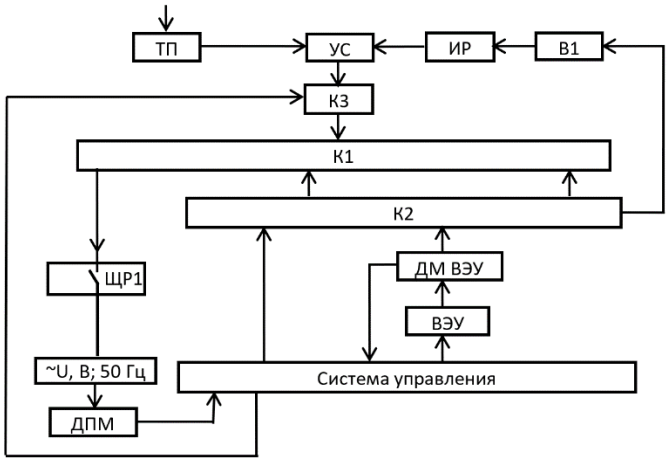


Рисунок 1. Структурная схема системы электроснабжения БС
при комбинированном электроснабжении от электросетей и ВЭУ

С выхода В1 выпрямленное напряжение подается на регулируемый инвертор ИР и далее на устройство согласования УС. После выполнения в УС условий для параллельной работы ВЭУ (через ИР) по команде от СУ срабатывает коммутатор К3. Электроэнергия с выхода УС через коммутатор К1, распределительный щит ЩР1 подается к приемникам БС. При этом мощность, вырабатываемая ВЭУ, является составной компонентой в общем балансе потребляемой приемниками мощности. В результате потребляемая мощность от централизованной энергосистемы через ТП снижается, что повышает эффективность в целом такой системы электроснабжения.

Таким образом предлагаемая схема позволяет снизить зависимость от возможных перебоев питания потребителей в зонах неустойчивого электроснабжения, повысить эффективность СЭ БС и обеспечить энергосбережение.

Разработка структуры автономной системы электроснабжения БС на основе гибридной ветро-дизельной энергетической установки. Для регионов страны с неразвитой инфраструктурой распределительных электрических сетей централизованной энергосистемы, значительной удаленностью от них или трудностями с подключением к стационарным сетям наиболее приемлемым вариантом электроснабжения БС является организация электроснабжения на базе автономной системы электроснабжения. Для решения задачи обеспечения электроэнергией в составе системы электроснабжения в качестве основных источников энергии целесообразно иметь ВЭУ, АКБ, а в качестве резервного источника– дизель-электрическую установку (ДЭУ). С целью достижения энергосбережения базовым принципом построения такой АСЭ БС является максимально возможное использование энергии ветра при минимальном применении энергии ДЭУ. Энергию ветра целесообразно оценивать текущим значением электрической мощности, вырабатываемой ВЭУ ($Р_{ВЭУ}$).

Алгоритм работы системы состоит в следующем. При текущем значении электрической мощности $Р_{ВЭУ,}$ большем текущего требуемого значения $Р_{Σ.ТР}$ приемники станции могут обеспечиваться от ВЭУ. Текущие значения генерируемых мощностей контролируются соответствующими датчиками (ДМ ВЭУ, ДМ ДЭУ, ДМ АКБ). Требуемое текущее значение мощности контролируется датчиком потребляемой мощности (ДПМ).

При недостаточном суммарном текущем значении $Р_{ВЭУ}$ включается в работу и обеспечивает потребителей станции ДЭУ. Таким образом, ДЭУ как резервный источник задействуется только в случае невозможности покрытия требуемой текущей мощности $Р_{Σ.ТР}$ от ВЭУ. Описанный алгоритм реализуется схемой, представленной на рисунке 2.

При достаточном уровне текущего значения $P_{ВЭУ}$ переменное напряжение с выхода ВЭУ через коммутатор К1, распределительный щит ЩР1 подается к приемникам станции и выпрямителю В1 для подзарядки АКБ.

При снижении уровня текущего значения $P_{ВЭУ}$ до установленного порогового значения, позволяющего покрыть дефицит требуемой мощности от АКБ, по команде от системы управления АКБ подключается к входу ИР, с выхода которого напряжение подается на устройство согласования (УС). На второй вход УС через коммутатор К1 подается напряжение от ВЭУ. После выполнения условий для параллельной работы ВЭУ и регулируемого инвертора по команде от системы управления срабатывает коммутатор К3.

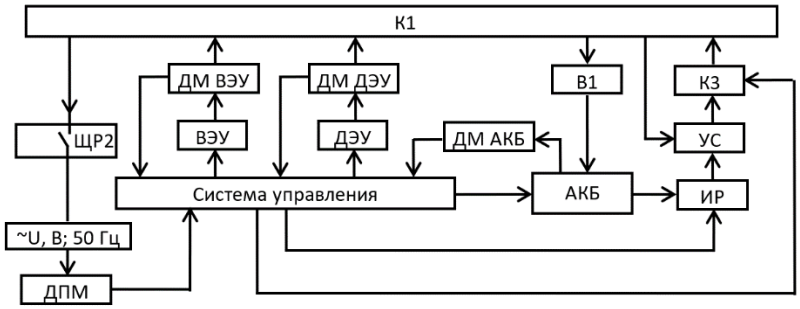


Рисунок 2. Структурная схема автономной системы электроснабжения на основе гибридной ветро-дизельной энергетической установки

Электроэнергия с выхода УС через коммутатор К1 распределительный щит ЩР1 подается к приемникам БС. При этом мощность АКБ является составной компонентой в общем балансе потребляемой БС мощности.

В том случае, если суммарное текущее значение электрической мощности $P_{ВЭУ}$ таково, что компенсировать дефицит требуемой мощности станции $P_{Σ.ТР}$ за счет АКБ оказывается невозможно, система управления через коммутатор К1 формирует команду на отключение всех приемников от ВЭУ**,** проводит запуск ДЭУ и после контроля ее выходных параметров переводит питание приемников с ВЭУ на ДЭУ через коммутатор К1 и распределительный щит ЩР1. Зарядка АКБ осуществляется от ДЭУ через коммутатор К1 и выпрямитель В1. Таким образом, предложенная структурная схема автономной системы электроснабжения на основе гибридной ветро-дизельной энергетической установки позволяет осуществить энергосбережение за счёт максимально возможного использования энергии ветра при минимальном применении энергии ДЭУ.

Выводы.

1. Электроснабжение объектов связи в регионах с достаточным ресурсом ветровой энергии целесообразно осуществлять на базе ветроэнергетических установок. Наиболее предпочтительными для этой цели являются установки с вертикальной осью вращения. Это обусловлено их улучшенными характеристиками.
2. В регионах централизованного электроснабжения для обеспечения энергосбережения, а также бесперебойной работы объектов связи целесообразно использовать параллельную работу ВЭУ и стационарной питающей сети.
3. В регионах децентрализованного электроснабжения для обеспечения требуемой бесперебойности и энергосбережения целесообразно электроснабжение объектов связи осуществлять на основе гибридной ветро-дизельной энергетической установки.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении государственной программы Российской Федерации "Развитие энергетики" (с изменениями на 2 марта 2020 года) [Электронный ресурс]: URL: //http://docs.cntd.ru/document/499091759 / (дата обращения 14.09.2021 г.)
2. 65% территории страны без электричества: Перспективы возобновляемых источников энергии в России [Электронный ресурс]: URL: https://tjournal.ru/flood/36775-65-territorii-strany-bez-elektrichestva-perspektivy-vozobnovlyaemyh-istochnikov-energii-v-rossii/ (дата обращения 22.09.2021 г.)
3. Автономное энергоснабжение энергокомплексами на базе возобновляемых источников энергии [Электронный ресурс]: URL: https://www.c-o-k.ru/articles/avtonomnoe-energosnabzhenie-energokompleksami-na-baze-vozobnovlyaemyh-istochnikov-energii / (дата обращения 22.09.2021 г.)
4. Лукутин Б.В., Муравлев И.О., Плотников И.А. Системы электроснабжения с ветровыми и солнечными электро-станциями: учебное пособие. Томск: Изд-во Томского политехнического университета, 2015. 128 с.
5. Национальный исследовательский университет «Высшая школа экономики». Научные подразделения. Институт статистических исследований и экономики знаний. Форсайт-центр. Новости. Солнечно-ветровые установки повысят эффективность преобразования энергии. [Электронный ресурс]: URL:https://foresight.hse.ru/news/152660612.html (дата обращения 24.09.2021 г.)
6. Перспективы развития и применения альтернативных источников энергии [Электронный ресурс]: URL: https://promdevelop.ru/perspektivnost-razvitiya-i-primeneniya-alternativnyh-istochnikov-energii/ (дата обращения 28.09.2021 г.)
7. Основные виды ветрогенераторов: вертикальные, горизонтальные. [Электронный ресурс]: URL: http://tcip.ru/blog/wind/osnovnye-vidy-vetrogeneratorov-vertikalnye-gorizontalnye.html (дата обращения 21.09.2021 г.).
8. Ветрогенераторы с вертикальной осью вращения российского производства. [Электронный ресурс]: URL: http://www.ekopower.ru/vetrogeneratoryi-s-vertikalnoy-osyu-vrashheniya-rossiyskogo-proizvodstva/ (дата обращения 08.09.2021 г.).
9. Сравнительный анализ ветрогенераторов Сравнительный анализ вертикально-осевых и горизонтально пропеллерных ветроустановок. [Электронный ресурс]: http://www.ecoteco.ru/id1198(дата обращения 04.10.2021 г.).
10. Что лучше - вертикальный или горизонтальный ветрогенератор? Преимущества и недостатки [Электронный ресурс]: URL:http://vetrogenerator.com.ua/vetrogenerator/vertikal/148-chto-luchshe-vertikalnyy-ili-orizontalnyy-vetrogenerator-preimuschestva-i-nedostatki.html. (дата обращения 04.10.2021 г.).
11. Соломин, Е.В. Технические особенности и преимущества ветроэнергетических установок / Е.В.Соломин, Р.Л.Холстед // Альтернативная энергетика и экология. – М.: НИИЭС, 2010. – №1. – С.36–41.
12. Соломин Е.В. Ветроэнергетические установки ГРЦ-Вертикаль // Альтернативная энергетика и экология, 2010 № 1.С. 10-15.

Т.Д. Фатхулин, С.Г. Хорикова, В.М. Щитов

АНАЛИЗ КЛЮЧЕВЫХ ОСОБЕННОСТЕЙ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ ОПТИЧЕСКИХ СЕТЕЙ (SDON)

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Москва, Россия
t.d.fatkhulin@mtuci.ru

Ключевые слова: технология, программно-конфигурируемые сети, программно-конфигурируемые оптические сети, реализация, технические решения, сервис.

В статье рассматриваются ключевые особенности реализации программно-конфигурируемых оптических сетей (ПКОС). Описаны концепции технологии программно-конфигурируемых сетей (ПКС), ее модель, приведены варианты реализации ПКС. Выявлены преимущества и недостатки этой технологии. Показано, что для организации предоставления современных сервисов клиентам в ПКС требуется обеспечить сетевую транспортную инфраструктуру посредством ПКОС. Представлена архитектура ПКОС. Показано, что в совокупности технологии DWDM, OTN, IP/MPLS и ПКС предлагают решения для реализации ПКОС.

T.D. Fatkhulin, S.G. Horikova, V.M. Shchitov

ANALYSIS OF PRINCIPAL FEATURES OF SOFTWARE-DEFINED OPTICAL NETWORKS (SDON) TECHNOLOGY

Moscow Technical University of Telecommunications and Informatics,
Moscow, Russia
t.d.fatkhulin@mtuci.ru

Keywords: technology, software-defined networks, software-defined optical networks, realization, technical solutions, service.

The article discusses the key features of the implementation of software-defined optical networks (SDON). The concepts of software-defined networks (SDN) technology and its model are described. Options for the implementation of SDN are given. The advantages and disadvantages of this technology are revealed. It is shown that in order to organize the provision of modern services to clients in SDN, it is required to provide the network transport infrastructure by means of SDON. The architecture of SDON is presented. It is shown that combination of DWDM, OTN, IP / MPLS and SDN technologies offer solutions for the implementation of SDON.

Введение

В современном мире технология программно-конфигурируемых сетей (ПКС, Software Defined Networks – SDN) представляет собой одно из самых перспективных направлений развития сетевой индустрии [1, 2]. ПКС дают возможность обеспечить гибкость в управлении потоками данных за счет разделения контура управления сетью и контура передачи данных [2]. Также технология ПКС позволяет устранить проблемы неполной совместимости сетевых решений и зависимости операторов сетей от производителей сетевого оборудования, которые существовали в традиционных сетях [1, 2].

Программно-конфигурируемые оптические сети ПКОС (Software Defined Optical Networks – SDON) являются подвидом ПКС. ПКОС позволяют обеспечить сетевую

транспортную инфраструктуру для реализации «облачных» технологий и организации предоставления современных сервисов клиентам.

Целью настоящей работы является анализ ключевых особенностей реализации технологии программно-конфигурируемых оптических сетей (ПКОС). Для достижения поставленной цели необходимо решить следующие задачи: проанализировать основные концепции технологии программно-конфигурируемых сетей (ПКС), подвидом которых являются ПКОС, рассмотреть варианты реализации ПКС, выявить преимущества и недостатки этой технологии, проанализировать архитектуру ПКОС, а также ключевые особенности технологий, реализующих ПКОС. Методологическую основу работы составляют методы теоретического анализа, сравнительный и описательный методы, а также метод обобщения.

Технология ПКС

Достоинства и возможности ПКС-подхода стали ощутимы совсем недавно [1]. Тем не менее, многие идеи, на которых он базируется (программируемость сетевых элементов, виртуализация сетей, отделение уровня управления от уровня передачи данных и логическая централизация управления), появились более 20 лет назад.

Еще в телефонных сетях предполагалось применить идею разделения уровней передачи данных и уровня управления передачей данных [1]. Апробация многих идей ПКС-подхода была проведена при исследовании активных сетей [1], работа над которыми велась в середине 1990-х гг. в американских университетах. В них пытались создать программируемые сети с упором на программирование уровня передачи данных (контура передачи данных). Были исследованы подходы к созданию программируемых сервисов в сети, что дало возможность вносить инновационные идеи и получить программируемую функциональность. Исследования дали возможность также изолировать трафик разных приложений, появились туннели и виртуальные частные сети (VPN). Появилась виртуализация сети [4].

В результате зародились следующие инновации, которые затем были применены в ПКС (рисунок 1):

- логически централизованное управление сетью [1, 2], а не конфигурирование отдельных сетевых элементов, что улучшило управление маршрутизацией;
- открытый интерфейс между контуром передачей данных и контуром управления [2], однако, против открытых стандартов выступили многие производители оборудования, которые боялись появления новых игроков на рынке;
- распределенное управление состоянием сети [2].

Все эти попытки отделения контура управления от контура передачи данных были вызваны практическими потребностями. Результаты таких попыток были воплощены в концепции технологии ПКС [1, 2].

Программно-конфигурируемые сети состоят из ПКС-контроллера (или нескольких ПКС-контроллеров) и ПКС-коммутаторов, которыми управляет ПКС-контроллер [1, 2]. ПКС-контроллер – программная платформа, работающая на выделенном типовом сервере. ПКС-коммутаторы – сетевые устройства (СУ) или сетевые элементы (СЭ), принимающие, обрабатывающие и передающие информационные потоки согласно правилам, установленным котроллером [1, 2, 3, 5 и 7]. С уровнем приложений (Application Plane) контроллер (Control Plane) взаимодействует через свой «северный» интерфейс [2]. С ПКС-коммутаторами (Data Plane) контроллер взаимодействует через свой «южный» интерфейс [2]. Если в сети имеется несколько ПКС-контроллеров, то они взаимодействуют между собой через свои «западно-восточные» интерфейсы [1].

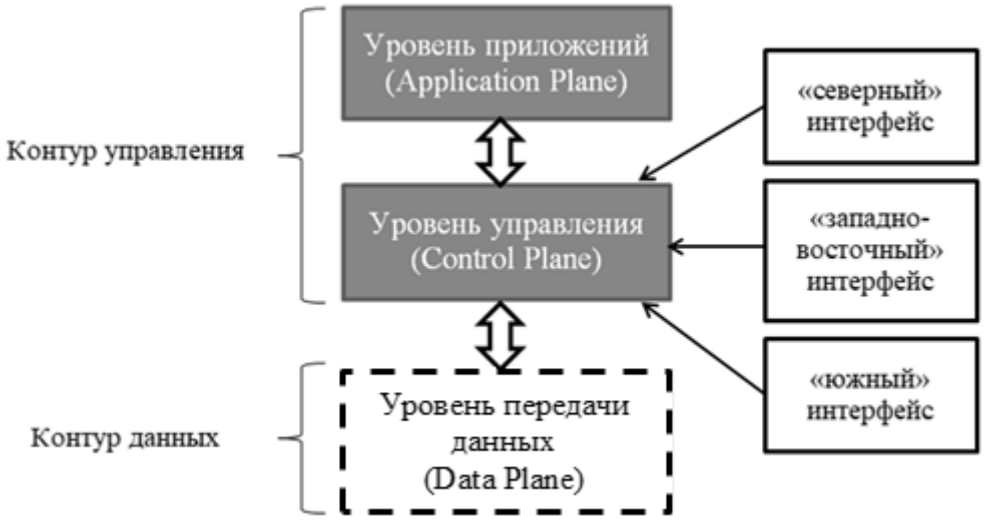


Рисунок 1. Модель технологии ПКС

Реализация технологии ПКС

Для взаимодействия контура управления и контура данных через «южный» интерфейс могут использоваться протоколы **OpenFlow, OpFlex, PCEP** и **NETCONF/YANG** [1], реализующие технологию ПКС.

Первым стандартизированным протоколом стал **OpenFlow** [1]. Он обычно передается поверх протокола TCP и использует для обеспечения безопасности на транспортном уровне протокол TLS, дает возможность любое устройство в контуре данных программно трансформировать в маршрутизатор, коммутатор, сетевой экран и т.д. Первая версия протокола была разработана в 2011 году (OpenFlow 1.0), при этом поддерживался небольшой набор действий обработки пакетов. На настоящий момент наибольшее распространение получила версия OpenFlow 1.3, созданная в 2012 году. В функционал добавились существенные изменения: более гибкая поддержка таблиц записей, возможность согласования разных параметров, поддержка заголовков протокола IPv6, совместимость с сетями с коммутацией по меткам (Multi-Protocol Label Switching - MPLS), метрики по потоку, временной счетчик (duration) для сбора статистики и др. Также на данный момент времени широко распространена версия 1.5.1, разработанная в 2015 году [1].

На уровне передачи данных использование коммутаторов, поддерживающих протокол OpenFlow, позволяет принимать новый поток, сопоставлять его с имеющимися у OpenFlow-коммутатора записями и применять соответствующие действия. Изначально протокол OpenFlow поддерживали компании NEC, HP и Pronto, затем список значительно расширился [1]. OpenFlow является наиболее революционным по сравнению с остальными протоколами, т.к. он создавался в предположении, что сетевое устройство (коммутатор, маршрутизатор) должно быть очень простым, т.е. оно может выполнять только несколько тривиальных команд. Таким образом, протокол OpenFlow предназначен для администрирования и программирования сетевых устройств [1, 2].

Протокол **OpFlex** разработан компанией Cisco Systems. Он используется в рамках их продукта Application Centric Infrastructure (ACI) [1]. Предлагается декларативный способ управления инфраструктурой транспортной сети, отличный от всех остальных протоколов для ПКС. В настоящем подходе предполагается передача спецификаций абстрактных политик между сетевыми элементами и контроллером.

Протокол **Path Computation Element Protocol (PCEP)** [1, 2] применяется для адаптации программно-конфигурируемого подхода к управлению сетями с коммутацией по меткам - Multi-Protocol Label Switching (MPLS). Он определен в RFC 5440.

Протокол **NETCONF/YANG** [1] разработан для сетей, в которых уже имеется большое число сетевого оборудования со своей ОС, мощным техническим обеспечением и встроенными сервисами. Протокол разработан организацией Internet Engineering Task Force (IETF) и описан в RFC 4741. Он дает возможность загружать на оборудование наборы команд с сервера в автоматическом режиме, заменяя ручной труд администратора в сети. Конкретная реализация протокола является вендорнозависимой.

Преимущества и недостатки технологии ПКС

При использовании технологии программно-конфигурируемых сетей для предоставления современных сервисов клиенту нужно учитывать как ее преимущества, так и недостатки. Наиболее важные из них представлены в таблице 1.

Таблица 1. Преимущества и недостатки технологии ПКС

Уровень ПКС	**Преимущества**	**Недостатки**
Контур управления	– централизованное управление всей сетью (возможность видеть и конфигурировать топологию всей сети (на L2 и L3-уровне), обновлять ПО всех СУ единовременно) – гибкость управления - эффективная маршрутизация – повышение удобства управления отдельными СУ – упрощение выполнения существующих задач и сервисов – упрощение добавления нового функционала к уже существующей сетевой архитектуре за счет применения программных средств – быстрое развертывание сервисов	– ПКС-контроллер – единая точка отказа – требуется высокая квалификация специалиста, программирующего контроллер – необходимо обеспечить безопасность контроллера от атак злоумышленников на аппаратном и программном уровнях – высокая стоимость контроллера – требуется обеспечить резервирование контроллера – при отсутствии резервирования контроллера - низкая отказоустойчивость ПКС
Контур передачи данных	– повышение производительности, т.к., OpenFlow-коммутаторы дают возможность увеличить скорость перемещения трафика – снижение расходов на управление сетью за счет применения виртуализации СУ – использование простого и более дешевого по сравнению с традиционными сетями оборудования (СУ) – повышение эффективности использования сетевых ресурсов – возможно независимое обновление оборудования – большие возможности по масштабированию сетей	– при отсутствии связи между контроллером и СУ сеть может стать неуправляемой – необходимо обеспечить безопасность каждого СУ на аппаратном и программном уровнях от их компрометации злоумышленниками (через СУ может быть атакован контроллер) – могут возникать сложности при стыковке с традиционными сетями – масштабируемость сети ограничена возможностями контроллера – для больших сетей нужно использовать несколько контроллеров

Из таблицы 1 видно, что преимущества технологии ПКС значительно весомее ее недостатков, многие из которых могут быть решены средствами самой ПКС [1, 2, 8, 9, 11].

Технология ПКОС

Главной целью внедрения технологии программно-конфигурируемых сетей является повышение качества обслуживания клиентов, что достигается за счет уменьшения времени предоставления сервисов клиентам и ускоренного ввода новых сервисов. В свою

очередь, для этого необходимо, чтобы сетевое оборудование могло технически реализовать основные концепции ПКС. На транспортном уровне для реализации концепции ПКС применяются программно-конфигурируемые оптические сети. ПКОС позволяют обеспечить сетевую транспортную инфраструктуру для организации предоставления современных сервисов клиентам. ПКОС базируются на технологиях SDN (ПКС), OTN, WDM и IP/MPLS [3].

Опишем архитектуру ПКОС (рисунок 2) [7-11]. Основным элементом архитектуры ПКОС также является контроллер. На нем установлена сетевая операционная система (СОС), которая позволяет управлять через «южный» интерфейс контроллера инфраструктурой контура передачи данных и предоставлять клиентам сервисы, используя установленные на контроллере приложения. Взаимодействие СОС с приложениями осуществляется через «северный» интерфейс контроллера. Важно отметить, что приложения контроллера в ПКОС в основном ориентированы на предоставление транспортных сервисов, реализуемых посредством OTN, WDM и IP/MPLS. Наиболее востребованными в ПКОС являются сервисы предоставления гарантированной скорости передачи данных и организации оптических частных сетей (OVPN) [10, 11]. В качестве сетевых элементов (СЭ) или сетевых устройств (СУ) в ПКОС выступают фотонные коммутаторы и мультисервисные транспортные платформы. Специфика управления такими СЭ и СУ определяется тем, что данные передаются посредством оптических сигналов. Пропускная способность каналов передачи данных может динамически изменяться благодаря тому, что контроллер определяет параметры оптического сигнала (например, используемые форматы модуляции и сетку частот) и дает команду СЭ и СУ на использование этих параметров на различных участках сети. При междоменном взаимодействии используются «западно-восточные» интерфейсы котроллеров ПКОС.

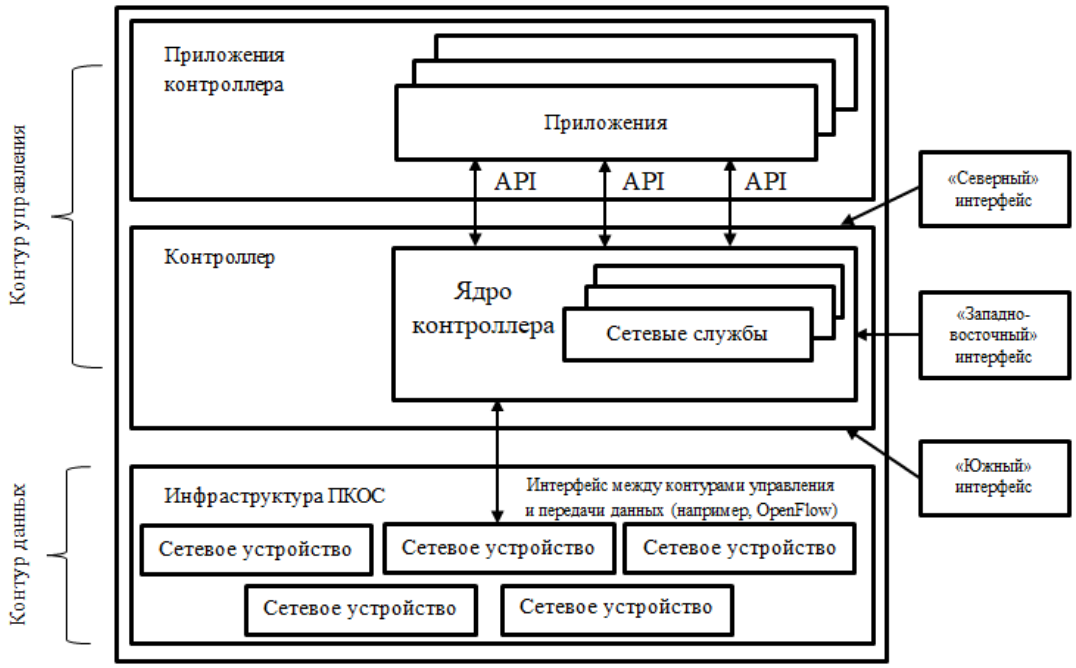


Рисунок 2. Архитектура программно-конфигурируемой оптической сети

Реализация технологии ПКОС

В работе [3, 6] показано, что в совокупности технологии DWDM, OTN, IP/MPLS и ПКС (SDN) предлагают решения для реализации программно-конфигурируемых оптических сетей (ПКОС). В сводной таблице 2 приведен ряд ключевых особенностей этих технологий, позволяющих предоставлять современные сервисы клиентам.

Таблица 2. Ключевые особенности технологий, реализующих ПКОС

Технология	Назначение	Применяемые технические решения
ПКС (SDN)	– централизация управления сетью – разделение уровней управления и передачи данных – применение унифицированного интерфейса между уровнями управления и передачи данных – автоматизация предоставления сервисов клиентам – реализация сервисов ПКОС	– ПКС-контроллер с СОС и сетевыми приложениями – виртуализация физических ресурсов сети – PCEP или OpenFlow для взаимодействия контроллера и СЭ в режиме реального времени – OSPF для повышения эффективности работы сети
IP/MPLS	– маршрутизация и коммутация сервисных потоков (L2/L3) – уменьшение нагрузки на СЭ – управление пропускной способностью – обеспечение SLA – реализация сервисов ПКОС	– маркировка трафика метками – LDP, RSVP – туннелированние – VPN – организация гибких сервисов VPLS (L2) и VPRN (L3)
OTN	– выбор типа транспондера для конкретной оптической несущей – размещение пакетного трафика в своих кадрах – обеспечение гарантированной передачи данных – гибкое использование полосы пропускания – реализация сервисов ПКОС	– заголовки соответствующих блоков для сигнализации – транспортные структуры (блоки ODU и OTU) с широким диапазоном скоростей передачи данных – многофункциональная сигнализация, мониторинг – проверочные коды FEC – отдельный контролирующий оптический канал (OSC)
DWDM	– определение числа оптических несущих в рабочих диапазонах – выбор шага между оптическими несущими – выбор форматов модуляции – предоставление оптических каналов уровню OTN – корректная передача оптического сигнала без искажений и ошибок – реализация сервисов ПКОС	– когерентные методы приема и передачи информации – поляризационное мультиплексирование – применение многоуровневых форматов модуляции – плотная сетка частот – технология Flexible Grid – технология суперканалов – ROADM с «бесцветными» и ненаправленными портами

Заключение

Таким образом, в результате проведенного анализа ключевых особенностей технологии ПКОС были решены все поставленные задачи и достигнута цель исследования. Показано, что ПКОС позволяют обеспечить сетевую транспортную инфраструктуру для организации предоставления современных сервисов клиентам.

СПИСОК ЛИТЕРАТУРЫ

1. *Антоненко, В.А., Смелянский Р.Л.* Концепции программного управления и виртуализации сетевых сервисов в современных сетях передачи данных: учебное пособие. – М.: КУРС, 2020. – 160 с.
2. *Давыдов К.С., Ухов Г.В., Фатхулин Т.Д.* Анализ ключевых особенностей технологии программно-конфигурируемых сетей (SDN) // «ИНФОКОМ-2019» / Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Часть I - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2019. – С. 288-296.

3. *Деарт В.Ю., Фатхулин Т.Д.* Анализ современного состояния транспортных сетей с целью внедрения технологии программно-конфигурируемых сетей (SDN) // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №6. - С. 4-9.
4. *Жаббаров И.Ш., Фатхулин Т.Д.* Обоснование выбора системы виртуализации, предоставляющей необходимый функционал для предприятия заданного уровня // «ИНФОКОМ-2019» / Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Часть I - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2019. – С. 241-249.
5. *Леохин Ю.Л., Фатхулин Т.Д.* Оценка возможности предоставления гарантированной скорости передачи данных в программно-конфигурируемой оптической сети // Вестник РГРТУ. 2020. №71. – С. 45-59.
6. *Фатхулин Т.Д., Барабаш Е.С., Будаев Н.С.* Техническое решение по построению распределенного «облака» на основе принципов протокола OSPF // REDS: Телекоммуникационные устройства и системы. 2020. Т.10. №1. – С. 43-47.
7. *Фатхулин Т.Д., Пугачева М.А.* Исследование влияния параметров клиентского трафика на возможность предоставления гарантированной скорости передачи данных в ПКОС // «ИНФОКОМ-2020» / Труды Северо-Кавказского филиала Московского технического университета связи и информатики - Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2020. – С. 264-274.
8. *Фатхулин Т.Д., Калатанова Е.С., Копиевский Н.Ю.* Общие проблемы и принципы анализа структур программно-конфигурируемых оптических сетей // «Технологии информационного общества» / Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества». (03-04 марта 2021 г. Москва, МТУСИ). М.: ООО «ИД Медиа Паблишер», 2021. - С. 185-187.
9. *Фатхулин Т.Д.* Разработка алгоритма предоставления гарантированной скорости передачи для пользователя в сетях, построенных по технологии транспортных программно-конфигурируемых сетей (T-SDN) // «Телекоммуникационные и вычислительные системы -2018» / Труды международной научно-технической конференции. – М.: Горячая линия – Телеком, 2018. – С. 126-129.
10. *Leokhin Yu., Fatkhulin T,* Approach to Estimating the Probability of Providing "Cloud" Services in the SDN // Proceeding of 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. – 2020. Russian, 19-20 March 2020, - pp. 1-9, DOI: 10.1109/IEEECONF48371.2020.9078593.
11. *Leokhin Yu., Fatkhulin T.,* Evaluation of Service Availability in Software-Defined Optical Network // Proceeding of 2021 Systems of Signals Generating and Processing in the Field of on Board Communications. – 2021. Russian, 16-18 March 2021, pp. 1-6, DOI: 10.1109/IEEECONF51389.2021.9416122.

А.И. Сакалова, А.Н. Чикалов

ИЗУЧЕНИЕ МИКРОКОНТРОЛЛЕРОВ ПРИ РЕАЛИЗАЦИИ ПРИНЦИПОВ МНОГОВАРИАНТНОСТИ И ИНДИВИДУАЛИЗАЦИИ ОБУЧЕНИЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: микроконтроллер, интерфейсы, обучение, многовариантность.

Рассматривается подход к разработке лабораторного комплекса, обеспечивающего изучение интерфейсов и протоколов микропроцессорных систем на основе технологической платформы ARDUINO. Такая реализация позволяет в полной мере использовать принципы индивидуализации и многовариантности обучения. Кроме того, комплекс позволяет удовлетворить современным требованиям содержательной актуальности, высокой наглядности, экономической доступности, способствовать практической подготовке обучаемых.

A.I. Sakalova, A.N. Chikalov

THE STUDY OF MICROCONTROLLERS IN THE IMPLEMENTATION OF THE PRINCIPLES OF MULTIVARIANCE AND INDIVIDUALIZATION OF LEARNING

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

Keywords: microcontroller, interfaces, training, multivariance.

An approach to the development of a laboratory complex providing the study of interfaces and protocols of microprocessor systems based on the ARDUINO technology platform is considered. This implementation makes it possible to fully use the principles of individualization and multivariate learning. In addition, the complex allows meeting the modern requirements of content relevance, high visibility, economic accessibility, and contribute to the practical training of trainees.

Современное образование имеет очень динамичный характер. Причинам тому являются модернизация технологий, увеличение их количества и сложности, интегрирование смежных технологий, лавинообразное нарастание числа новых компетенций, повышающиеся требования к эффективности персонала.

Поэтому к образовательной среде перманентно предъявляются все новые, порой не всегда достаточно обоснованные и не вполне реалистичные требования. Сама система образования, как правило, имеет весьма ограниченные материальные, технические и организационные возможности. Контингент обучаемых в силу целого ряда причин имеет очень различный уровень исходной подготовки. Все это делает задачу удовлетворения предъявляемых требований в плане обучения очень непростой.

Одним из возможных путей решения задач освоения нового материала может стать использование принципов многовариантности, индивидуализации и дифференциации обучения. Эти принципы органично взаимосвязаны, однако каждый из них имеет свои акценты и особенности.

Многовариантность предполагает возможность выбора темпа и уровня освоения материала, условий и инструментов обучения, принятие самостоятельного решения

студентами по выбору образовательной траектории. Это может касаться как дисциплин в целом, так и изучения отдельных тем и вопросов, используемых средств.

Индивидуализация предполагает учет и развитие индивидуальных особенностей каждого студента при решении всех вопросов обучения во всех формах взаимодействия с ним.

Наконец, дифференциация имеет целью достижения цели обучения при учете особенностей всех студентов. Этот принцип реализуется через группировку по успеваемости, выстраиванию индивидуальных маршрутов освоения материала, формирование индивидуальных целей и т.д. [1].

Все эти принципы применимы к дисциплинам различных блоков учебного плана. Однако следует отметить общую тенденцию современных учебных планов к сокращению аудиторных часов занятий со студентами. Это, в частности, приводит к сокращению времени взаимодействия студентов с техникой и лабораторным оборудованием и созданию условий для ухудшения практических навыков и снижению уровня овладения планируемыми компетенциями. Поэтому следует более тщательно выбирать тематику практических занятий, уделять особое внимание методике проведения занятий, продумывать состав и возможности лабораторного оборудования для студентов различного уровня начальной подготовки, обеспечивать наличие необходимого количества экземпляров техники для эффективного проведения занятий. Следует более тщательно продумать структуру теоретической части материала, приблизив конкретный результат ее изучения на каждом этапе к высокой степени готовности для последующего практического занятия.

В современных учебных планах для специалистов в области компьютерных технологий неуклонно увеличивается время на изучение студентами принципов организации и структурно–функциональных характеристик новейших микропроцессоров и микроконтроллеров, их системы команд, методов адресации, сфер применения, а также принципов и методик написания для них управляющих программ, приемов практического использования в автоматизированных методах анализа информации и регулирования.

И одним из важнейших вопросов в этой области является взаимодействие центрального ядра вычислительной системы с объектами внешнего мира. Периферийные устройства составляют неотъемлемую часть такой системы, а изучение драйверов таких устройств принципиально необходимо. Однако современные персональные компьютеры и ноутбуки, к сожалению, достаточно плохо позволяют демонстрировать студентам все тонкости организации вычислительного процесса:

- во-первых, работа всех функциональных узлов современного компьютера скрыта от пользователя операционной системой, а литература с детализацией отдельных процессов либо отсутствует, либо недоступна;
- во-вторых, аппаратная база компьютеров часто меняется, что, зачастую, создает большие проблемы с поддержкой учебных материалов в актуальном состоянии;
- в-третьих, аппаратура и программное обеспечение современных компьютеров общего назначения сложны и на подробное их изучение просто не хватает времени, которое отведено учебной программой;
- наконец, повреждение персональных компьютеров, которое вполне вероятно на этапах проведения с ними учебных экспериментов может иметь тяжелые последствия. Это может быть связано не только с существенными материальными затратами на восстановление аппаратной части, но и длительным восстановлением программного обеспечения. Все это выводит компьютер из образовательного процесса и создает проблемы для проведения занятий в аудитории.

Поэтому для изучения различных типов внешних устройств, обучения написанию драйверов для них необходим специальный лабораторный стенд, позволяющий устранить имеющиеся недостатки и в полной мере реализовать указанные выше принципы обучения.

Такой лабораторный стенд должен иметь следующие характеристики;

- быть экономически доступным для реализации, в том числе при изготовлении тиража;
- включать возможность реализации современных типовых протоколов взаимодействия с типовыми внешними устройствами;
- обеспечивать простоту и наглядность в настройке и демонстрации результатов работы обучаемых;
- позволять экономически приемлемую перманентную модернизацию в соответствии с тенденциями развития цифровой техники;
- допускать многовариантную аппаратную схему реализации типовых внешних устройств;
- иметь развитую номенклатуру технической литературы.

Все возможные интерфейсы и протоколы освоить технически невозможно в силу ограниченного учебного времени практических занятий. Поэтому в качестве драйверов, обеспечивающих интерфейс с типовыми внешними устройствами следует рассматривать следующие:

- драйвер дискретных портов ввода-вывода для управления индикаторами и устройствами ввода;
- драйвер подключения клавиатуры;
- драйвер ЖК-индикаторов;
- последовательный интерфейс I2C (Inter-Integrated Circuit) - последовательная асимметричная шина для связи между интегральными схемами внутри электронных приборов;
- универсальный последовательный интерфейс UART (Universal Asynchronous Receiver-Transmitter) - узел вычислительных устройств, предназначенный для организации связи с другими цифровыми устройствами, в частности, компьютерами через штатный порт;
- драйвер таймеров и системы прерываний для обеспечения встраивания микропроцессоров в технологические процессы.

Для реализации лабораторного стенда со всеми заявленными вышеуказанными свойствами оптимально подходит платформа ARDUINO. Подключение к персональному компьютеру или ноутбуку, возможность программирования на языках низкого и высокого (язык С) уровней, нелицензионное программное обеспечение позволяют без лишних затрат создать полноценную среду разработки. Технологическая платформа ARDUINO имеет широкий набор внутренних периферийных устройств, внешних согласованных модулей и датчиков, что позволяет просто и наглядно строить, и модернизировать аппаратную часть лабораторного стенда.

В СКФ МТУСИ и раньше предпринимались попытки создания устройств в учебных целях на базе микроконтроллеров [2, 3]. Однако эти работы касались конкретных устройств с неизменяемой конечной задачей. Это ограничивало возможности с точки зрения многовариантности, не позволяло редуцировать задания и в полной мере обеспечивать индивидуальный подход при выстраивании методики проведения занятий.

Структура лабораторного стенда определяется решаемыми задачами учебного характера и концептуально может быть представлена в двух вариантах.

Первый вариант предполагает включение всего комплекса оборудования, обеспечивающего проведение всех практических занятий в рамках дисциплины, например, «Периферийные устройства и интерфейсы». В состав этой структуры должны войти следующие основные элементы:

- модуль управления – это программно–аппаратное устройство, преобразующее сигналы от системы первичной автоматики в управляющие воздействия на исполнительный механизм. В качестве такого модуля выступает открытая программируемая аппаратная платформа для работы с различными объектами ARDUINO;
- плата расширения. Она предназначена для создания дополнительных линий цифрового управления при наличии большого числа внешних устройств. Сама плата ARDUINO не обладает достаточным количеством таких линий.

Ее реализация возможна на дискретных двунапрвленных регистрах с возможностью их адресации за счет имеющихся линий управления ARDUINO. Количество создаваемых портов будет определяться составом управляемого оборудования и скоростными возможностями процессора.

Альтернативой для реализации платы расширения является использование 8-разрядных расширителей портов, например, типа PCA9538PW. Порты имеют 8 конфигурируемых на вход или выход разрядов, допускают инвертирование полярности и управляются по шине I2C. Такой вариант при достаточной скорости позволяет минимизировать использование линий цифрового управления ARDUINO:

- внешнее ОЗУ – для хранения пользовательских программ;
- внешняя память данных – для хранения отлаженных модулей и актуальных данных о результатах обучения;
- модуль взаимодействия с оператором – обеспечивает отображение текущей визуальной и звуковой информации, взаимодействие с комплексом с помощью матричной клавиатуры и отдельных светодиодных индикаторов. Для отображения информации в этом модуле для обеспечения многовариантности должны быть как в виде матрицы автономных светодиодов, так и виде модулей со встроенным контроллером с управлением по последовательному интерфейсу;
- модуль ручных переключателей для создания тестовых сигналов;
- порты для входных и выходных аналоговых сигналов;
- порт для связи с компьютером.

Для такой структуры разрабатывается необходимое целевое для данного учебного занятия программное обеспечение на ПЭВМ в среде IDE, загружается в память программ ARDUINO и осуществляется его запуск. Дальнейшее управление осуществляется процессором контроллера.

При этом в составе программного обеспечения могут использоваться все ранее разработанные драйверы и привлекаться управляемое ими внешнее оборудование. При необходимости использования элементов управления привлекаются средства модуля взаимодействия с оператором, оперативная информация отображается на индикаторах модуля. Для имитации поступления дискретных данных используется модуль ручных переключателей. При использовании аналоговых обменов задействуются порты аналоговых входных и выходных сигналов.

При этом через аналоговые и дискретные порты можно будет подключить реальные оконечные устройства, например, электродвигатели, датчики различного назначения. Если мощность двигателей будет превышать имеющуюся, то сделать это можно через платы силовой коммутации. Конкретные технические решения должен обосновать и принять обучаемый.

Такая структурная схема позволяет обеспечить единый подход для разработки типовых интерфейсов, организовать их использование на одном модуле управления, комплексно задействовав его встроенные возможности. Такая стратегия больше приближена к реальной практике, позволяет учесть взаимное влияние разрабатываемых интерфейсов, дает возможность последовательно наращивать программное обеспечение, использовать возможности ранее разработанных драйверов для новых объектов управления, учитывать временные параметры и взаимное влияние процедур управления. Однако изначально определить все технические параметры такого стенда в условиях образовательного процесса не представляется возможным. Временные затраты обучаемых на разработку программных продуктов не нормированы, объем учебных заданий еще не прошел апробацию, гарантировать полное освоение всех этапов предыдущих занятий каждым обучаемы и использование им их результатов не представляется возможным. Поэтому реализовать принципы индивидуализации, многовариантности и дифференциации весьма затруднительно. Поэтому такую структуру целесообразно создавать после наработки статистики для каждого занятия в отдельности и получения достоверных данных по ее эффективности.

Поэтому на начальном этапе предпочтителен второй вариант: автономная структура лабораторного комплекса, создаваемая для каждого конкретного занятия. Такой вариант вполне реализуем на базе предлагаемой технологической платформы. Компоновка структуры обеспечивается самими обучаемыми, выполняется это быстро, очень наглядно и способствует наращиванию практических навыков работы с компьютерной техникой.

Сложность создаваемой схемы и формулировка конечных задач может быть определена исходя из индивидуальных особенностей обучаемого, уровня его текущей подготовки и потенциальных возможностей. Допустимы последовательно усложняющиеся задачи, самостоятельный выбор варианта обучаемым и другие композиции.

На примере изучения драйверов для управления светодиодной матрицей иерархия схем может представлять следующую усложняющуюся последовательность. При этом предполагается построение самой схемы, разработка и отладка драйвера со своими входными и выходными параметрами для управления матрицей и разработка, и отладка программы с использованием драйвера по индивидуальным заданиям различного уровня сложности. Такая вариативность позволяет в полной мере использовать принципы индивидуализации и дифференциации обучения.

1. Схема управления матрицей с помощью портов самого микроконтроллера. При этом строки и столбцы матрицы подключаются непосредственно к портам микроконтроллера. На практике это делают через транзисторные ключи - сборки типа ULN2003A, ULN2003AI, ULN2004A, ULQ2003A, ULQ2004A для обеспечения требуемой мощности сигнала.

Такая схема является самой простой, совершенно прозрачной по принципам управления и пригодна для начального обучения. Хорошо иллюстрирует эффекты динамической индикации. Однако такое включение использует очень много разрядов параллельных портов микроконтроллера, что делает затруднительным его применение для других задач управления.

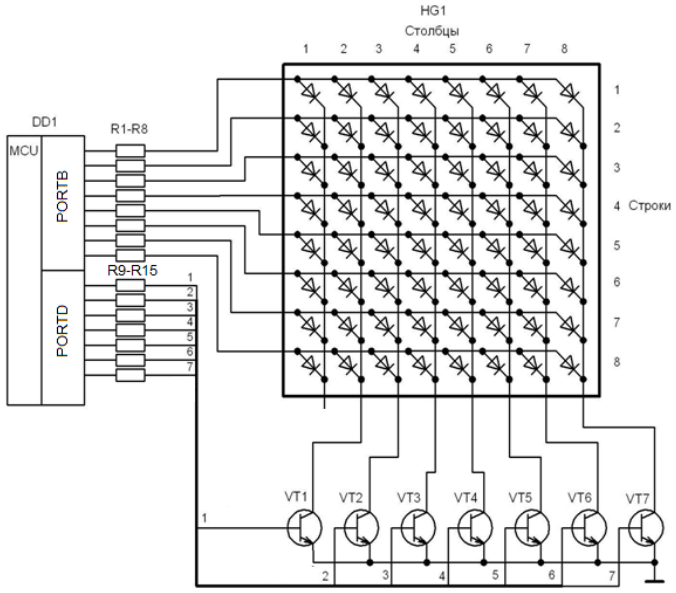


Рисунок 1.

2. Схема управления матрицей с помощью внешних регистров. В такой схеме строки и столбцы подключаются к отдельным дискретным регистрам, которыми можно управлять от одного порта микроконтроллера, добавив его минимальным числом сигналов синхронизации. Это уменьшает число задействованных линий портов микроконтроллера, но принципиально проблему не решает.

3. Схема управления с использованием регистров сдвига. В качестве регистров можно использовать ИМС типа 74HC595, из которых образуется единая сдвиговая цепочка [4, 5].

Для управления матрицей светодиодов достаточно всего трех выводов. По переднему фронту тактового сигнала SHCP происходит последовательный прием данных по входу DS без выдачи на внешние выводы и изменения их прежнего состояния. При установке же единицы на входе STCP осуществляется фиксация данных и выдача их на внешние выводы регистров. Они сохраняются до появления следующей единицы.

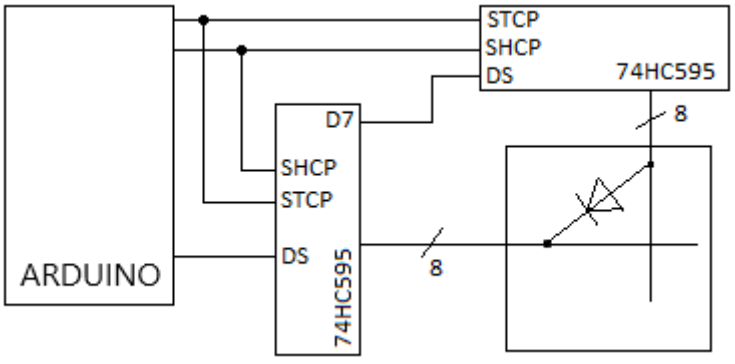


Рисунок 2.

Такая схема практически не требует дополнительных элементов, позволяет наращивать число матриц, использует всего три управляющих вывода контроллера, способна работать на частоте до 100 МГц. Это создает широкие возможности для многовариантности, особенно при наращивании количества матриц и способа подключения регистров, также и выбора траектории усвоения материала.

4. Схема с использованием последовательного интерфейса модуля MAX7219

Модуль MAX7219 специально подготовлен для подключения нескольких матриц без дополнительных схем. Конструктивно это осуществляется простым присоединением следующего модуля к сквозным контактам на границах с обеих сторон печатной платы. Модуль позволяет управлять 7-сегментными индикаторами и матрицами 8x8 в режиме динамической индикации, при этом регулировать выходной ток.

Управление модулем осуществляется по последовательному интерфейсу с использованием всего трех линий. Данные подаются на вход DIN, тактируются сигналом CLK, схема активизируется по сигналу CS.

Этот модуль наиболее совершенен для решения задач индикации. Одновременно, он может стать основой для решения задач многовариантности и дифференциации обучения. Разработка дисплеев разной конфигурации потребует самостоятельной разработки драйверов различной сложности. Возможны варианты с использованием уже имеющихся библиотек, например, Max72xxPanel, Adafruit_GFX, GyverMAX7219. Поэтому возможности в этом случае обширны, а постановка задач соответствует проектам современного уровня сложности, а полученные результаты могут иметь реальную практическую значимость.

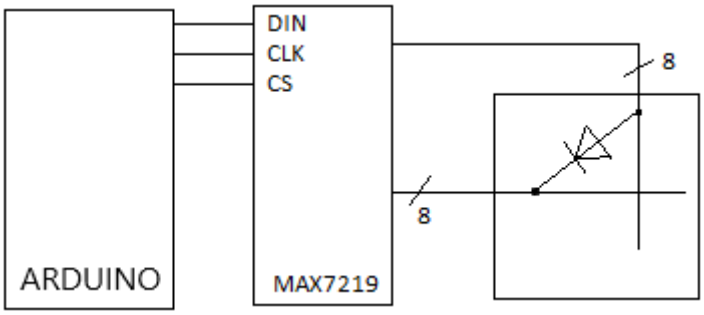


Рисунок 3.

Таким образом, использование лабораторного стенда при изучении интерфейсов на базе современных микроконтроллеров позволяет в полной мере решать задачи многовариантности и индивидуализации обучения. При этом такие технические решения соответствуют современным требованиям содержательной актуальности, высокой наглядности, экономической доступности, способствуют совершенствованию практической подготовки обучаемых.

СПИСОК ЛИТЕРАТУРЫ

1. Бордовская Н.В., Реан А.А. Педагогика. Учебник для вузов - СПб: Питер,2000.-. -- 304 с. – (Серия «Учебник нового века»).
2. Легостаев М.А., Чикалов А.Н. Учебная автоматизированная многоканальная система полива растений для архитектуры "Умный дом". - Труды СКФ МТУСИ по материалам Международной НПК СКФ МТУСИ Инфоком-2020, стр.452-458.
3. Гладыщук С.В., Чикалов А.Н. Многофункциональное устройство проверки параметров обитаемости помещений. - Труды СКФ МТУСИ по материалам Международной НПК СКФ МТУСИ Инфоком-2020, стр.464-469.
4. Обмен данными с помощью регистра сдвига 74HC595 URL: http://arduinokit.ru/arduino/prosto-o-slozhnom-sdvigovyj-registr-74hc595.html.
5. Увеличение выходов с регистром 74HC595 URL: http://arduino.ru/Tutorial/registr_74HC595

6. Описание MAX7219 URL: https://www.makerguides.com/max7219-led-dot-matrix-display-arduino-tutorial/

Т.Н. Николаева, А.Н. Чикалов

ИСПОЛЬЗОВАНИЕ JQUERY-АНИМАЦИИ ДЛЯ СОЗДАНИЯ ИНТЕРАКТИВНЫХ БЛОКОВ САЙТА ПРОДАЖ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: анимация, интерактив, библиотека, плагин.

В данной статье рассматривается подход к разработке интерактивных блоков сайта продаж с использованием анимации, основанной на библиотеке jQuery. Подключение данной библиотеки позволяет разработчику упростить процесс создания интерактива сайта, а также разнообразить возможности анимирования интерфейса, тем самым повышая интерес и лояльность аудитории (пользователей) к сайту и упрощение подачи информации о предоставляемых услугах.

T.N. Nikolaeva, A.N. Chikalov

USE OF JQUERY-ANIMATION TO CREATE INTERACTIVE BLOCKS OF THE SELLING SITE

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

Keywords: animation, interactive, library, plugin.

This article discusses an approach to developing interactive blocks for a selling site using animation based on the jQuery library. Connecting this library allows the developer to simplify the process of creating an interactive site, as well as to diversify the interface animation capabilities, thereby increasing the interest and loyalty of the audience (users) to the site and simplifying the presentation of information about the services provided.

В условиях современной реальности совершенствование компьютерных технологий и широкое распространение интернета открывает новые возможности для сферы предпринимательской деятельности. Цифровая среда, в которую вовлечены нынешние пользователи предоставляет доступ к новейшим средствам маркетинга и рекламы для привлечения клиентов [1, 2]. Исходя из вышесказанного, перспектитвным инструментом для повышения рентабельности бизнеса является сайт продаж [3, 4].

Анимации в веб-сайтах полезны в большом количестве ситуаций. С ее помощью решается целый ряд конкретных задач:

- заполнение времени ожидания, которое необходимо пользователю для загрузки страницы. В итоге те нетерпеливые пользователи, которые могли бы покинуть сайт, остаются на нем, и в результате растет конверсия сайта;
- реализация с помощью анимации приветствий и повышение лояльности аудитории – для этого, например, подходят фоновые видео;

- демонстрация с помощью интерактива работы продукта без большого количества картинок и текста;
- повышение удобства сайта для пользователя за счет оптимизации взаимодействия с веб-страницей. Например, карусель с изображениями удобнее, чем длинный список появляющихся картинок с подписями;
- увеличение объема отображаемой информации за счет анимированных боковых меню. Это позволяет получить больше информации о товаре сразу, без необходимости прокрутки страницы вниз;
- предоставление визуальной обратной связи для пользователей: различные предупреждения, сообщения об ошибках, предложения дальнейших действий. Они становятся более заметными и понятными.

Существует несколько способов разработки анимаций [5].

Самым простым является анимация элементов на базе каскадной таблицы стилей (CSS). CSS-анимации делают возможными переходы между различными состояниями и используют при этом наборы ключевых кадров. С CSS-анимациями нет необходимости в использовании внешних библиотек. Однако с CSS-анимациями невозможно создавать сложные физические эффекты и имитировать реалистичное движение. Они также не сработают, если необходимо сделать больше трех анимаций подряд, а также сложных последовательных анимаций.

Другим способом создания интерактива является анимирование страницы через язык программирования JavaScript. Javascript-анимации предлагают больше возможностей и гибкости, чем переходы и анимации, написанные на CSS. Именно с помощью Javascript создаются продвинутые анимации, такие как подпрыгивание, пауза, остановка и замедление. Но следует учитывать, что сложные анимации, написанные на Javascript, могут увеличить время загрузки страницы. Поэтому, несмотря на то что в базовом Javascript есть собственный функционал анимаций, чаще всего их создают с помощью дополнительных библиотек.

Самой распространенной и удобной в использовании библиотекой является jQuery. jQuery — набор функций JavaScript, фокусирующийся на взаимодействии JavaScript и HTML. Библиотека jQuery помогает легко получать доступ к любому элементу сайта, обращаться к атрибутам и содержимому элементов, манипулировать ими. Также библиотека jQuery предоставляет удобный API для работы веб-интерфейсами.

Библиотека jQuery содержит несколько кросс-браузерных методов для анимации элементов, например, скольжение и плавное исчезновение, без привлечения дополнительных библиотек или плагинов. CSS-стили придают элементам страницы визуальные свойства, которые описывают их внешний вид. jQuery анимация представляет собой интерактивный процесс изменения свойств html-элементов от одного значения к другому.

Работу с jQuery можно разделить на 2 типа:

a. Получение jQuery-объекта с помощью функции $(). Передав в неё CSS-селектор, можно получить jQuery-объект всех элементов HTML, попадающих под критерий и далее работать с ними с помощью различных методов jQuery-объекта. В случае, если метод не должен возвращать какого- либо значения, он возвращает ссылку на jQuery объект, что позволяет вести цепочку вызовов методов согласно концепции текучего интерфейса;
b. Вызов глобальных методов у объекта $(), удобных итераторов по массиву.

Эффекты, которых нет в библиотеке jQuery, можно создавать с помощью метода animate(). Интерпретатор браузера динамически, без перезагрузки страницы, изменяет выбранные свойства на указанные значения. Анимация происходит для всех элементов обернутого набора. Чтобы добавить эффекты для конкретного элемента, нужно

воспользоваться фильтрами jQuery для отбора. Метод позволяет анимировать любое CSS-свойство, имеющее числовое значение.

Для любого свойства предварительно должно быть установлено начальное значение, а в CSS-объявлении должна использоваться полная запись каждого свойства. Функция обратного вызова вызывается один раз после завершения анимации. Функции не передается никаких аргументов, но анимации выполняется для элемента, переданного свойству this в качестве контекста. Значениями свойств могут также выступать hide, show или toggle, в результате чего к элементу применится вычисляемое значение — отображение, скрытие или переключение исходных состояний свойств.

Метод animate() позволяет изменять CSS-свойства выбранных элементов с возможностью одновременной анимации нескольких свойств, задавая продолжительность анимации в миллисекундах.

Также, для упрощения работы разработчика имеется возможность использования jQuery-плагинов. Реализация одних и тех же функций в различных приложениях побуждает разработчиков заново писать один и тот же код несколько раз, лишь незначительно изменяя его под конкретное приложение. Плагины jQuery позволяют забыть разработчикам о данной проблеме. Разработчик может один раз написать плагин, который позволяет реализовать определенную функцию и затем использовать его в необходимых приложениях, написав только одну строчку кода.

В качестве примера приведена часть кода информационной системы сайта продаж жилого комплекса с использованием jQuery-плагина SlickSlider.

```
        $('.slider').slick({
           cssEase:'linear'
           ,

                 autoplay:
                 true,autoplaySp
                 eed:0,

                 speed:
           10000,arrows:
           false,variableWidth:
           true,variableHeight:t
           rue,centerMode:true,

           //centerPadding:'60px',sli
           desToShow: 3,responsive:[

              {

                 breakpoint:76
                 8,settings:{

cssEase: 'linear',

autoplay: true,

autoplaySpeed:0,

                 speed:
                    10000,arro
                    ws:false,

                    variableWidth:
                    true,variableHeight:
                    true,centerMode:true,

                    //centerPadding:
                    '40px',slidesToShow:3

                 }

}
```

Для более сложных и настраиваемых плагинов, предоставляющих большое количество возможностей настройки, лучше иметь настройки по-умолчанию, которые расширяются (с помощью $.extend) во время вызова плагина.

Плагины для jQuery позволяют извлечь максимальную пользу из этой библиотеки, и абстрагировать наиболее удачные решения и часто используемые функции в повторно используемый код, который может сохранить время и сделать процесс разработки более эффективным.

Таким образом, использования библиотеки jQuery существенно упрощает процесс разработки бэкэнда сайта в области анимирования интерфейса и создания интерактива. JQuery-анимация открывает широкие возможности разработчикам программного обеспечения, а также привлекает большее количество пользователей на сайт.

СПИСОК ЛИТЕРАТУРЫ

1. Качмар С.А., Чикалов А.Н. Моделирование графики при помощи шейдеров DirectX. - Труды СКФ МТУСИ по материалам Международной НПК СКФ МТУСИ Инфоком-2019, 29-30 апреля 2019, стр.467-471
2. Ромашко С.С., Чикалов А.Н. Программное обеспечение для информационного терминала предприятия на базе ВЕБ-интерфейса на языке XHTML. - Труды СКФ МТУСИ по материалам Международной НПК СКФ МТУСИ Инфоком-2020, стр.469-473.
3. Беквит Г.Н. «Продавая незримое. Руководство по современному маркетингу услуг». – Изд. «Альпина Паблишер», 2018, 220с.
4. Кондратенко Г. Реактивные веб-сайты / Кондратенко Г., Мациевский Н., Степанищев Е.М.: Интернет-Университет Информационных Технологий – 336с.
5. Гультяев А.К., Машин В.А. Проектирование и дизайн пользовательского интерфейса. – СПб.: КОРОНА принт, 2000. – 352 с.

А.В. Бородин, А.А. Бородина

ПЬЕЗОЭЛЕКТРИЧЕСКИЙ ЭФФЕКТ И ЕГО ПРИМЕНЕНИЕ В ДАТЧИКАХ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: пьезоэлектрический эффект, пьезоэлектрические материалы, датчики, поляризация.

В статье перечислены основные области применения пьезоэлектрических датчиков. В пьезоэлектрических материалах механическая энергия может непосредственно превращаться в электрическую за счет пьезоэлектрического эффекта. Пьезоэлектрические датчики обладают хорошими эксплуатационными характеристиками, широкими динамическими и частотными диапазонами, малыми размерами, высокой надежностью и не требуют источников питания. Датчики на основе пьезоэффекта позволяют измерять целый ряд физических величин в различных режимах.

A.V. Borodin, A.A. Borodina

PIEZOELECTRIC EFFECT AND ITS APPLICATION IN SENSORS

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

Keywords: piezoelectric effect, piezoelectric materials, sensors, polarization.

The article lists the main areas of application of piezoelectric sensors. The piezoelectriceffect allows mechanical energy to be directly converted into electrical one in piezoelectric materials. Piezoelectric sensors have good performance, wide dynamic and frequency ranges, small size, high reliability and do not require power supplies. The piezoelectric effect-based sensors can measure a wide range of physical quantities in various modes.

Технический уровень информационно-измерительных систем определяется качеством первичных преобразователей информации (датчиков). В эксплуатационных условиях датчики испытывают ряд дестабилизирующих факторов, наиболее существенными из которых являются высокие и низкие температуры, статические и динамические давления, значительные уровни вибрации. Для контроля и управления параметрами механических процессов в наиболее жестких эксплуатационных условиях широкое распространение получили пьезоэлектрические датчики давлений, усилий, ускорений, использующие прямой пьезоэлектрический эффект. Они обладают хорошими эксплуатационными характеристиками, широкими динамическими и частотными диапазонами, малыми размерами, высокой надежностью и не требуют источников питания.

Пьезоэлектриками называют твердые диэлектрики, в которых имеют место прямой и обратный пьезоэффекты. Прямой пьезоэффект – это возникновение поляризации P под воздействием механических напряжений. Или изменение поляризации, если в отсутствие напряжений существовала поляризация – спонтанная или вызванная электрическим полем. Обратный пьезоэффект – это возникновение механических деформаций под действием электрического поля. Как прямой, так и обратный пьезоэффекты являются линейными эффектами.

Кристаллы, обладающие спонтанной поляризацией только в определенном интервале температур, относятся к классу сегнетоэлектриков. В этих кристаллах спонтанный дипольный момент возникает из-за смещения подрешеток ионов. Спонтанный дипольный момент в сегнетоэлектриках существует только в определенном интервале температур устойчивой сегнетоэлектрической фазы. Обе граничные температуры этого интервала называют температурами Кюри – верхней и нижней.[1] Ионы, входящие в кристаллическую решетку сегнетоэлектрика и являющиеся причиной возникновения спонтанной поляризации, могут смещаться под действием механических напряжений. Это означает, что механическое напряжение кристалла сегнетоэлектрика приводит к возникновению электрической поляризации.[2]

Все пироэлектрики, в том числе и все сегнетоэлектрики, являются пьезоэлектриками, но не наоборот. Характерным пьезоэлектриком – не пироэлектриком является кварц SiO_2. Он широко применяется в качестве генератора и приемника акустических колебаний, а также для измерений механических напряжений. Пьезоэлектрический эффект в кварце сравнительно не велик (в ряде сегнетоэлектриков, например, в ниобате лития $LiNbO_3$, он значительно больше), но обладает высокой стабильностью. Пьезоэлектриками являются многие кристаллические вещества: кварц, турмалин, пьезокерамики: титанат бария, ниобат лития, титанат висмута, цирконат-титанат свинца, а также пленочные текстуры.[3]

Пьезоэлектрические преобразователи лучше всего согласуются с задачей об измерении сил. Пьезоэлектрический датчик знакопеременных сил устанавливают между источником вибрации и исследуемым объектом. Измеряемая сила действует на резьбовые втулки, связанные с двумя металлическими пластинками, между которыми находится пьезоэлектрический элемент – кристалл или керамика. Под действием нагрузок на пластинках появляются заряды, и возникающее электрическое напряжение оказывается пропорциональным искомой силе.

Так как силы выражаются векторами, то для их описания единственной скалярной величины может оказаться недостаточно. Для измерения нескольких компонент сил применяют датчики, содержащие пьезоэлектрические пластинки, чувствительные не только к сжатию под влиянием нормальных нагрузок, но и по одной пластинке для каждого направления усилия скалывания.

Дело в том, что пьезоэффект может проявляться как при действии продольных, так и скалывающих сил. Кварцевые пластики можно вырезать из кристаллов так, чтобы они были чувствительны только к сжатию или только к скалывающим усилиям, действующим некоторых выбранных направлениях. Элементы, ответственные за различные направления, механически последовательно соединяют между собой. Усилие, измеренное таким образом, нет необходимости разлагать на составляющие в обрабатывающих устройствах, так как каждая из пластинок реагирует только на свою компоненту. В типичных случаях взаимные влияния не превышают 1%.[4]

Пьезоэлектрические датчики одинаковой чувствительности можно включать в измерительные схемы и параллельно. Снимаемый электрический сигнал соответствует алгебраической сумме действующих сил. На основе этого принципа конструируют, например, пьезодинамические платформы, используемые, в частности, для измерений усилий резания при различных видах обработки конструкционных материалов, а также при исследовании динамических характеристик разнообразных технических устройств. Пьезоэлектрические датчики, «набранные» из различным образом ориентированных элементов, могут служить не только многокомпонентными динамометрами, но и датчиками крутящих моментов.

Большое разнообразие датчиков для измерения давлений объясняется тем, что само понятие давления охватывает протяженную область значений – от глубокого вакуума до сверхвысоких избыточных давлений в различных средах. В то же время развитие ряда отраслей техники, например, авиационной, космической, атомной энергетики и др., поставило задачу об измерении динамических и импульсных давлений в экстремальных условиях эксплуатации и привело к созданию специальных классов пьезоэлектрических датчиков акустических и быстропеременных давлений.[5]

Современный этап развития науки и техники характеризуется постоянным возрастанием требований к эффективности контроля и диагностирования состояния сложных технических объектов. Для поддержания их высокой надежности и безаварийности требуется увеличение количества контролируемых параметров и применение разнообразных датчиков физических величин.

СПИСОК ЛИТЕРАТУРЫ

1. *Бородин А.В., Бородина А.А.* Пьезоэлектрический эффект и его применение в трансформаторах. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 2. с.59-62.
2. *Бородин А.В., Явтушенко П.В.* Использование поликристаллических материалов для создания пьезоэлектрических трансформаторов. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2018. №1. с.56-58.

3. *Резниченко Л.А., Шилкина Л.А.*, Разумовская О.Н., Дудкина С.И., Гагарина Е.С., Бородин А.В. Диэлектрические и пьезоэлектрические свойства твердых растворов на основе ниобата натрия. // Неорганические материалы. - 2003, т.39, №2, с.187-199.
4. *Крупенин В.Л., Веприк А.М.* Об измерениях в машиностроительных отраслях (обзор). // Вестник научно-технического развития. – 2009, №1(17), с.3-17.
5. *Богуш М.В.* Пьезоэлектрические датчики для экстремальных условий эксплуатации. Пьезоэлектрическое приборостроение: сборник в 3 томах. Т. 3. Издательство СКНЦ ВШ, 2006, 346с

И.Я. Бурнашев, Н.А. Басий, Д.А. Чех

ОПТИМИЗАЦИЯ ОБМЕНА СООБЩЕНИЯМИ ДАННЫХ В ЦИФРОВОЙ СИСТЕМЕ ПЕРЕДАЧИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет», Ростов-на-Дону, Россия

Ключевые слова: цифровая система передачи, система обмена данными, сеть передачи данных, маргинальная задержка, центр коммутации, распределение потоков.

В статье рассмотрены проблемы и некоторые направления развития цифровых систем передачи на примере систем обмена данными, так как ряд крупных и средних сетей передачи данных государственного и производственного предназначения до сих пор предопределены эксплуатировать низкоскоростные и слабо надежные каналы связи.

I.Ya. Burnashev, N.A. Basiy, Czech D.A.

OPTIMIZATION OF DATA MESSAGING IN THE DIGITAL TRANSMISSION SYSTEM OF THE TELECOMMUNICATION NETWORK

Federal State Budgetary Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia

Keywords: digital transmission system, data exchange system, data transmission network, marginal delay, switching center, flow distribution.

The article discusses the problems and some areas of development of digital transmission systems on the example of data exchange systems, since a number of large and medium-sized data transmission networks of state and industrial purposes are still predetermined to operate low-speed and weakly reliable communication channels.

Телекоммуникационные системы разделяются на первичные и вторичные сети, где проводится широкое внедрение цифровых систем передачи. Отметим, что большое количество каналов и групповых трактов организовано на основе медных кабелей, имеющих серьезные недостатки. Вторичные сети связи чаще реализуют обмен информацией на базе электронно-вычислительных машин, поэтому удобно рассмотреть оптимизацию доставки информации по средствам обмена данными цифровых каналов.

Структура системы обмена данными сети связи представлена на рисунке 1.

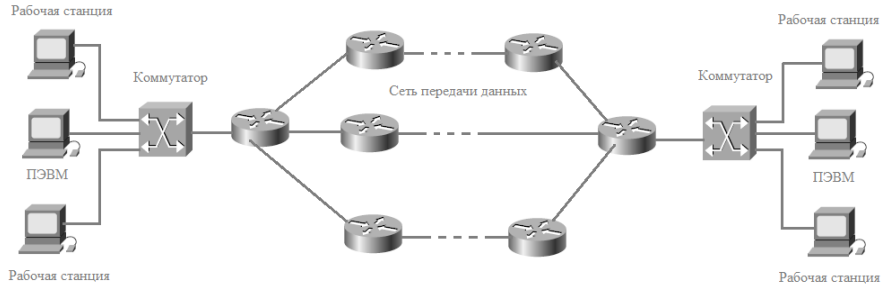


Рисунок 1. Структура системы обмена данными сети связи

Определим характеристики системы передачи по параметрам задержки пакета.

Известно, что для достижения минимума средней задержки пакета в сети передачи данных в качестве характеристик состояния сети необходимо использовать не обычные, а так называемые маргинальные задержки. С этой точки зрения представляет интерес влияние маргинальной задержки на оптимальность принимаемых маршрутных решений.

Пусть λ_{ij} - интенсивность потока пакетов от отправителя i к получателю j, φ_{ikj} - маршрутная переменная, определяющая долю потока пакетов, предназначенных для j-го получателя, проходящих по маршруту (i,k), γ_{ij} - интенсивность передачи пакетов данных от i –го центра коммутации до коммутационного центра j, f_{ij} - интенсивность передачи пакетов данных по тракту (i,k), которая включает входной и транзитный трафики.

Теперь справедливы следующие соотношения

$$\gamma_{ij} = \lambda_i(j) + \sum_l \lambda_{lj}\varphi_{lij}, \tag{1.1}$$

$$f_{ij} = \sum_l \gamma_{ik}\varphi_{ikj}, \tag{1.2}$$

Уравнение (1.1) является уравнением баланса потока пакетов на каждом центре коммутации (ЦК) $i \neq j$ и вместе с уравнением (1.2) связывает потоковые переменные с маршрутными переменными.

Обозначим через $N_{ij}(f_{ij})$ в соответствии с рядом литературы среднее число пакетов, передаваемых по ветви (i,k), умноженное на среднее время задержки одного пакета. Выбрав в качестве показателя эффективности использования адаптивного алгоритма маршрутизации, среднее время доставки пакетов можно получить аналитические выражения для сети в целом. При известных предположениях о независимости и пуассоновском входном потоке, получено выражение для среднего времени доставки пакетов:

$$\bar{T} = \frac{1}{\lambda_0}\sum_{l=1}^{L}\frac{f_l}{c_l - f_l}, \tag{1.3}$$

где c_l - пропускная способность тракта l;

λ_l - интенсивность потока, проходящего по тракту l;

$f_l = \lambda_l / \mu$ - загрузка тракта l;

μ - интенсивность обслуживания потока;

$\lambda_0 = \sum\sum_{ij} \lambda_{ij}$, λ_{ij} – интенсивность входного потока пакетов тракта **l** для $(i,j) \in N_{ЦК}$

.

Тогда, с учетом (1.3)

$$N_{ij}(f_{ij}) = \frac{f_{ij}}{c_{ij} - f_{ij}}; \tag{1.4}$$

$$N_T = \lambda_0 T = \sum_{(i,j)\in L} \frac{f_{ij}}{c_{ij} - f_{ij}}. \tag{1.5}$$

Полагая функцию N_{ij} выпуклой по аргументу f_{ik} и дополняя уравнение баланса потоков (1.1) условием неотрицательности переменных f_{ik} можно сформулировать задачу выпуклого программирования с целевой функцией (1.5).

Пусть f_{ijk}^0 – решение задачи (1.5) для всех $(i,j) \in L$ и $k \in N_{ЦК}$. Тогда маршрутные переменные могут быть определены из соотношения (1.2).

$$\varphi_{ijk}^0 = \frac{f_{ijk}^0}{\gamma_{ij}} = \frac{f_{ijk}^0}{\sum_{k=1}^{N_{ЦК}} f_{ijk}} \tag{1.6}$$

Решение (1.6) задачи (1.5) имеет ряд недостатков, затрудняющих его использование в сети передачи данных системы обмена данными. Основным недостатком следует считать, что (1.6) дает оптимальное распределение потоков в сети в целом, а не оптимальную процедуру маршрутизации. Наиболее существенным свойством решения задачи (1.5) позволяющим установить связь между оптимальным распределением потоков и оптимальной процедурой маршрутизации, является утверждение, что любой составной маршрут передачи пакетов сообщений данных для $(l,m) \in N_{ЦК}$, является кратчайшим путем в метрике

$$D_{ij}'(f_{ij}) = \frac{dN_{ij}(f_{ij})}{df_{ij}}. \tag{1.7}$$

Составной маршрут между центрами коммутации l и *m* есть любой маршрут из совокупности $m \in M$, такой, что в любом тракте $(i,j) \in mf_{ij}(m) > 0.$

Маргинальная задержка (1.7) определяет приращение задержки в тракте (i,k) при “малом” увеличении потока. При этом, под “малым” увеличением интенсивности потока чаще всего понимается увеличение потока на величину $\Lambda\mu_{ik}$, а определение маршрута,

близкого к оптимальному, сводится к отысканию кратчайшего пути $(l,m) \in N_{ЦК}$ в метрике маргинальных задержек (1.7).

В связи с этим представляет интерес оценка маргинальной задержки (1.7). В ряде источников обосновывается предположение о близости маргинальной задержки и периода занятости тракта (i,j), связанного с наличием очереди к исходящему направлению передачи (i,j). Для систем массового обслуживания *M/G/1* преобразование Лапласа-Стильеса функции распределения периода занятости *П(t)* записывается в виде:

$$П^*(s) = B^*\left[s + \lambda_{ij} - \lambda ij П^*(s)\right], \tag{1.8}$$

где $B^*[s]-$ преобразование Лапласа-Стильеса функции распределения времени передачи пакета.

Среднее значение периода занятости определяется из соотношения

$$M_{\xi i} = -\frac{dП^*(s)}{ds}\bigg|_{s=0} = \frac{M[t_П]}{1-\lambda_{ij}M[t_П]}, \tag{1.9}$$

где $M[t_П]-$ математическое ожидание времени передачи пакета.

Среднее значение периода занятости при математическом ожидании длины очереди в ветви (i,j) $\overline{q}_{ij}$ можно определить из тождества Вальда:

$$M_{\xi 2} = \overline{q}_{ij} \cdot M_{\xi 1} = \overline{q}_{ij} \cdot \frac{M[t_П]}{1-\lambda_{ij}M[t_П]}. \tag{1.10}$$

Тогда среднее значение периода занятости, связанного с постановки в очередь к каналу передачи (i,j) дополнительного пакета, определяется из соотношения:

$$M_{\xi 3} == (\overline{q}_{ij} + 1) \cdot \frac{M[t_П]}{1-\lambda_{ij}M[t_П]}. \tag{1.11}$$

Учитывая, что время передачи пакета в сети передачи данных является случайной дискретной величиной, а каналы имеют низкое качество и могут выходить из строя, $M[t_П]$ можно записать в виде:

$$M[t_П] = \frac{1}{\kappa_Г(ij)\mu_{ij}c_{ij}} \sum_{z=1}^{Z} P_{ij}(z)z \tag{1.12}$$

где $\kappa_Г(ij)-$ коэффициент готовности канала (тракта) (i,j);

$P_{ij}(z)-$ статистическая вероятность передачи пакета по каналу связи (i,j) z раз;

Z – максимальное значение кратности повторения передачи пакета.

Основные черты процесса определения маршрутов, близких к оптимальным, сводятся к следующему.

Каждый $ЦК_i, i \in N_{ЦК}$ с интервалом τ_k получает оценку маргинальных задержек в соответствии с (1.12) от всех остальных ЦК $j \neq i, \quad i, j \in N_{ЦК}$.

Используя процедуру поиска кратчайшего пути в $G(N_{ЦК}, N_{TP}), N_{ЦКi}$ определяет отображение и тем самым строит для себя таблицу маршрутов.

Основу алгоритмов маршрутизации в большинстве схем составляют алгоритмы поиска кратчайших путей в графе $G(N_{ЦК}, N_{TP})$. Наиболее широко используемыми методами поиска кратчайших путей являются методы Дийкстры и Флойда.

Метод Дийкстры определяет кратчайшие пути от $ЦК_i$ до всех остальных ЦК и потому используется в сетях с децентрализованным алгоритмом маршрутизации. Алгоритм Флойда определяет маршруты для всех пар $(i, j) \in N_{ЦК}$ и используется в сетях централизованными или зоновыми алгоритмами маршрутизации. Использование в этом случае алгоритма Дийкстры для определения кратчайших путей увеличивает время расчета до 50%.

Нижняя оценка времени, необходимого алгоритму Дийкстры для определения кратчайших путей между *i*-м и всеми другими ЦК полносвязного графа, определяется из соотношения

$$T(Д) = \frac{3N_{ЦК}(N_{ЦК} - 1)}{2} \quad \max\left\{t_{ср}, t_{сл}\right\},$$

где $t_{ср}, t_{сл}$ – время выполнения операций сравнения и сложения соответственно.

Верхняя оценка сложности при использовании алгоритма Флойда определяется зависимостью

$$T(Ф) = 2N_{ЦК}^2(N_{ЦК} - 3)\max\left\{t_{ср}, t_{сл}\right\}.$$

Оценки *T(Д)* и *T(Ф)* для сети с $N_{ЦК} \leq 250$, при использовании ПЭВМ, не превышает 0,12 сек и 0,5 мин соответственно.

Полученные аналитические зависимости могут быть использованы для оценки маргинальной задержки применительно к условиям работы цифровой системы передачи.

СПИСОК ЛИТЕРАТУРЫ

1. *Мизин И.А., Богатырев В.А., Кулешов А.П.* Сети коммутации пакетов : учебное пособие для ВВУЗов связи – М. : Радио и связь, 1986. – 328 с.
2. Коршун В.Г. Выбор и оценка эффективности способов маршрутизации в СОД : учебное пособие для ВВУЗов связи – Л. : ВАС, 1986. 236 с.

О.А. Сафарьян[2], И.А. Пилипенко[2],
И.А. Федяев[2], И.А.Енгибарян[1], В.И. Юхнов[1]

ВЛИЯНИЕ ДОПЛЕРОВСКОГО СДВИГА ЧАСТОТЫ НА ДЕМОДУЛЯЦИЮ СИГНАЛОВ В МЕЖСПУТНИКОВЫХ КАНАЛАХ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
«Донской государственный технический университет» (ДГТУ),
г. Ростов-на-Дону, Россия[2]

Ключевые слова: связь с подвижными объектами, доплеровский сдвиг частоты, сигнальное созвездие.

Рассматриваются вопросы, позволяющие уточнять влияние доплеровского сдвига частоты на демодуляцию сигналов в межспутниковых каналах связи. Проанализированы два основных фактора, связанные с уменьшением отношения сигнал/шум и поворотом сигнального созвездия. Представлены результаты численных исследований влияния указанных факторов в зависимости от величины доплеровского сдвига частоты.

O.A. Safar'yan[2], I.A. Pilipenko[2],
I.A. Fediaev[2], I.A. Engibaryan[1], V.I. Yukhnov[1]

EFFECT OF DOPPLER FREQUENCY SHIFT ON DEMODULATION OF SIGNALS IN INTER-SATELLITE COMMUNICATION CHANNELS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Don State Technical University (DSTU), Rostov-on-Don, Russia[2]

Keywords: communication with moving objects, Doppler frequency shift, signal constellation

The questions allowing to clarify the influence of the Doppler frequency shift on the demodulation of signals in inter-satellite communication channels are considered. Two main factors related to the decrease in the signal-to-noise ratio and the rotation of the signal constellation are analyzed. The results of numerical studies of the influence of these factors depending on the magnitude of the Doppler frequency shift are presented.

Одним из наиболее сложных вопросов связи с подвижными объектами является организация передачи сигналов по межспутниковым каналам связи. Организация таких каналов передачи данных обеспечивает повышения эффективности применения космических систем и орбитальных группировок при решении задач в околоземном космическом пространстве. К таким задачам можно отнести картографирование земной поверхности, дистанционное зондирование Земли в интересах получения метеоданных глобального изменения климата, состояния океана и атмосферы.

Для повышения скорости передачи информации, в том числе и в межспутниковых каналах связи, используются сложные широкополосные сигналы (ШПС), в частности, фазоманипулированные сигналы (ФМ-сигналы) и сигналы с ортогонально-частотным разделением (OFDM-сигналы).

Еще одна тенденция развития спутниковых каналов связи, наряду с применением многопозиционных видов цифровой манипуляции сигналов, заключается в увеличении

частоты несущего колебания. Это позволяет снизить массогабаритные размеры приемо-передающей аппаратуры, добиться узких диаграмм направленности антенн, способствующих помехозащищенности связи и ослаблению интерференционных помех, увеличить информационную скорость каналов. В то же время ограничивающим фактором при организации спутниковых каналов связи является эффект доплеровского смещения несущей частоты, величина которого в *V*- и *W*-диапазонах частот может составлять единицы мегагерц, негативно влияющий на качество связи, ухудшая соотношение «сигнал – шум» и увеличивающий число ошибок при демодуляции сигналов [1-5].

Целью доклада является представление и анализ эффектов, связанных с влиянием доплеровского сдвига частоты принимаемого радиосигнала на демодуляцию сигналов.

Высокочастотный многопозиционный сигнал $S_{РЧ}$ на входе демодулятора определяется соотношением

$$S_{RF} = \sin\left((\omega_0 + \Delta\omega)t + \theta(t)\right) + S_N(t), \quad (1)$$

где $\omega_0 = 2\pi f_0$ - частота несущего колебания; $\Delta\omega = 2\pi\Delta f$ - доплеровский сдвиг частоты, обусловленный взаимным движением спутников; $\theta(t) = \varphi_k$ - начальная фаза в k-м импульсе посылки, определяемая видом модуляции и передаваемым информационным сообщением; $S_N(t)$ - шумовая составляющая принимаемого сигнала, пересчитанная к выходу линейного тракта.

Сигнал с выхода линейного тракта, в состав которого входят устройство понижения частоты (переноса сигнала в более низкочастотный диапазон), усилитель, разделяется на два канала. Структура каждого из каналов является одинаковой и включает: смеситель, фильр низких частот, интегратор.

Различие этих каналов заключается в том, что на одноименные входы смесителей синфазного и квадратурного каналов подаются сигналы, имеющие по отношению друг к другу фазовый сдвиг $\pi/2$. После прохождения в каждом из каналов ФНЧ и интегратора сигналы поступают на вход решающего устройства, где выделяется значение начальной фазы сигнала и соответственно выполняется демодуляция.

Наличие доплеровского сдвига частоты определяет два наиболее существенных фактора, влияющих на демодуляцию сигналов - снижение отношения сигнал шум на выходе интегратора, что приводит к повышению вероятности битовой ошибки и поворот сигнального созвездия, который может привести к неправильной демодуляции принимаемого сигнала.

Сигналы на выходе смесителей могут быть записаны следующим образом:

- на выходе смесителя синфазного канала

$$S_{см}^{(I)} = \left[\sin\left((\omega_0 + \Delta\omega)t + \theta(t)\right) + S_N(t)\right] \cdot \sin(\omega_0 t), \quad (2)$$

- на выходе смесителя квадратурного канала

$$S_{см}^{(Q)} = \left[\sin\left((\omega_0 + \Delta\omega)t + \theta(t)\right) + S_N(t)\right] \cdot \cos(\omega_0 t), \quad (3)$$

В свою очередь, сигналы на выходе соответствующих ФНЧ могут быть записаны следующим образом:

- в синфазном канале

$$S_{ФНЧ}^{(I)} = 0,5\cos\left(\Delta\omega\cdot t+\theta(t)\right)+S_N(t)\cdot\sin\omega_0\cdot t, \quad (4)$$

– в квадратурном канале

$$S_{ФНЧ}^{(Q)} = 0,5\sin\left(\Delta\omega\cdot t+\theta(t)\right)+S_N(t)\cdot\cos\omega_0\cdot t. \quad (5)$$

Сигналы (4) и (5) поступают соответственно на вход интеграторов синфазного и квадратурного каналов, на выходе которых формируются низкочастотные сигналы

– в синфазном канале

$$S_{инт}^{(I)} = \begin{cases} \sqrt{\left[\dfrac{\sin\left(\Delta\omega\cdot\tau+\varphi_k\right)-\sin\left(\varphi_k\right)}{\Delta\omega}\right]^2+\sigma_N^2}, & \Delta\omega\neq 0, \\ \sqrt{\left[\tau\cdot\cos\varphi_k\right]^2+\sigma_N^2}, & \Delta\omega = 0, \end{cases} \quad (6)$$

– в квадратурном канале

$$S_{инт}^{(Q)} = \begin{cases} \left[\dfrac{\cos\left(\Delta\omega\cdot\tau+\varphi_k\right)-\cos\left(\varphi_k\right)}{\Delta\omega}\right]^2+\sigma_N^2, & \Delta\omega\neq 0, \\ \left[\tau\cdot\sin\varphi_k\right]^2+\sigma_N^2, & \Delta\omega = 0, \end{cases} \quad (7)$$

где σ_N^2 - мощность теплового шума в каналах демодулятора.

Результаты исследования влияния доплеровского сдвига частоты на уровень сигнала на выходе соответствующего интегратора приведены на рисунке 1 при длительности импульса 10^{-3} с.

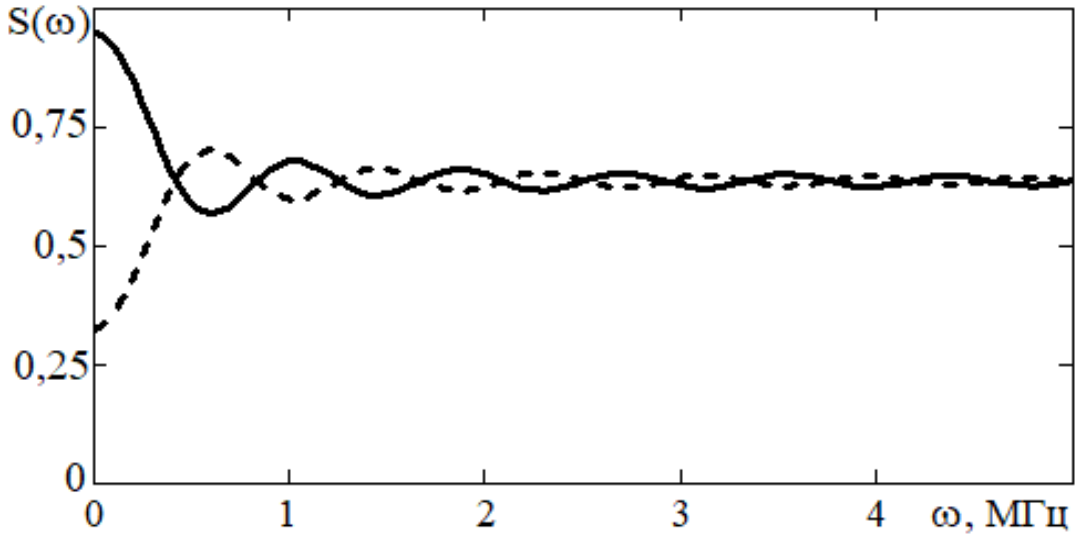


Рисунок 1. Уровень сигнала на выходе интегратора:
синфазного канала - сплошная линия, квадратурного канала - штриховая линия

Представленные зависимости показывают, что при увеличении доплеровского сдвига частоты уровни сигнала стремятся к одному значению, определяемому уровнем шумов на выходе интегратора или соответственно отношением сигнал/шум в канале связи. Последнее означает невозможность выделения начальной фазы при манипуляции сигнала и соответственно нарушение демодуляции сигналов.

Вторым эффектом, связанным с влиянием доплеровского сдвига частоты на демодуляцию сложных сигналов, является поворот сигнального созвездия на угол $\Delta\omega_д \cdot T/2$. Указанный эффект непосредственно следует из соотношений (6), (7). Кроме того, указанный эффект был отмечен в работах [4, 6].

На рисунке 2 приведена зависимость величины допустимого сдвига несущей частоты фазоманипулированного сигнала от числа символов *M* в алфавите манипуляции.

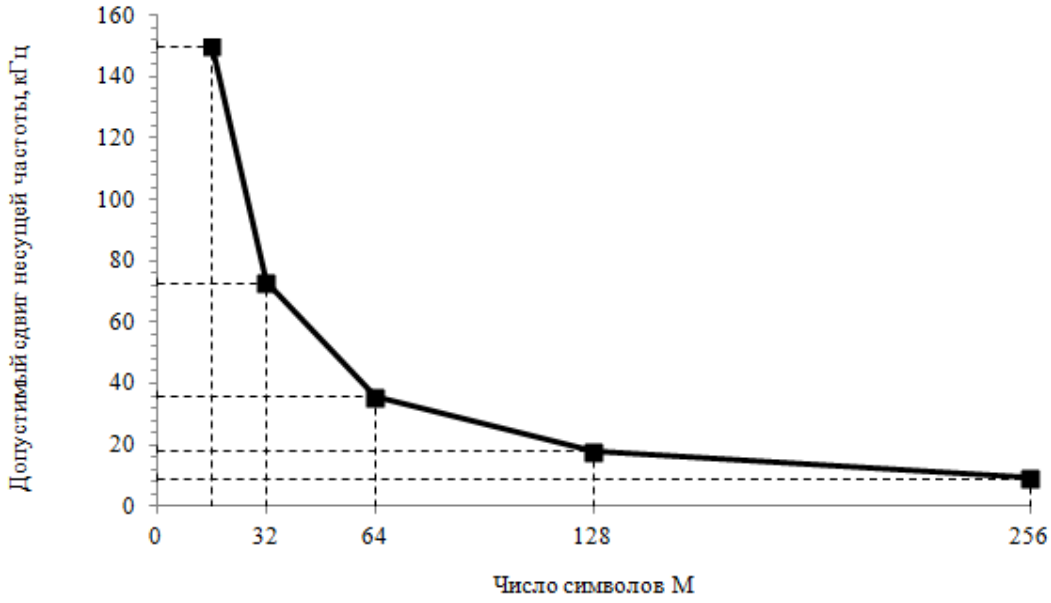


Рисунок 1. Уровень сигнала на выходе интегратора:
синфазного канала - сплошная линия, квадратурного канала - штриховая линия

Таким образом, можно отметить, что устойчивая связь с подвижными объектами и, в первую очередь, межспутниковая связь возможна только при компенсации доплеровского сдвига частоты, возникающего в канале связи. Приведенные зависимости позволяют определить величину нескомпенсированного значения доплеровского сдвига частоты.

Работа выполнена при материальной поддержке РФФИ, грант № 19-01-00151/21

СПИСОК ЛИТЕРАТУРЫ

1. Камнев В. Е., Черкасов В. В., Чечин Г. В. Спутниковые сети связи: Учеб. пособие. – М.: «Альпина Паблишер», 2004. – 536 с.
2. Спилкер Дж. Цифровая спутниковая связь. Пер. с англ. / Под ред. В. В. Маркова. – М.: Связь, 1979. – 592 с.
3. Енгибарян И.А., Юхнов В.И., Федяев И.А. Оценка влияния смещения частоты на прием фазоманипулированных сигналов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2020, С. 226-230.

4. Савченко В. И. Исследование влияния эффекта Доплера на канальные сигналы в системах беспроводной связи. Выпускная квалификационная работа. – НИУ «БелГУ», г. Белгород, 2018, – 69 с.
5. Ершов Р. А. Методы оценки частотно-временны́х параметров широкополосных сигналов спутниковых систем связи. Диссертация на соискание учёной степени кандидата технических наук. – ННГУ, г. Нижний Новгород, 2017, – 142 с.
6. Barabolya B. A., Karavaev S. V., Musinov V. M., Petukhov A. V., Prygunov A. G. Assessment of doppler frequency shift influense on phase manipulated signals reception in satellite data channels. XXVI International Scientific and Technical Conference Radiolocation, Navigation, Communication, conference proceeding. Voronezh, 29 September – 1 October 2020.

О.А. Сафарьян[2], И.А. Пилипенко[2], И.А.Енгибарян[1], В.И. Юхнов[1]

ЭКСПЕРТНЫЕ ОЦЕНКИ ПАРАМЕТРОВ СИГНАЛОВ В СИСТЕМАХ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
«Донской государственный технический университет» (ДГТУ),
г. Ростов-на-Дону, Россия[2]

Ключевые слова: модель сигнала, частотно-временные параметры сигнала, метод статистической стабилизации частоты, многомерная функция правдоподобия.

Рассматриваются вопросы построения экспертной системы для оценивания параметров сигнала в системах связи. Показано, что переход от одномерной к многомерной функции распределения и далее к экспертной системе позволяет уменьшить дисперсию оценок частоты несущего колебания сигналов в информационно-измерительной системе. Отмечены условия и правила выбора гипотез для получения оценок текущих значений частоты и относительной нестабильности генераторов.

O.A. Safar'yan[2], I.A. Pilipenko[2], I.A. Engibaryan[1], V.I. Yukhnov[1]

EXPERT ASSESSMENTS OF SIGNAL PARAMETERS IN COMMUNICATION SYSTEMS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Don State Technical University (DSTU), Rostov-on-Don, Russia[2]

Keywords: signal model, time-frequency parameters of the signal, method of statistical frequency stabilization, multidimensional likelihood function.

The issues of constructing an expert system for estimating signal parameters in communication systems are considered. It is shown that the transition from a one-dimensional to a multidimensional distribution function and further to an expert system makes it possible to reduce the variance of estimates of the frequency of the carrier oscillation of signals in the information and measurement system. The conditions and rules for the selection of hypotheses for

obtaining estimates of the current values of frequency and relative instability of generators are noted.

Используемые в системах связи сигналы представляют собой многомерные случайные процессы. Многомерный характер случайных процессов, используемых для описания сигналов, определяется, в первую очередь, следующими основными факторами:

- изменение параметров сигнала в соответствии с передаваемым информационным сообщением;
- шумами в канале (линии) связи, обусловленными тепловыми шумами, приемом сигналов других абонентов и др.;
- случайным изменением условий функционирования генераторов, формирующих сигналы.

В современных системах связи используются цифровые методы изменения информационных параметров сигналов, основой которых являются методы фазовой манипуляции [1]. Применение указанных методов связано с необходимостью обеспечения высокой стабильности частоты в каналах связи, которая может достигаться путем управления параметрами генераторов, однако поддержание требуемой стабильности определяется возможностью получения несмещенных, эффективных и состоятельных оценок параметров сигнала. К параметрам, определяющим для сигналов с фазовой манипуляцией высокую стабильность частоты, относятся:

- частота несущей, на основе которой формируется сигнал;
- относительная нестабильность частоты несущей сигнала.

Одним из методов повышения стабильности частоты, который может находить применение в системах связи, является метод статистической стабилизации или статистического оценивания частоты сигнала [2-7]. В [8, 9] предложено обобщение данного метода для одновременного оценивания текущего значения частоты несущей и относительной нестабильности генераторов. Однако при разработке данного метода сделано предположение о нормальном законе распределения отклонений частоты и относительной нестабильности от номинальных значений по нормальному закону распределения. В то же время более точное формирование оценок указанных параметров может быть получено с использованием экспертной обработки оценок, формируемых при рассмотрении различных законов распределения.

Целью доклада является рассмотрение метода экспертных процедур для получения оценок параметров генераторов, функционирующих одновременно и независимо в составе единой системы.

Представим измеряемое значение фазы сигнала n-го генератора на измерительном интервале следующим выражением

$$\Phi_n^{(m)} = \Phi_n^{(0)} + f_n^{(0)} \cdot \Delta t + (\Delta f_n + 2\delta f_n) \cdot t_0, \quad n = 1, ..., N \qquad (1)$$

где Φ_n - измеренное значение фазы сигнала, полученное для n-го генератора на измерительном интервале; $\Phi_n^{(0)} = f_n^{(0)} \cdot t_0$; $\Delta f_n = f_n - f_{0,n}$; Δt - отклонение длительности измерительного интервала от номинального значения, обусловленное нестабильностью генератора Γ_0, используемого в качестве устройства, задающего длительность измерительного интервала; N - число одновременно и независимо функционирующих генераторов; M - число гипотез о законах распределения случайных значений параметров одновременно и независимо функционирующих генераторов.

При линеаризации соотношения (1) отклонение частоты n-го генератора от номинального значения может быть представлено в виде [8]

$$\Delta f_n = \frac{\Delta\Phi_n - f_n^{(0)} \cdot \Delta t}{t_0} - 2\delta f_n \quad , \tag{2}$$

где $\Delta\Phi_n = \Phi_n - \Phi_n^{(0)}$.

Обозначим плотность распределения отклонений частоты n-го генератора $p_n\left(\Delta t, \delta f_n, \delta\sigma_n\right)$, зависящую от всех оцениваемых параметров Δt, δf_n и $\delta\sigma_n$. На основе введенных функций функция правдоподобия может быть представлена в виде

$$L\left(\mathbf{\Delta t}, \mathbf{\delta f}, \mathbf{\delta\sigma}\right) = \sum_{n=1}^{N} p_n\left(\mathbf{\Delta t}, \mathbf{\delta f}, \mathbf{\delta\sigma}\right) \quad , \tag{3}$$

где Δt; $\mathbf{\delta f} = \left\{\delta f_1, ..., \delta f_N\right\}$; $\mathbf{\delta\sigma} = \left\{\delta\sigma_1, ..., \delta\sigma_N\right\}$.

Оценки $\Delta\hat{t}_m$, определяются из условия максимума функции правдоподобия (3), что приводит к решению системы $2N+1$ уравнений

$$\begin{cases} \dfrac{\partial L\left(\Delta t, \mathbf{\delta f}, \mathbf{\delta\sigma}\right)}{\partial \Delta t_m} = 0, \\ \dfrac{\partial L\left(\mathbf{\Delta t}, \mathbf{\delta f}, \mathbf{\delta\sigma}\right)}{\partial \delta f_n} = 0,\ n = 1, ..., N, \\ \dfrac{\partial L\left(\mathbf{\Delta t}, \mathbf{\delta f}, \mathbf{\delta\sigma}\right)}{\partial \delta\sigma_n} = 0,\ n = 1, ..., N. \end{cases} \tag{4}$$

Получаемое решение зависит от выбранной закона распределения (плотности вероятности) случайных величин. С учетом этого для получения оценок выполняется согласование полученных результатов, которое проводится с использованием правила средней оценки. Использование указанного правила в данном случае является наиболее обоснованным, так как сводится к получению взвешенной оценки полученных результатов. В качестве весов выбираются значения, обратные полученным дисперсиям оценок.

Повышение объективности получаемых оценок может быть достигнуто на основе обработки результатов с использованием коэффициентов конкордации [10]

$$W = \frac{12\sum_{m=1}^{M} d_m^2}{N^2\left(M^3 - M\right)} \quad , \tag{3}$$

где d - отклонение суммы рангов для n-го генератора от среднего значения рангов, получаемых для каждой гипотезы оценивания.

Коэффициент конкордации вычисляется для каждого из оцениваемых параметров генераторов. При оценке степени согласованности результатов, получаемых с

использованием различных гипотез, принимают, что значение коэффициента конкордации должен быть не менее 0,75.

В случае совпадения экспертных оценок получаемое значение принимается за текущее значение параметра генератора. В противном случае проводится расширение числа используемых гипотез о законах распределения случайных величин.

Формирование экспертных оценок на основе данного подхода позволяет исключить следующие недостатки:

- сложность организации экспертизы, определяемой отбором экспертов в достаточном количестве и качестве, так как в качестве экспертов выступают предположения о принятых законах распределения;
- сложность согласования полученных данных, так как итоговый результат определяется в виде взвешенной суммы результатов, полученных для каждого закона распределения;
- возможная субъективность экспертов, поскольку взвешенное суммирование результатов дает возможность существенно снизить вес заведомо неправильного предположения;
- возможное влияние на результат выбранной формы проведения получения экспертных оценок, в частности при открытом опросе возникает возможность конформизма мнений.

Таким образом, можно отметить, что экспертное оценивание отклонений фаз сигналов в системе, одновременно и независимо функционирующих при использовании предложенной трехмерной функции правдоподобия, формируемой на основе различных законов распределения, принципиально снимает ограничения на требования точного задания значений параметров генераторов. Указанный результат соответственно расширяет возможности применения метода статистической стабилизации или статистического оценивания частоты и относительной нестабильности генераторов в системах связи.

Работа выполнена при материальной поддержке РФФИ, грант № 19-01-00151/21.

СПИСОК ЛИТЕРАТУРЫ

1. Алешин Л.И. Защиты информации в системах управления. – М.: МГУК. – 2009.
2. Сафарьян О.А. Метод статистической стабилизации частоты независимо работающих генераторов в инфокоммуникационных системах: дис. канд. техн. наук: 05.12.04: защищена 23.04.15: утв. 6.10.15 № 1192/нк-6 / Сафарьян Ольга Александровна. – Ростов-на-Дону, 2014. – 151 с.
3. Сафарьян О.А. Метод оценки частоты генераторов в условиях непрогнозируемого изменения длительности интервала измерений // Вестник ДГТУ, 2014, № 4. Ч. 2. - С. 47-54.
4. Габриэльян Д.Д., Прыгунов А.А., Прыгунов А.Г., Сафарьян О.А. Метод оценки частот в системе генераторов // Физические основы приборостроения, 2012, Т. 1. № 2. - С. 72-77.
5. Енгибарян И.А., Сафарьян О.А. Использование свойств эмерджентности в инфокоммуникационных системах // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Часть 1. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2016, С. 122-126.
6. Юхнов В.И., Енгибарян И.А., Пилипенко И.А., Сафарьян О.А. Моделирование сигналов в распределенных информационно-измерительных системах // Труды Северо-Кавказского филиала Московского технического университета связи и

информатики. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2019, С. 152-155.
7. Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Сахаров И.А. Оценка вариации Аллана при использовании метода статистической стабилизации частоты генераторов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Часть 1. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2019, С. 156-159.
8. Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Пилипенко И.А. Аналитические зависимости для оценок отклонения частоты и длительности формируемых сигналов в информационно-телекоммуникационных системах // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, Часть 1. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2020, С. 68-71.
9. Юхнов В.И., Енгибарян И.А., Сафарьян О.А., Пилипенко И.А. Оценивание параметров сигналов в распределенных информационно-измерительных системах с использованием трехмерной функции правдоподобия // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Часть 1. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2020, С. 72-76.
10. Введение в экспертные системы / П. Джексон: 3-е изд. – М.: Издательский дом «Вильямс», 2001. – 623 с

С.Г. Беликов, Н.В. Руденко, В.В. Евстафьев, Д.А. Жукова

ИССЛЕДОВАНИЕ ИСТОЧНИКА ВТОРИЧНОГО ЭЛЕКТРОПИТАНИЯ МОБИЛЬНОГО СРЕДСТВА СВЯЗИ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
г. Ростов-на-Дону, Россия

Ключевые слова: источники вторичного электропитания мобильных средств связи, компьютерное моделирование, исследование характеристик.

В статье решена задача компьютерного моделирования импульсного источника вторичного электропитания мобильного средства связи с широтно-импульсным регулированием. Разработана виртуальная модель такого источника в программной среде *Multisim*, которая позволяет оценить качество регулирования и стабилизации выходного напряжения, а также энергетические свойства источника. Предложен алгоритм и методика исследования этой модели. Эти результаты могут быть использованы при проектировании, а также в учебных целях.

S.G. Belikov, N.V. Rudenko, V.V. Evstafiev, D.A. Zhukova

RESEARCH OF SECONDARY POWER SUPPLY SOURCE MOBILE COMMUNICATION WITH INFORMATION TECHNOLOGIES

Federal State Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia

Key words: sources of secondary power supply of mobile communications, computer modeling, study of characteristics.

The article solves the problem of computer modeling of a pulsed source of secondary power supply of a mobile communication device with pulse-width control. A virtual model of such a source has been developed in the Multisim software environment, which makes it possible to evaluate the quality of regulation and stabilization of the output voltage, as well as the energy properties of the source. An algorithm and a method for studying this model are proposed. These results can be used in design as well as for educational purposes.

Введение. Развитие источников вторичного электропитания (ИВЭП) мобильных средств связи (МСС) идёт по пути снижения массогабаритных и повышения удельных энергетических характеристик [1]. Важным достижением в этом направлении стало применение импульсных ИВЭП с бестрансформаторным входом на базе преобразователей постоянного напряжения с широтно-импульсным регулированием. С целью проектирования таких ИВЭП с заданными характеристиками и их исследования целесообразно разработать виртуальную модель ИВЭП и алгоритм её исследования

Постановка задачи. Задача формулируется следующим образом. Разработать виртуальную модель импульсного ИВЭП МСС и алгоритм её исследования.

Для решения поставленной задачи целесообразно решить следующие вопросы:

- выбрать электрическую принципиальную схему ИВЭП, задаться её характеристиками и выбрать программное обеспечение для моделирования;
- разработать виртуальную модель источника;
- предложить алгоритм исследования характеристик источника.

Выбор электрической принципиальной схемы источника. В качестве объекта исследования выбран источник электропитания автомобильной радиостанции БИЗОН КМ-9000 *UHF*. Автомобильная радиостанция Бизон КМ9000 *UHF* предназначена для работы в профессиональном диапазоне 400-470 МГц. Благодаря радиопередатчику мощностью 45Вт, радиостанция "БИЗОН"КМ9000 *UHF* обеспечивает большую зону покрытия и может использоваться как в автомобиле, так и на стационарных объектах. Наличие 512 каналов, позволяют использовать радиостанцию в крупных сетях связи и организовывать взаимодействие между группами абонентов [2, 3]. Основные характеристики [3]:

- диапазон частот: *UHF* 400-470 МГц;
- мощность: 45 Вт;
- напряжение питания: 13,8 В;
- напряжение на выходе блока питания: 5 В;
- коэффициент пульсаций выходного напряжения не выше 1%;
- температурный режим: от -30 до +60 ‘С.

Выбор программного обеспечения для моделирования. В последние годы на рынке программного обеспечения появилась программная среда *Multisim*. Эта программная среда имеет примерно такой же интерфейс, как и *EWB*, но имеет следующие достоинства [4, 5]:

– в её библиотеке содержится более 16000 электронных компонентов, сопровождаемых аналитическими моделями, пригодными для быстрого моделирования;
– в её библиотеке виртуальных приборов содержится большое количество контрольно-измерительных приборов, по внешнему виду и характеристикам приближённых к их промышленным аналогам.

Таким образом, исследование ИВЭП целесообразно выполнять в программной среде *Multisim*. Это обусловлено большой элементной базой, базой виртуальных приборов, а также удобством схемотехнического моделирования.

Разработка виртуальной модели источника и назначение её элементов. На основе принципиальной электрической схемы выбранного источника питания в программной среде *Multisim* разработана его виртуальная модель, представленная на рисунке 1.

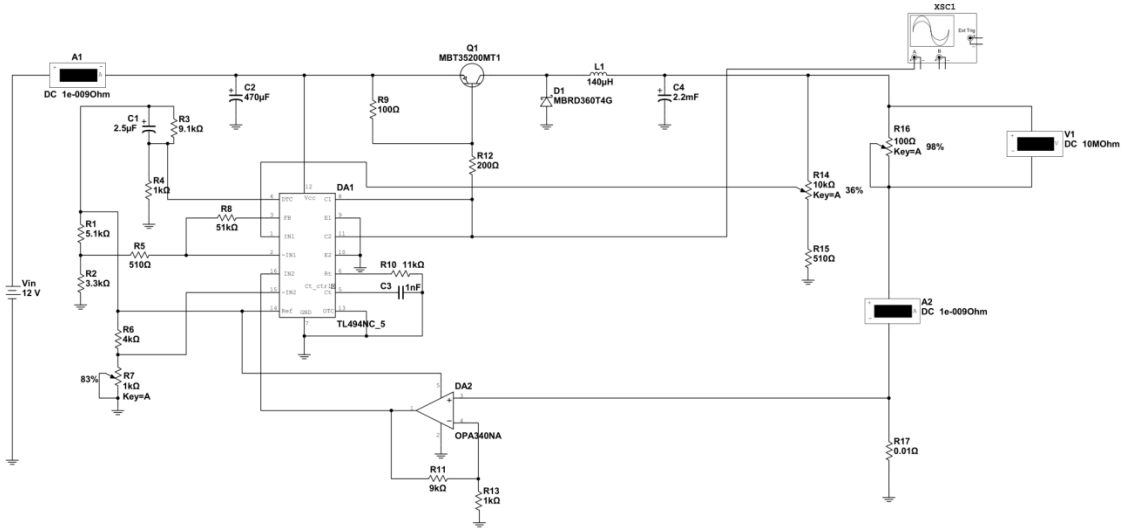


Рисунок 1. Виртуальная модель ИВЭП

Наиболее важным элементом данной схемы является микросхема *DA*1, которая является ШИМ контроллером с возможностью контроля выходного напряжения и тока. Это контроллер *TL*494 фирмы T*exas Instruments* - самый распространённый ШИМ-контроллер, на базе которого создавалась основная масса компьютерных блоков питания, и силовые части различных бытовых приборов. Отечественный аналог этой микросхемы - М1114ЕУ4 (КР1114ЕУ4) [6, 7].

Для питания понижающего преобразователя напряжения используется источники химической энергии *Vin* , значениями от 9 до 30 В.

Транзистор *Q*1 работает в режиме ключа, подключая источник питания к нагрузке в течении времени его включения, которое задается микросхемой *DA*1. Резистором *R*12 задается ток базы транзистора, а резистор *R*9 предназначен для надежного закрывания транзистора. Делитель напряжения *R*1 и *R*2 формирует опорное напряжение для усилителя ошибки по напряжению. Резистор *R*8 представляет собой обратную связь с выхода усилителя ошибки. Улучшает стабильность усилителя ошибок и задает, совместно с резистором *R*5, коэффициент усиления усилителя ошибки.

Делитель напряжения *R*6 и *R*7 формируют опорное напряжение для усилителя ошибки по току. *R*7 позволяет регулировать опорное напряжение и тем самым регулировать ограничение тока нагрузки. Конденсатор *C*1 и резистор *R*4 формируют плавный пуск схемы. Делитель напряжение *R*3 и *R*4 позволяют задавать «мертвое время» (минимальное

время в выключенном состоянии). Конденсатор *C*2 уменьшает потери в источнике питания, делая потребление энергии от него более постоянным.

Резистор *R*10 и Конденсатор *C*3 являются частотозадающими для генератора прямоугольных импульсов, используемых для формирования сигнала ШИМ.

Дроссель *L*1 запасает энергию, полученную за время включения транзистора, и уменьшает пульсации тока. Конденсатор *C*4 служит для запасания энергии, уменьшения пульсаций выходного напряжения. При переходе транзистора в выключенное состояние, дроссель и конденсатор отдают свою запасенную энергию в нагрузку.

Делитель напряжения *R*14 и *R*15 представляют собой обратную связь для контроля и управления выходного напряжения. Изменение переменного сопротивления R14 позволяет изменять выходное напряжение. Резистор *R*16 выполняет роль нагрузки преобразователя напряжения и выполнен в виде переменного сопротивления.

Резистор *R*17 работает как датчик тока и предназначен для контроля и ограничения выходного тока, проходящего через нагрузку. Т.к. сопротивление датчика тока достаточно мало, то на нем будет падать напряжение недостаточное для корректной работы усилителя ошибки, поэтому в качестве дополнительного усиления используется микросхема *DA*2, а резисторы *R*11 и *R*13 выставляют коэффициент усиления этой микросхемы, равный 10.

В качестве измерителей входного и выходного токов используются амперметры *A*1 и *A*2 соответственно. Для измерения выходного напряжения используется вольтметр *V*1. Для отслеживания сигнала управления ШИМ используется осциллограф *XSC*1.

Осциллограмма ШИМ-сигнала при линейном законе изменения коэффициента заполнения представлена на рисунке 2.

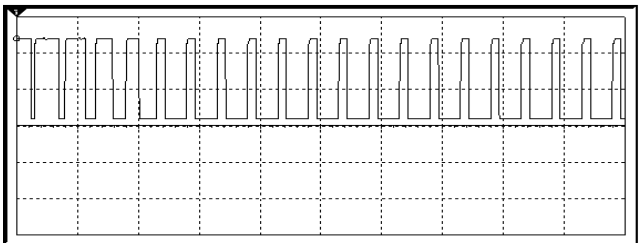


Рисунок 2. Осциллограмма ШИМ-сигнала при линейном законе изменения коэффициента заполнения

Алгоритм исследования характеристик источника. Разработан алгоритм исследования характеристик ИВЭП с помощью виртуальной модели. Он включает следующие этапы:

- снятие временных диаграмм выходного напряжения, подтверждающие правильность функционирования источника;
- снятие и построение графиков внешней, регулировочной и эксплуатационной характеристик источника;
- построение энергетических характеристик источника.

Временные диаграммы выходного напряжения при разных значениях тока нагрузки представлены на рисунке 3.

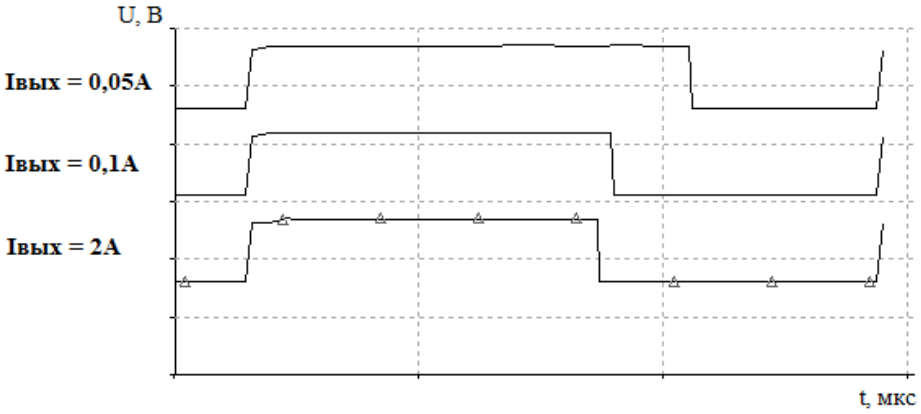


Рисунок 3. Временные диаграммы выходного напряжения при разных значениях тока нагрузки

Из рисунка 3 видно, что с увеличением тока нагрузки уменьшается выходное напряжение и возникает увеличение времени работы транзистора, что компенсирует это уменьшение, подтверждая правильность функционирования схемы.

Внешняя характеристика ИВЭП представлена на рисунке 4. Она получена путём изменения тока нагрузки на резисторе *R*16 при постоянном напряжении входного напряжении.

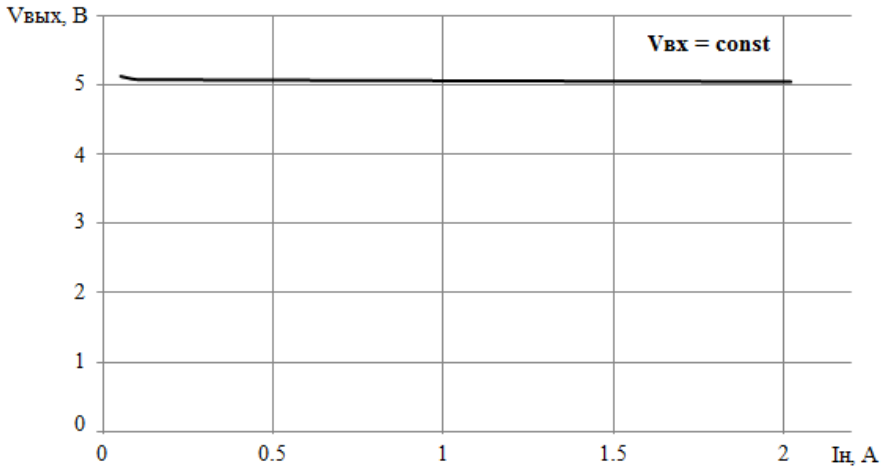


Рисунок 4. Внешняя характеристика источника

Внешняя характеристика обладает высокой жесткостью, относительное отклонение напряжения не превышает 0,5%, что соответствует современным требованиям к ИВЭП малой мощности [1].

Регулировочная характеристика представлена на рисунке 5 и показывает, как нужно изменять коэффициент заполнения при изменении тока нагрузки для обеспечения постоянного напряжения на выходе источника.

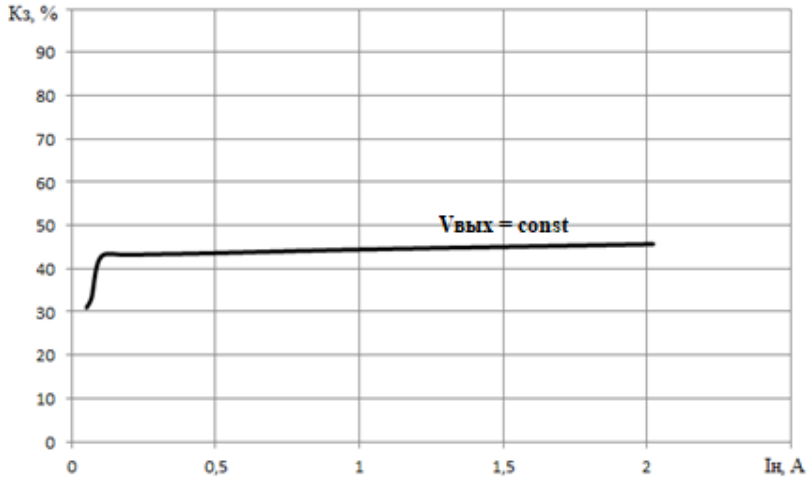


Рисунок 5. Регулировочная характеристика источника

Эксплуатационная характеристика источника представлена на рисунке 6. Она позволяет исследовать свойства ИВЭП как стабилизатора напряжения. Из рисунка 6 видно, что при изменении входного напряжения от 10 до 26 В выходное напряжение изменяется от 5 до 5,15 В. При этом ток нагрузки остаётся неизменным. Если принять номинальные значения напряжений $U_{вх.н}$ = 16 В, а $U_{вых.н}$ = -5,1 В, то можно определить коэффициент стабилизации:

$$K_{ст} = \frac{\Delta U_{вх}}{U_{вх.н}} : \frac{\Delta U_{вых}}{U_{вых.н}} = \frac{\Delta U_{вх}}{\Delta U_{вых}} \cdot \frac{U_{вых.н}}{U_{вх.н}} = \frac{16}{0{,}15} \cdot \frac{5{,}1}{16} = 34 .$$

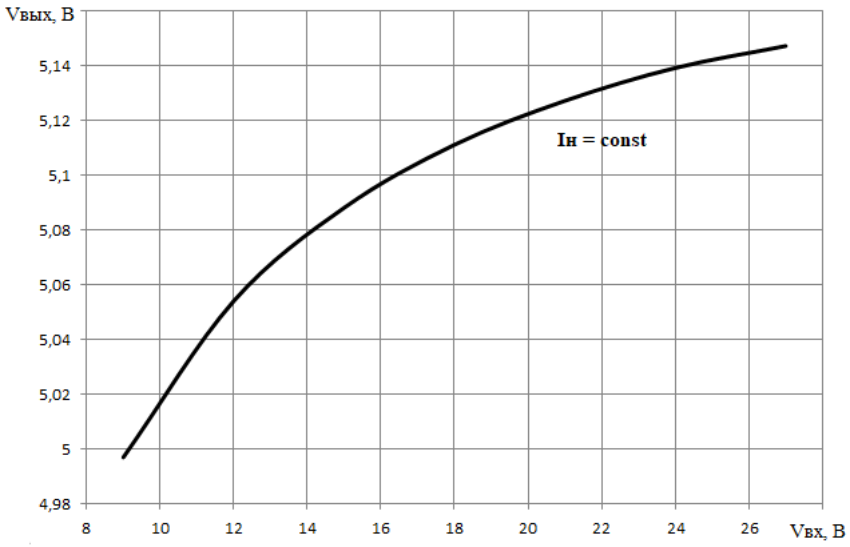


Рисунок 6. Эксплуатационная характеристика источника

Энергетическая характеристика ИВЭП – зависимость КПД от тока нагрузки при постоянном входном напряжении – представлена на рисунке 7.

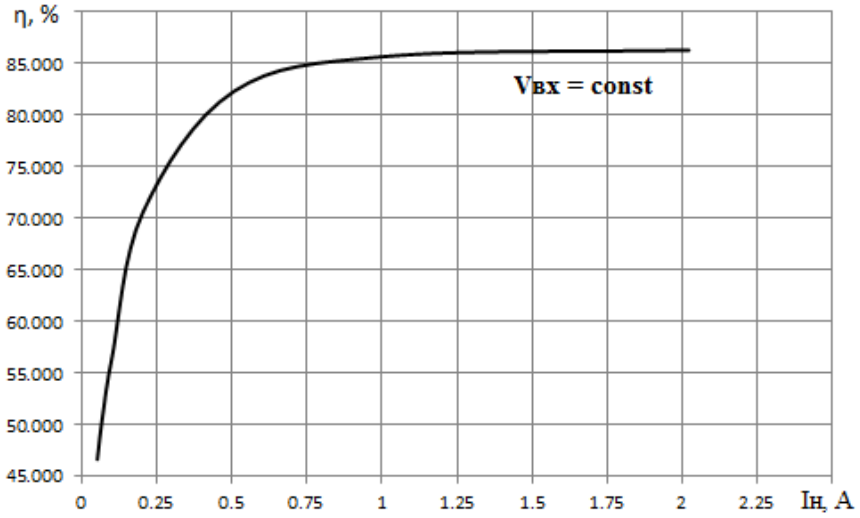


Рисунок 7. Энергетическая характеристика источника

При этом КПД источника рассчитывается как отношение выходной активной мощности источника к входной активной мощности при разных токах нагрузки. Из этой характеристики следует, что при изменении нагрузки в диапазоне от 0,3 $I_{ном}$ до 1,5 $I_{ном}$ КПД изменяется от 82% до 86,5%, что соответствует современным требованиям к ИВЭП малой мощности [1].

Вывод. Разработана виртуальная модель импульсного источника вторичного электропитания мобильного средства связи с широтно-импульсным регулированием, которая позволяет оценить качество регулирования и стабилизации выходного напряжения, а также энергетические свойства источника. Предложен алгоритм и методика исследования этой модели. Эти результаты могут быть использованы при проектировании, а также в учебных целях.

СПИСОК ЛИТЕРАТУРЫ

1. *Битюков В.К.* Источники вторичного электропитания: учебник / В.К. Битюков, Д.С. Симачков, В.П. Бабенко. – Москва : Инфра-Инженерия, 2019. 376 с.
2. Портал компании РАДИО ПРЕДЛОЖЕНИЕ [Электронный ресурс]: URL:http://www.radiooffer.ru/radiostancii/bizon/avtomobilnaya_radiostanciya_bizon_km9000_uhf_45_vt1/ (дата обращения: 21.10.2021 г.).
3. Радиостанция «Бизон». Руководство по технической эксплуатации ИЖ1.101017/018РО. 2017.
4. *Любимов Э.В.* Теория и практика электротехнических расчётов в среде *Mathcad* и *Multisim*. СПб.: Наука и Техника, 2012. 400 с.
5. *Хернитер М. Е.* Электронное моделирование в *Multisim*. М.: ДМК Пресс, 2010. 488 с.
6. Компания *Texas Instruments*: официальный сайт. Обновляется в течение суток. – URL: https://www.ti.com/product/TL494(дата обращения: 21.10.2021).
7. *Петрушов Н.* TL494, что это за "зверь" такой? // Портал «В помощь радиолюбителю» [Электронный ресурс]: URL: http://vprl.ru/publ/tekhnologii/nachinajushhim/tl494_chto_ehto_za_zver_takoj/9-1-0-151 (дата обращения: 21.10.2021 г.).

М.В. Деремов[1], Н.В. Руденко[1], В.В. Ершов[2]

О ВОЗМОЖНОСТИ УПРАВЛЕНИЯ ГИБРИДНЫМИ ЭНЕРГЕТИЧЕСКИМИ УСТАНОВКАМИ СИСТЕМ ЭЛЕКТРОПИТАНИЯ АВТОНОМНЫХ ОБЪЕКТОВ СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
г. Ростов-на-Дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: вихревые ветроэнергетические установки, регулирование скорости вращения, солнечные батареи, регулирование наклона панели, повышение надёжности.

В статье рассмотрен вопрос о возможности управления ветроэнергетическими генераторами и солнечными батареями в составе гибридных энергетических установок систем электропитания автономных объектов связи. Проведен сравнительный анализ различных типов регуляторов скорости вращения. В результате был предложен способ управления перекрытием потоков ветра. Показано, что перекрытие ветрового потока в вихревых ветроэнергетических установках позволяет регулировать скорость вращения и повысить надёжность и эффективность их эксплуатации. Использование вихревых установок в сочетании с солнечными панелями, размещёнными на поверхности конуса, обеспечит эффективное использование солнечной энергии за счет регулирования угла наклона конуса.

M.V. Deremov[1], N.V. Rudenko[1], V.V. Ershov[2],

ABOUT THE POSSIBILITY OF HYBRID ENERGY CONTROL AUTONOMOUS POWER SUPPLY INSTALLATIONS COMMUNICATION OBJECTS

Federal State Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Key words: vortex wind turbines, speed control, solar panels, panel tilt control, reliability enhancement.

Введение. В России диапазон применения ветровых потоков очень широкий. Значение среднегодовой скорости ветра на территории нашей страны варьируется как в меньшую, так и в большую сторону (рисунок 1) [1].

Рисунок 1. Ветровые ресурсы России (скорость ветра на высоте 10 м)

Анализ мировой практики эксплуатации современных ВЭУ с горизонтальной осью вращения позволяет выделить следующие скоростные режимы работы [3-6]:

- при среднегодовой скорости ветра менее 4...5 м/с применение ВЭУ не эффективно;
- при среднегодовой скорости ветра 4...5 м/с большинство ВЭУ начинают отдавать полезную мощность;
- при среднегодовой скорости ветра 5...8 м/с ВЭУ разгоняются до номинального режима;
- при среднегодовой скорости ветра 8...11 м/с ВЭУ работают в режиме номинальной мощности и частоты вращения;
- в диапазоне скоростей от 8...11 м/с до 23...25 м/с ВЭУ вырабатывают избыточную по отношению к номинальной мощности энергию, а частота вращения может превысить расчётную;
- при скоростях более 23...25 м/с ВЭУ выключаются из работы, так как усилия испытываемые ветроколесом и башней, становятся слишком большими.

На основании анализа скоростных режимов ВЭУ можно сделать следующий вывод, для использования всего диапазона ветровой энергии, целесообразно применять регуляторы скорости вращения. В настоящее время мощные и супермощные установки регулируются за счет изменения угла наклона ветроколеса, что существенно усложняет конструкцию и приводит к снижению надежности [2].

Кроме этого, для повышения надежности целесообразно использовать гибридные энергетические установки с использование ВЭУ и солнечных батарей (СБ) [7, 8]. Однако, эффективность СБ зависит от угла падения светового потока на плоскость солнечной панели.

Таким образом, изучение возможностей управления гибридными энергоустановками систем электропитания автономных объектов связи является актуальной задачей.

Результаты исследований. Задача формулируется следующим образом обосновать возможности управления гибридными энергоустановками систем электропитания автономных объектов связи

Для решения задачи необходимо провести анализ характеристик известных типов регуляторов. В настоящее время существует несколько способов управления ВЭУ. Достоинства и недостатки наиболее известных регуляторов представлены в таблице 1 [2].

Таблица 1. Сравнительная характеристика различных типов регуляторов скорости вращения

Тип регулятора	Критерии оценивания	
1	2	3
	Достоинства	Недостатки
Управление без изменения частоты вращения	– простота; – высокий КПД.	– узкий диапазон применения; – надежность.
Управление изменением установочного угла лопастей	– широкий диапазон применения; – благоприятные режимы эксплуатации.	– сложность конструкции; – надежность; – высокая стоимость.
Управление изменением передаточного отношения редуктора-мультипликатора ветродвигателя	– широкий диапазон применения; – простота.	– сниженная эффективность; – надежность.

Из таблицы 1 видно, что основным недостатком известных способов управления ВЭУ является сниженная надежность. Поэтому возникает задача применения установок с упрощенным регулированием, которые повышают надежность такой системы и расширяют диапазон эффективного использования ветрогенераторов.

В условиях сильных ветров, например, при скорости ветра 25 м/с, современные установки блокируют, чтобы они не вышли из строя [3]. Предлагается способ управления перекрытием потоков ветра, что особенно перспективно в ветрогенераторах с вертикальной осью вращения. При этом появляется возможность регулирования скорости вращения, как в сторону увеличения, так и в сторону уменьшения.

Известна ветроэнергетическая установка (рисунок 2), запатентованная в Донском государственном техническом университете (г. Ростов-на-Дону) [6-8]. Данная установка содержит привод 1 и рычаг 2 с заслонкой 3, которая двигается перпендикулярно ветру, перекрывая его поток.

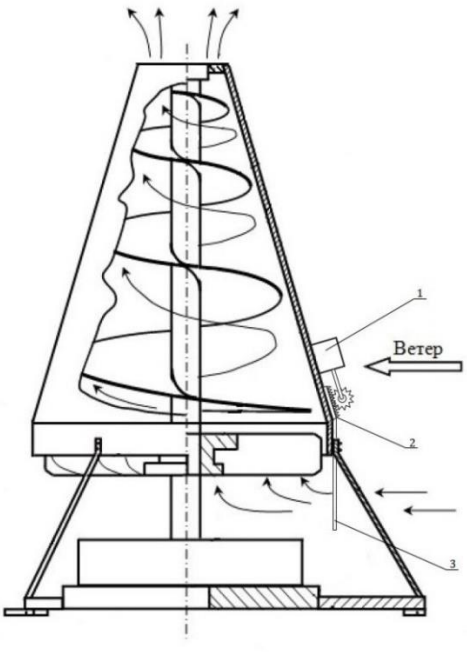


Рисунок 2. Конструкция вихревой ветроэнергетической установки

Кроме этого, для эффективного использования СБ можно регулировать угол наклона солнечных панелей. Эксплуатация солнечных панелей под углом в 45 градусов дает максимальную среднегодовую выработку электроэнергии. Поэтому изготовление таких установок изначально под этим углом упростит регулирование этих панелей в зависимости от сезона. Оптимальный для летнего времени года угол наклона – 30-40 градусов, для зимнего периода – 70 и более градусов [4, 5]. Использование вихревых установок в сочетании с солнечными панелями, размещёнными на поверхности конуса, обеспечит эффективное использование солнечной энергии за счет регулирования угла наклона конуса.

Выводы.

1. Перекрытие ветрового потока в вихревых ветроэнергетических установках позволяет регулировать скорость вращения и повысить надёжность и эффективность их эксплуатации.
2. Применение солнечных панелей в гибридных установках и в вихревых ветроэнергетических установках повышает надежность и упрощает работу за счет регулирования угла наклона конуса.

СПИСОК ЛИТЕРАТУРЫ

1. Ресурсы и эффективность использования источников энергии в России/ Коллектив авторов. СПб.: Наука, 2002. 314 с.
2. Исследование алгоритмов управления и совершенствование системы автоматического управления ветроэнергетической установки с вертикальной осью вращения. [Электронный ресурс]: URL: https://masters.donntu.org/2019/fkita/ivannikov/diss/index.htm (дата обращения 13.10.2021 г.)
3. Мегаконструкции. Самые большие ветрогенераторы. [Электронный ресурс]: URL: https://habr.com/ru/post/373021/ (дата обращения 14.10.2021 г.)
4. Угол наклона и ориентация солнечных батарей для максимальной производительности. [Электронный ресурс]: URL: https://tcip.ru/blog/solar-panels/ugol-naklona-i-orientatsiya-solnechnyh-batarej-dlya-maksimalnoj-proizvoditelnosti.html (дата обращения 14.10.2021 г.)
5. Оптимальный угол наклона солнечных батарей. [Электронный ресурс]: URL:
6. https://nsia-energy.ru/info/articles/16-optimalnyj-ugol-naklona-solnechnykh-batarej (дата обращения 15.10.2021 г.)
7. *Руденко Н.В., Ершов В.В., Пугачев И.В., Коньшина Н.А.* Ветроэнергетическая установка: патент на изобретение № 2689661 Рос. Федерация. Бюл. №16, 2019
8. *Rudenko N.V., Ershov V.V., Konshina N.A.* Energy Conservation in High-Rise Buildings Based on Environmentally-Friendly Renewable Energy Sources // IOP Conf. Series: Earth and Environmental Science. 2019. V. 224 (1). [Электронный ресурс] // URL: http://iopscience.iop.org/article/10.1088/1755-1315/224/1/012020/pdf (дата обращения: 15.10.2021).
9. *Rudenko N., Ershov V., Trints V.* Increasing power supply efficiency of livestock complexes at small farms using renewable energy sources // IOP Conf. Series: Earth and Environmental Science403 (2019) 012123. doi:10.1088/1755-1315/403/1/012123. [Электронный ресурс] // URL: https://iopscience.iop.org/article/10.1088/1755-1315/403/1/012123/pdf (дата обращения: 15.10.2021).

Г.В. Терещенко, Д.Л. Устименко

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПРОВОДНОЙ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, новые технологии, информационное общество, 5G, 6G, связь, интернет.

В статье рассмотрены актуальные тенденции современного информационного общества, определены основные тенденции в формировании инфокоммуникационных технологий во всем мире.

G.V. Tereshchenko, D.L. Ustimenko

CURRENT STATE AND PROSPECTS FOR THE DEVELOPMENT OF WIRELESS COMMUNICATIONS

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

Keywords: information technology, new technologies, information society, 5G, 6G, communications, Internet.

The article examines the current trends of the modern information society, identifies the main trends in the formation of info communication technologies around the world.

Цель работы: исследование состояния систем связи нынешнего времени, рассмотрение возможных перспектив развития

Задача работы: разобраться, как устроены сети 5G; оценить возможности применения 5G технологий; рассмотреть возможности сети 6G и сравнить с сетью 5G.

Таблица 1. Обозначения

1G, 2G, 3G, 4G, 5G, 6G	Первое, второе, третье, четвертое, пятое, шестое поколение беспроводной связи
AI	Искусственный интеллект
GL	Глубокое обучение
ML	Машинное обучение
VR	Виртуальная реальность
AR	Дополнительная реальность
ТГц	Терагерц

Введение

Системы беспроводной связи играют очень важную роль в современном обществе в сфере развлечений, бизнеса, коммерции, здравоохранения и безопасности. Эти системы

продолжают развиваться от одного поколения к другому, и в настоящее время мы наблюдаем развертывание беспроводных систем пятого поколения (5G) по всему миру. Ученые и представители отрасли уже обсуждают беспроводные системы 6G, которые станут шестым поколением эволюции.

Когда появилась первая мобильная сеть звонить на мобильные телефоны было довольно сложно. Первые телефоны были объемные и использовались не простыми потребителями.

Когда появилось первое поколение беспроводной связи, оно было основано на аналоговой передаче информации, сеть использовалась исключительно для голосовых вызовов и некоторых других несущественных возможностей.

Сеть второго поколения была основана уже на цифровом способе передачи информации. Скорость передачи данных у 2G была 200 kbps, что в 50 раз быстрее 1G.

3G уже могла полностью поддерживать интернет-приложения.

Когда же появилось 4G скорость передачи увеличилась, возможности увеличились. На сегодняшний день технология 4G используется почти везде. Но уже разработана сеть 5G, а также обсуждается сеть 6G.

На сегодняшний день

Технология 5G

5G спроектирована с помощью различных новых технологий вот одни из преобладающих:

- Программно-определяемая сеть (Software Defined Networking- (SDN)) предлагает возможность централизованно контролировать, интеллектуально маршрутизировать сетевой трафик с использованием программных приложений.
- Сетевая функция виртуализации (Network Function Virtualization - (NFV)) — это концепция, которая используется для упаковки сетевых функций.
- Пограничные вычисления с множественным доступом (Multi-Access Edge Computing (MEC))
- Нарезка сети (network slicing). Она подразумевает то, что разные ресурсы сети “нарезаются” для разных целей.

1. eMBB (Enhanced mobile broadband) — Расширенная мобильная широкополосная связь, обеспечивает высокую скорость передачи данных в широкой зоне покрытия
2. mMTC (Massive machine type communications) – возможность подключения очень большого числа устройств (датчики, счетчики и т. д.)
3. URLLC (Ultra-reliable and low latency communications) – высоконадежное соединения с низкой задержкой передачи данных. [1, С. 2]

5G (пятое поколение мобильной связи) в отличие от 4G (четвертое поколение) имеет более высокую частоту — это означает что у этой технологии более широкая полоса для передачи данных, что в свою очередь значит более высокую скорость передачи данных (широкую полосу легче вывести на широких частотах). Технология умеет работать в двух диапазонах:

- средний (3.5 ГГц)
- миллиметровый (от 24 ГГц и больше)

У технологии 4G диапазон меньше (до 6 ГГц). Поэтому основной прирост скорости передачи данных происходит именно из-за более высоких частот. Но более высоким частотам сложнее проходить через твердые объекты, то есть идет большая потеря сигнала. Поэтому в отличие от 4G, которая распространяет сигнал во все стороны, передатчик 5G формирует отдельный сигнал для каждого приемника, стараясь так чтобы сигнал ни с чем не пересекался,

технология называется beamforming (формирование луча) она вычисляет положение пользователя по отраженным сигналам, в том числе и от поверхностей зданий.

Целесообразно использовать технологию 5G там, где требуется большая пропускная способность это стадионы, вокзалы, торговые и бизнес-центры, в аэропортах и других местах, где чаще всего находится большое количество людей. Проведение такой сети в не общественные места нецелесообразно так как это дорого и нет нужды в высокой пропускной способности.

Перспективы развития

Технология 6G

Шестое поколение (6G) – это новая беспроводная технология, к которой приступают многие ученые и исследователи. Основные обещания 6G заключаются в расширении преимуществ AI и ML в беспроводных сетях. 6G также обеспечит достижения в технических показателях, таких как высокая пропускная способность, улучшенное использование радиочастотных диапазонов и многое другое с использованием методов AI и ML. Одной из основных технологий машинного обучения, рассматриваемой в качестве ключевой технологии для 6G, будет DL из-за его достижений в обучении на основе сценариев. Например, DL может решить, к какой точке доступа подключиться в 6G и какой контроллер ресурсов имеет больше доступных ресурсов. Интересно отметить, что DL успешно используется в задачах классификации и дает хорошие результаты, но роль DL в беспроводных сетях все еще остается неизученной областью.

Модели машинного обучения (ML) – это вычислительные системы, которые используются для изучения отличительных характеристик системы, которые не могут быть представлены математической моделью. Как только модель обучена на заданных данных, она может эффективно принимать решение по неизвестным данным, а также выполнять задачи, основанные на арифметических вычислениях. Это позволит моделировать машинное обучение для мобильности, доступности, управления сетевой связью, а также улучшить и автоматизировать управление производительностью сети.

Глубокое обучение (DL) – это функция AI, которая выявляет закономерности человеческого мышления и использует это понимание для создания шаблонов на основе искусственных нейронных сетей.

- Используя DL, можно создать больше шаблонов, добавив больше слоев к существующей нейронной сети. Это обеспечивает высокую размерность.
- Процесс обучения в DL не сложен
- DL не влияет на вычислительную мощность.
- DL требует большого количества памяти и вычислительных ресурсов для обработки.
- DL требует очень сложных методов оптимизации, что делает его более дорогостоящим и сложным.
- DL требует больших наборов данных, что затрудняет понимание и реализацию. Это также влияет на точность вывода.

Согласно видению Samsung, раннее коммерческое внедрение сетей 6G ожидается в 2028 году, но массовое развёртывание сотовых сетей следующего поколения вряд ли произойдёт раньше 2030 года. [3, С. 7]. Samsung утверждает о пиковой скорости передачи данных в 1000 Gbps при задержке менее 100 мкс. [3, С. 19]. Как же достигается такая скорость? Дело в том, что ученные используют терагерцовый (ТГц) диапазон.

Зачем же нам такие технологии, если существует 5G? Технологии не стоят на месте, общество развивается и соответственно открываются потребности в новых поколениях беспроводной связи, которые будут превосходить по скорости, производительности и многим другим параметрам старые поколения связи. Например, 6G поможет улучшить управление

беспилотными автомобилями, для них беспрерывная связь важнее всего, хотя бы один сбой и могут пострадать пассажиры, автомобили будут знать положение друг друга и заранее перестраивать маршрут чтобы не стоять в пробках. Системы таких автомобилей будут сами строить маршрут, а это не возможно без новых поколений сети, 5G такого не умеет. Или же в нашу жизнь активно входят VR и AR. А это огромное количество данных, которые требуют большой скорости передачи данных, то, что мы используем 4G и 5G не дает нам больших возможностей в этой сфере. Так или иначе 6G это всего лишь усовершенствование 5G.

Вывод

На примере 5G и 6G были рассмотрены перспективы развития технологий и их значение. Каждое новое поколение беспроводной сети будет давать человечеству все больше возможностей. Каждая из них будет отражаться, как и на самом человеке, так и на человечестве в целом. Перед ними будут стаять все больше новых задач, которые нужно будет решить. Общество должно развиваться, человек должен развиваться, а не стоять на месте.

СПИСОК ЛИТЕРАТУРЫ

1. Wijethilaka, Shalitha; Liyanage, Madhusanka. Mobile Edge Computing A key technology towards 5G. IEEE, 22.03.2021 URL: https://researchrepository.ucd.ie/bitstream/10197/12083/2/IEEE_COMST_Slicing___IoT_survey__Final_Submission__%20%281%29.pdf
2. ZHASNIT KAUR, M. ARIF KHAN, MOHSIN IFTIKHAR, MUHAMMAD IMRAN, KAZI EMAD Machine learning techniques for 5G and beyond // IEEE, 13.01.2021 URL: https://ieeexplore.ieee.org/stamp/stamp.jsp
3. The Next Hyper Connected Experience for All // Samsung 14.07.2020 URL: https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf

И.С. Ионов[1], Н.В. Болдырихин[2]

ОБЗОР МЕТОДОВ ФИЛЬТРАЦИИ ВИДЕОПОТОКА

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: фильтрация, шум, видеопоток, подавление шума, методы фильтрации шума.

В статье проанализированы современные методы фильтрации видеопотоков, позволяющие повысить качество видеоизображения. Показаны особенности реализации данных методов, выявлены достоинства и недостатки.

I.S. Ionov[1], N.V. Boldyrikhin[2]

OVERVIEW OF VIDEO STREAM FILTERING METHODS

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Key words: filtering, noise, video stream, noise suppression, noise filtering methods.

The article analyzes modern methods of filtering video streams, which can improve the quality of the video image. The features of the implementation of these methods are shown, the advantages and disadvantages are revealed.

Шумоподавление является одной из самых распространенных проблем при обработке как статичных изображений, так и видеопотока [1-5]. При применении цифровой техники, любой сигнал подвержен цифровому шуму. Данные шумы могут появляться по самым разным причинам, таким как неисправности оборудования, помехи в канале передачи данных и другим. В результате данные, полученные с шумами, искажаются.

Целью данной статьи является обзор методов фильтрации видеопотока.

Поскольку видеопоток представляет собой временную последовательность кадров, то для него, кроме пространственных шумов, встречающихся в изображениях, характерны также шумы во временной координате.

Методы фильтрации видео можно условно разделить на три категории:

- пространственные методы, подразумевающие устранение шума в пределах одного кадра посредством усреднения соседних пикселей;
- временные методы, основанные на усреднении параметров пикселей между несколькими идущими подряд кадрами;
- пространственно – временные методы, комбинированные методы, сочетающие в себе возможности пространственных и временных методов фильтрации.

Одним из самых простых методов устранения шума является *линейное усреднение пикселей* [1], подразумевающее для каждого пикселя анализ определенного количества соседних пикселей в пределах некоторого окна заданного размера. Новое значение пикселя может вычисляться, как среднее арифметическое значение параметров соседей, при этом может задаваться некоторое пороговое значение параметров, по которому отбираются соседние пиксели для усреднения, т.е. в этом случае анализируются не все пиксели окна.

При линейном усреднении так же может быть использована взвешенная сумма. Весовые коэффициенты при этом определяются расстоянием до анализируемого пикселя.

Данный метод также применим и во временной области. В этом случае усреднение происходит не по соседним пикселям, а по соседним кадрам, на которых будет браться один и тот же пиксель.

Другим методом устранения шума является *размытие по Гауссу*. Это способ размытия изображения с помощью функции Гаусса [4]. Данный метод используется в камерах низкого класса для устранения шума, применение которого приводит к необратимой потере деталей на изображении.

Фильтрацию шума также выполняют с помощью методов *математической морфологии* [2].

Использование методов математической морфологии, сужения и расширения, а также их комбинаций закрытия и раскрытия также применяется в устранении шума в изображениях.

Данный метод не подходит для фильтрации фотореалистичных изображений, так как результат получается искусственным.

Медианная фильтрация – метод, похожий на линейное усреднение пикселей, где анализируются соседние по отношению к центральному пиксели [4,5]. При данном виде фильтрации центральный элемент окна заменяется медианой всех пикселей в окне. Медианой является центральный элемент отсортированной последовательности значений яркости пикселей, находящихся в окне. Например, если в окно попали пиксели со значениями яркости 120, 90, 100, 130, 80, отсортировав значения получим: 80, 90, 100, 120, 130. В данном примере медианой будет являться значение 100.

Минусом данного вида фильтрации является то, что он может размывать мелкие детали изображения, если они меньше размеров окна.

Метод главных компонент [4,5], суть которого заключается в следующем: при удалении шума из блока пикселей необходимо представить окрестность этого блока в виде набора точек в многомерном пространстве, применить к нему PCA (principal component analysis) и оставить только первые компоненты преобразования. При этом предполагается, что в первых компонентах содержится основная полезная информация, оставшиеся же компоненты содержат ненужный шум. Применив обратное преобразование после редукции базиса главных компонент, мы получим изображение без шума.

Анизотропная диффузия – при использовании данного метода, яркость каждого пикселя воспринимается как значение температуры [4,5]. Таким образом все изображение представляет собой карту температур. Процесс шумоподавления включает моделирование процесса теплопереноса:

$$I_t = c * \Delta \mathrm{I}$$

где c – коэффициент теплопроводности, ΔI – разность яркостей(«температур») двух пикселей.

Кроме рассмотренных методов, для фильтрации изображений достаточно часто применяются методы на основе вейвлет-преобразования и методы основанные на преобразовании Фурье. Данные методы дают хороший результат, но содержат сложные математические расчеты. По этой причине, методы основанные на вейвлетах и преобразовании Фурье используются для обработки статичных изображений и для видео малопригодны.

Все из рассмотренных алгоритмов фильтрации могут применяться как для изображений, так и для видеопотока. Каждый из приведенных алгоритмов имеет свои особенности и определенную область применения. Для достижения наилучшего результата необходимо выбирать метод фильтрации с учетом входных данных, предполагаемого характера шума, скорости работы и объемов вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. *Тамьяров А.В., Шестов Р.В.* Анализ методов предварительной обработки изображения на основе усредняющих фильтров // Вестник Волжского университета им. В.Н. Татищева. -2011, № 18, с. 109-115.
2. *Тимченко В.И., Хмельницкая К.А., Чернов И.Н.* Применение математической морфологии в оптоэлектронных системах обнаружения предаварийных ситуаций // Сборник: Актуальные проблемы инфотелекоммуникаций в науке и образовании / Под редакцией С. В. Бачевского, составители: А. Г. Владыко, Е. А. Аникевич. -2018. с. 300-304.
3. *Лукин В.В.* Современные методы и проблемы фильтрации многоканальных изображений // DSPA: Вопросы применения цифровой обработки сигналов. -2011, т. 1, № 1, с. 3-6.
4. *Грузман И.С.* Цифровая обработка изображений в информационных системах. - Новосибирск: НГТУ, 2000, 168с.
5. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. -М: Техносфера, 2005. - 1072 с.

А.С. Абрамян

АНАЛИЗ БЕСПРОВОДНОГО ДОСТУПА В ЛОКАЛЬНЫХ СЕТЯХ СВЯЗИ

Южный федеральный университет, г. Ростов-на-Дону, Россия

Ключевые слова: информационные системы, телекоммуникационная сеть, беспроводной доступ, локальные сети, технология доступа.

В статье предлагается анализ технологий построения локальных сетей с беспроводным доступом: сети с базовым набором услуг: Ad-Hoc BSS и инфраструктурная BSS, сети с технологией Wi-Fi**.** Рассмотрены типы волн, которые распространяются в условиях препятствий: Земные, Ионосферные, Прямые, Тропосферные. Показан пример реальной зоны покрытия. Затронута тема развития мобильной телефонии, как беспроводного доступа в сети связи.

A.S. Abramyan

ANALYSIS OF WIRELESS ACCESS IN LOCAL COMMUNICATION NETWORKS

South Federal University, Rostov-on-Don, Russia

Keywords: information systems, telecommunications network, wireless access, local area networks, access technology.

The article offers an analysis of technologies for building local networks with wireless access: networks with a basic set of services: Ad-Hoc BSS and infrastructure BSS, networks with Wi-Fi technology. The types of waves that propagate under obstacles are considered: Terrestrial, Ionospheric, Direct, Tropospheric. An example of a real coverage area is shown. The topic of the development of mobile telephony as a wireless access in a communication network is touched upon.

Локальные сети связи

Сети и оборудование стандарта IEEE 802.11, также известные как Wi-Fi — по имени консорциума Wi-Fi1 Alliance, который занимается вопросам совместимости и сертификации оборудования стандартов IEEE 802.11, — занимают лидирующие позиции в мире беспроводных локальных сетей. Стандарт 802.11 определяет в качестве основного структурного элемента WLAN сеть с базовым набором услуг (Basic Service Set, BSS). BSS представляет собой набор беспроводных сетевых устройств, который разделяет среду передачи и работает с одинаковыми характеристиками доступа к среде: частота и схема модуляции сигналов. Сети BSS не являются традиционными сотами (как в мобильных сетях), их зоны покрытия могут находиться друг от друга на большом расстоянии, а могут частично или полностью перекрываться — стандарт 802.11 даёт здесь свободу проектировщику сети.

Стандарт 802.11 имеет два типа топологий сетей BSS:

- топология на основе связей «точка-точка» (то есть узлы непосредственно взаимодействуют друг с другом), сеть с такой топологией в стандарте 802.11 называют независимой (Independent BSS, IBSS) или сетью «по случаю» (Ad-Hoc BSS). Так как устоявшегося названия для такого типа сети в русскоязычной технической литературе нет, будем называть ее сетью Ad-Hoc;
- централизованная топология с использованием одного центрального узла. Центральный элемент называют базовой станцией, а соответствующие сети — инфраструктурными сетями (Infrastructure BSS, или просто BSS).

Рисунок 1. Сети с базовым набором услуг: Ad-Hoc BSS и инфраструктурная BSS.

Сеть Ad-Hoc BSS представляет собой набор узлов, которые взаимодействуют через общую электромагнитную среду на основе децентрализованного алгоритма доступа. Сеть AdHoc создается самопроизвольным способом на некоторый (обычно небольшой) период времени. Хотя базовая станция в сети Ad-Hoc отсутствует, в каждый момент времени в сети имеется один или несколько узлов, которые берут на себя ведущую роль. Нужно сказать, что сети Ad-Hoc функционируют автономно, в них нет никаких средств для связи с другими сетями.

Пользователи инфраструктурной BSS могут обмениваться информацией только с базовой станцией, а она транзитом обеспечивает взаимодействие между отдельными пользователями, то есть весь трафик в BSS проходит через базовую станцию. Инфраструктурная BSS образует широковещательный домен. [1]

Беспроводный доступ

Возможность передавать информацию без проводов, которые привязывают абонентов к определенной точке, всегда была очень привлекательной. Доказательство тому - мобильная телефония. Первый мобильный телефон был изобретен еще в 1910 году Ларсом Магнусом Эрикссоном (Lars Magnus Ericsson). Этот телефон предназначался для автомобиля и был беспроводным только во время движения. Однако в движении им нельзя было пользоваться — для разговора нужно было остановиться, выйти из автомобиля и с помощью длинных жердей присоединить телефон к придорожным телефонным проводам (рис. 2). Понятно, что определенные неудобства и ограниченная мобильность воспрепятствовали коммерческому успеху этого вида телефонии.

Рисунок 2. Первый мобильный телефон.

Прошло много лет, прежде чем технологии радиодоступа достигли определенной степени развития и в конце 70-х обеспечили производство сравнительно компактных и недорогих радиотелефонов. С этого времени начался бум мобильной телефонии, продолжающийся до настоящего времени.

Впрочем, беспроводная связь не обязательно означает мобильность. Широко используется так называемая фиксированная беспроводная связь, когда взаимодействующие узлы постоянно располагаются в пределах небольшой территории, например в определенном здании. Фиксированная беспроводная связь применяется вместо проводной, когда по какой-то причине невозможно или невыгодно использовать кабельные линии связи. Причины могут быть разными: малонаселенная или труднодоступная местность; здания, имеющие историческую ценность, стены которых непозволительно подвергать испытанию прокладкой кабеля; необходимость организации временной связи, например, при проведении конференции в здании, в котором отсутствует проводной канал, имеющий достаточную для качественного обслуживания пропускную способность, и т. д.

Развитие технологии сотовых телефонных сетей привело к тому, что эти сети стали очень широко использоваться для мобильного доступа к Интернету и, начиная с поколения 4G, стали скорее мобильными компьютерными сетями, чем мобильными телефонными сетями, так как основной услугой в них стал доступ к Интернету, а телефонные услуги стали предоставляться также с использованием протокола IP и Интернета. [2]

Зона покрытия

Зачастую в помещениях зона покрытия имеет сложную форму. Один из примеров — на рис. 3 ниже.

Рисунок 3. Пример реальной зоны покрытия (тепловая карта).

Сложная форма покрытия связана не только с теми препятствиями, которые преодолевает электромагнитное излучение, но и с диаграммой направленности, которую имеет каждая антенна.

Даже у направленной антенны, кроме основного или центрального лепестка, есть еще несколько боковых, существование которых необходимо учитывать при построении беспроводной сети в стесненных условиях. [3]

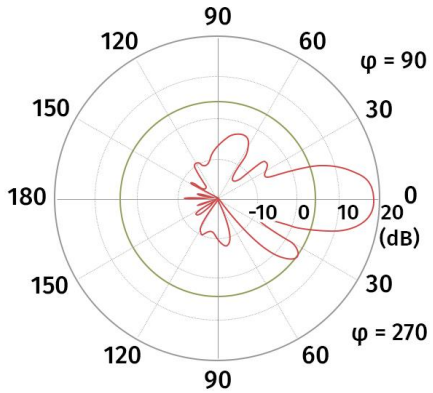


Рисунок 4. Диаграмма направленности антенны с ярко выраженным центральным лепестком.

Передаваемый трафик

В отличие от Ethernet, имеющего кадр только одного типа — кадр данных, в технологии Wi-Fi поддерживаются кадры нескольких типов, причем их структура гораздо сложнее.

Существует три типа кадров Wi-Fi:

- кадры данных;
- кадры слоя управления;
- кадры слоя менеджмента.

Тип кадра, а также его подтип определяются значением соответствующих полей двухбайтового поля «Управление кадром». А пока давайте сосредоточимся на кадрах данных. Одна из особенностей кадра Wi-Fi - наличие в нем четырех полей MAC-адреса. Их назначение зависит от конфигурации сети. Когда две точки доступа взаимодействуют друг с другом напрямую, используются все четыре MAC-адреса: исходная станция, две точки доступа и конечная станция. Когда станция связывается с Интернет-сайтом, используются только три адреса: пользовательская станция, точка доступа и маршрутизатор системы распределения. Кадр Wi-Fi имеет ряд полей, которые помогают узлам связи обнаруживать и восстанавливать поврежденные и потерянные кадры.

Поле данных может содержать до 2312 байт пользовательских данных. Кадры Wi-Fi могут быть фрагментированы, и цель фрагментации здесь отличается от цели той же операции в протоколе IP. Там пакет фрагментируется, когда его размер превышает MTU в промежуточном маршрутизаторе. Здесь фрагментация используется для ускорения передачи данных в условиях высокого уровня помех в радиосети, поскольку чем меньше размер кадра, тем выше вероятность того, что он будет принят без искажений. [4]

Радиофизические характеристики

Характеристики беспроводной линии связи (расстояние между узлами, территория охвата, скорость передачи информации и т. п.) во многом зависят от частоты используемого электромагнитного сигнала. На рис. 5 показаны диапазоны электромагнитного спектра. Обобщая, можно сказать, что они и соответствующие им беспроводные системы передачи информации делятся на четыре группы.

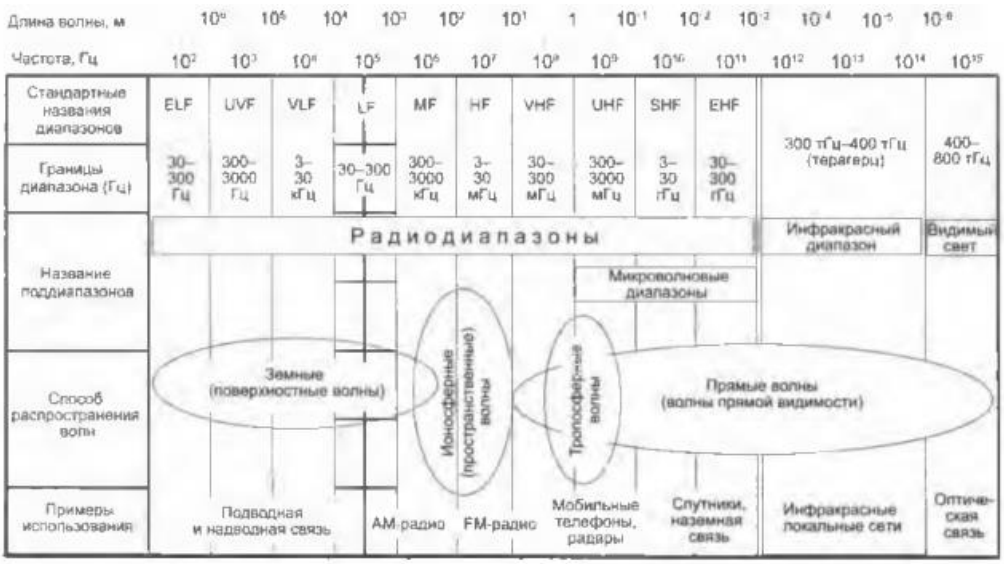


Рисунок 5. Диапазоны электромагнитного спектра.

Диапазон до 300 ГГц имеет общепринятое стандартное название - радиодиапазон. ITU разделил его на несколько поддиапазонов (показано на рисунке), от очень низких частот (ELF) до сверхвысоких частот (EH F). Радиостанции, которые мы привыкли работать в диапазоне от 20 кГц до 300 МГц, и для этих диапазонов существует, хотя и не определено в стандартах, часто используемое название «радиовещание». Сюда входят, в частности, низкоскоростные системы AM и FM1, предназначенные для передачи данных со скоростью от нескольких десятков до сотен килобит в секунду. Примером могут служить радиомодемы, которые соединяют два сегмента ЛВС на скорости 2400, 9600 или 19200 кбит / с.

Некоторые диапазоны от 300 МГц до 3000 ГГц также имеют нестандартное название для микроволновых диапазонов. Микроволновые системы представляют собой широчайший класс систем, объединяющих микроволновые каналы, спутниковые каналы, беспроводные локальные сети и фиксированные системы беспроводного доступа, также называемые системами беспроводного локального шлейфа (WLL).

Инфракрасный находится выше микроволнового диапазона. Микроволновый и инфракрасный диапазоны также широко используются для беспроводной передачи информации. Поскольку инфракрасное излучение не может проникать через стены, системы инфракрасных волн служат для формирования небольших сегментов локальных сетей в одной комнате.

В последние годы видимый свет также начал использоваться для передачи информации (с помощью лазеров). Системы видимого света используются как высокоскоростная альтернатива двухточечным линиям связи с микроволновой печью для доступа на короткие расстояния. [5]

Вспомним несколько важных физических явлений, связанных с распространением волн вообще и электромагнитных волн в частности. На рис. 6 показано, что сигнал, встречая препятствие, может распространяться в соответствии с тремя механизмами: отражением, дифракцией и рассеянием. Когда сигнал встречает препятствие, которое частично прозрачно для данной длины волны и в то же время имеет размеры, намного превышающие длину волны, часть энергии сигнала отражается от этого препятствия. Если сигнал встречает непроницаемое для него препятствие (например, металлическую пластину), намного превышающее длину волны, то возникает дифракция - препятствие как бы огибает сигнал, что позволяет принимать его даже без помех. находясь в зоне прямой видимости. И, наконец, при встрече с препятствием, размер которого соизмерим с длиной волны, сигнал рассеивается, распространяясь под разными углами. [6]

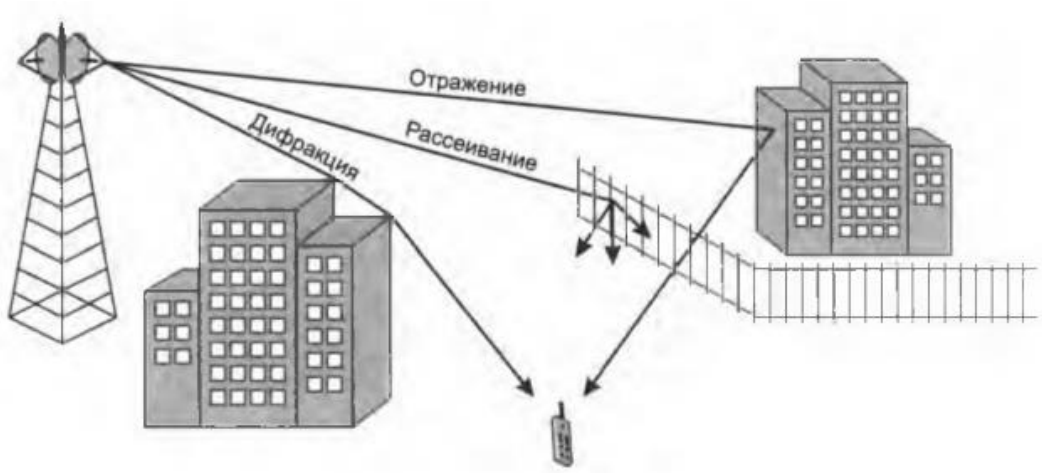


Рисунок 6. Отражение, дифракция и рассеивание электромагнитной волны.

Земные или **поверхностные** волны распространяются по поверхности земли. Следуя более или менее по местности, они могут путешествовать на большие расстояния, до нескольких сотен километров, далеко за линией видимого горизонта.

Такой способ распространения волн характерен для электромагнитного излучения низкой частоты - до 2 МГц. Электромагнитные волны этой частоты рассеиваются в атмосфере таким образом, что не проникают в верхние слои атмосферы. Самый известный пример земной волны - длинноволновый радиосигнал АМ. Основная причина, по которой волны следуют за земной поверхностью, — это дифракция. В этом случае непреодолимое препятствие, намного превышающее длину волны, представляет собой выпуклость земли. Способность волны огибать препятствие зависит от отношения длины волны к размеру препятствия; чем меньше это отношение, тем слабее дифракция. Отсюда ясно, что для электромагнитных сигналов высокой частоты эффектом дифракции можно пренебречь.

Ионосферные (пространственные) волны характерны для сигналов средних и высоких частот от 2 до 30 МГц. Сигналы, излучаемые наземной антенной, отражаются ионосферой (менее плотными ионизированными верхними слоями атмосферы) на землю и, следовательно, могут распространяться далеко за пределы видимого горизонта на расстояния даже большие, чем поверхностные волны. При достаточной мощности передатчика радиоволны в этих диапазонах из-за многократных отражений от ионосферы могут даже обогнуть земной шар. Ионосферные волны широко используются в радиовещании и особенно в международном радиовещании, например, такими компаниями, как BBC (BBC Radio World Service).

Прямые волны, или **волны прямой видимости**, как следует из их названия, распространяются только по прямой линии от передатчика к приемнику. Причем последний может располагаться как на земле, так и в космосе. Такой тип распространения волн характерен для электромагнитных сигналов с частотой выше 30 МГц - они не могут ни отражаться от ионосферы, ни огибать выступы Земли. Выше 4 ГГц их поджидает неприятность: они начинают поглощаться водой, а значит, не только дождь, но и туман могут вызвать резкое ухудшение качества передачи СВЧ-систем. Инфракрасный и видимый свет могут передаваться только на линии прямой видимости, так как они не проходят сквозь стены.

Тропосферные волны могут генерироваться излучением очень высокой и сверхвысокой частоты (30 МГц - 3 ГГц). Как упоминалось выше, электромагнитные сигналы из этого диапазона не могут быть отражены ионосферой. Однако они могут распространяться за счет преломления и рассеяния на неоднородностях в тропосфере - слое атмосферы, ближайшем к Земле. Неоднородности тропосферы — это области пространства, где воздух в определенные моменты времени имеет температуру, давление и влажность, которые отличаются от средних значений для окружающей среды. Тропосферные волны позволяют передавать сигнал, пусть и

очень слабый, на расстояние до 1000 км. Чем выше несущая частота, тем выше возможная скорость передачи данных. Преобладает потребность в высокоскоростной передаче информации, поэтому все современные системы беспроводной передачи информации работают в высокочастотных диапазонах, начиная с 800 МГц, несмотря на преимущества, которые сулят низкочастотные диапазоны из-за распространения сигнала вдоль земной поверхности или отражения от ионосферы. [7]

В заключении, в статье были рассмотрены такие вещи, как: сети с базовым набором услуг: Ad-Hoc BSS и инфраструктурная BSS, сеть с технологией Wi-Fi на примере помещения со сложной зоной покрытия. Рассмотрен тип передаваемого трафика в сети Wi-Fi, диапазон частот и длин волны, а также проведён анализ типов передаваемых электромагнитных волн и их поведения (отражение, дифракция и рассеивание).

СПИСОК ЛИТЕРАТУРЫ

1. Олифер. Компьютерные сети связи.
2. https://habr.com/ru/article/456918/
3. А. Ю. Аганов, А. В. Кузичкин, В. В. Попов, А. А. Таранов АО «Научно исследовательский институт телевидения»
4. Сборник трудов МТСИ
5. С. В. Кулешов Потенциальные свойства цифровых каналов передачи данных
6. А.А. Карпук Оптимизация присвоения частот радиолиниям
7. Проблемы инфокоммуникаций Научный журнал А.О. Зенкевич Л.Л. Гладков О.К. Барановский

Б.П. Борисов, А.А. Соловьёв

АНАЛИЗ ВОЗМОЖНОСТЕЙ И ГРАНИЦ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ FTTX И PON

Южный федеральный университет, г. Ростов-на-Дону, Россия

Ключевые слова: телекоммуникационная сеть, подключение абонентов, технология доступа, интернет, оптическое волокно, связь, кабельное подключение, пассивная оптическая сеть.

В статье предлагается сравнительный анализ наиболее популярных технологий построения телекоммуникационных сетей: активная оптическая сеть (AON), пассивная оптическая сеть (PON) и оптоволокно до точки X (Fiber To The x). Исследованы и проанализированы потенциальные возможности использования той или иной технологии, их конкретные вариации. В статье показаны этапы развития телекоммуникационных сетей посредством представления информации о работе и используемых компонентах для разнообразных вариантов построения сетей.

B.P. Borisov, A.A. Solovev

ANALYSIS OF POSSIBILITIES AND LIMITS OF USING OF FTTX AND PON TECHNOLOGIES

South Federal University, Rostov-on-Don, Russia

Keywords: telecommunication network, subscriber connection, access technology, Internet, optical fiber, communication, cable connection, passive optical network.

The article offers a comparative analysis of the most popular technologies for building telecommunication networks: active Optical Network (AON), passive optical network (PON) and fiber to point X (Fiber to x). The potential possibilities of using one or another technology, their specific variations are investigated and analyzed. The article shows the stages of development of telecommunication networks by presenting information about the operation and components used for a variety of options for building networks.

FTTx, аббревиатура от Fiber To The x — общий термин, обозначающий широкополосную телекоммуникационную сеть, сеть передачи данных, в которой используется оптоволоконный кабель [1].

Технология FTTx имеет множество вариаций (названия, которым даются путём замены буквы “x” на какую-либо другую). Ниже перечислена большая часть из них:

- FTTN (Fiber to the Node) — волокно до сетевого узла. Волокно протягивается вплоть до уличного узла коммутации, городская или районная станция или узел связи, находящимся в основном на расстоянии в 1-2 километра до конечного потребителя, с дальнейшей прокладкой меди от шкафа до абонентского здания (как правило по технологии xDSL [2]). В качестве последней мили как правило выступает коаксиальный кабель или витая пара, что удешевляет этот тип технологии, в сравнении с FTTP, более дешёвым, при практически идентичных параметрах (скорости, качества соединения, вероятности ошибки и т. д.), на которой реализованы высокоскоростные протоколы передачи данных, по типу IP, TCP/IP, UDP, FTP [3];
- FTTC (Fiber to the Curb) — волокно до микрорайона (под “микрорайоном” может подразумевать район города, квартал или группа домов). FTTC имеет много общего с FTTN, но при рассматриваемом типе FTTx распределительный шкаф (РШ) располагается ближе к клиентским помещениям, не далее чем 300 метров. Непосредственно до домов-абонентов выполняется посредством медных кабелей, схожих с технологиями Ethernet или IEEE 1901. FTTC применяется при необходимости строительства подстанций связи, именуемых выносами [4]. Для последней мили могут быть использованы коаксиалы, связь по опоре ЛЭП или кабели витой пары. Один из протоколов управления – IEEE P1905;
- FTTDP (Fiber to the Distribution Point) — волокно до точки распределения, отличающиеся от вышеописанных технологий тем, что распределительная коробка, точка распределения, находится в нескольких метров от конечных потребителей. Близость точки распределения позволяет обеспечить абонентам скорость порядка гигабайта [5];
- FTTP (Fiber to the Premises) – волокно до помещения, что является обобщением технологий FTTB и FTTH;
- FTTB (Fiber to the Building) – волокно до здания. Оптический кабель прокладывается непосредственно до здания, до технического этажа или подвального помещения, где и располагается точка распределения – это

коммутатор доступа (КД). Дальнейшее подключение до конкретных пользователей осуществляется по технологиям, как и в случае с FTTN и FTTC (Ethernet, xDSL и т. п.). В основном используется в тех случаях, когда стоит необходимость построения сети на базе Ethernet. Обладает высоким показателем ширины полосы пропускания (в сравнении с FTTC) при более низких затратах на строительство (в сравнении с FTTH), как следствие, преобладает при строительстве новых многоквартирных домов;

– FTTH (Fiber to the Home) – волокно до квартиры или частного дома. Волокно тянется до границы жилого помещения, до медиа шлюза (МШ), располагающегося в пределах жилья, а далее услуги предоставляются с использованием сетевого протокола канального уровня PPPoE [6]. Как и отмечалось выше, стоимость построения сети по такой технологии выше, чем при использовании технологии FTTB, почему и востребована эта технология только в случаях строительства малоэтажных и частных домов. При этом FTTH обладает наивысшим уровнем полосы пропускания, дешевле в обслуживании за счёт меньших физических размеров технических помещений и, следовательно, в меньшем объёме потребляемого электричества и, наконец, является наиболее стандартизированной именно эта технология [7].

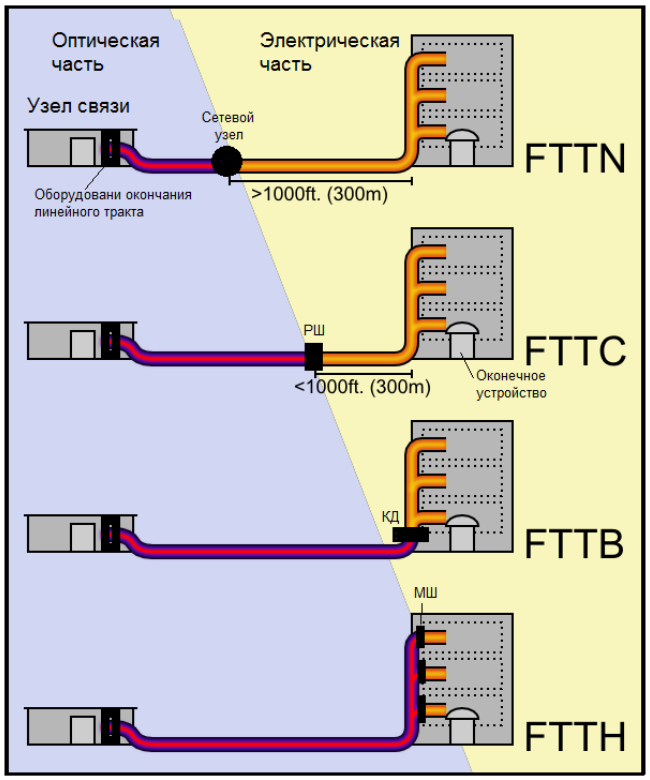


Рисунок 1. Визуальные отличия типов технологии FTTx

PON (Passive Optical Network) – пассивная оптическая сеть (рисунок 2), распределительная сеть которой базируется на древовидной волоконно-кабельной структуре. Кабели проводятся непосредственно до здания, будь то офис или жилой дом, подключаясь на узлах к пассивным оптическим разветвителям (так называемые сплиттеры). Древовидная архитектура PON позволяет эффективно наращивать пропускную способность и узлы сети в зависимости от потребностей абонентов конкретно в данный момент, либо же от потенциальных будущих потребностей нынешних абонентов или будущих пользователей [8].

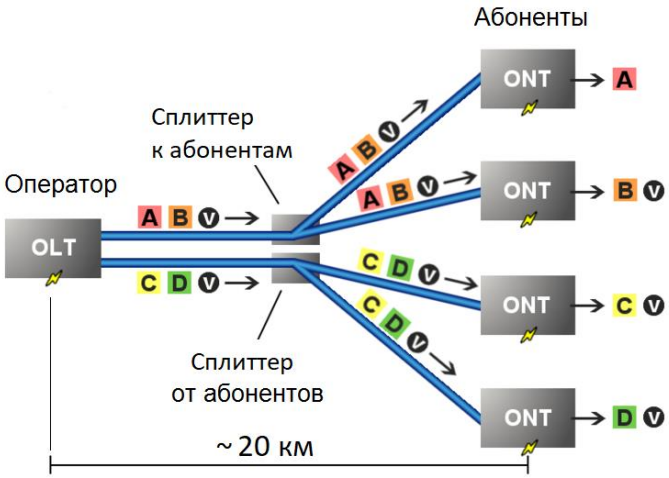


Рисунок 2. Пример работы PON

AON (Active Optical Network) – активная оптическая сеть (рисунок 3) является двухточечной структурой, pear to pear, иначе говоря. В активной оптической сети каждый потребитель имеет свою оптоволоконную линию, выделенную персонально для него, оканчивающуюся концентратором.

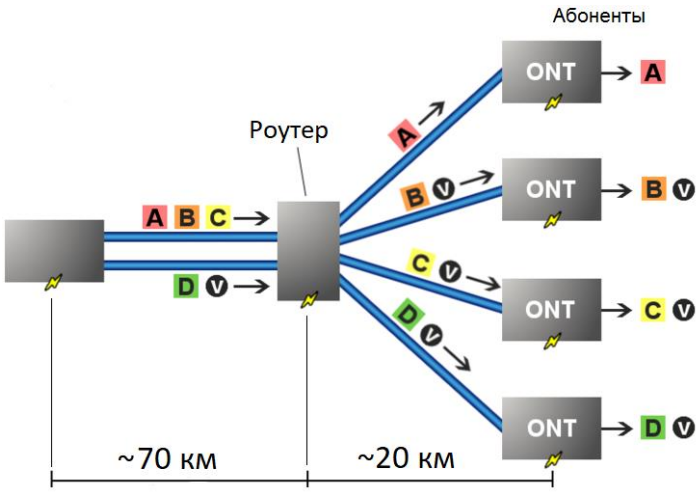


Рисунок 3. Пример работы AON

Принципиальное отличие AON от PON заключается в том, что активная сеть строится на передаче оптического сигнала при помощи такого электрооборудования, как коммутатор, маршрутизатор и медиаконвертер. В основном при использовании этой технологии оптический сигнал преобразуется в электрический и обратно и уже снова полученный оптический сигнал направляется именно к тому пользователю, которому он и был предназначен. Эти сигналы избегают коллизий, так как электрооборудование обладает буферизацией.

На рисунках буквой “V” обозначены видео-файлы, предназначенные для многих или вообще всех абонентов. Буквами “A”, “B”, “C” и “D” обозначаются файлы, предназначенные для конкретных пользователей.

Сети AON во многом схожи с сетями типа Ethernet, используемые в образовательных учреждениях, офисах и различных подобных заведениях. С тем отличием, что Ethernet проводится в пределах самого заведения для создания локальной сети между сотрудниками/учащимися, а активная оптика предназначена для подключения строений к центральным зданиям операторов связи. при обслуживании распределительным шкафом

вплоть до 1000 абонентов максимум (но чаще берут около половины от этого количества, 400-600 абонентов).

Отличия PON от AON заключаются в том, что PON работает по принципу “точка – много точек”, от одного оптического канала сигнал разделяется на “порции” сети при помощи сплиттера, разветвителя. После “порции” информации распределяются по абонентским каналам, тем самым передавая индивидуальные для каждого потребителя данные. При этом для сети с пассивной технологии не применяются никакие активные элементы (например, усилители, повторители и т. д.). В системе PON однополосное соединение по оптоволокну с терминалом оптической линии центрального офиса, именуемого OLT, подключается к оптическим сетевым терминалам либо же сетевым оптическим блоком (ONT и ONU соответственно). Сплиттер же может устанавливаться как в помещении заказчика, так и за его пределами.

Ключевые отличия пассивной оптической сети от активной оптической сети заключаются в использовании сплиттера, оборудования, не нуждающегося в стороннем питании, так как он представляет собой многозеркальную конструкцию, где под нужным углом отражается часть сигнала, предназначенная для конкретного пользователя. Но, как следствие из конструкции, сложнее выявить сбои в передаче информации (полоса пропускания не персонализирована), требуется тонкая настройка, а также остаётся относительно великий риск того, что одна информация может накладываться на другую.

Но PON-технология куда дешевле и проще в корректировке, нежели AON, при использовании которой остаётся риск выхода из строя электрооборудования, а также стоимость обслуживания и использования гораздо выше, так как оборудование требует стороннего питания (которое так же подвержено некоторым сбоям).

FTTx и PON отличаются примерно в схожей манере: для FTTx требуется питание между конечным потребителем и оператором связи, простота в обслуживании, не требующая особенно глубоких знаний в тонкостях передачи данных и работы сетей, абоненты могут располагаться на значительном удалении друг от друга (высокая скорость передачи данных по оптоволокну), практически отсутствуют неиспользуемые волокна и области кабеля, простота в исправлении неполадок, возможность совмещения интернета и аналогового телевидения [9]. Важно отметить, что вышеописанные сравнения актуальны в том случае, когда производится сравнение PON и FTTx.

Вывод: FTTx на данный момент является уже не передовым этапом развития технологий широкополосных телекоммуникационных сетей, так как по прошествии лет выявились проблемы в обслуживании, перебоях и т. п. В то же время PON и AON, как и практически любая технология, базирующаяся на оптоволокне, является следующем уровнем развития инфокоммуникационных сетей и обладают рядом преимуществ перед слегка устаревшими FTTx: скорость передачи данных, упрощённое обслуживание, удешевлённое устройство самой сети. Но при этом в некоторых случаях могут возникать сложности конкретно в конструировании волновода, так как даже совсем незначительные дефекты могут привести к ухудшенной работе сети (уменьшенная скорость, неполная “передача” информации, возникновение коллизий). Касательно границ применения имеем следующее. Технология AON менее глобальная, если сравнивать с технологией PON, и является наиболее подходящим вариантом для пользования небольшой группой лиц. Пассивная оптическая сеть, в свою очередь, лучше подходит для длинных дистанций, когда абоненты располагаются на значительном удалении друг от друга.

СПИСОК ЛИТЕРАТУРЫ

1. Fiber to the x [Электронный ресурс] // Режим доступа: https://ru.Wikipedia.org/wiki/Fiber_to_the_x
2. Сети FTTx [Электронный ресурс] // Режим доступа: http://www.ftth.ru/networks-fttx/

3. Протоколы передачи данных: что это, какие бывают и в чём разница? [Электронный ресурс] // Режим доступа: https://tproger.ru/explain/protokoly-peredachi-dannyh-chto-jeto-kakie-byvajut-i-v-chjom-razlichija/
4. Что такое FTTx технология доступа (FTTH, FTTB, FTTC) [Электронный ресурс] // Режим доступа: https://192-168-1-1.ru/FTTx-tehnologiya-dostupa/
5. Active Ethernet grown in PON's shadow [Электронный ресурс] // Режим доступа: http://nxtcommnews.com/ethernet/news08/active-ethernet-pon
6. Could ultrafast broadband over copper speed the rollout of gigabit internet? [Электронный ресурс] // Режим доступа: https://www.techrepublic.com/blog/european-technology/could-ultrafast-broadband-over-copper-speed-the-rollout-of-gigabit-internet/
7. FTTX: ГДЕ ОПТИМАЛЬНОЕ МЕСТО ДЛЯ "X" [Электронный ресурс] // Режим доступа: http://www.muvicom.ru/publications/FTTx.html
8. PON [Электронный ресурс] // Режим доступа: https://ru.wikipedia.org/wiki/PON
9. Подключение по технологии PON и технологии Fttx. В чем разница? И что лучше? [Электронный ресурс] // Режим Доступа: https://globalscience.ru/news/sovteh/8148-podklyuchenie-po-tehnologii-pon-i-tehnologii-fttx-v-chem-raznica-i-chto-luchshe.html

В.А. Головской А.А. Мозоль

ОЦЕНИВАНИЕ ПОГРЕШНОСТИ ПРОГНОЗИРОВАНИЯ РАДИАЛЬНОЙ ЗОНЫ ПОКРЫТИЯ БАЗОВОЙ СТАНЦИИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: распространение радиоволн, система подвижной радиосвязи, зона покрытия, модель Окумура-Хата, ослабление мощности.

В статье рассмотрено влияние случайного характера параметров системы подвижной радиосвязи и условий распространения радиоволн на погрешность прогнозирования радиальной зоны покрытия базовой станции для модели Окумура-Хата, а также представлен разработанный аналитический аппарат для численного оценивания указанного влияния. Приведены результаты моделирования.

V.A. Golovskoy, A.A. Mozol`

THE ESTIMATION OF THE ERROR OF FORECASTING THE RADIAL COVERAGE ZONE OF THE BASE STATION

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

Keywords: propagation, mobile radio network, coverage zone, model Okumura-Hata, path loss.

The article considers the influence of the random nature of the parameters of the mobile radio communication system and the conditions of radio wave propagation on the error in predicting the radial coverage area of the base station for the Okumura-Hata model, and also presents the developed analytical apparatus for the numerical estimation of this influence. The simulation results are presented.

ВВЕДЕНИЕ

Запросы частных пользователей систем подвижной радиосвязи (СПР), бизнеса и государственных органов на высокое качество передачи данных в СПР формируют облик будущих систем и средств передачи данных. Актуальной тенденцией развития телекоммуникаций является внедрение новых технологий и увеличение загруженности радиочастотного спектра [1]. Осложняющим фактором для внедрения новых технологий является «бронирование» некоторых диапазонов частот для нужд федеральных органов исполнительной власти, обеспечивающих безопасность и оборону государства. Вследствие этого, исследования различных аспектов повышения эффективности функционирования СПР являются перспективными и важными для развития общества и государства. Одним из направлений таких исследований является развитие теории частотно-территориального планирования СПР, а конкретнее – анализа точностных характеристик моделей распространения радиоволн (РРВ) и их корректировки [2-6]. С учетом того, что модели используются для расчета зон покрытия базовых станций (БС), входящих в состав СПР, данное направление представляется актуальным [2, 3, 7-9]. В работах [5, 10] предприняты попытки анализа и коррекции известных моделей РРВ, а в работе [6] предложен подход к оцениванию дисперсии ослабления радиосигнала для различных моделей. Однако, с точки зрения практики, наибольший интерес представляют значения радиусов зон покрытия БС [2-4, 8, 9].

Зона обслуживания СПР представляет собой объединение радиальных зон покрытия БС, являющихся элементами этой системы. Для СПР, использующих фиксированные БС, прогнозирование зон покрытия успешно осуществляется с использованием специализированных программных приложений, реализующих статистические или детерминированные методы расчета. При этом в работах [8, 11] было показано, что СПР функционируют в условиях динамично меняющейся радиообстановки.

Для одновременной реализации противоречивых требований по обеспечению электромагнитной совместимости с другими системами и максимизации зоны покрытия необходимо предусмотреть возможность выбора и корректировки модели РРВ.

Как правило, величину ослабления мощности сигнала в радиоканале определяют основные параметры, значения которых подвержены девиации в процессе эксплуатации СПР. Известен [12] статистический аппарат расчета ослабления мощности радиосигнала, заключающийся в эмпирическом описании аналитической зависимости ослабления мощности радиосигнала от значений таких параметров как несущая частота, расстояние между БС и мобильной станцией (МС), высоты антенн БС и МС, а также степень застройки местности. Таким образом, реальные условия эксплуатации СПР позволяют рассматривать значения указанных параметров как случайные величины, а ослабление мощности радиосигнала – как функцию случайных величин. Применительно к СПР такое допущение оправдано по следующим причинам [6]: во-первых, пространственное местоположение МС относительно БС, является переменным в пределах зоны их функционирования; во-вторых, в современных и перспективных системах, использующих наборы частот, рабочая частота одной БС (МС) может принимать конечное число фиксированных значений из некоторого известного множества; в-третьих, степень застройки местности в пределах зоны покрытия БС может быть различной и меняться с течением времени.

Таким образом, изменение во времени основных параметров модели РРВ, а также наличие неучтенных факторов обуславливает погрешность прогнозирования зоны обслуживания БС. Величина этой погрешности зависит от погрешности определения радиальной зоны покрытия БС. Построение модели, позволяющей оценивать величину погрешности прогнозирования радиальной зоны покрытия БС от значений ее случайных параметров, представляет теоретический интерес и практическую ценность.

Ввиду изложенного цель настоящей работы состоит в разработке аналитического аппарата для оценивания влияния параметров СПР и условий РРВ на погрешность прогнозирования радиальной зоны покрытия БС.

ПОСТАНОВКА ЗАДАЧИ

Рассмотрим радиоканал «uplink» от МС к БС. Мощность сигнала МС на входе радиоприемника БС может быть представлена следующей функцией:

$$P_r\left(\vec{\mathbf{x}}'\right) \approx P_t + G - L\left(\vec{\mathbf{x}}'\right), \quad (1)$$

где $\vec{\mathbf{x}}'$ – вектор аргументов функции, заданный неточно; $\vec{\mathbf{x}}' = \vec{\mathbf{x}} + \Delta\vec{\mathbf{x}}$; $\vec{\mathbf{x}} = \left[x_j,\ j = \overline{1,3} \right]^T = \left[f, h_r, h_t \right]^T$ – вектор параметров модели (1); $\Delta\vec{\mathbf{x}} = \left[\Delta f, \Delta h_r, \Delta h_t \right]^T$ – вектор погрешностей задания (девиаций) параметров модели (1); $M\left[\Delta\vec{\mathbf{x}}\right] = \vec{\mathbf{0}}$; $D\left[\Delta\vec{\mathbf{x}}\right] = \left[\sigma_j^2,\ j = \overline{1,3} \right]^T$; P_t – полная мощность, подводимая к антенне МС; $G = G_t + G_r$; G_t – коэффициент усиления передающей антенны; G_r – коэффициент усиления приемной антенны; $L\left(\vec{\mathbf{x}}'\right)$ – затухание радиосигнала при распространении, определяемое отношением передаваемой мощности сигнала к принимаемой. Величины P_r, P_t в выражении (1) имеют размерность дБ, а величины G, L – дБмВт.

Согласно [13], для функционирующих в городах СПР модель Окумура-Хата рассматривается как референцная, что позволяет сделать вывод об удовлетворяющих свойствах этой модели. Для указанной модели аналитическая зависимость ослабления величины L мощности радиосигнала МС от значений основных параметров имеет следующий вид [12]:

$$L\left(f, h_r, h_t, d\right) = 69{,}55 + 26{,}16\lg\left(f\right) - 13{,}82\lg\left(h_r\right) - A\left(h_t\right) + \left(44{,}9 - 6{,}55\lg\left(h_t\right)\right)\lg\left(d\right), \quad (2)$$

где $f \in \left[200, 1500\right]$ – несущая частота, МГц; h_r – высота подъема антенны БС, м; h_t – высота подъема антенны МС, м; d – расстояние между БС и МС, км; $A\left(h_t\right) = \left(3{,}2\left[\lg\left(11{,}75\, h_t\right)\right]^2 - 4{,}97\right)$ – поправочный коэффициент для высоты антенны МС для городских условий.

Требуется для модели Окумура-Хата (2) получить аналитическую зависимость, позволяющую численно оценить влияние девиации основных параметров модели (1) на погрешность прогнозирования радиальной зоны покрытия БС.

ОСНОВНЫЕ АНАЛИТИЧЕСКИЕ СООТНОШЕНИЯ

Зона покрытия БС определяется геометрическим местом точек, в которых выполняется условие [2, 5]

$$P_r \geq P_{r\min}, \quad (3)$$

где P_r – мощность сигнала на входе радиоприемника БС; $P_{r\min}$ – чувствительность радиоприемника БС. Учитывая, что для границы зоны покрытия выполняется условие $P_r = P_{r\min}$, преобразуем выражение (1) к виду

$$L\left(\vec{\mathbf{x}}'\right) \approx P_t - P_r\left(\vec{\mathbf{x}}'\right) + G. \quad (4)$$

Полагая для простоты вычислений, что $G_t, G_r = const$, выразим из (4) параметр d с учетом (3) и (2):

$$d = 10^{\Theta}, \quad (5)$$

где $\Theta = \left(\Psi - 26{,}16\lg f + 13{,}82\lg h_r + \left(3{,}2\lg h_t + 6{,}4\lg\left(11{,}75\right)\right)\lg h_t\right)\left(44{,}9 - 6{,}55\lg h_t\right)^{-1}$;

$$\Psi = P_t - P_r\left(\vec{\mathbf{x}}'\right) + G - 70,86.$$

Для оценки влияния погрешностей $\Delta\vec{\mathbf{x}} = \left[\Delta x_j,\ j = \overline{1,3}\right]^T$ задания (девиации) основных параметров $\vec{\mathbf{x}} = \left[x_j,\ j = \overline{1,3}\right]^T$ модели (1) на погрешность определения радиальной зоны покрытия d БС в городских условиях РРВ, по аналогии с [6], будем полагать, что параметры $\vec{\mathbf{x}}$ и $\Delta\vec{\mathbf{x}}_i$ представляют собой нормально распределенные случайные величины с соответствующими значениями математических ожиданий $M\left[\vec{\mathbf{x}}\right] = \left[M\left[f\right], M\left[h_r\right], M\left[h_t\right]\right]^T$ и дисперсий $\sigma_j^2,\ j = \overline{1,3}$. Тогда, полагая $d = 10^{\Theta}$ функцией случайных аргументов $\vec{\mathbf{x}}'$, применим к выражению (5) широко используемый на практике принцип линеаризации функции в окрестности ее математического ожидания:

$$\sigma_d^2 \approx \sum_{j=1}^{3}\sigma_j^2\left(\partial d/\partial x_j\right)_{\left|M\left[X_j\right]\right.}^2 + 2\sum_{j<k}\left(\partial d/\partial x_j\right)_{\left|M\left[X_j\right]\right.}\left(\partial d/\partial x_k\right)_{\left|M\left[X_k\right]\right.} r_{jk}\sigma_j\sigma_k, \quad (6)$$

где r_{jk} – коэффициент корреляции случайных величин X_j и X_k, σ_j – среднеквадратическое отклонение (СКО) случайной величины X_j.

В частном случае, когда $r_{jk} = 0$, выражение (6) примет вид $\sigma_d^2 \approx \sum_{j=1}^{3}\sigma_j^2\left(\partial d/\partial x_j\right)_{\left|M\left[X_j\right]\right.}^2$.

Применительно к (5) выражение для дисперсии σ_d^2 примет следующий вид:

$$\sigma_d^2 \approx \left(\partial d/\partial f\right)^2\sigma_f^2 + \left(\partial d/\partial h_r\right)^2\sigma_{h_r}^2 + \left(\partial d/\partial h_t\right)^2\sigma_{h_t}^2, \quad (7)$$

где $\partial d/\partial f = -10^{\Theta} f^{-1} 26,24\left(44,9 - 6,55\lg h_t\right)^{-1}$;

$\partial d/\partial h_r = 10^{\Theta} 13,67 h_r^{-1}\left(44,9 - 6,55\lg h_t\right)^{-1}$; $\partial d/\partial h_t = 10^{\Theta}\left(\partial\Theta/\partial h_t\right)\ln\left(10\right)$;

$\partial\Theta/\partial h_t = 2,75\left(1,07 + \Psi - 22,16\lg f + 13,82\lg h_r + \left(3,2\lg h_t + 8\right)\lg h_t\right) h_t^{-1}\left(44,9 - 6,55\lg h_t\right)^{-2}$.

Выражение (7) позволяет исследовать влияние случайного характера параметров f, h_r, h_t на дисперсию σ_d^2 оценки радиальной зоны покрытия БС.

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для численной оценки влияния случайного характера высоты антенны h_t на величину погрешности прогнозирования радиальной зоны покрытия БС рассмотрим, по аналогии с [6], некоторую СПР, содержащую в своем составе технические средства со следующими характеристиками: $P_t = 37$ дБмВт, $P_r = -119$ дБмВт, $G = 10,15$ дБ, набор рабочих частот БС $f \in \left[150, 550, 950\right]$ МГц. Величины высот подъема антенн приняты $h_r = 40$ м и $h_t = 1,5$ м, при этом СКО $\sigma_{h_t} \in \left[0, 0,05, \ldots, 0,5\right]$ м и $M\left[f\right] = \left\{150, 550, 950\right\}$ МГц, $M\left[h_r\right] = 40$ м, $M\left[h_t\right] = 1,5$ м. В соответствии с целью настоящей статьи ограничимся анализом влияния σ_{h_t} на оценивание границы радиальной зоны покрытия, и зафиксируем для моделирования величины $\sigma_f = 10^{-4}$ МГц $\sigma_{h_r} = 0,4$ м.

С учетом (5) и (7) получены оценки минимальных и максимальных значений радиусов зон покрытия БС на основании выражения $R_{\min(\max)} = 10^{\Theta} \pm 3\sigma_d$.

На рисунке 1 показаны значения абсолютных погрешностей $\Delta R(\sigma_{h_t})$ оценок радиусов зон покрытия БС $\Delta R = \left| R_{\max} - d \right|$.

На рисунке 2 приведены значения относительных погрешностей δR оценок радиусов зон покрытия БС, полученные согласно выражению $\delta R = \left(\left| R_{\max} - d \right| / d \right) 100\%$.

Результаты моделирования позволяют увидеть значительные величины ошибок оценивания, учет которых необходим при планировании СПР.

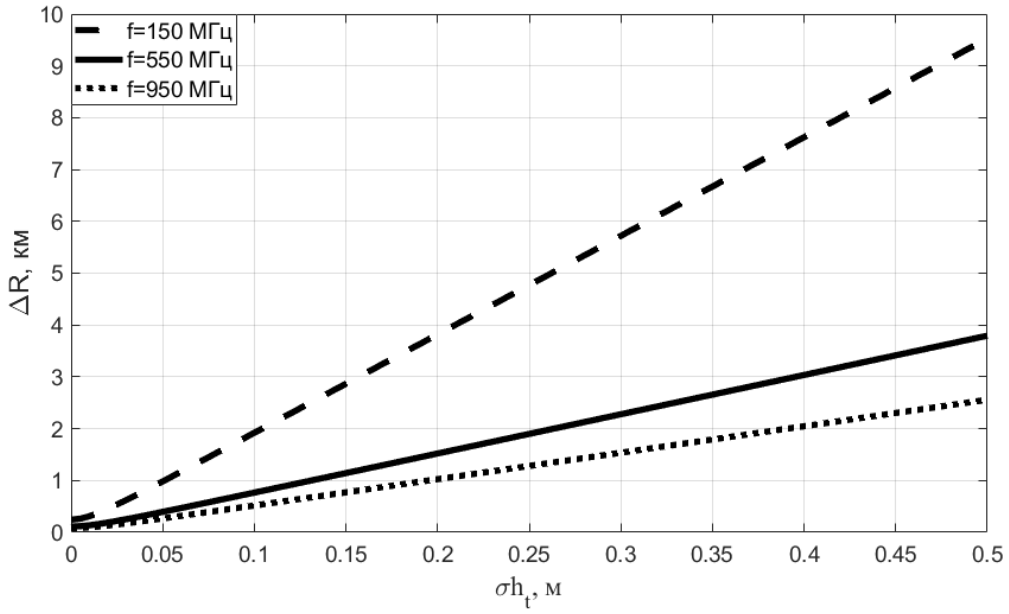


Рисунок 1. Зависимость абсолютной погрешности ΔR от σ_{h_t}

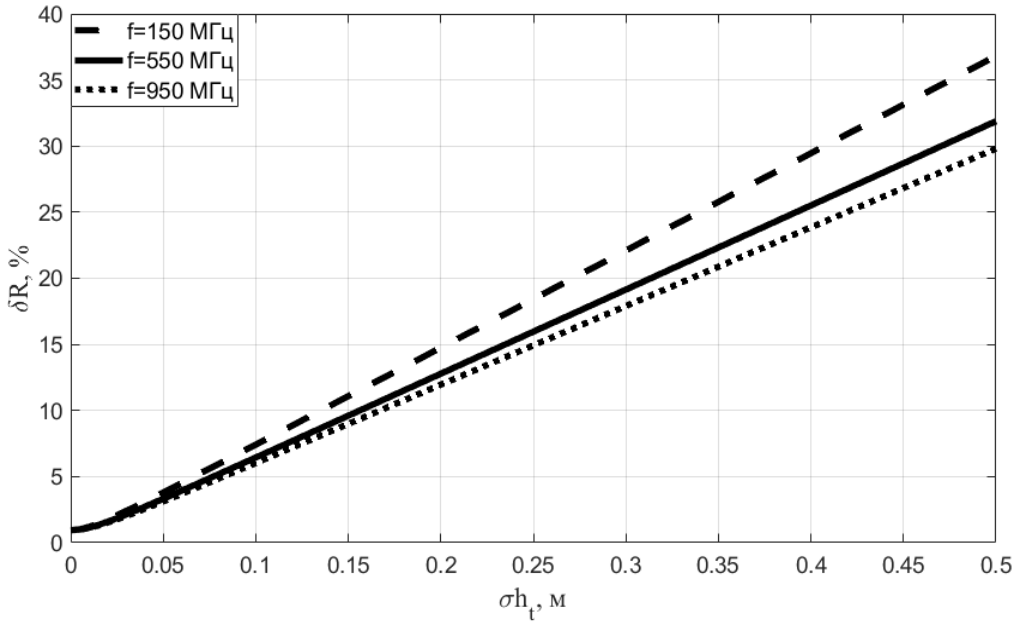


Рисунок 2. Зависимость относительной погрешности δR от σ_{h_t}

ЗАКЛЮЧЕНИЕ

В статье предложен аналитический аппарат для оценивания влияния случайного характера параметров СПР и условий РРВ на погрешность прогнозирования радиальной зоны покрытия БС. Дальнейшее развитие результатов настоящей работы видится в обосновании принятых допущений и разработке метода, позволяющего оценивать погрешности прогнозных значений радиальных зон покрытия для различных моделей РРВ и корректировать модели.

СПИСОК ЛИТЕРАТУРЫ

1. Reaching consensus in Egypt for future digital communications / ITU News MAGAZINE. 06/2019. p. 11-12. Geneva: ITU, 2019. [Электронный ресурс]. – Режим доступа: https://www.itu.int/ru/myitu/Publications/2020/03/24/09/44/ITU-News-Magazine-No-6-2019 (дата обращения: 23.10.2021).
2. *Бегишев В.О., Сопин Э.С., Молчанов Д.А., Самуйлов А.К., Гайдамака Ю.В., Самуйлов К.Е.* Оценка эффективности механизма резервирования полосы пропускания для технологии mmWave в сетях связи пятого поколения. // Информационно-управляющие системы. – 2019, № 5, с. 51-63. doi:10.31799/1684-8853-2019-5-51-63.
3. *Дворников С.В., Балыков А.А., Котов А.А.* Упрощенная модель расчета потерь сигнала в радиолинии, полученная путем сравнения квадратичной формулы Введенского с существующими эмпирическими моделями. // Системы управления, связи и безопасности. – 2019, № 2, с. 87-99. DOI: 10.24411/2410-9916-2019-10204.
4. *Лапцевич А.А., Половеня С.И.* Проектирование системы мобильной связи стандарта LTE при создании эталонной сети сотовой подвижной электросвязи на территории республики Беларусь. // Проблемы инфокоммуникаций. – 2019, № 1-1 (9), с. 28-35.
5. *Мозоль А.А., Головской В.А.* Полуэмпирический способ определения зоны покрытия базовой станции системы подвижной радиосвязи. // Вестник Воронежского института МВД России. – 2014, №3, с. 30-40.
6. *Булычев Ю.Г., Мозоль А.А., Головской В.А.* Оценка дисперсии ослабления радиосигнала в системах подвижной радиосвязи. // Радиотехника. – 2016, №3, с. 23-27.
7. *Mishra R.A.* Advanced Cellular Network Planning and Optimisation: 2G/2.5G/3G. Evolution to 4G. / Edited A.R. Mishra. Chichester : John Wiley & Sons Ltd, 2007. – 542 p.
8. *Свистунов А.С.* Эмпирические модели распространения радиоволн для анализа внутрисистемной электромагнитной совместимости и безопасности сетей сотовой связи с микросотовой структурой. // Журнал Белорусского государственного университета. Физика. – 2018, № 2, с. 107-116.
9. *Красилов А.Н., Хоров Е.М., Царицын М.В.* О емкости сети 5G для трафика URLLC. // Информационные процессы. – 2019, т. 19, № 3, с. 231-237.
10. *Мозоль А.А., Головской В.А.* О коррекции моделей распространения радиоволн для систем когнитивного радио / Антенны и распространение радиоволн // Сб. науч. тр. Всероссийской НТК, 17-19 октября 2018 г. Санкт-Петербург. – СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), 2018, с. 83-87.
11. *Козирацкий Ю.Л., Иванцов А.В.* Алгоритм оперативной оценки радиоэлектронной обстановки в интересах обеспечения электромагнитной совместимости. // Технологии ЭМС. – 2015, № 2(53), с. 18-22.
12. *Saunders S.R., Aragon-Zavala A.* Antennas and propagation for wireless communication systems. Chichester : John Wiley & Sons Ltd, 2007. – 546 p.
13. Recommendation ITU-R P.1546-6. Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 4 000 MHz. – Geneva: ITU, 2019. [Электронный ресурс]. – Режим доступа: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1546-6-201908-I!!PDF-E.pdf (дата обращения: 20.10.2021).

В.В. Евстафьев, Н.В. Руденко, Р.Р. Нагметуллаев, Е.А. Кузёма

АНАЛИЗ СПОСОБОВ ДИАГНОСТИРОВАНИЯ УЗКИХ МЕСТ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
г. Ростов-на-Дону, Россия

Ключевые слова: телекоммуникационные системы, способы диагностирования, узкие места, сравнительный анализ, направления совершенствования.

В статье выполнен анализ известных способов диагностирования узких мест телекоммуникационных систем по шести критериям. Предложены следующие направления совершенствования этих способов: необходимо развивать эти способы в направлении увеличении до нескольких десятков и более диагностируемых элементов; требуется искать более достоверные критерии узких мест, чем загруженность элементов; необходимо оценивать производительность системы как интегральную характеристику качества функционирования; требуется минимизировать вычислительные затраты при реализации способа с целью оперативного выявления и устранения узких мест. Эти результаты могут быть использованы при проектировании и эксплуатации сетей 5*G*.

V.V. Evstafiev, N.V. Rudenko, R.R. Nagmetullaev, E.A. Kuzyoma

ANALYSIS OF METHODS FOR DIAGNOSING NARROW PLACES TELECOMMUNICATION SYSTEMS

Federal State Educational Institution of Higher Education "Don State Technical University",
Rostov-on-Don, Russia

Key words: telecommunication systems, methods of diagnostics, bottlenecks, comparative analysis, directions of improvement.

The article analyzes the known methods of diagnosing bottlenecks in telecommunication systems based on six criteria. The following directions for improving these methods are proposed: it is necessary to develop these methods in the direction of increasing up to several tens or more diagnosed elements; it is required to look for more reliable criteria for bottlenecks than the load of elements; it is necessary to evaluate the performance of the system as an integral characteristic of the quality of functioning; it is required to minimize computational costs when implementing the method in order to quickly identify and eliminate bottlenecks. These results can be used in the design and operation of 5G networks.

Введение. Современное развитие телекоммуникационных систем (ТКС) позволяет предоставлять широкий сервис своим клиентам [1]. Одним из основным направлением дальнейшего развития ТКС является внедрение международных стандартов 5*G*. Такое внедрение позволяет обеспечить согласованное функционирование использование имеющихся ресурсов ТКС.

Платформа сети 5*G* предоставляет для операторов значительные преимущества, выражающиеся прежде всего, в расширении функциональных возможностях и характеристик сети (*performance*) и повышении удовлетворённости пользователей (*User Experience*).

На рисунке 1 [2] показаны основные параметры ТКС IMT2020 (5*G*), по сравнению с показателями *IMT-Advanced* (4*G*), которые позволяют этого достичь.

Рисунок 1. Практические преимущества 5G

Пиковая скорость: сеть 5*G* обеспечивает в 20 раз бо̀льшую скорость по сравнению с 4G, то есть, около 20 Гбит/с.

Скорость на пользователя (средняя) при этом может достигать 100 Мбит/с и более.

Эффективность использования спектра, количество информации, которую можно передать на единицу частотного диапазона, в сети 5G будет по крайней мере в 3 раза выше, чем в 4G [3].

Мобильность пользователя, скорость, с которой может перемещаться пользователь с терминалом 5G по площади покрытия сети без потери хендовера между базовыми станциями, в сети 5G достигает 500 км/час, что даёт возможность пользоваться услугами 5G в скоростных поездах.

Задержка в сети 5G снижается до 1 мс и менее, в то время как в сети 4G можно достичь минимум 10-миллисекундной задержки. Это позволяет использовать технологию 5G для критичных коммуникаций и видеонаблюдения, услуг тактильного интернета, *AR/VR* и пр. [4].

Плотность терминалов в сети 5G повышается на порядок и может достигать нескольких миллионов устройств на 1 кв. км, то есть, на 1 квадратном метре поверхности могут располагаться несколько десятков или даже сотен миниатюрных устройств (например, сенсоров *IoT*).

Энергоэффективность сети 5G на порядок лучше, чем в сети предыдущего поколения. Ёмкость трафика на единицу площади, то есть скорость передачи данных квадратный метр площади покрытия сети, в 5G на два порядка выше, чем в сети 4G [3, 4].

Тем не менее расходы на пропуск всё возрастающего трафика по сетям операторов связи по состоянию на 2019 год не покрывается доходами от традиционных услуг. Поиск новых услуг, т.н. «*killer application*» традиционных телеком-платформ обычно не даёт ожидаемых результатов, что видно из рисунка 2 [3].

Рисунок 2. Разрыв доходов операторов связи

При этом, основной рост трафика и доходов происходит не в секторе устройств людей, а в секторе устройств интернета вещей, который является одной из базовых целей функционала 5*G*.

К тому же анализ рынка телекоммуникационных услуг показывает, что 50% пользователей ожидают по крайней мере, 99,9% доступности сервиса [5]. А это приводит к дополнительным издержкам (затратам) в реализации различных бизнес-процессов. Например, финансовые потери в результате отсутствия связи на бирже в течение 1 минуты чреваты убытками порядка 110 000$ [5].

Таким образом, на практике приходится наблюдать как ТКС с значительными ресурсами и техническими возможностями не могут обеспечить требования потребителей. Указанное несоответствие объясняется тем, что в системе возникают узкие места (УМ), которые и ограничивают более полное использование ресурсов системы [6]. Следует отметить, что УМ меняют свое «местоположение» в зависимости от изменения условий динамики нагрузки, используемых ресурсов, требований по качеству предлагаемых телекоммуникационных услуг, а также при возникающих отказов элементов ТКС и т. п..

Поэтому проблема более точного и оперативного диагностирования УМ ТКС является важной и актуальной и для проектировщиков, и для эксплуатационников ТКС, и для потребителей телекоммуникационных услуг. Все они заинтересованы в повышении эффективности функционирования ТКС.

Постановка задачи. Таким образом, задачей настоящей статьи является:

- проведение анализа различных способов диагностирования УМ систем, выявление их достоинств и недостатков, сравнение их между собой по различным критериям;
- на основе вышеперечисленных процедур предложить направления по разработке приемлемых для практики способов диагностирования УМ ТКС.

Результаты исследования. Известен способ диагностирования узких мест производственной системы [7], предполагающий выявление узких мест по визуальному наблюдению производственного процесса с уточнением следующих характеристик:

- наивысшая загрузка (под загрузкой понимается отношение интенсивности входного потока в элемент к интенсивности обслуживания) элемента (в узком месте оборудование и персонал загружены полностью);
- наличие очереди и затора деталей, полуфабрикатов и т. п. на обработку (обслуживание) в узком месте;
- объем производства ограничен производительностью узкого места.

Недостатком способа [7] является отсутствие автоматической диагностики узких мест производственной системы, что не позволяет осуществить их оперативное устранение.

Недостатки способа [7] устраняются в способе, рассмотренным в статье [8], который позволяет выявлять узкие места в архитектуре локальных сетей, а также недостатки прикладного программного обеспечения, следствием которых оказывается неэффективное использование пропускной способности сервера и сети. Предполагается использовать для диагностики программные анализаторы протоколов, например, *Observer* компании *Network Instruments*. Измеряется утилизация элементов сети – степень (доля) использования ресурса, элемента. Если утилизация элемента (ресурса) превышает допустимое значение, то этот элемент (ресурс) является узким местом.

Недостатком указанного способа является невозможность анализа систем (сетей) при большом количестве элементов и (или) при любой произвольной конфигурации.

Недостатки способа [8] частично устраняет способ диагностирования узких мест, изложенный в статье [9]. В этом источнике показано, что использование при имитационном моделировании аппарата систем массового обслуживания (СМО) при анализе бизнес-процессов позволяет решить задачу анализа узких мест, определять среднее количество обслуживающих устройств, загрузки элементов СМО и среднее время пребывания заявки в сети (т.е. производительность сети). Показано также, что узкое место создается узлом, у которого коэффициент загрузки приближается к единице. В ходе проведения эксперимента на предлагаемой модели мультиагентного процесса преобразования ресурсов формируется статистика и диагностируются УМ. При этом используемый аппарат СМО обеспечивает возможность анализа систем любой конфигурации.

Недостатком этого способа является то, что при диагностировании узких мест не используется универсальная аналитическая модель в виде формул по определению итоговых характеристик, а применяемая имитационная модель на основе аппарата СМО для проведения эксперимента мультиагентного процесса ограничивает анализ систем при большом количестве элементов и является ресурсоемкой.

Наиболее приемлемым для эффективного практического применения является способ диагностирования узких мест, предлагаемый в источнике [10].

Указанный способ предполагает использование в качестве критерия узкого места – загрузку элементов системы (отношение интенсивности входного потока в элемент к интенсивности обслуживания элемента). При этом загрузки элементов системы вычисляются на модели СМО. В этом способе, как и в ранее рассмотренных способах, осуществляется поиск узких мест по критерию загрузки элементов, но не основе имитационного моделирования, а с помощью операционного анализа вероятностных СМО. Это позволяет получить расчетные характеристики на уровне средних значений.

Недостатки способа [10] следующие:

1. Указанный способ не позволяет проводить анализ систем (сетей) при большом количестве элементов, что особенно актуально при анализе современных телекоммуникационных систем.
2. Способ не обеспечивает высокую точность определения узкого места, что обусловлено низкой информативностью выбранного критерия, в качестве которого применяется загрузка элемента. На практике не всегда самый «нагруженный» элемент больше всех ограничивает производительности системы. На производительность системы влияют также производительности её элементов, что не учитывается в способе [10].

Результаты сравнительного анализа анализируемых выше способов диагностирования УМ ТКС приведен в таблице 1.

Таблица 1. Результаты сравнительного анализа способов диагностирования узких мест телекоммуникационных систем

Критерии, используемые для сравнительного анализа способов диагностирования узких мест ТКС	Источники			
	[7]	[8]	[9]	[10]
1. Поиск УМ по признаку «загрузка» элемента (узла)	да	да, измеряют уровень утилизации (степень использования элемента)	да	да
2. Интегральная характеристика – производительность системы (сети), задержка		да	да	да
3. Возможность анализа систем (сетей) при большом количестве элементов	нет	нет	нет	нет
4. Возможность анализа системы (сети) любой конфигурации	нет	нет	да	да
5. Используется аналитическая модель (формулы по определению характеристик)	нет (наблюдают очереди и заторы к УМ)	нет, применяется программный анализатор протоколов	нет	да
6. Используются результаты вычислительного эксперимента	Нет (наблюдают очереди и заторы к УМ)	нет, применяется программный анализатор протоколов	да, в результате эксперимента формируется статистика, диагностируются УМ	нет

Сравнительный анализ способов диагностирования УМ ТКС проведен с использованием шести критериев. Он показывает необходимость совершенствования и разработки более эффективных методов. По мнению авторов статьи, основные направления совершенствования способов диагностирования УМ ТКС следующие:

1. Способ должен позволять диагностировать УМ ТКС при большом количестве элементов (несколько десятков и более). Устранение УМ локально (при малом количестве элементов) далеко не всегда ведет к устранению УМ глобально (в объеме всей ТКС).
2. Необходимо использовать другие критерии, более информативные для выявления УМ. Критерий как «загрузка» элемента опосредованно диагностирует УМ. Приближение значения загрузки к единице говорит, в первую очередь, о том, что данный ресурс эффективно используется. Конечно, может быть, этот элемент и будет узким местом, но не всегда.
3. Способ диагностирования УМ ТКС должен позволять оценивать производительность ТКС как интегральную характеристику качества функционирования.
4. Немаловажное значение для способа диагностирования УМ имеет вычислительные затраты на реализацию, что в последствии отразиться на оперативности выявления УМ. Такое требование придаст способу универсальность и применимость его не только при проектировании ТКС, но при эксплуатации для оперативного устранения УМ вследствие изменения различных условий.

Вывод. Анализ известных способов диагностирования узких мест телекоммуникационных систем позволяет предложить следующие направления совершенствования этих способов:

- необходимо развивать эти способы в направлении увеличении до нескольких десятков и более диагностируемых элементов;
- требуется искать более достоверные критерии узких мест, чем загруженность элементов;
- необходимо оценивать производительность системы как интегральную характеристику качества функционирования;
- требуется минимизировать вычислительные затраты при реализации способа с целью оперативного выявления и устранения узких мест.

СПИСОК ЛИТЕРАТУРЫ

1. Сети связи пост-NGN / Б.С .Гольдштейн, А.Е. Кучерявый.- СПб.: БХВ-Петербург.2013.- 160 с.
2. Emerging Trends in 5G/IMT2020// Geneva Mission Briefing Series. September 2016 [Электронный ресурс]: URL: https://www.itu.int/en/membership/documents/missions/gva-mission-briefing-5g-28sept2016.pdf (дата обращения: 21.10.2021 г.).
3. *Лелли Т.* 5G (пятое поколение мобильной связи) // Портал TADIVISER [Электронный ресурс]: URL:https://www.tadviser.ru/index.php/(дата обращения: 21.10.2021 г.).
4. Развитие сетей 5G в мире // Портал TADIVISER [Электронный ресурс]: URL:https://www.tadviser.ru index.php/(дата обращения: 21.10.2021 г.).
5. *Шувалов В.П., Егунов М.М., Минина Е.А.* Обеспечение показателей надежности телекоммуникационных систем и сетей.- М.: Горячая линия – Телеком, 2016, 168с.
6. *Evstafev V.V., Rudenko N.V.* Improving the dynamics of information flows for optimizing telecommunication systems // IOP Conf. Ser.: Mater. Sci. Eng. 1029 012131. Publishingdoi:10.1088/1757-899X/1029/1/012131.
7. Совершенствование производственных процессов принципы управления [Электронный ресурс] // quality.eup.ru [сайт]. URL: https://quality.eup.ru/DOCUM4/spp.html (дата обращения: 21.10.2021 г.).
8. *Юдицкий С., Подлазов В., Борисенко В.* «Узкие места» в локальных сетях. [Электронный ресурс] // Журнал сетевых решений /LAN, 1998, № 09 [сайт]. URL: https://www.osp.ru/lan/1998/09/133684 (дата обращения: 21.10.2021).
9. *Ван Кай В.В., Аксенов К.А., Аксенова О.П., Киселёва М.В.* Использование аппарата операционного анализа вероятностных сетей для определения количества приборов обслуживания мультиагентной модели // Современные проблемы науки и образования. – 2012. – № 3.; URL: http://www.science-education.ru/ru/article/view?id=6290 (дата обращения: 22.10.2021).
10. *Томашевский В.Н., Жданова Е.Г.* Имитационное моделирование в среде GPSS.-М.: Бестселлер, 2003. 416с.

И.А. Казачанский, Е.М. Хорольский

СОВРЕМЕННАЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ ИНФРАСТРУКТУРА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: телефонная связь, телефонная сеть, интернет, ВОЛС, ШПД.
В статье рассматривается электропроводная телефонная сеть и её текущее состояние.

I.A. Kazachansky, E.M. Khorolsky

ELECTRONIC TELEPHONE NETWORK

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

Keywords: telephone communication, Internet, Volt, ACPD.
The article discusses the electrically conductive telephone network.

Современный мир невозможен без телекоммуникационных технологий, которые стирают государственные границы и расстояние между людьми, делают доступной мобильную и видеосвязь и позволяют решать множество задач в сфере управления, образования, коммерции. Каждый человек сталкивается с ними ежедневно, деля телефонные звонки, проверяя почту или покупая товары в интернет-магазинах.

Общее понятие информационных и коммуникационных технологий включает в себя совокупность методов, процессов и устройств, позволяющих получать, собирать, накапливать, хранить, обрабатывать и передавать информацию, закодированную в цифровом виде или существующую в аналоговом виде.

В более узком смысле под телекоммуникационными технологиями понимается совокупность программных и аппаратных средств, позволяющих устанавливать связь без использования проводов и передавать пакеты информации, включающие также аудио и видеоинформацию.

Телекоммуникационные технологии могут быть рассмотрены как сервисы, предоставляемые провайдерами различного уровня.

По этому принципу можно выделить следующие виды телекоммуникационных технологий:

- телефонная связь, современная телефонная связь позволяет легко переключаться с аналогового стандарта на цифровой, подключать к интернет городские телефоны и соединять в одну сеть аналоговые и мобильные устройства;
- радиосвязь, которая сегодня превратилась в сотовую связь, телефон, перемещаясь в пределах сети, оказывается в зоне действия различных передающих устройств;
- спутниковая связь, которая используется провайдерами для создания систем мобильной связи и для государственных систем связи;

– интернет – наиболее распространенный вид телекоммуникационных технологий, при которых подключение к сети может осуществляться как проводным, так и беспроводным способом.

Высокий спрос на все сложные и разнообразные услуги, усиливающаяся конкуренция на рынке услуг связи, высокие требования пользователей к многообразию, функциональности и качеству услуг способствуют поиску новых принципиально подходов к развитию телекоммуникационной отрасли.

Стратегией социально-экономического развития Ростовской области на период до десяти лет, определено, что информационно-коммуникационная инфраструктура является комплексной технологической платформой, обеспечивающей доступ населения и организаций к услугам связи и широкому спектру услуг, предоставляемых в электронном виде в различных сферах деятельности. В целом интенсивное развитие информационно-коммуникационных технологий и инфраструктуры во многом способствует повышению конкурентоспособности Ростовской области на национальном и мировом уровнях.

Приоритетными направлениями государственной политики в области развития информационных технологий являются:

– формирование современной информационно-телекоммуникационной инфраструктуры;
– обеспечение высокого уровня доступности информационно-телекоммуникационной инфраструктуры, предоставление качественных услуг на ее основе;
– развитие экономики РФ на основе использования информационных технологий;
– повышение качества образования, медицинского обслуживания, науки, социальной защиты населения, содействие развитию культуры и средств массовой информации на основе информационно-коммуникационных технологий;
– обеспечение конкурентоспособности и технологического развития информационно-коммуникационных технологий;
– повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, в том числе противодействие использованию информационных и телекоммуникационных технологий в целях угрозы национальным интересам Российской Федерации.

Областная электропроводная телефонная сеть имеет в своем составе более 80 процентов оборудования, основанного на использовании цифровых технологий.

Топология внутризоновой сети телефонной связи имеет кольцевую структуру, базируется на волоконно-оптических линиях связи (далее – ВОЛС), а также охватывает все административные центры муниципальных районов и городских округов в Ростовской области. Протяженность ВОЛС составляет более 15 000 км.

В конце десятилетия в рамках реализации федерального проекта по устранению цифрового неравенства высокоскоростными современными услугами связи с использованием ВОЛС обеспечено 394 населенных пункта Ростовской области с численностью жителей от 250 до 500 человек. В данных населенных пунктах Ростовской области установлены и функционируют точки коллективного доступа к информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет) по технологии Wi-Fi, услуги доступа от которых предоставляются на безвозмездной основе.

Для оказания услуг фиксированной телефонной связи жителям населенных пунктов Ростовской области в каждом населенном пункте с постоянно проживающим населением

установлен таксофон для оказания универсальных услуг связи. Вызовы на телефонные номера экстренных оперативных служб и иные номера, как фиксированной телефонной связи, так и подвижной радиотелефонной связи, осуществляются на безвозмездной основе. Всего на территории Ростовской области эксплуатируются более 2 466 таксофонов.

За последнее время продолжила снижаться плотность фиксированной телефонной связи, которая характеризуется количеством абонентских устройств на 100 человек населения. Показатель составляет менее 19 процентов. Тенденция к снижению плотности фиксированной телефонной связи – это мировая практика, которая связана с необходимостью быть на связи в любое время, в любом месте, исходя из чего предпочтение отдается мобильным средствам связи.

Замедление темпов роста в сфере фиксированной телефонной связи заставляет операторов расширять свое присутствие в других сегментах, делать ставку на модернизацию сетевой инфраструктуры. Набор услуг операторов электропроводной связи уже давно не ограничивается предоставлением услуг привычной телефонии, а существенно расширяется за счет продвижения услуг передачи данных с использованием широкополосного доступа к сети Интернет (далее также – ШПД). Значительный упор делается на предоставление доступа с применением технологии FTTB (оптика до дома), PON (пассивная оптическая сеть), развертывание мультисервисных сетей NGN (сети нового поколения), позволяющих оптимизировать корпоративные коммуникации. Также в небольших населенных пунктах предполагается развивать сети WiMAX.

Определяющим фактором роста в сфере проводной связи является оказание услуг ШПД. В крупных городах в Ростовской области рынок ШПД уже достиг насыщения, и операторы связи стремятся не просто расширить абонентскую базу, но и удержать ее в условиях высокой конкуренции. В средних и малых городах конкуренция ниже, и запас по росту абонентской базы присутствует. В сельских населенных пунктах конкуренция практически отсутствует. Во многих из них нет возможности пользоваться услугой доступа к сети Интернет, сравнимой по качеству с городом. Жители ряда сельских населенных пунктов могут воспользоваться только спутниковым и мобильным доступом к сети Интернет.

Число домашних хозяйств, имеющих доступ к ШПД, – важный показатель, демонстрирующий степень доступности высокоскоростной сети Интернет для населения Ростовской области. В итоге данный показатель в Ростовской области составил 78,1 процента от общего числа домашних хозяйств, что соответствует 19-му месту в РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция развития связи в Ростовской области на период до 2030 года Официальный портал Правительства Ростовской области официальный сайт. – Москва. – URL: https://www.donland.ru/activity/2723// (дата обращения: 24.10.2021). – Текст: электронный.
2. Нормативное регулирование цифровой среды» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/862/ (дата обращения: 24.10.2021). – Текст: электронный.
3. Цифровые технологии» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/878/ (дата обращения: 24.10.2021). – Текст: электронный.

И.А. Казачанский, И.В. Решетникова

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ IP-ТЕЛЕФОНИИ НА БАЗЕ SIP ПРОТОКОЛА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: VoIP, IP-телефония, телекоммуникации, SIP протокол, связь Интернет, инфокоммуникации.

В статье рассмотрены вопросы реализации функций IP-телефонии, взаимодействие абонентов SIP, ключевые возможности протокола и сравнение SIP и H.323.

I.A. Kazachansky, I.V. Reshetnikova

TECHNOLOGY OF CONSTRUCTION OF IP-TELEPHONY BASED ON SIP PROTOCOL

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

Keywords: VoIP, IP-telephony, telecommunications, SIP protocol, Internet communications, info-communications.

The article considers the implementation of IP-telephony functions, the interaction of SIP subscribers, the key features of the protocol and the comparison of SIP and H.323.

Связь – это значительный и характерный элемент в существовании современного человеческого общества. Сложно представить жизнь без телефонов в наш технически развивающийся век. А ведь столетие назад человечество и не мечтало о том, что можно будет послать сообщение из двух совершенно разных уголков земли за доли секунды. С каждым годом исследователи сферы инфокоммуникаций разрабатывают все новые, и порой, даже уникальные устройства и системы, а также улучшают уже существующие. Так как научно-технический прогресс не собирается стоять на месте, то и развитие средств связи никогда не остановится. На сегодняшний день телекоммуникации — это одна из самых быстроразвивающихся высокотехнологических и наукоемких отраслей мировой экономики. Степень развития технологических разработок, производства и внедрения в различные сферы деятельности телекоммуникационных систем во многом формируют положительный образ передового государства.

Глобальная сеть Интернет очень интенсивно и быстро развивается и благодаря ее широкому распространению появился новый вид связи, который основывается на использовании IP протоколов и IP-серверов, реорганизуя голосовой сигнал в цифровой формат. Такой формат связи получил название IP-телефония или VoIP. Данная технология позволила превратить такую незаменимую вещь, как телефонные переговоры, в удобный, качественный, универсальный и, что немаловажно, дешевый инструмент общения, который стал доступен каждому.

В классификации телекоммуникационных систем телефония занимает значительное место. Это сфера науки техники и технологий, включающая изучение основ построения сетей телефонной связи, создание аппаратных комплексов для ее осуществления и применения и является самым перспективным видом связи.

IP-телефония — это технология, которая позволяет задействовать другую любую сеть с пакетной коммутацией, сделанной на базе протокола IP, в качестве средства для организации

и ведения международных, междугородных и местных телефонных звонков в режиме реального времени.

На современном уровне развития, IP-телефония уже имеет ряд серьезных плюсов, если сравнивать ее с традиционной:

- услуги IP-телефонии стоят намного меньше обычной междугородной и международной связи;
- если сравнивать ее с обычной телефонией, то оборудование каналов связи проще, и, следовательно, меньше эксплуатационные расходы;
- сети с коммутацией пакетов имеют более высокую степень отказоустойчивости, чем сети, которые используют коммутацию каналов, в них лучше используется производительность каналов связи;
- конечный пользователь получает новый набор устройств доступа от традиционных телефонов и факсов до компьютеров;
- предоставляется широкая возможность настройки большого набора услуг.

Для передачи информации VoIP может использоваться либо протокол H.323, либо более перспективный протокол SIP. [1]

В рамках установленного стандарта H.323 абоненты могут обмениваться не только голосовой информацией, но и видеоинформацией, то есть пользоваться оборудованием для организации видеоконференций. Шлюз не входит в число обязательных компонентов сети H.323. Он необходим только в случае, когда требуется установить соединение с терминалом другого стандарта. Эта связь обеспечивается трансляцией протоколов установки и разрыва соединений, а также форматов передачи данных. Шлюзы H.323 сетей широко применяются в IP телефонии для сопряжения IP сетей и цифровых или аналоговых коммутируемых телефонных сетей.

SIP (*Session Initiation Protocol* – протокол установления сеанса) описывает как именно клиентское приложение (например, software telephone) может подать запрос на начало соединения у другого, возможно, физически удалённого клиента, который находится в той же сети, используя его уникальное имя. Протокол описывает способ установления и завершения пользовательского Internet-сеанса, включая обмен мультимедийным содержимым. На рисунке 1 показано взаимодействие абонентов SIP. [2]

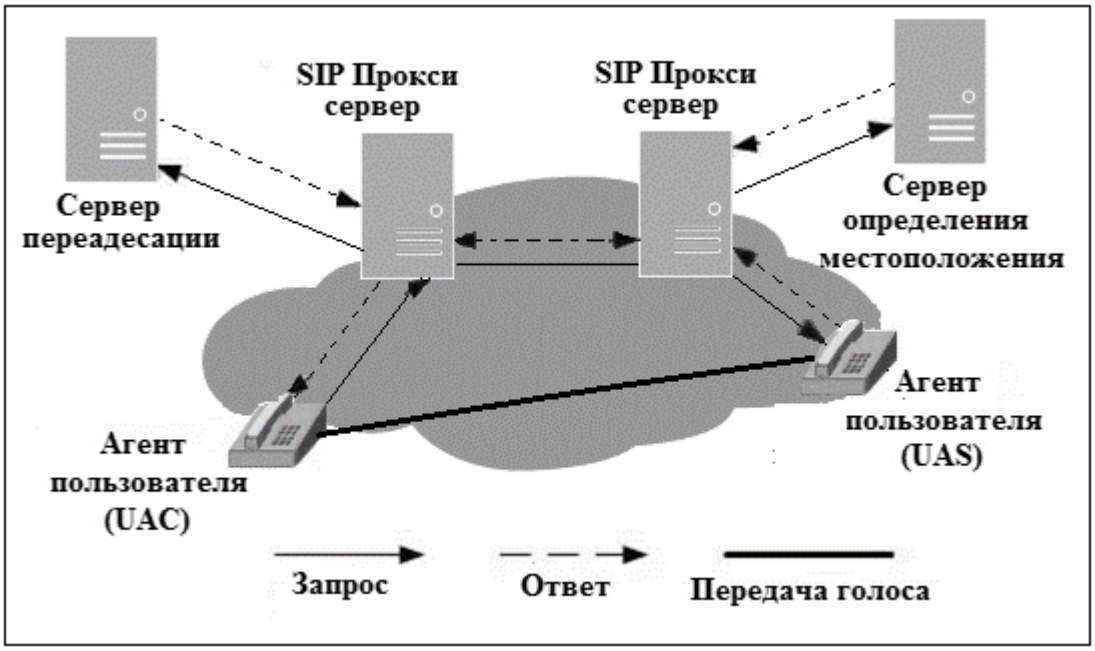


Рисунок 1. Взаимодействие абонентов SIP

На рисунке видно, что два телефонных аппарата, которые хотят разговаривать по SIP, есть два Proxy сервера (регистр). Сплошной линей обозначен разговорный трафик, который идет между абонентами. Облако на рисунке — это IP-облако, штрихпунктирными линиями обозначена сигнализация. Абонент А взаимодействует со своим прокси сервером, отправляет туда сигнализацию, а этот прокси сервер находит абонента В, он знает, что находится на другом прокси сервере, взаимодействует с ним. RTP трафик уже может проходить на прямую без участия прокси серверов.

Протокол, в котором связь рассчитана на RTP трафик, видео трафик и на сообщение, согласно архитектуре, NGN можно передавать с помощью SIP.

Типы запросов SIP:

- INVITE – приглашение на сеанс связи. Обычно содержит SDP-описание сеанса;
- ACK – подтверждает прием ответа на запрос INVITE;
- BYE – завершает сеанс связи. Может быть передан любой из сторон, участвующей в сеансе;
- CANCEL — отменяет обработку ранее переданных запросов, но не влияет на запросы, которые уже закончили обрабатываться;
- REGISTER — переносит адресную информацию для регистрации пользователя на сервере определения местоположения;
- OPTIONS — запрашивает информацию о функциональных возможностях сервера. [3]

SIP протокол имеет ряд ключевых возможностей:

- Мультимедийность;
- Индивидуальная мобильность для каждого пользователя. Возможность передвигаться без каких-либо ограничений в пределах сети, исходя из этого услуги связи должны предоставляться им в любой зоне данной сети. Каждому абоненту присваивается персональный идентификатор, а сеть предоставляет услуги связи вне зависимости от того, где он находиться;
- Маштабируемость сети. В первую очередь характеризуется возможностью увеличивать количество элементов сети если она расширяется. Построенная на базе протокола SIP серверная структура сети вполне соответствует этому требованию;
- Доступность и легкость. По мнению специалистов, SIP дает возможность наполнить решения и продукты новыми возможностями и сервисами. Что касается легкости, то можно сказать, что используемые в SIP сообщения имеют текстовый формат и поддерживают вложение любых типов данных. Исходя из этого, голосовое соединение может сопровождаться обменом данными между приложениями. Разговор через SIP протокол дополняется передачей данных от одного пользователя другому, к примеру, электронной визитки, цифровых фотографий и т.д.;
- Архитектура Клиент-Сервер;
- Альтернатива реакции на события. Возможность клиента «подписаться» на конкретное событие (к примеру, обновление статуса пользователя), и с его наступлением сервер вышлет нужное обновление;

SIP протокол имеет схожесть с широко используемым протоколом HTTP, который тоже можно сигнальным (запрос клиентами нужных документов у сервера). При установлении соединении параметры сессии соответствуют описанию с SDP и передаются клиенту вместе с заголовками протокола. Так же очень схожи коды ответов протокола SIP со стандартными кодами протокола HTTP. Если ответ удачный, то клиенту посылается 200, а если адрес не найден, то 400. В случае ошибки авторизации 404 и др. Каждый клиент SIP имеет индивидуальный идентификатор SIP-URI, по внешним признакам похожим на адреса

электронной почты students@lists.sfedu.ru. Следовательно, имя пользователя SIP состоит из персональной части (до знака @), которая определяет, например, организацию. DNS-имени может быть использовано в качестве доменной части.

Протоколы SIP-T, SIP-I являются расширенными версиями протокола SIP и дополняют его в части процедур передачи сообщений протокола ISUP-R по сети электросвязи с коммутацией пакетов посредством механизмов трансляции и инкапсуляции.

В протоколе SIP есть три основных типа установления соединения:

- с участием прокси сервера;
- с участием сервера переадресации;
- соединение между пользователями.

Различие между вариантами подключения состоя в том, что поиск и приглашение пользователя происходит разным способами.

В первом случае поиск и приглашение выполняет прокси сервер. Пользователь, который совершает вызов, должен иметь постоянный SIP-адрес пользователя, с которым он хочет связаться. Во втором случае пользователь самостоятельно устанавливает соединение, а сервер отвечает за преобразование постоянного адреса вызываемого абонента в текущий. В третьем случае пользователю необходимо иметь текущий адрес вызываемого пользователя.

Приведенные варианты установления соединения являются простейшими, и прежде чем вызов дойдет до вызываемого пользователя, он пройдет через некоторое количество прокси-серверов, или может быть отправлен на сервер переадресации, а уже после на прокси-сервер.

Сравнение протоколов SIP и H.323 представлены в таблице 1

Таблица 1. Сравнение SIP и H.323

Параметр сравнения	SIP	H.323
Дополнительные услуги	Оба протокола поддерживают приблизительно одинаковый набор услуг	
Персональная мобильность пользователей	Имеется хороший набор средств поддержки мобильности	Персональная мобильность поддерживается, но менее гибко
Расширяемость протокола	Удобная расширяемость, простая совместимость с предыдущими версиями	Расширяемость поддерживается, но существует ряд сложностей
Масштабируемость сети	Оба протокола обеспечивают хорошую масштабируемость сети	
Время установления соединения	Достаточно одной транзакции	Требуется несколько транзакций.
Сложность протокола	Простой, мало запросов, текстовый формат сообщений	Сложный, много запросов и протоколов, двоичное представление сообщений
Совместимость оборудования	Практически никакой. Каждый производитель SIP устройств соблюдает только тот набор рекомендаций (RFC), который ему нравится, ибо набор этих рекомендаций очень велик. Совместим фактически только базовый вызов	Практически полная. Стандарты устоявшиеся и имеют чёткий набор спецификаций

Несмотря на то, что первоначально SIP-протокол был разработан для голосовых сервисов, сегодня он поддерживает широкий спектр приложений, включая видеоконференции, потоковые мультимедиа, обмен мгновенными сообщениями, онлайн-игры и передачу файлов и факсов через IP-сеть. [2,3]

Изначально SIP протокол ориентирован на сети, которые используют многоадресную рассылку. Этот протокол в идеале подходит для осуществления групповых оповещений, например, для Call-центра. В этот момент, протокол H.323 оказывает больше вариантов

управления услугами, как со стороны аутентификации и учета, так и со стороны контроля использования сетевых ресурсов. В этой части возможности SIP протокола беднее.

SIP протокол имеет возможность распределять приоритеты, в то время как у H.323 такой возможности не имеется.

Со стороны реализации H.323 на много сложнее SIP, и H.323 тратит на установку соединения на много больше времени.

СПИСОК ЛИТЕРАТУРЫ

1. *Гордиенко В.Н., Кунегин С.В., Шевелев С.В.* Современные высокоскоростные цифровые телекоммуникационные системы. Ч. 5. Передача мультимедийного трафика по высокоскоростным IP-сетям: Учебное пособие / МТУСИ. - М., 2001. - 35 с
2. *А.А. Нерсесянц* Учебное пособие для самостоятельной работы студентов по дисциплинам: «Сети связи», «Мультисервисные сети связи» Ростов-на-Дону: СКФ МТУСИ, 2018. – 164 с.:
3. Протокол установления сеанса https://ru.wikipedia.org/wiki/ Протокол_установления_сеанса (дата обращения (15.03.2020)
4. *Гольдштейн Б. С. Елагин В. С., Сенченко Ю. Л.* «Телекоммуникационные протоколы» [Книга]. - [б.м.] : СПб.: БХВ – Санкт-Петербург, 2011 г.

И.А. Казачанский, И.В. Решетникова

ИССЛЕДОВАНИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ СЕТИ IP-ТЕЛЕФОНИИ ПО СТАНДАРТУ H323

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: VoIP, IP-телефония, телекоммуникации, шлюз, Интернет.

В статье рассмотрены вопросы реализации функций IP-телефонии по стандарту Р323, протоколы подключения и принципы функционирования информационного шлюза.

I.A. Kazachansky, I.V. Reshetnikova

RESEARCH OF PRINCIPLES OF CONSTRUCTION OF IP-TELEPHONY NETWORK BY H323 STANDARD

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

Keywords: VoIP, IP-telephony, telecommunications, gateway, Internet.

The article discusses the implementation of IP-telephony functions according to the P323 standard, connection protocols and the principles of operation of the information gateway.

На сегодняшний день телекоммуникации одна из самых быстроразвивающихся высокотехнологических и наукоемких отраслей мировой экономики. Степень развития технологических разработок, производства и внедрения в различные сферы деятельности

телекоммуникационных систем во многом формируют положительный образ передового государства.

Постоянное развитие сети Интернет и ее распространение привело к появлению принципиально новой технологии, основанной на использовании Интернет-протоколов и IP-серверов, преобразующих привычный голосовой сигнал в цифровой формат. Такая связь получила название IP-телефония или VoIP. Данная технология позволила превратить такую незаменимую вещь, как телефонные переговоры, в удобный, качественный, универсальный и, что немаловажно, дешевый инструмент общения, который стал доступен каждому.

В классификации телекоммуникационных систем телефония занимает значительное место. Это сфера включает изучение основ построения сетей телефонной связи, создание аппаратных комплексов для ее осуществления и применения и является самым перспективным видом связи.

“IP-телефония (или англ. VoIP - Voice over Internet protocol) - технология, которая использует сеть с пакетной коммутацией сообщений на базе протокола IP для передачи голоса в режиме реального времени.” [1] Особенность функционирования заключается в передаче информации по каналам сети Интернет, а не по классическому способу передачи по телефонным сетям. Этот способ предоставляет отличную возможность использовать качественную связь с значительной экономией денежных средств. Это возможно благодаря:

- ТфОП имеют избыточную производительность, когда VoIP применят технологию сжатия голосовых пакетов разрешая всецело эксплуатировать емкость телефонной линии;
- Доступ к глобальной сети имеют все желающие, это позволят сократить растрату денежных средств на подключение или вовсе исключить их;
- Звонки в ЛВС могут обращаться к внутреннему серверу и происходить без внимания внешней АТС.

Функции IP-телефонии будет реализовывать устройство – шлюз, которое с сетевой точки зрения осуществляет преобразование управляющей информации и данных, поступающих из одной сети (например, PSTN) в пакеты глобальной сети Интернет и обратно. Причем такое преобразование не должно искажать исходный речевой сигнал, а режим передачи обязан сохранять обмен информацией между абонентами в реальном масштабе времени. [2]

Функции, которые реализует шлюз при соединении типа "точка-точка" состоят в следующем:

- реализация физического интерфейса с коммуникационной сетью;
- детектирование и генерация сигналов абонентской сигнализации;
- преобразование сигналов абонентской сигнализации ТфОП в сигнализацию пакетной сети и обратно, а конкретно сопряжение сигнализации ОКС-7 с сигнализацией SIP;
- преобразование речевого сигнала в пакеты данных и обратно;
- соединение абонентов;
- передача по сети сигнализационных и речевых пакетов;
- разъединение связи. [2]

Шлюз (H.323 Gateway) объединяет традиционную телефонную сеть с IP сетью. Он обеспечивает трансляцию упакованного в пакеты оцифрованного и зачастую сжатого голоса в форму, пригодную для передачи по ТфОП. [3]

Шлюз – это устройство, которое связывает сети с разными типами системного и прикладного программного обеспечения (например, ТфОП и Internet). [3]

Различают пять типов шлюзов:

- Транспортные шлюзы (Media Gateway – MG), могут видоизменять форматы передаваемых данных. Например, циклы ИКМ-30 в IP-пакеты и обратно;

– Шлюзы сигнализации (Signaling Gateway – SG), могут преобразовывать сигналы различных систем. Например, смысловое преобразование сигналов ОКС-7 (ТфОП или сотовая сеть GSM) и SIP (Internet);
– Транкинговый шлюз (Trunking Gateway (TGW)) – имеет возможность одновременно выполнять функции MG и SG;
– Шлюз доступа (Access Gateway (AGW)) – может выполнять функции MG и SG для оборудования доступа, подключаемого через интерфейс V5;
– Резидентный шлюз доступа (Residential Access Gateway (RAGW)) – выполнение функции подключения пользователей, использующих терминальное оборудование ТфОП/ЦСИС к мультисервисной сети;
– Для передачи информации VoIP может использоваться либо протокол H.323, либо более перспективный протокол SIP. [3]

В рамках установленного стандарта H.323 абоненты могут обмениваться не только голосовой информацией, но также и видеоинформацией, то есть использовать оборудование для организации видеоконференций. Шлюз не состоит в числе обязательных компонентов сети H.323. Он нужен только в том случае, когда требуется установление соединения с терминалом другого стандарта. Эта связь обеспечивается трансляцией протоколов установки и разрыва соединений, а также форматов передачи данных. Шлюзы H.323 сетей широко применяются в IP телефонии для сопряжения IP сетей и цифровых или аналоговых коммутируемых телефонных сетей.

Стандарты H.323 определяется следующими основными компонентами VoIP-соединения, которые изображены на Рисунке 1:

– Терминал;
– Шлюз (gateway);
– Привратник (Контроллер зоны);
– Устройство многоточечной конференции (MCU). [4]

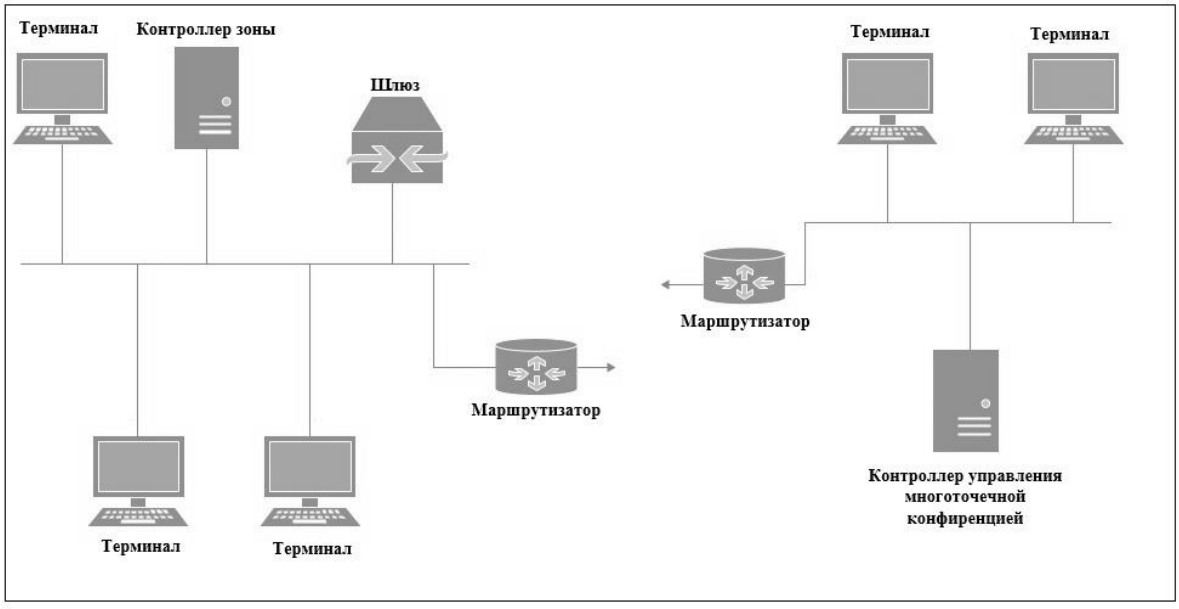


Рисунок 1. Структурная схема сети IP-телефонии по стандарту H.323

Терминал (Terminal) – оконечное сетевое мультимедийное (голос, видео, данные) устройство, обеспечивающее дуплексную речевую связь с другим терминалом, шлюзом или контроллером управления многоточечной конференции. Другими словами, по стандарту

терминал - оборудование конечных точек сети, которые имеют связь друг с другом в режиме VoIP либо видеоконференцсвязи. [4,5]

H.323 – стандарт должен выполнять поддержку следующих протоколов:

- H.245 абонентское оборудование узнает о функциональных возможностях (например: какие аудио и видеокодеки могут поддерживаются, сколько аудио и видеопотоков будут использовать абоненты в рамках данного соединения);
- H.225 - установка соединения между H.323-устройствами;
- RAS предназначен для учета звонков и контроля доступа в сеть;
- RTP/RTCP для передачи звуковых и видео пакетов;
- H.323 – стандарт должен также поддерживать звуковой кодер-декодер в соответствии с G.711. [4,5]

Протоколы H.225 и RAS используются между H.323-оконечными точками (терминалами и шлюзами) и контроллером зоны для обеспечения:

- обнаружения контроллера зоны (GRQ);
- регистрации оконечной точки;
- определения расположения оконечной точки;
- управления аутентификацией;
- задания маркера доступа. [4,5]

RAS-сообщения передаются через ненадежные RAS-каналы, поэтому при обмене сообщениями возможны потери, задержки и повторные передачи.

В контроллере зоны или в привратнике заострен весь интеллект сети IP-телефонии.

Привратник (H.323 Gatekeeper) – это специальный сетевой объект, который устанавливает, соединения между абонентами через разные сети с коммутацией пакетов реализует следующие функции: [5]

- регистрация и авторизация абонентов;
- трансляция адресов (например, DNS-имена в телефонные номера);
- маршрутизация вызовов к IP-телефону или шлюзу.

Это устройство отвечает за управление одной зоной сети, в которой находятся: терминалы, шлюзы и т.д. зарегистрированные только у этого привратника. Другие части зоны сети H.323 могут соединятся между собой с помощью маршрутизатора и быть территориально разнесены.

Обычно один привратник обслуживает так называемую зону, то есть часть сети, находящуюся под административным управлением одной организации.

Устройство многопользовательских конференций (H.323 Multipoint Conference Unit, MCU) - управляет проведением многопользовательских конференций, согласует параметры соединения всех участников в режиме централизованной, децентрализованной или комбинированной конференции. Возможно переключение или смешивание медиа-потоков. [4,5]

Маршрутизатор производит выбор маршрута, анализируя свое представления о настоящей конфигурации сети и соответствующего условия выборки маршрута. В большинстве случаев, в качестве критерия может выступает время прохождения маршрута, которое в локальных сетях совпадает с длиной маршрута, измеряемой в количестве пройденных узлов маршрутизации (в больших сетях также учитывается и время, необходимое для передачи пакета по каждой линии связи)

Передача голосовой информации IP-сети вместо стандартной сети с коммутацией каналов предусматривает конфигурацию, для которой необходима установка шлюзов. Устройство осуществляет сжатие поступающей информации (голоса), преобразует всё это в IP-пакеты и отправляет в сеть IP.

Шлюз размещается между взаимодействующими сетями и является посредником, переводящим сообщения, поступающие из одной сети, в формат другой сети. Может быть

реализован как чисто программными средствами, установленными на обычном компьютере, так и на базе специализированного компьютера. Трансляция одного стека протоколов в другой представляет собой сложную интеллектуальную задачу, требующую максимально полной информации о сети, поэтому шлюз использует заголовки всех транслируемых протоколов. [6]

Для организации взаимодействия различных сетей в настоящее время используется следующий подход, который показан, на рисунке 2 основан на использовании шлюзов, которые обеспечивают согласование двух стеков протоколов путем преобразования (трансляции) протоколов.

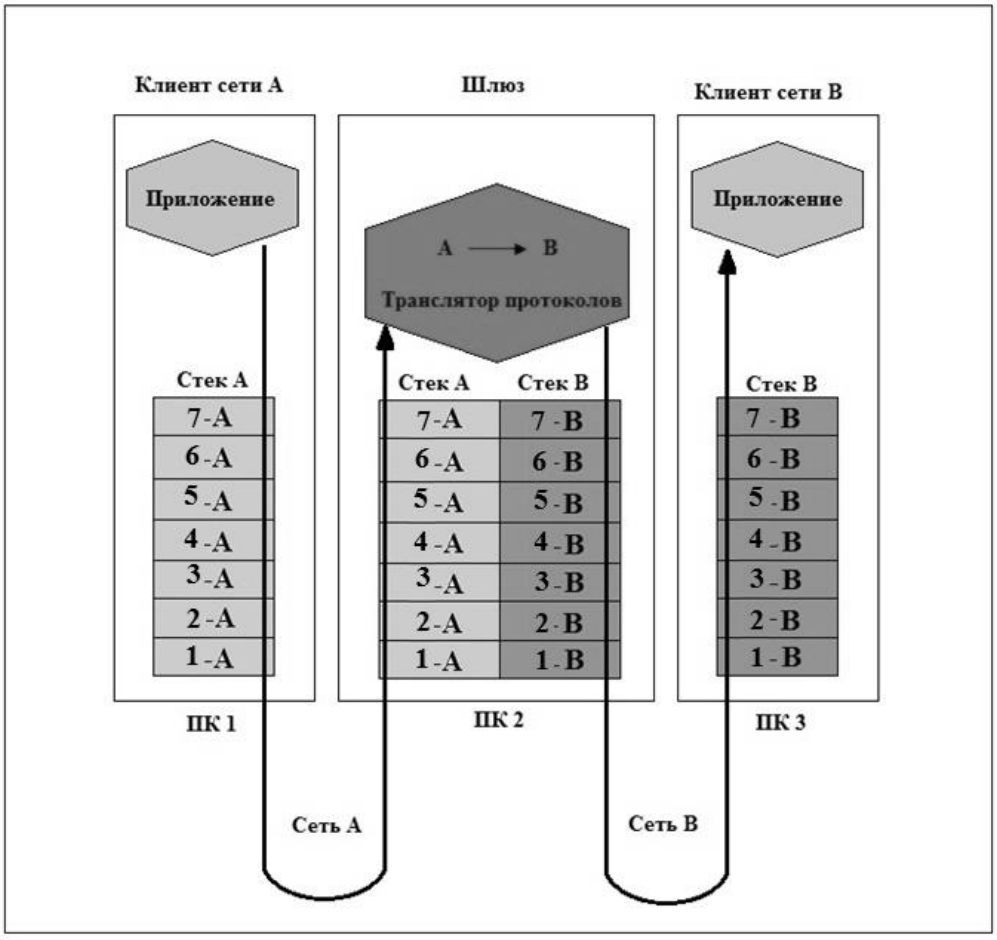


Рисунок 2. Принципы функционирования шлюза

Шлюз согласует коммуникационные протоколы одного стека с коммуникационными протоколами другого стека. Рассмотрим принцип работы шлюза.

В показанном примере на рисунке 3 шлюз, размещенный на компьютере 2, согласовывает протоколы клиентского компьютера 1 сети А с протоколами серверного компьютера 3 сети В, две сети при этом используют полностью отличающиеся стеки протоколов. Как видно из рисунка 2, в шлюзе реализованы оба стека протоколов.

Запрос от прикладного процесса клиентского компьютера сети А поступает на прикладной уровень его стека протоколов. В соответствии с этим протоколом на прикладном уровне формируются соответствующий пакет (или несколько пакетов), в которых передается запрос на выполнение сервиса. Некоторому серверу сети В. Пакет прикладного уровня передается вниз по стеку компьютера сети А, а затем в соответствии с протоколами канального и физического уровней сети А поступает в компьютер 2, то есть в шлюз. Здесь он передается от самого нижнего к самому верхнему уровню стека протоколов сети А. Затем пакет прикладного уровня стека сети А преобразуется (транслируется) в пакет прикладного уровня

серверного стека сети. В. Алгоритм преобразования пакетов зависит от конкретных протоколов и, как уже было сказано, может быть достаточно сложным. В качестве общей информации, позволяющей корректно провести трансляцию, может использоваться, например, информация о символьном имени сервера и символьном имени запрашиваемого ресурса сервера (в частности, это может быть имя каталога файловой системы). Преобразованный пакет от верхнего уровня стека сети В передается к нижним уровням в соответствии с правилами этого стека, а затем по физическим линиям связи в соответствии с протоколами физического и канального уровней сети В поступает в другую сеть к нужному серверу. Ответ сервера преобразуется шлюзом аналогично. [6]

Сети IP-телефонии предоставляют возможности для вызовов трёх основных типов подключения:

– «От телефона к телефону»;

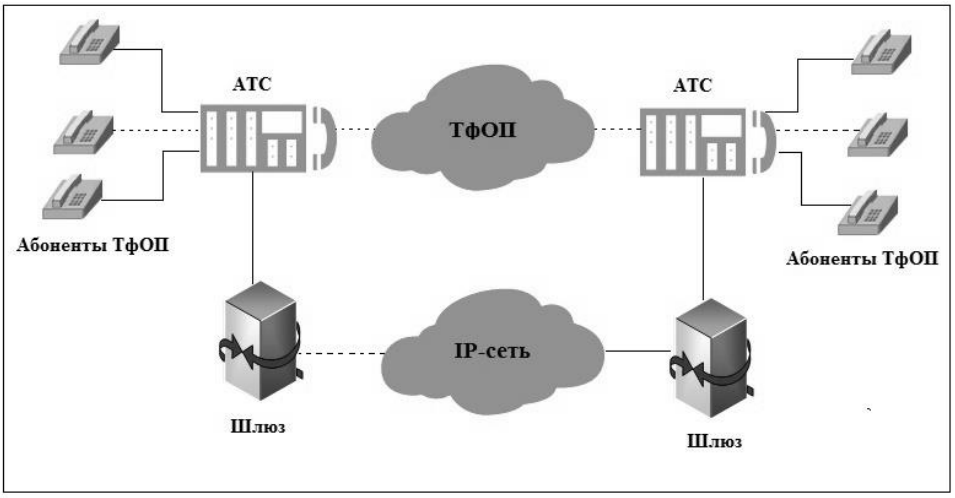


Рисунок 3. Схема связи «От телефона к телефону»

Вызов идет с обычного телефонного аппарата к АТС, на один из выходов, в которой подключен шлюз IP-телефонии, и через IP-сеть доходит до другого шлюза, который осуществляет обратные преобразования. [7]

– «От компьютера к телефону»;

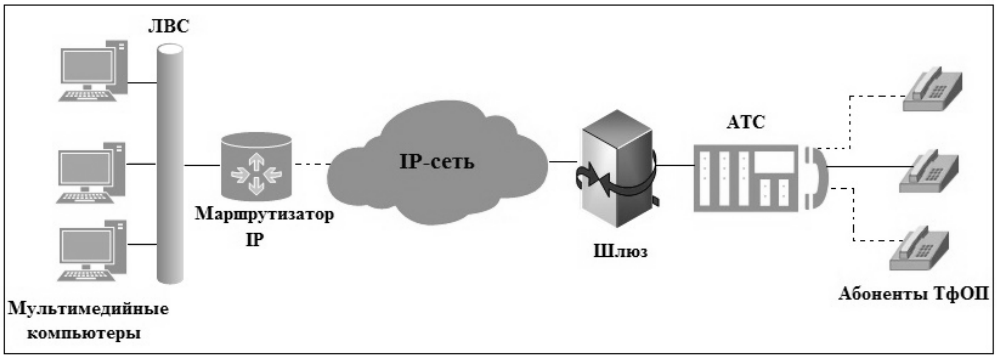


Рисунок 4. Схема связи «От компьютера к телефону»

Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату, микрофон и акустические системы, подключается к IP-сети или к сети Интернет, и с другой стороны шлюз IP-телефонии имеет соединение через АТС с обычным телефонным аппаратом. [7]

Следует отметить, что в соединениях первого и второго типов вместо телефонных аппаратов могут быть включены факсимильные аппараты, и в этом случае сеть IP-телефонии должна обеспечивать передачу факсимильных сообщений. [7]

– «От компьютера к компьютеру».

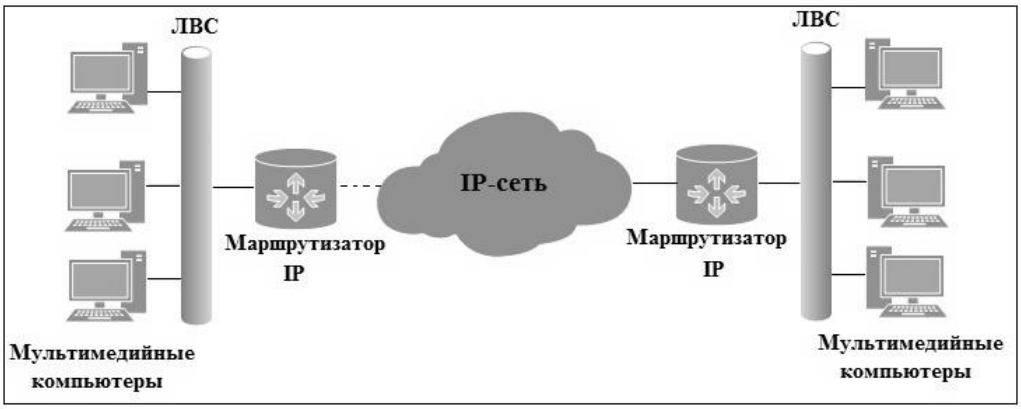


Рисунок 5. Схема связи «От компьютера к компьютеру»

Этот сценарий сейчас наиболее популярен. Соединение устанавливается через IP-сеть между двумя мультимедийными компьютерами, оборудованными аппаратными и программными средствами для работы с IP-телефонией (микрофоном, WEB-камерой). При данной схеме включения имеется возможность организовать сеансы видеотелефонии, видеоконференции, передачу мгновенных сообщений и передачу файлов. [7]

Термин IP-телефония эквивалентен термину VoIP (Voice over IP – голос поверх IP). Internet-телефония - более узкое понятие, когда в роли транспортной среды выступает сеть Internet.

СПИСОК ЛИТЕРАТУРЫ

1. *И.В., Баскаков.* IP-телефония в компьютерных сетях / Баскаков И.В. и др. – М.: НОУ "ИНТУИТ", 2016 – 226 с.
2. *Гордиенко В.Н., Кунегин С.В., Шевелев С.В.* Современные высокоскоростные цифровые телекоммуникационные системы. Ч. 5. Передача мультимедийного трафика по высокоскоростным IP-сетям: Учебное пособие / МТУСИ. - М., 2001. - 35 с
3. *А.А. Нерсесянц* Учебное пособие для самостоятельной работы студентов по дисциплинам: «Сети связи», «Мультисервисные сети связи» Ростов-на-Дону: СКФ МТУСИ, 2018. – 164 с.:
4. Информационным и телекоммуникационным технологиям http://kunegin (дата обращения 10.03.2020)
5. *В.Г. Олифер, Н.А. Олифер.* Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов, 5-е издание СПб: Питер. 2016. – 992 с.: илл.
6. Шлюзы, принцип работы https://studfiles.net/preview/2949858/page:31/ (дата обращения 9.03.2020)
7. Виды соединений в сети IP-телефонии http://helpiks.org/6-84553.html (дата обращения 1.03.2020)

В.Г. Кобак, В.В. Шевченко, С.А. Швидченко[1], Д.А. Жуковский[2]

ИСПОЛЬЗОВАНИЕ ЭКСПЕРИМЕНТАЛЬНОГО АЛГОРИТМА В КАЧЕСТВЕ ЭЛИТНОЙ ОСОБИ ПРИ РЕШЕНИИ ОДНОРОДНОЙ МИНИМАКСНОЙ ЗАДАЧИ

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: распределительная NP- полная задача, однородная система, эвристический алгоритм без возвратов, модифицированная модель Голдберга, кроссовер, мутация, вычислительные эксперименты, множество заданий, списочные алгоритмы, начальная популяция.

В данной работе рассматривается решение распределительной задачи для однородных систем с помощью эвристического алгоритма без возвратов, генетической модели. Для решения этой получили большое распространение генетические, списочные и другие эвристические алгоритмы. Предлагается для решения однородной минимаксной задачи алгоритм без возвратов, основанный на идее алгоритма Романовского. Аналитически доказать, насколько экспериментальный алгоритм лучше или хуже списочных алгоритмов не получается в силу сложности задачи. При решении модифицированной моделью Голдберга использовалась элитная особь, где в качестве элитной особи использовался экспериментальный алгоритм. Проведён вычислительный эксперимент, по которому сделаны выводы об эффективности алгоритмов.

V.G. Kobak, V.V. Shevchenko, S.A. Shvidchenko[1], D.A. Zhukovsky[2]

USING AN EXPERIMENTAL ALGORITHM AS AN ELITE INDIVIDUAL IN SOLVING A HOMOGENEOUS MINIMAX PROBLEM

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: distributive NP-complete problem, homogeneous system, heuristic algorithm without returns, modified Goldberg model, crossover, mutation, computational experiments, multiple tasks, list algorithms, initial population.

In this paper, we consider the solution of a distributive problem for homogeneous systems using a heuristic algorithm without returns, a genetic model. To solve this problem, genetic, list and other heuristic algorithms have become widespread. An algorithm without returns based on the idea of the Romanovsky algorithm is proposed for solving a homogeneous minimax problem. Analytically, it is impossible to prove how much the experimental algorithm is better or worse than the list algorithms due to the complexity of the task. When solving the modified Goldberg model, an elite individual was used, where an experimental algorithm was used as an elite individual. A computational experiment was carried out, according to which conclusions were made.

Введение. В настоящее время широкое распространение и развитие получили вычислительные устройства с многопроцессорной архитектурой. Причём такие устройства могут входить в состав более сложных в организации многомашинных комплексов, позволяющие решать сложные вычислительные задачи путём распределения вычислительного процесса между вычислительными ресурсами. Однако в процессе распараллеливания

вычислительного процесса может возникнуть дисбаланс в загрузке доступных вычислительных ресурсов. Поэтому важной задачей является равномерное распределение загрузки всех вычислительных ресурсов. Решение этой задачи даёт использование алгоритмов составления расписаний. Построение оптимального расписания распределения заданий по процессорам относится к задачам -полным, т.е. трудоемкость решения распределительной задачи определяется по экспоненте как $O(n^m)$, где O – временная асимптотическая сложность алгоритма, а n и m – целые числа больше единицы, обозначающие количество устройств и заданий соответственно, которые задают размерность распределительной задачи nm. В рамках теории расписаний исследуются методы, позволяющие упорядочить последовательность выполнения совокупности работ таким образом, чтобы время выполнения задачи в целом было минимальным.

Постановка задачи. Задача теории расписаний для однородных систем обработки информации может быть сформулирована следующим образом. Имеется система обслуживания, состоящая из N независимых устройств $P = \{p_1, p_2, \dots, p_n\}$. На обслуживание поступает набор из M параллельных и независимых заданий $T = \{t_1, t_2, \dots, t_m\}$. $\tau(t_i, p_j)$ – длительность обслуживания задания t_i устройством p_j, определяется матрицей T_τ. При этом каждое задание должно выполняться хотя бы на одном из процессоров. В каждый момент времени отдельный процессор обслуживает не более одного задания и выполнение задания не прерывается для передачи на другой процессор. Необходимо определить такое распределение заданий по устройствам без прерываний, чтобы время выполнения всей совокупности заданий было минимальным. Задача составления расписания сводится к разбиению исходного множества заданий на n непересекающихся подмножеств, т.е $T_i: \forall\, i, j \in [1, n] \to T_i \cap T_j = 0$ и $\bigcup_{i=1}^{n} T_i = T$. Критерий минимизации времени завершения обслуживания заданий, является минимаксным критерием и определяется в следующем виде: $f = \max\limits_{1 \le j \le n} f_j \to min$, где $f_j = \sum_{\tau(t_i, p_j) \in T} \tau(t_i, p_j)$ – время завершения работы процессора p_j [1, 4, 11].

Методы решения распределительной задачи. Существует два класса методов решения распределительных задач: точный и приближенный. К точным методам можно отнести алгоритмы Романовского и Алексеева, а также алгоритм точного перебора. Второй класс содержит в себе различные списочные, эвристические, и др. К списочным методам можно отнести алгоритм критического пути, алгоритм Пашкеева, и др. Эвристические методы – генетические алгоритмы, метод отжига, метод роящихся частиц и др. Для получения оптимального решения однородной распределительной задачи используются точные методы решения. С увеличением размерности, в силу ее NP-полноты, а также при сужении диапазона ресурсных оценок распределяемых заданий оптимальное решение за доступное время может стать недостижимым. В этой ситуации приходится ориентироваться на быстрые, но приближенные методы, позволяющие получить решение близкое к оптимальному, такие, как генетические алгоритмы.

Списочные методы. В качестве метода нахождения приближенного решения можно использовать списочные методы, некоторые из них описаны ниже.

Первым списочным алгоритмом является алгоритм критического пути, который можно сформулировать следующим образом:

1. Задания матрицы загрузки упорядочиваются в порядке убывания значений элементов.
2. Текущее задание распределяется на прибор с наименьшей загрузкой. Если таких приборов несколько, то задание распределяется на прибор, стоящий слева.
3. Алгоритм заканчивает работу, когда все задания распределены по обработчикам.

Вторым списочным алгоритмом является алгоритм Пашкеева. Принцип его действия описывается так:

1. Задания матрицы загрузки упорядочиваются в порядке убывания значений элементов.

2. Оценивается загрузка на крайних обработчиках (первом и последнем).
3. Задания распределяются последовательно по N приборам начиная с крайнего с наименьшим значением нагрузки.
4. Алгоритм заканчивает работу, когда все задания распределены по обработчикам.

Экспериментальный списочный алгоритм основан на идее алгоритма Романовского, формулируется следующим образом:

1. Задания матрицы загрузки упорядочиваются в порядке убывания значений элементов.
2. Производим вычисление нижней границы поиска оптимального решения $Ua = \frac{\sum_{i=0}^{m} m_i}{n}$.
3. Верхняя же граница поиска Ub изначально равняется нижней.
4. Находим размер "Свободного места" по формуле $FR = (Ub * n) / \sum_{i=0}^{m} m_i$.
5. Последовательно назначаем задания обработчикам проверяя следующие условия: Нагрузка на устройство с назначенным заданием не должна быть больше верхней границы нагрузки. Или должно выполняться хотя бы одно из этих двух условий:
   - Значение обработчика с назначенными текущим и минимальным по значению заданием не должно превышать верхнюю границу нагрузки.
   - Разница между верней границей нагрузки и значением нагрузки процессора с помещенным заданием не должно превышать текущее значение "Свободного места".
6. Если условие выполняется, то помещаем задание на обработчик, удаляя его из множества заданий.
7. После прохода всего множества заданий проверяем суммарную нагрузку на процессор. Если нагрузка на процессор превышает верхнюю границу, то уменьшаем "Свободное место" на разницу между верней границей и нагрузкой процессора.
8. После прохода всех обработчиков проверяем, если осталось свободное место, то увеличиваем верхнюю границу на 1 и повторяем алгоритм, иначе выходим из алгоритма.

Модифицированная модель Голдберга. В качестве метода решения однородной минимаксной задачи может быть использован генетический алгоритм, а именно модифицированная модель Голдберга, которую можно описать следующей последовательностью шагов:

Шаг 1. Формируется начальное поколение, состоящее из заданного числа особей, сформированных случайно и/или же с использованием различных полиномиальных алгоритмов.

Шаг 2. Турнирный отбор особей и применение операторов кроссовера и мутации с известной вероятностью возникновения для создания нового поколения.

Шаг 3. Проверка условия конца работы алгоритма, которая обычно заключается в неизменности лучшего решения в течение заданного числа поколений. Если проверка прошла неуспешно, то переход на шаг 2.

Шаг 4. Лучшая особь выбирается как найденное решение [4,5,6].

Одна из модификаций модели Голдберга — стратегия элитизма. Стратегия элитизма подразумевает использование "элитной" особи для сохранения лучшего решения. В процессе кроссинговера и мутации элитная особь не изменяется, но участвует в формировании новых особей. Если в процессе нахождения решения появляется особь сильнее элитной, то она заменяет ее собой.

Элитные особи при формировании начального поколения могут формироваться различными способами, как случайно, так и с помощью различных приближенных алгоритмов.

В нижеописанном эксперименте для формирования элитной особи будут использоваться списочные методы, описанные выше. Для определения какой из алгоритмов лучше (т.е. дает решение более близкое к оптимальному) был проведен обширный вычислительный эксперимент, где в качестве элитных особей выступали решения, полученные как списочными алгоритмами, так и экспериментальным алгоритмом.

Вычислительный эксперимент. Для оценки эффективности алгоритмов был проведен вычислительный эксперимент с помощью программного средства написанного на языке программирования C#. В качестве аппаратного обеспечений использован ноутбук с процессором Intel Core i5-9300H и оперативной памятью объемом 16 гигабайт. В качестве исходных данных были использованы 200 случайно сгенерированных матриц размерностями $4,8,16,32 \times 251$ с диапазоном значений 15-25. В качестве критериев оценки используем средние значения результатов и среднее время.

Таблица 1. Усредненные значения результатов работы алгоритмов в первом случае

N*M	Модели генетических алгоритмов	Статистика	Алгоритмы формирования									
			Случайное формирование		Алгоритм критического пути (сортировка по убыванию)		Алгоритм критического пути (сортировка по возрастанию)		Алгоритм Пашкеева		Экспериментальный алгоритм	
			Без элитных особей	1 элитная особь	Без элитных особей	1 элитная особь	Без элитных особей	1 элитная особь	Без элитных особей	1 элитная особь	Без элитных особей	1 элитная особь
4*251	Модифицированная модель Голдберга	Среднее значение (Tmax)	1356.79	1356.845	1356.74	1356.645	1356.715	1356.685	1356.56	1356.635	1356.535	1356.535
		Среднее время (с)	9.6790611435	10.105605874	10.2545920455	9.4520971655	10.626522883	9.799377137	10.153537504	10.653504049	10.1181925945	10.11588862295
8*251		Среднее значение (Tmax)	631.77	631.51	631.755	631.475	631.755	631.75	631.74	631.605	630.64	630.62
		Среднее время (с)	11.80712932225	11.760787738	10.998396015	11.347194447	11.116594785	10.69059292	10.476114201	11.7665996105	7.1833922755	8.6343759485
16*251		Среднее значение (Tmax)	321.645	321.87	318.795	318.795	321.67	321.73	319.685	319.705	318.52	318.515
		Среднее время (с)	15.4963281205	15.647822705	8.9891913595	8.7966011	12.131735553	11.9121667965	9.709091128	10.0183177405	9.685999911	9.7231377815
32*251		Среднее значение (Tmax)	181.88	182.21	177.04	177.05	180.255	180.525	178.045	182.405	174.76	174.76
		Среднее время (с)	29.2616648705	28.4877941255	15.0634057565	14.9531110665	19.101618997	18.3306869875	15.3573379445	29.0191018565	13.9308058695	13.9912339615

Заключение.

Оценивая полученные результаты, можно сделать вывод об эффективности использования экспериментального алгоритма качестве метода формирования элитной особи в начальном поколении. На различных количествах заданий, он дает стабильно хороший результат.

СПИСОК ЛИТЕРАТУРЫ

1. *Головкин Б.А.* Расчет характеристик и планирование параллельных вычислительных процессов. Москва: Радио и связь, 1983. С. 216.
2. *Кобак В.Г.,* Титов Д.В. Исследование турнирного отбора в генетическом алгоритме для решения однородной минимаксной задачи // Математические методы в технике и технологиях — ММТТ — 21: сб. трудов Междунар. науч. конф. — Саратов. 2008. №.2. С. 12.
3. *Кобак В.Г.,* Поркшеян В.М., Кузин А.П. Использование различных вариантов мутации при решении неоднородной минимаксной задачи модифицированной моделью Голдберга // Научно-практический журнал «Аспирант». 2017. №10. С. 26-29.
4. *Аль-Хулайди А.А.,* Чернышев Ю.О. Разработка параллельного алгоритма нахождения оптимального решения транспортной задачи на кластере // Инженерный вестник Дона. 2011. №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/445/.
5. *Нетёсов А.С.* Эволюционно-генетический подход к решению задач оптимизации. Сравнительный анализ генетических алгоритмов с традиционными методами оптимизации // Инженерный вестник Дона. 2011. №3 URL: ivdon.ru/ru/magazine/archive/n3y2011/459/.
6. *Курейчик В. М.,* Кныш Д. С. Параллельный генетический алгоритм. Модели и проблемы построения // Интегрированные модели и мягкие вычисления в искусственном интеллекте: сб. науч. тр. V Междунар. науч.- практ. конф., Москва: Физматлит, 2009. С. 41-51.
7. *Goldberg D.* Genetic Algorithms In Search, Optimization, and Machine Learning. USA: Addison-Wesley Publishing Company, Inc., 1989. pp. 28-33.
8. *Affenzeller M.,* Wagner S., Winkler S., Beham A. Genetic Algorithms and Genetic Programming: Modern Concepts and Practical Applications. USA: CRC Press, 2009. P. 364.
9. *Каширина И.Л.* Введение в эволюционное моделирование. Воронеж, 2007. С. 40.
10. *Панченко Т. В.* Генетические алгоритмы. Астрахань: Астраханский университет, 2007. С. 87.
11. *Кобак В.Г.,* Шевченко В.В., Жуковский А.Г., Швидченко С.А. Использование различных подходов к формированию начального поколения в генетическом алгоритме при решении однородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 229-230.

В.Г. Кобак, Р.С. Шкабрий[1], А.Г. Жуковский, А.Н. Иванов[2]

РЕШЕНИЕ НЕОДНОРОДНОЙ МИНИМАКСНОЙ ЗАДАЧИ МОДИФИКАЦИЕЙ АЛГОРИТМА ПЛОТНИКОВА-ЗВЕРЕВА

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: Плотников–Зверев, генетический алгоритм, неоднородная минимаксная задача, матрица, строка, переменный барьер.

В данной работе исследуется модификация алгоритма Плотникова–Зверева «с двумя матрицами» для решения неоднородной минимаксной задачи. Был проведен вычислительный

эксперимент, который выявил преимущество использования данного алгоритма перед стандартным алгоритмом Плотникова – Зверева и его модификации «с переменным барьером».

V.G. Kobak, R.S. Shkabri[1], A.G. Zhukovsky, A.N. Ivanov[2]

SOLUTION OF AN INHOMOGENEOUS MINIMAX PROBLEM BY MODIFICATION OF THE PLOTNIKOV-ZVEREV ALGORITHM

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: Plotnikov-Zverev, genetic algorithm, heterogeneous minimax problem, matrix, string, variable barrier.

In this paper, we study a modification of the Plotnikov-Zverev algorithm "with two matrices" for solving an inhomogeneous minimax problem. A computational experiment was carried out, which revealed the advantage of using this algorithm over the standard Plotnikov-Zverev algorithm and its "variable barrier" modification.

В рамках данной работы рассматривается решение неоднородной минимаксной с использованием нескольких вариантов модификаций алгоритма Плотникова – Зверева. Был проведен вычислительный эксперимент, который выявил преимущество использования алгоритма «с двумя матрицами».

В связи с сильным ростом многопроцессорных систем, для которых важно решение большого объема задач за минимальное время, появилась необходимость эффективного распределения заданий по ресурсам. Данная задача является минимаксной задачей и относится к теории расписаний. Существуют различные алгоритмы для решения такой задачи, которые можно разделить на классы точных и приближенных. Точные алгоритмы выдают решение за непозволительно в большинстве случаев долгое время. В данной работе рассматриваются алгоритмы приближенных решений, такие алгоритмы дают приближенное к оптимальному решение за более короткое время в сравнении с точными алгоритмами.

Одним из таких способов является алгоритм, Плотникова-Зверева модификации которого рассматриваются в данной работе. Математическая постановка задачи приведена в работе [1,2,3].

Алгоритм рассматриваемы в данной работе является модификацией алгоритма «с переменным барьером» данный алгоритм подробно рассмотрен в работе [4,5]

Модифицированный алгоритм Плотникова-Зверева [6,7,8] с использованием двух матриц, одна из которых сформирована из строк не вписавшихся в барьер, можно описать в виде последовательности следующих шагов:

Шаг 1. Матрица заданий, сортируются в порядке убывания сумм элементов строк.

Шаг 2. В каждой строке находится минимальный элемент.

Шаг 3. Высчитывается барьер: сумма минимальных элементов каждой строки делится на количество процессов.

Шаг 4. Используется метод минимальных элементов до тех пор, пока один из столбцов не упрется в барьер.

Шаг 5. Строка, которая упирается в барьер формирует новую матрицу добавляясь в конец если матрица уже не пустая, если же матрица еще пустая, то становится первой строкой.

Шаг 6. Возвращаемся к шагу 4 до тех пор, пока не закончится начальная матрица загрузки.

Шаг 7. В результате выполнения образовалась новая матрица, которую распределяем алгоритмом Плотникова – Зверева учитывая результат прошлых шагов.

Рассмотрим данный алгоритм на примере матрицы загрузки, уже отсортированной в порядке убывания сумм строк, и изображенной на рисунке 1.

23	25	12
13	20	24
14	11	25
20	16	10
13	13	19
17	13	14
18	10	12
15	11	13
12	13	10

Рисунок 1. Начальная матрица загрузи

Барьер данного алгоритма равен (12+13+11+10++13+13+10+11+10)/3 = 34 На рисунке 2 изображены шаг 4 и шаг 5 алгоритма, описанного выше. В результате выполнения шагов 4 и 5 образовалась матрица изображенная на рисунке 3.

23	25	[12]
[13]	20	24
14	[11]	25
20	16	[10]
[13]	13	19
17	[13]	14
18	10	12
15	11	13
12	13	[10]
---	---	---
26	**24**	**32**

Рисунок 2. Выполнение шагов 4 и 5 алгоритма с двумя матрицами

18	10	12
15	11	13

Рисунок 3. Матрица, образованная в результате шагов 4 и 5

Данную матрицу распределяем алгоритмом Плотникова – Зверева с учетом выполнения прошлых шагов. Данный этап изображен на рисунке 4.

26	**24**	**32**
18	10	12
26	**34**	**32**
15	11	13
41	**34**	**32**

Рисунок 4. Распределение новой матрицы с учетом предыдущих шагов

Для определения эффективности данного алгоритма в сравнении с алгоритмом Плотникова – Зверева и его модификации с переменным барьером для нахождения приближенных решений минимаксной задачи был поставлен вычислительный эксперимент, позволяющий собрать статистику решений различными способами [9,10]. Для проведения

вычислительного эксперимента было написано программное средство на языке программирования C++ в среде разработки Microsoft Visual Studio 2019. В качестве аппаратного обеспечения использовался ноутбук с процессором Intel Core I5 9300H и ОЗУ 16 ГБ. Эксперименты проводились на 500 различных матрицах, усредненные результаты которых приведены в таблице 1.

Таблица 1. Результат вычислительного эксперимента

Алгоритм	M*N											
	3*53	3*153	3*253	4*53	4*153	4*253	5*53	5*153	5*253	6*53	6*153	6*253
Плотникова-Зверева	329	945	1560	234	667	1101	180	509	840	145	410	637
С переменным барьером	299	840	1381	212	586	959	163	445	728	132	358	583
С двумя матрицами	296	837	1376	209	582	955	160	442	724	129	355	579

Таким образом, обобщив результаты, приведенные в таблице 1, можно сделать вывод что модификация «с двумя матрицами» значительно превосходит по эффективности решения неоднородной минимаксной задачи стандартный алгоритм Плотникова – Зверева, а также превосходит модификацию этого алгоритма «с переменным барьером».

СПИСОК ЛИТЕРАТУРЫ

1. *Алексеев О.Т.* Комплексное применение методов дискретной оптимизации – М.: Наука, 1987г.
2. *Коффман Э.Г.* (ред.) Теория расписаний и вычислительные машины. – М.: Наука, 1984.
3. *Титов Д.В.,* Кобак В.Г. Анализ подходов к улучшению результатов работы генетического алгоритма при решении однородной минимаксной задачи. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей Всерос. научно-техн. конф.– Пенза: ПДЗ, 2008. – С. 76-78.
4. *Кобак В. Г.,* Жуковский А. Г., Шкабрий Р. С. Сравнительный анализ модификаций алгоритма плотникова-зверева по различным критериям с использованием барьера при решении минимаксной задачи //Известия высших учебных заведений. Северо-Кавказский регион. Технические науки. – 2021. – №. 1 (209).
5. *Кобак В. Г.,* Муратов М. А. Сравнительный анализ критериев эффективности при решении неоднородной минимаксной задачи списочным алгоритмом //Advanced Engineering Research. – 2011. – Т. 11. – №. 7.
6. *Кобак В.Г.,* Жуковский А.Г., Кузин А.П. Исследование применения одноточечного кроссовера при решении неоднородной минимаксной задачи, Электронный научный журнал //Инженерный вестник Дона. 2018. №1. URL: http://www.ivdon.ru/ru/magazine/archive/n1y2018/4714/.
7. *Кобак В. Г.*, Поркшеян В. М., Шкабрий Р. С., Швидченко С. А. Исследование алгоритма Плотникова-Зверева и его модификаций при решении неоднородной минимаксной задачи //Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2020. – №. 1. – С. 215-218.
8. *Кобак В. Г.,* Шкабрий Р. С., Жуковский А. Г., Колдынская Л. М. Исследование модификации алгоритма Плотникова-Зверева «с переменным барьером» при разных способах сортировки элементов //Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2020. – №. 1. – С. 223-225.

9. *Аль-Хулайди А.А.,* Чернышев Ю.О. Разработка параллельного алгоритма нахождения оптимального решения транспортной задачи на кластере // Инженерный вестник Дона. 2011. №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/445/. 249 Труды СКФ МТУСИ – 2020.
10. *Нетёсов А.С.* Эволюционно-генетический подход к решению задач оптимизации. Сравнительный анализ генетических алгоритмов с традиционными методами оптимизации // Инженерный вестник Дона 2011. №3 URL: ivdon.ru/ru/magazine/archive/n3y2011/459/.

В.Г. Кобак, А.Е. Кушнарева, С.А. Швидченко[1], Д.А. Жуковский[2]

РЕШЕНИЕ ЗАДАЧИ КОММИВОЯЖЕРА МОДИФИЦИРОВАННОЮ МОДЕЛЬЮ ГОЛДБЕРГА С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КРОССОВЕРОВ

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: задача Коммивояжера, генетический алгоритм, модель Голдберга, кроссовер, мутация.

В статье рассмотрено решение задачи Коммивояжера одноэтапной моделью Голдберга. Для генетического алгоритма использованы упорядоченный и измененный кроссоверы, мутация обменом. Разработано программное средство для анализа эффективности генетического алгоритма при различных кроссоверах.

V.G. Kobak, A.E. Kushnareva, S.A. Shvidchenko[1], D.A. Zhukovsky[2]

SOLVING THE TRAVELING SALESMAN PROBLEM WITH A MODIFIED GOLDBERG MODEL USING VARIOUS CROSSOVERS

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: traveling salesman problem, genetic algorithm, Goldberg model, crossover, mutation.

The article considers the solution of the Traveling Salesman problem by the one-stage Goldberg model. Ordered and modified crossovers, mutation by exchange are used for the genetic algorithm. A software tool has been developed to analyze the effectiveness of the genetic algorithm in various crossovers.

Введение

Задача Коммивояжера представляет собой одну из самых важных, практически значимых и классических задач комбинаторной оптимизации. Постановка задачи: необходимо найти самый быстрый и выгодный маршрут, включающий все пункты только один раз, при этом возвращаясь в исходную точку. Данная задача, берущая свое начало из работ Гамильтона, состоит в определении кратчайшего гамильтонова цикла в графе [1]. Задача Коммивояжера,

сформулированная в общем виде, часто встречается в таких сферах, где необходимо определить наименьшее упорядочение объектов или действий.

В данной статье рассматривается использование одноэтапного генетического алгоритма для решения задачи Коммивояжера для графа с 29 вершинами. Существуют следующие подходы к нахождению лучшего решения: метод ветвей и границ, полного перебора, динамическое программирование. Но поскольку задача Коммивояжера может быть решена не с любым количеством городов, вышеперечисленным подходам необходимо длительное время и большее количество вычислительной мощности. С увеличением количества городов увеличивается и количество различных вариантов обхода маршрута [2]. Задача Коммивояжера становится трансвычислительной, находящейся за пределами Бримерманна, при количестве городов, равном или превыщающем 66 [3].

Подходы решения

В рамках данной статьи предлагается использование одноэтапной модели Голдберга. Этапы работы модели Голдберга:

Этап 1. Формируется начальное поколение, которое состоит из заданного числа особей.

Этап 2. Отбор особей и применение ГА операторов кроссовера и мутации с заданной вероятностью для формирования нового поколения.

Этап 3. Проверка условия окончания работы алгоритма, заключающегося в неизменности лучшего решения в течение заданного количества поколений. При неуспешной проверке происходит переход на 2 этап.

Этап 4. Лучшая особь выбирается как найденное решение.

В данной работе хромосомы используют путевое представление [4], упорядоченный [4] и измененный кроссоверы [4], мутацию обменом.

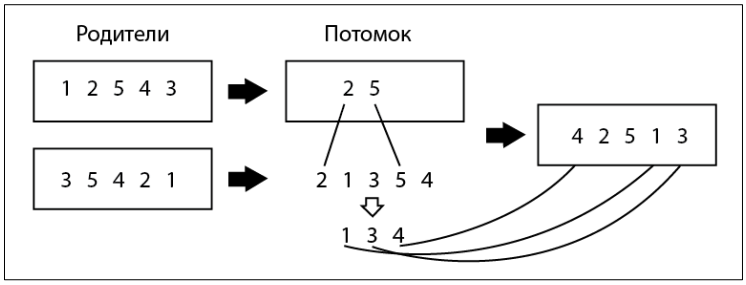


Рисунок 1. Схема упорядоченного кроссовера

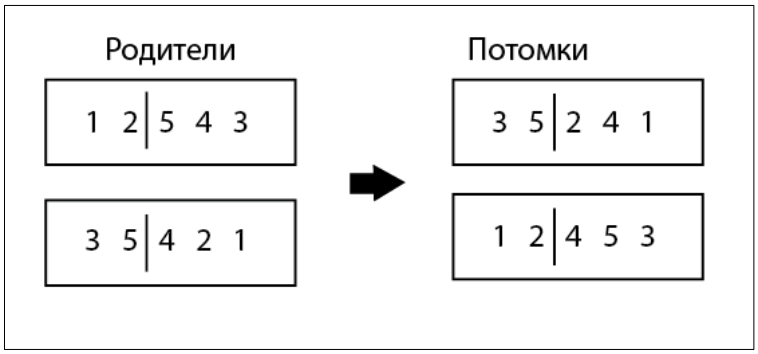


Рисунок 2. Схема измененного кроссовера

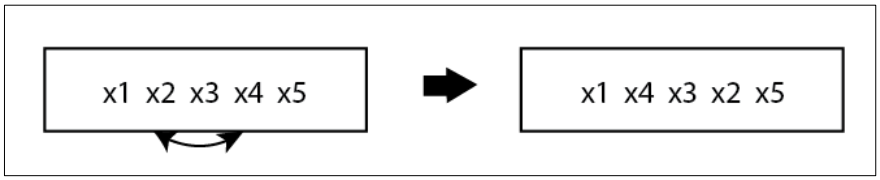


Рисунок 3. Схема мутации обменом

Вычислительный эксперимент

В данной статье был поставлен вычислительный эксперимент для оценки эффективности применения упорядоченного, измененного кроссоверов и их совместного действия в одноэтапной модели Голдберга для решения задачи Коммивояжера. Было разработано программное средство, которое позволило провести данный эксперимент.

Эксперимент был проведен на тестовом графе из пакета TSP_LIB [5,6,7,8], разработанного Гейдельбергским университетом, Гейдельберг, Германия. Был использован граф bayg29, длина оптимального маршрута которого составила 9074. Параметры генетического алгоритма: вероятность кроссовера – 100%, вероятность мутации – 100%, количество запусков – 50 раз. Количество особей и количество повторений до останова менялось для разных запусков и принимало следующи значения: 100, 300, 500, 1000.

На рисунке 4 представлены результаты одноэтапного генетического алгоритма при измененном, упорядоченном кроссовере и их совместном действии.

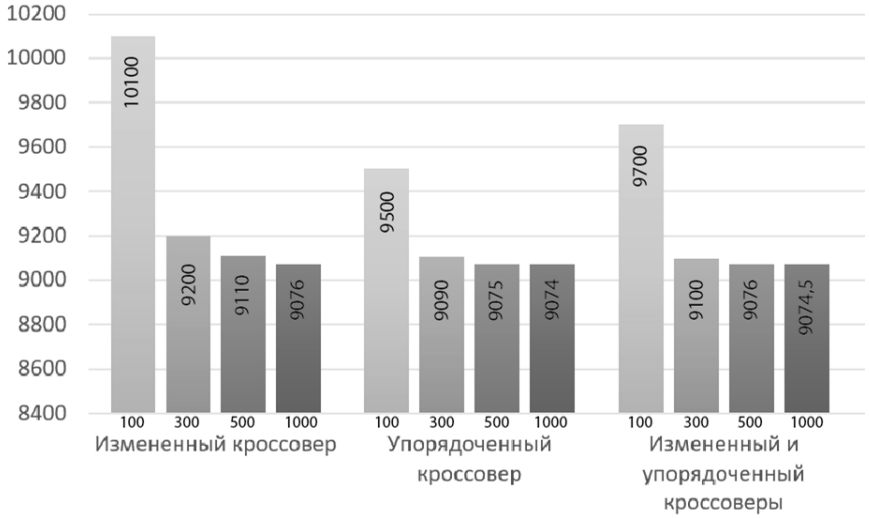


Рисунок 4. Результаты одноэтапного генетического алгоритма при различных кроссоверах

Можно заметить, как с ростом количества особей и количества запусков до останова улучшается точность результатов. Запуски с максимальным количеством особей позволяют добиться точного решения. При этом увеличивается время работы алгоритма. Время работы представлено на рисунке 5 и указано в минутах.

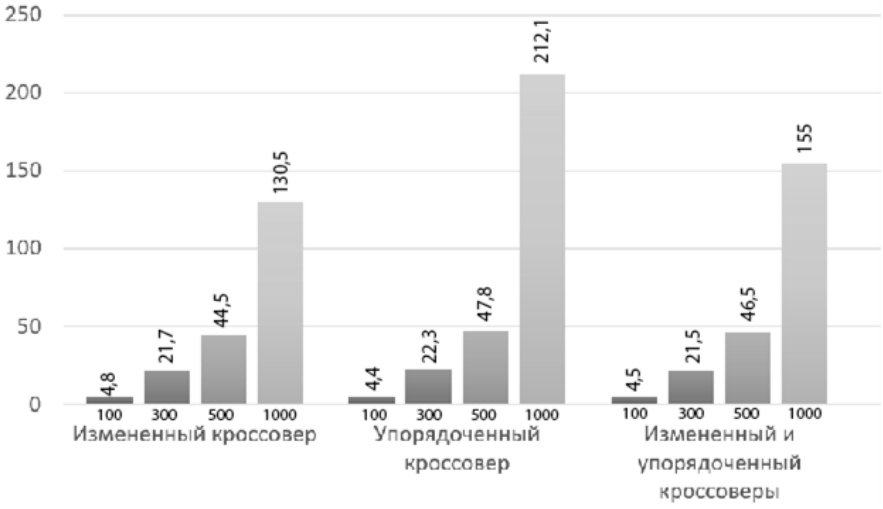


Рисунок 5. Время работы одноэтапного генетического алгоритма при различных кроссоверах

Из рисунков видно, что наилучшее решение получается при упорядоченном кроссовере. Однако данный кроссовер имеет самое долгое время выполнения генетического алгорима, которое и приводит к лучшему результату. Далее по эффективности следует совместное действие упорядоченного и измененного кроссоверов. Самым быстрым и самым неточным является измененный кроссовер.

Выводы

Проведенный с помощью разработанного программного средства вычислительный эксперимент показал эффективность использования различных кроссоверов при решении задачи Коммивояжера. Увеличение количества особей и количества запусков до останова приводит к росту точности решения и одновременно замедлению время работы алгоритма. Более близким к точному и более долгим является одноэтапный генетический алгоритм с упорядоченным кроссовером.

СПИСОК ЛИТЕРАТУРЫ

1. *Мудров В.В.* Задача о Коммивояжере. – М.: Книжный дом «ЛИБРОКОМ», 2019.
2. *Копец Д.* Классические задачи Computer Science на языке Python. – М.: Прогресс книга, 2021.
3. Optimization through evolution and recombination. Holtz.org URL: holtz.org/Library/Natural%20Science/Physics/Optimization%20Through%20Evolution%20and%20Recombination%20-%20Bremermann%201962.htm (дата обращения: 18.09.2021)
4. *Каширина И.Л.* Введение в эволюционное моделирование. – Воронеж: Воронежский государственный университет, 2007.
5. TSPLIB. The Zuse Institute Berlin (ZIB). URL: elib.zib.de/pub/mptestdata/tsp/tsplib/tsplib.html (дата обращения: 18.09.2021)
6. *Кобак В.Г.,* Поркшеян В.М., Шкабрий Р.С., Швидченко С.А. Исследование алгоритма плотникова-зверева и его модификаций при решении неоднородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 215-218.
7. *Кобак В.Г.,* Шевченко В.В., Жуковский А.Г., Швидченко С.А. Использование различных подходов к формированию начального поколения в генетическом алгоритме при решении однородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 229-230.
8. *Кобак В.Г.,* Кавтарадзе И.Ш., Бормотов В.В., Швидченко С.А. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 257-260.

В.Г. Кобак, В.М. Поркшеян, А.Е. Кушнарева[1], А.Г. Жуковский[2]

РЕШЕНИЕ ЗАДАЧИ КОММИВОЯЖЕРА МОДИФИЦИРОВАННОЮ МОДЕЛЬЮ ГОЛДБЕРГА С НАЧАЛЬНЫМ ПОКОЛЕНИЕМ, ФОРМИРУЕМЫМ ЭВРИСТИЧЕСКИМИ АЛГОРИТМАМИ

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: задача Коммивояжера, генетический алгоритм, модель Голдберга, кроссовер, мутация, эвристические методы

Рассмотрено решение задачи Коммивояжера модифицированной моделью Голдберга с формированием начальной популяции при помощи различных эвристических алгоритмов. Для генетического алгоритма были использованы измененный и упорядоченный кроссоверы, мутация обменом. Разработано программное средство для анализа эффективности формирования начального поколения эвристическими методами.

V.G. Kobak, V.M. Porksheyan, A.E. Kushnareva [1], A.G. Zhukovsky[2]

THE SOLUTION OF THE TRAVELING SALESMAN PROBLEM BY THE MODIFIED GOLDBERG MODEL WITH THE INITIAL GENERATION FORMED BY THE EVRISTIC ALGORITHMS

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: traveling salesman problem, genetic algorithm, Goldberg model, crossover, mutation, heuristic methods

The solution of the Traveling Salesman problem by the modified Goldberg model with the formation of the initial population using various heuristic algorithms is considered. Modified and ordered crossovers, mutation by exchange were used for the genetic algorithm. A software tool has been developed to analyze the effectiveness of the formation of the initial generation by heuristic methods.

Введение

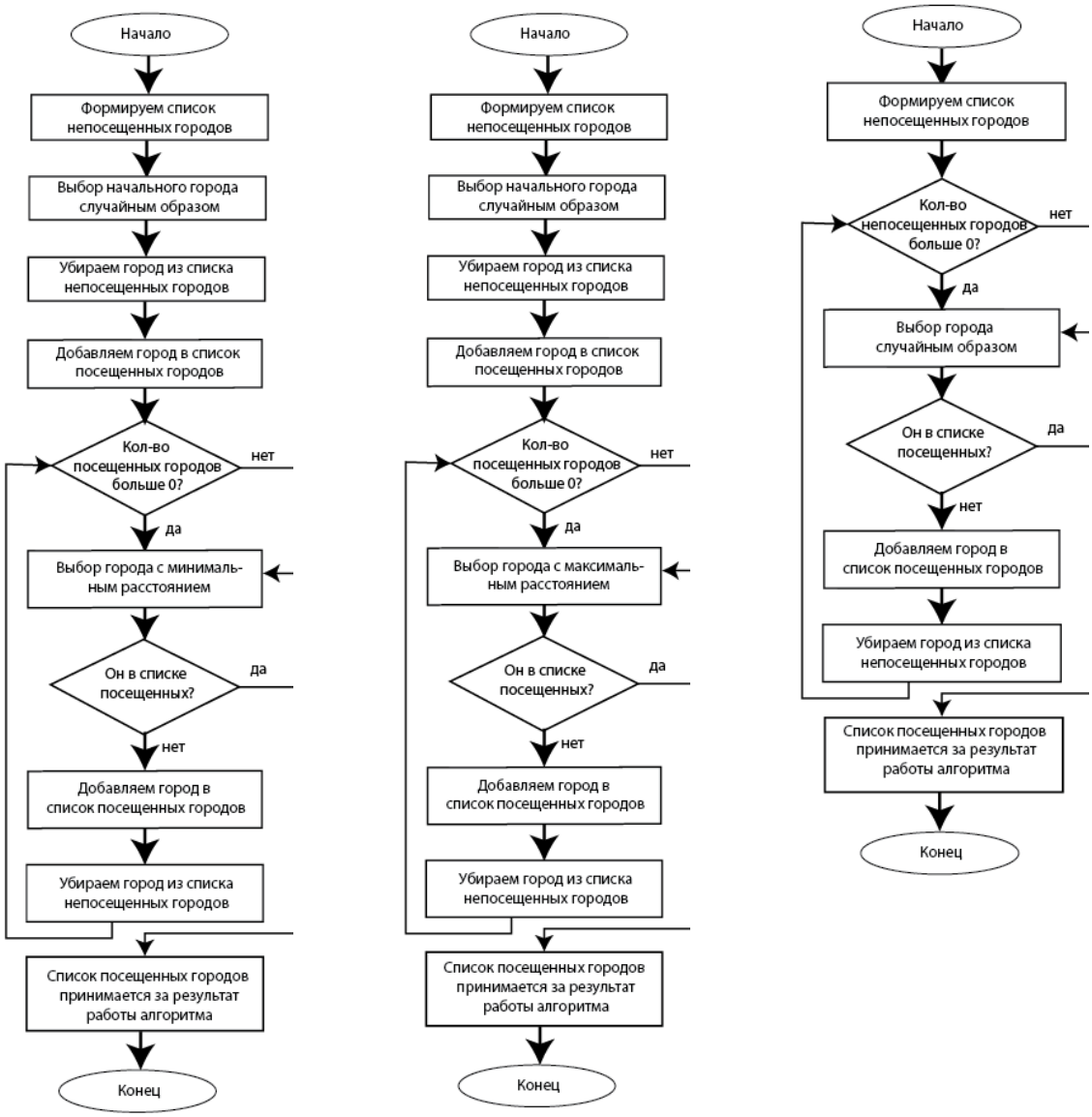
Задача Коммивояжера является NP – полной задачей. Она используется в исследовании операций, комбинаторной оптимизации, а также в теоретической информатике. Задача Коммивояжера задает следующий вопрос: «Какой самый кратчайший и возможный маршрут можно получить, учитывая список городов и расстояния между каждой парой городов, включая каждый город и возвращаясь в исходный?» [1]. Такие показатели как итоговое время в пути, суммарная длина маршрута принимаются в качестве меры выгодности маршрута. В своей классической формулировке данная задача используется в логистике, теории расписаний, планировании.

В данной статье рассматривается решение задачи Коммивояжера для графа с 51 вершиной модифицированной моделью Голдберга с начальным поколением, которое формируется при помощи эвристических алгоритмов. Генетические алгоритмы оперируют не решениями, как классические алгоритмы поисковой оптимизации, а некоторыми их кодировками, моделируя природные механизмы репродукции, естественного отбора и т.д. Эти

механизмы моделируются с помощью кроссоверов, мутаций и селекции. Эффективность генетического алгоритма зависит от таких деталей, как метод кодирования решений, выбор операторов [2,6,7,8,9]. Использование в генетических алгоритмах методов, которые позволяют повышать качество начальной популяции, существенно влияет на качество получаемых решений.

Подходы решения

В данной статье используется модифицированная модель Голдберга, которая представлена особым отбором особей для скрещивания и формирования нового поколения. Каждая особь имеет возможность принять участие в кроссовере. Для каждой особи партнер выбирается случайным образом, вместе они порождают пару потомков. Из первого родителя, участвовавшего в кроссовере, и его потомков выбирается лучшая особь, которая переходит в следующее поколение.



Рисунки 1 – 3. Блок – схемы работы эвристических алгоритмов

Рассмотрим этапы работы вышеописанной модели:

Этап 1. Формирование начального поколения из заданного числа особей (входного параметра).

Этап 2. Выбор пар особей скрещивания, кроссовера, мутации и отбора в следующее поколение.

Этап 3. Если количество поколений без изменения в лучшем значении больше конкретного значения (являющегося входным параметром), перейти ко 2 этапу (проверка условия завершения алгоритма).

Этап 4. Принятие лучшей особи в качестве решения.

В рамках данной статьи для формирования начального поколения предлагается использовать эвристические алгоритмы, которые также называются «жадными» эвристиками. Их особенность заключается в том, что в ходе создания решения, алгоритмы на каждом шаге стремятся добавить определенный и точный фрагмент, обеспечивающий оптимальный результат [3,7,8,9]. Имеются следующие эвристические алгоритмы:

1. Выбирается начальная вершина и каждый следующий раз с помощью жадного алгоритма берем вершину, до которой минимальное расстояние;
2. Выбирается начальная вершина и каждый следующий раз с помощью «жадного» алгоритма берем вершину, до которой максимальное расстояние;
3. Выбирается начальная вершина и каждый следующий раз с помощью «жадного» алгоритма берем случайную вершину.

В рамках данной работы используется путевое представление [4], измененный [4], упорядоченные кроссовер [4], а также мутация обменом [4].

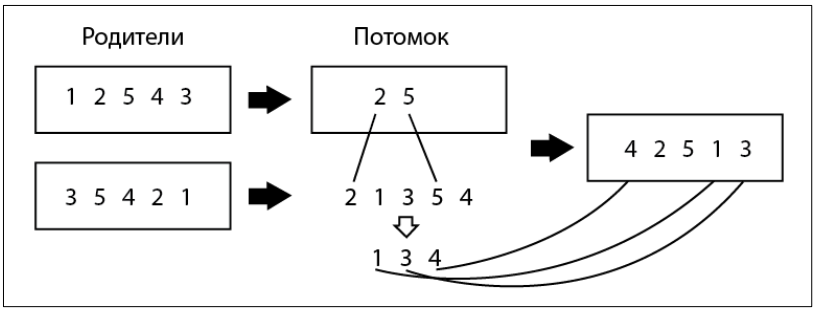


Рисунок 4. Схема упорядоченного кроссовера

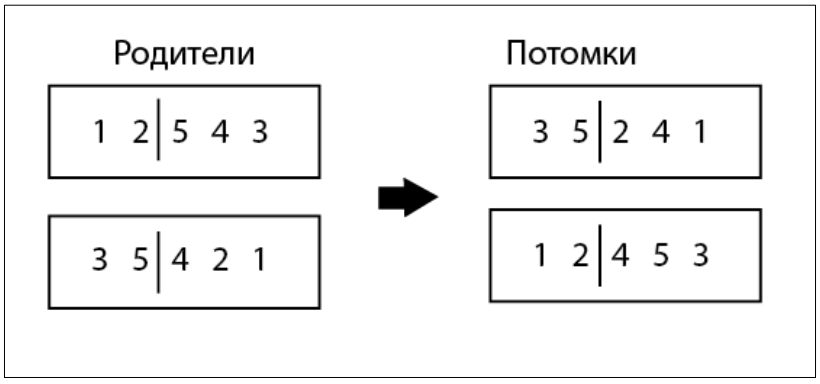


Рисунок 5. Схема измененного кроссовера

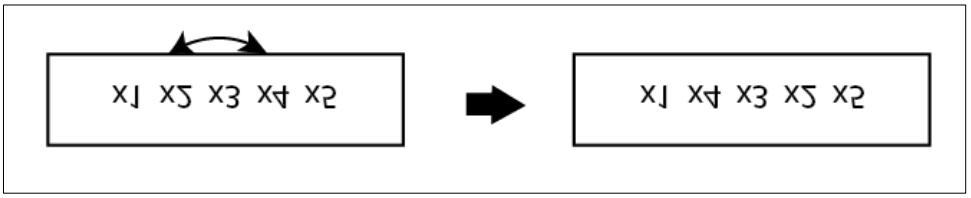


Рисунок 6. Схема мутации обменом

Вычислительный эксперимент

В данной статье был поставлен вычислительный эксперимент для оценки эффективности применения эвристических алгоритмов для формирования начального поколения в модифицированной модели Голдберга для решения задачи Коммивояжера. Для проведения данного эксперимента было разработано программное средство.

Эксперимент проводился на тестовом графе eil51 из пакета TSP_LIB, разработанного Гейдельбергским университетом, Гейдельберг, Германия. Длина оптимального маршрута для данного графа – 428.

Параметры генетического алгоритма: вероятность мутации – 100%, вероятность кроссовера - 100%, количество запусков – 50 раз. Количество особей до останова принимало значения 100, 300, 500, 1000.

Результаты вычислительного эксперимента представлены в виде трех таблиц. Каждая таблица имеет 4 столбца:

1. Распределения эвристических алгоритмов: 1111111…, 2222222…, 333333…, 123123…, 111222333… ;
2. Количество особей, количество повторов лучшего решения;
3. Время выполнения (в минутах);
4. Оптимальное решение.

Таблица 1. Результаты вычислительного эксперимента для измененного кроссовера

111111	100, 100	5	443 – 484 (в поколениях 129 – 520)
	300, 300	37	435 – 462 (в поколениях 352 – 1457)
	500, 500	129	433 – 458 (в поколениях 789 – 1885)
	1000, 1000	275	431 – 458 (в поколениях 1314 – 3229)
222222	100, 100	13	474 – 674 (в поколениях 451 – 1517)
	300, 300	79	437 – 525 (в поколениях 1186 – 3050)
	500, 500	155	434 – 500 (в поколениях 1291 – 3028)
	1000, 1000	243	433 – 474 (в поколениях 1853 – 4301)
333333	100, 100	20	475 – 670 (в поколениях 408 – 2327)
	300, 300	90	444 – 500 (в поколениях 1122 – 3074)
	500, 500	158	434 – 502 (в поколениях 1581 – 3860)
	1000, 1000	270	436 – 485 (в поколениях 1781 – 4229)
123123	100, 100	13	458 – 688 (в поколениях 345 – 1595)
	300, 300	82	433 – 516 (в поколениях 1054 – 3439)
	500, 500	180	436 – 499 (в поколениях 1569 – 4824)
	1000, 1000	255	437 – 480 (в поколениях 1699 – 3648)
111222333	100, 100	14	456 – 632 (в поколениях 441 – 1549)
	300, 300	85	439 – 488 (в поколениях 1311 – 3494)
	500, 500	147	433 – 488 (в поколениях 1367 – 3226)
	1000, 1000	263	435 – 488 (в поколениях 1768 – 4657)

Таблица 2. Результаты вычислительного эксперимента для упорядоченного кроссовера

111111	100, 100	4	432 – 507 (в поколениях 100 – 935)
	300, 300	87	431 – 463 (в поколениях 446 – 2058)
	500, 500	216	430 – 436 (в поколениях 1350 – 3264)
	1000, 1000	642	430 – 434 (в поколениях 1351 – 1851)
222222	100, 100	9	445 – 643 (в поколениях 352 – 1724)
	300, 300	123	430 – 467 (в поколениях 1360 – 2980)
	500, 500	223	428 (1 раз в поколении 2504) 430 – 454 (в поколениях 1716 – 3727)
	1000, 1000	602	428 (1 раз в поколении 4129) 431 – 455 (в поколениях 2112 – 5722)
333333	100, 100	12	444 – 597 (в поколениях 428 – 1639)
	300, 300	96	432 – 470 (в поколениях 1171 – 2356)
	500, 500	196	432 – 465 (в поколениях 1707 – 4534)
	1000, 1000	502	428 (1 раз в поколении 3930) 430 – 448 (в поколениях 1948 – 5156)
123123	100, 100	16	449 – 453 (в поколениях 320 – 1440)
	300, 300	64	433 – 463 (в поколениях 1287 – 3300)
	500, 500	205	431 – 453 (в поколениях 1412 – 4203)
	1000, 1000	620	428 (2 раза в поколениях 2630, 2819) 429 – 453 (в поколениях 1909 – 6156)
111222333	100, 100	20	440 – 639 (в поколениях 407 – 1721)
	300, 300	76	433 – 465 (в поколениях 1172 – 2669)
	500, 500	206	430 – 455 (в поколениях 1435 – 3405)
	1000, 1000	644	428 (1 раз в поколении 5417) 429 – 445 (в поколениях 2296 – 5700)

Таблица 3. Результаты вычислительного эксперимента для совместного действия измененного и упорядоченного кроссоверов

111111	100, 100	3	438 – 505 (в поколениях 100 – 596)
	300, 300	46	431 – 458 (в поколениях 507 – 1823)
	500, 500	189	431 – 443 (в поколениях 1196 – 2796)
	1000, 1000	306	431 – 440 (в поколениях 1505 – 3253)
222222	100, 100	12	448 – 587 (в поколениях 570 – 1594)
	300, 300	71	433 – 461 (в поколениях 1351 – 2590)
	500, 500	142	430 – 451 (в поколениях 1579 – 3057)
	1000, 1000	364	428 (1 раз в поколении 2599) 430 – 450 (в поколениях 2286 – 3822)
333333	100, 100	12	449 – 575 (в поколениях 411 – 1623)
	300, 300	77	431 – 466 (в поколениях 1367 – 2957)
	500, 500	169	428 (1 раз в поколении 1908) 430 – 462 (в поколениях 1648 – 3823)
	1000, 1000	324	428 (4 раза в поколениях 4278, 3370, 3453, 3774) 430 – 451 (в поколениях 2162 – 4701)
123123	100, 100	12	439 – 643 (в поколениях 288 – 1282)
	300, 300	103	431 – 472 (в поколениях 1374 – 2669)
	500, 500	141	430 – 458 (в поколениях 1498 – 3344)
	1000, 1000	312	430 – 447 (в поколениях 2451 – 4556)
111222333	100, 100	12	450 – 602 (в поколениях 386 – 1856)
	300, 300	108	430 – 462 (в поколениях 1379 – 3982)
	500, 500	148	430 – 453 (в поколениях 1595 – 3415)
	1000, 1000		428 (1 раз в поколении 2836) 430 – 449 (в поколениях 2114 – 4612)

Можно заметить, что с ростом количества особей и количества запусков до останова точность решений увеличивается. Эвристические алгоритмы улучшают начальную

популяцию, что позволяет добиться точного решения быстрее, чем если формировать начальное поколение случайным образом. Также качество решений при формировании начальной популяции случайным методом хуже, чем при использовании «жадных» алгоритмов.

Выводы

В ходе данной работы были предложены различные способы формирования начального поколения при помощи эвристических алгоритмов для решения задача Коммивояжера модифицированной моделью Голдберга. Вычислительный эксперимент, проведенный с помощью разработанного программного средства, показал, что выбор метода формирования начальной популяции оказывает влияние на качество решения, получаемого генетическим алгоритмом. При использовании «жадных» алгоритмов процент отклонения получаемого решения от оптимального (точного) значительно меньше.

СПИСОК ЛИТЕРАТУРЫ

1. Задача коммивояжера. Вопросы теории. URL: http://www.mathnet.ru/links/0438e576c6b3cd4ba389c93eb24bf1bc/at6414.pdf (дата обращения 05.10.2021)
2. *Батищев Д.И.,* Неймарк Е.А., Старостин И.В. Применение генетических алгоритмов к решению задач дискретной оптимизации. – Нижний Новгород: Инновационная образовательная программа ННГУ, 2007.
3. *Неймарк Е.А.* Улучшение качества начальной популяции эволюционно – генетического алгоритма для задача Коммивояжера. – Нижний Новогород: Инновационная образовательная программа ННГУ, 2017.
4. *Каширина И.Л.* Введение в эволюционное моделирование. – Воронеж: Воронежский государственный университет, 2007.
5. TSPLIB. The Zuse Institute Berlin (ZIB). URL: elib.zib.de/pub/mptestdata/tsp/tsplib/tsplib.html (дата обращения: 06.10.2021)
6. *Кобак В.Г.,* Поркшеян В.М., Шкабрий Р.С., Швидченко С.А. Исследование алгоритма плотникова-зверева и его модификаций при решении неоднородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 215-218.
7. *Кобак В.Г.,* Шевченко В.В., Жуковский А.Г., Швидченко С.А. Использование различных подходов к формированию начального поколения в генетическом алгоритме при решении однородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 229-230.
8. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.
9. *Кобак В.Г.,* Кавтарадзе И.Ш., Бормотов В.В., Швидченко С.А. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 257-260.

В.Г. Кобак, О.И. Цеменко, С.А. Швидченко[1], А.Г. Жуковский[2]

ИССЛЕДОВАНИЕ НЕОДНОРОДНОЙ МИНИМАКСНОЙ ЗАДАЧИ МОДИФИЦИРОВАННЫМ МОДЕЛЬЮ ГОЛДБЕРГА С ПОВТОРАМИ

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: неоднородная минимаксная задача, теория расписания, генетический алгоритм, модель Голдберга, скрещивание, мутация, турнирный отбор, повторы

Аннотация: рассматривается проблема решения неоднородной минимаксной задачи из теории расписания. Задача входит в класс NP-по млных, для которых до сих пор не найден точный алгоритм решения за полиноминальное время для большой размерности. В качестве возможного решения был выбран генетический способ, а именно модифицированная модель Голдберга. В этой модели используется принцип участия каждой особи в скрещивании с возможностью мутации и принцип турнирного отбора.

V.G. Kobak, O.I. Tsemenko, S.A. Shvidchenko[1], A.G. Zhukovsky[2]

INVESTIGATION OF AN INHOMOGENEOUS MINIMAX PROBLEM BY A MODIFIED GOLDBERG MODEL WITH REPETITIONS

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: heterogeneous minimax problem, schedule theory, genetic algorithm, Goldberg model, crossing, mutation, tournament selection, repetitions

Abstract: the problem of solving an inhomogeneous minimax problem from schedule theory is considered. The problem belongs to the class of NP-posets, for which an exact algorithm for solving in polynomial time for large dimension has not yet been found. A genetic method, namely a modified Goldberg model, was chosen as a possible solution. This model uses the principle of participation of each individual in crossbreeding with the possibility of mutation and the principle of tournament selection.

Введение

Распространенным случаем решения задач теории расписания являются NP-полные задачи, для которых нахождение точного решения невозможно за полиноминальное быстрое время [1]. Одну из таких мы рассмотрим в статье, а именно, неоднородную минимаксную задачу. Для решения был выбран один из самых распространенных способов решения – это генетический алгоритм.

Постановка задачи

Рассмотрим математическую постановку неоднородной минимаксной задачи. Имеется вычислительная система (ВС), состоящая из N независимых устройств (процессоров или приборов) $P = \{p_1, p_2, \ldots, p_n\}$. На обслуживание ВС поступает набор из M независимых параллельных заданий (работ) $T = \{t_1, t_2, \ldots, t_n\}$. Известно время $\tau(t_i, p_j)$ – длительность обслуживания задания t_i устройством p_j определяется матрицей T_τ. Приборы в общем случае не идентичны, задание t_i может быть обслужено любым из устройств, и устройство p_j может обрабатывать одновременно не более одного задания. Необходимо определить такое

распределение задания по устройствам, при котором общее время работы будет минимальным. Критерием минимизации времени выполнения заданий, является минимаксный критерий, который определяется в виде: $f = \max_{1 \le j \le n} f_j \rightarrow min$, где $f_j = \sum_{\tau(t_i,p_j) \in T} \tau(t_i, p_j)$ – время завершения работы устройства p_j.

Методы

Для решения поставленной задачи могут использоваться различные генетические модели. Но в данной работа будем рассматривать модель Голдберга и ее модификация. В модели Голдбегра каждая особь участвует в создании следующего поколения с возможностью мутации, позволяющей увеличить разнообразие особей, и бинарным турнирным отбором, благодаря которому улучшаются результаты работы алгоритма [2].

В данной работе будет рассматриваться классический одноточечный кроссовер [3, 4], изображенный на рисунке 1. Последовательно для каждой особи, которая будет являться основным родителем, случайным образом будет подбираться второй партнер, для получения двух потомков.

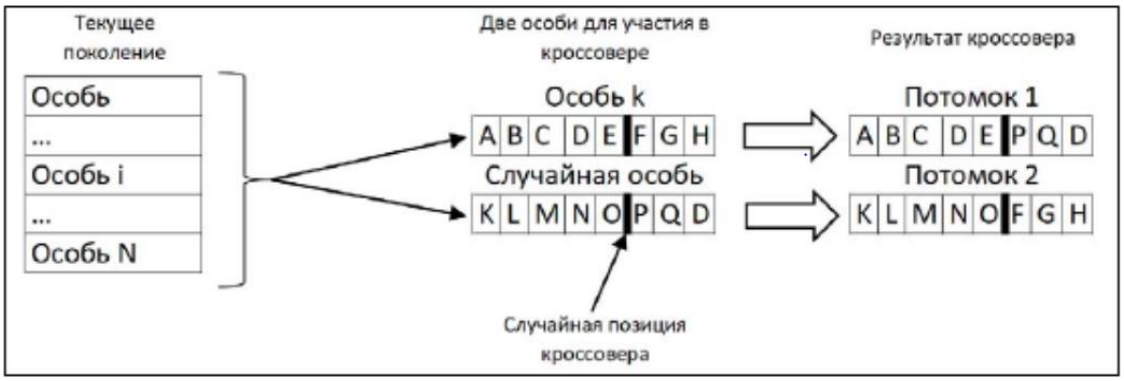


Рисунок 1. Одноточечный кроссовер

Для каждого полученного в результате кроссовера потомка, есть возможность мутации особи. Для мутации выбран классический одноточечный принцип, рисунок 2.

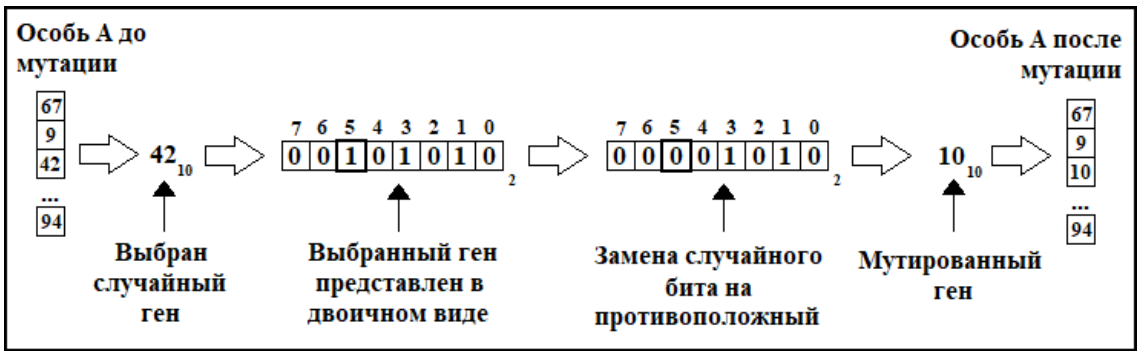


Рисунок 2. Одноточечная мутация

Алгоритм отбора работает следующим образом, из двух потомков выбирается тот, у которого время выполнения всех задач на устройствах будет минимальным, и, если выбранный потомок будет лучше основного родителя, то встает на его место в следующем поколении, в обратном случае, этот родитель переходит в следующее поколение [5,6,7,8]. Рассмотрим алгоритм пошагово:

1. Создаем начальное поколение, случайно задавая гены каждой особи.
2. Производим скрещивание для каждой особи и мутации потомков.
3. Путем отбора находим особь для следующего поколения.

4. Вычисляем для каждой особи время завершения работы всех её устройств и выбираем минимальное значение. Это значение лучший результат текущего поколения.
5. Проверяем условие окончания алгоритма, а именно, неизменность лучшего результата на протяжении заданного числа поколений. В обратном случае переходим к шагу 2.
6. Лучший результат последнего поколения фиксируем как решение.

Модификация модели Голдберга

В данной статье была выбрана модификация модели Голдберга повторами. Повтор – дополнительный запуск всего алгоритма, начиная от формирования нового начального поколения, заканчивая получением лучшего результата на протяжении заданного числа поколений, с целью утверждения полученного ранее результата. Повторы продолжаются до тех пор, пока новые полученные результаты будут хуже или равны текущему лучшему результату заданное число раз. В случае, если по время повторов будет найден результат лучше текущего, то счетчик повторов сбрасывается и процесс повторов начинается заново. Таким образом, такой подход позволяет получить более точное решение, за счёт уточнения результата.

Вычислительный эксперимент

Так как аналитически доказать, что повторы улучшают качество решения практически невозможно, для решения этой проблемы были поставлены вычислительные эксперименты с различными размерностями и количеством повторов.

Для вычислительного эксперимента было реализовано программное средство на языке Python. В рамках исследования оценивались такие параметры, как время поиска решения и полученный результат. Для каждого эксперимента было сгенерировано 50 матриц заполненные случайным образом, для получения усредненного результата, при 100% вероятности кроссовера и мутации. Количество работающих устройств N = 6, количество поступающих заданий M = 39. Время обработки задавалось случайно в диапазоне от 10 до 25.

Полученные результаты экспериментов представлены в таблицах 1 и 2. Столбец с 0 повторов отвечает за результаты не модифицированной модели Голдберга.

Таблица 1. Показания времени получения результата

		Повторы			
		0	1	2	3
Размерность	100	2.3	6.16	10.92	15.26
	300	16.764	42.78	71.38	96.32
	500	41.4	110.54	173.18	231.62

Таблица 2. Показания полученных результатов

		Повторы			
		0	1	2	3
Размерность	100	92.34	91.58	90.36	89.9
	300	87.02	85.76	84.98	84.66
	500	84.7	83.72	83.68	83.14

Как видно из таблицы 1, при увеличении числа повторов, время получения результата значительно возрастает по отношению экспериментом без повторов. Но при этом, из таблицы 2, можно заметить, что при увеличении повторов полученные результаты становятся более точными в каждой из размерностей.

Для более наглядного отображения, результаты представлены в виде гистограммы. На рисунке 3 показана гистограмма от времени получения результата, в минутах. На рисунке 4 изображена гистограмма полученных результатов.

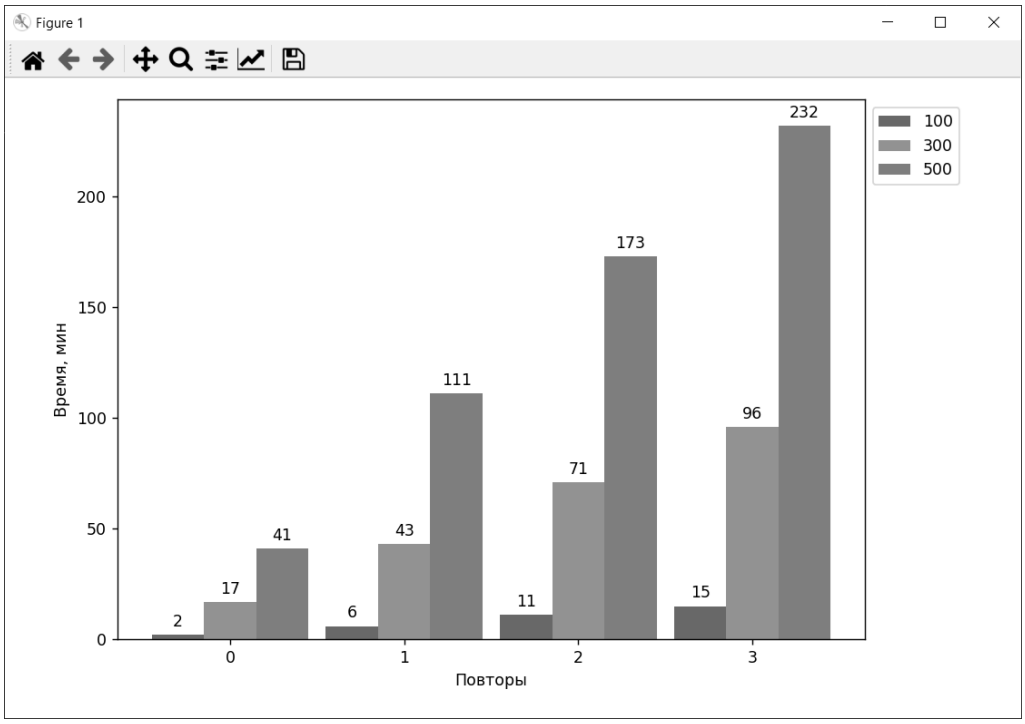


Рисунок 3. Гистограмма от времени получения результата

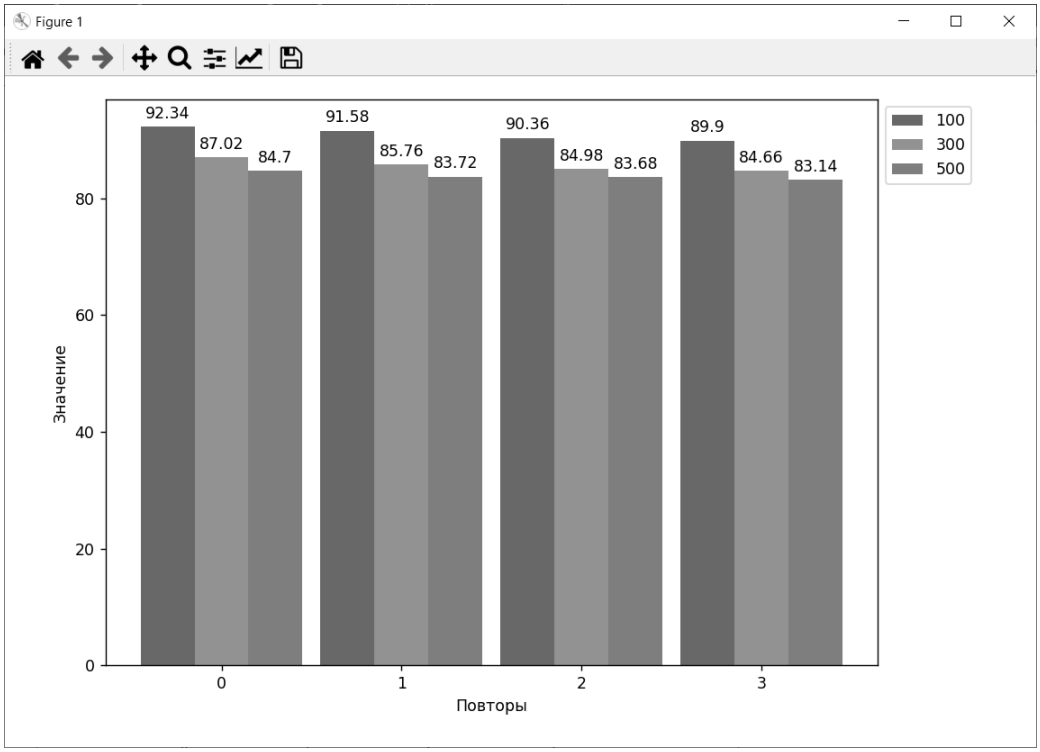


Рисунок 4. Гистограмма полученных результатов

Заключение.

1. С увеличением числа повторов, время для получения результатов значительно увеличивается.
2. С увеличением числа повторов, полученные результаты становятся более близкими к оптимальному решению.

СПИСОК ЛИТЕРАТУРЫ

1. *Алексеев О.Т.* Комплексное применение методов дискретной оптимизации. М.: Наука, 1987.
2. *Каширина И.Л.* Введение в эволюционное моделирование. Воронеж, 2007, 40с.
3. *Кобак В.Г.,* Жуковский А.Г., Кузин А.П. Исследование применения одноточечного кроссовера при решении неоднородной минимаксной задачи //Инженерный вестник Дона, 2018, №1. URL: ivdon.ru/ru/magazine/archive/n1y2018/4714.
4. *Кобак В.Г.,* Жуковский А.Г., Кузин А.П., Тхазаплижева А.Н. Подход к уменьшению времени работы модифицированной модели Голдберга при решении неоднородной минимаксной задачи //Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5665.
5. *Кобак В.Г.,* Жуковский А.Г., Кузин А.П., Исследование модификаций турнирного отбора при решении неоднородной минимаксной задачи модифицированной моделью Голдберга. //Инженерный вестник Дона, 2018, №2. URL: ivdon.ru/ru/magazine/archive/N2y2018/496.
6. *Кобак В.Г.,* Поркшеян В.М., Шкабрий Р.С., Швидченко С.А. Исследование алгоритма плотникова-зверева и его модификаций при решении неоднородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 215-218.
7. *Кобак В.Г.,* Шевченко В.В., Жуковский А.Г., Швидченко С.А. Использование различных подходов к формированию начального поколения в генетическом алгоритме при решении однородной минимаксной задачи. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 229-230.
8. *Кобак В.Г.,* Кавтарадзе И.Ш., Бормотов В.В., Швидченко С.А. Решение задачи коммивояжера модифицированной моделью голденберга с помощью различного вида мутаций. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 257-260.

О.В. Моногаров, И.В. Решетникова

СЛУЖБА ОПЕРАТИВНОЙ ПОМОЩИ ГРАЖДАНАМ ПО ЕДИНОМУ НОМЕРУ «122»

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: единый номер «122», контакт-центр, Служба оперативной помощи гражданам, COVID-19.

В статье рассматривается состав и работа Службы оперативной помощи гражданам по единому номеру «122».

O.V. Monogarov, I.V. Reshetnikova

OPERATIONAL ASSISTANCE SERVICES TO CITIZENS BY A SINGLE NUMBER «122»

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

Keywords: single number «122», contact center, Operational Assistance Service for citizens, COVID-19.

The article discusses the composition and work of the Operational Assistance Service for citizens by a single number «122».

В условиях распространения новой коронавирусной инфекции COVID-19 организована деятельность службы оперативной помощи гражданам по единому номеру «122». Данная Служба (структура) реализует комплекс взаимосвязанных организационных, кадровых, информационно-технологических, телекоммуникационных и технических ресурсов. Комплекс направлен на выполнение мероприятий по информированию граждан об оказании медицинской помощи гражданам в условиях распространения новой коронавирусной инфекции COVID-19.

Короткий телефонный номер «122» появился в РФ в конце ноября 2020 года. Крупнейшие российские операторы уже тогда сделали звонки на него бесплатным. В Постановление 18 января 2021 года №11, подписанным Председателем Правительства Михаилом Мишустиным, за операторами закрепили обязанность обеспечить бесплатный вызов на единый номер «122». Документ разработало Минцифры. Такое поручение дал Михаил Мишустин по итогам заседания президиума Координационного совета по борьбе с распространением COVID-19, состоявшегося 29 декабря 2020 года.

Например, в Санкт-Петербурге Служба «122» была запущена в эксплуатацию еще в апреле 2020 года и была ориентирована на оказание круглосуточной информационной поддержки по вопросам противодействия COVID-19. В Санкт-Петербурге есть возможность позвонить в Службу «122» из социальной сети «Одноклассники». Это можно сделать как с мобильного устройства, так и с персонального компьютера.

Служба состоит из Региональных контакт-центров и Федерального контакт-центра. Региональный контакт-центр организован в каждом субъекте РФ с целью обеспечения информационного взаимодействия Службы с гражданами. Федеральный контакт-центр предназначен для приема вызовов в случае недостаточности ресурсов Службы на уровне субъекта Российской Федерации.

Служба ставит перед собой такие цели и задачи, как:

- обеспечение удобного и бесплатного канала для телефонных обращений граждан по вопросам организации оказания медицинской помощи, вопросам записи на прием к врачу и вызова на дом, правилах вакцинации от COVID-19;
- обеспечение установленного норматива времени соединения позвонившего гражданина с оператором Службы;
- повышение удовлетворенности граждан качеством предоставленных по телефону консультаций по вопросам получения медицинской помощи и сервисов, вызова врача на дом, записи на прием к врачу и организации сдачи тестов на выявление COVID-19, а также других вопросов, связанных с вакцинацией от COVID-19.

Порядок организации и работы Службы в регионе определяется высшим должностным лицом субъекта РФ.

В состав службы входят:

- Министерство здравоохранения РФ. Оно обеспечивает методическую поддержку Службы по вопросам организации медицинской помощи гражданам, в том числе в части разработки типовых ответов (сценариев) оказания консультаций и сервисов на базе Службы;
- Министерство цифрового развития, связи и массовых коммуникаций РФ, которое осуществляет координацию действий операторов связи по подготовке инфраструктуры сети связи общего пользования для обеспечения работы единого номера «122» во всех субъектах РФ и обеспечивает функционирование Федерального контакт-центра. Организует запуск систем распределения и обработки вызовов, поступающих в Службу, на базе ВАТС (Виртуальная автоматическая телефонная станция) в регионах, не имеющих таких систем. ВАТС – цифровой сервис, осуществляющий функции автоматической телефонной станции, предоставляющий возможность организовать сеть с использованием пользовательского оборудования на базе сервисной платформы с выделением номеров в коде АБС и 8-800;
- Уполномоченный орган исполнительной власти субъектов РФ. Он координирует работы, проводимые в субъекте РФ по созданию Службы и внедрению систем распределения и обработки вызовов, поступающих в Службу;
- Органы исполнительной власти субъекта РФ, обеспечивающие комплектование Службы, формирование необходимой инфраструктуры рабочих мест сотрудников, подключаемых к системе распределения и обработке вызовов, поступающих в Службу, внедрение скриптов оказания консультаций и предоставления услуг позвонившим гражданам, а также контроль качества оказанных сервисов;

- Руководители медицинских организаций, подведомственных органам исполнительной власти субъектов РФ в сфере охраны здоровья, а также иных медицинских организаций, участвующих в реализации территориальной программы обязательного медицинского страхования (организует работу сотрудников, ответственных за прием и обработку вызовов, оказание консультаций и предоставление информации позвонившим гражданам).

Граждане могут обратиться в Службу при помощи телефонного звонка на номер «122», на номер «горячей» линии COVID-19, созданный в субъекте РФ, а также на местные номера медицинских организаций, подведомственным органам исполнительной власти субъектов РФ в сфере охраны здоровья. Далее оператор связи, действующий в регионе, обеспечивает маршрутизацию входящих вызовов на местные номера государственных медицинских организаций, на единый номер «122». В случае превышения времени ожидания ответа в 60 секунд происходит автоматическое перенаправление вызовов.

Входящий звонок может обрабатываться по следующим сценариям или их сочетаниям:

- интерактивным голосовым меню (ИГМ);
- виртуальным онлайн-консультантом (голосовой чат-бот), голосовым чат-ботом, в том числе с использованием искусственного интеллекта, для автоматизированной обработки речи (при наличии технической возможности);
- уполномоченным оператором Службы.

Интерактивное голосовое меню (ИГМ) – это сервис, предназначенный для выбора позвонившим гражданином сценария обслуживания с использованием тонального набора номера. При формировании настроек меню ИГМ могут использоваться следующие варианты:

«1» - консультация по вопросам получения медицинской помощи;

«2» - запись к врачу;

«3» - вызов врача на дом;

«4» - организация получения результатов проведения лабораторных исследований;

«5» - жалобы по вопросам организации медицинской помощи;

«6» - информация о правилах вакцинации от COVID-19;

«О» - соединение с оператором Службы.

Если гражданин не выбрал сценарий обслуживания, вызов автоматически переключается на оператора Службы.

Например, в Москве с 21.04.21 в сетях местной телефонной связи и сетях подвижной радиотелефонной связи обеспечивается маршрутизация вызовов экстренных оперативных служб по единому номеру «112» в Систему-112, а также на номера соответствующих экстренных оперативных служб: «101», «102», «103», «104». А в сетях местной телефонной связи используется действующий формат набора номера – двузначные номера: «01», «02», «03», «04».

Как писалось ранее, Федеральный контак-центр предназначен для приема вызовов на номер «122» в случае недостаточности ресурсов Регионального контакт-центра. Автоматическое перенаправление вызовов обеспечивается в случае превышения времени ожидания ответа оператора свыше 120 секунд или в случае, если заняты все каналы Регионального контакт-центра Службы. Задачами Федерального контакт-центра являются информирование граждан по вопросам организации медицинской помощи и прием жалоб на невозможность дозвониться в Службу Регионального контакт-центра. Заявки об инцидентах направляются в Региональные органы исполнительной власти через Платформу обратной связи.

В состав Службы на Региональном уровне могут входить операторы из числа сотрудников государственных медицинских организаций субъекта РФ, участвующие в приеме и обработке телефонных вызовов, а также операторы привлекаемых центров телефонного обслуживания граждан. Также в состав Службы на временной основе могут включаться волонтеры. Для обеспечения требуемого качества сервиса число операторов может быть скорректирована с учетом эпидемиологической ситуации и динамики нагрузки на Службу. Рабочие места операторов Службы должны быть:

- подключены к системе распределения и обработки вызовов, поступающих на номер «122» и местные телефонные номера медицинских и иных организаций, служб 103 и 112;
- обеспечены необходимым компьютерным и сетевым оборудованием, с защищенным доступом к сети Интернет, организованном в соответствие с требованиями законодательства РФ в сфере защиты персональных данных и защиты критической информационной инфраструктуры;
- подключены к специальному программному обеспечению региональных медицинских информационных систем.

В организации деятельности Регионального контакт-центра применяется система распределения и обработки вызовов на базе технологий ВАТС, которые предоставляют возможность организовать сеть связи с использованием пользовательского оборудования на базе сервисной платформы с выделением номеров в коде АБС и 8-800. Задачами системы распределения и обработки вызовов являются:

- распределение нагрузки телефонных вызовов в соответствие с заданными Службы правилами;
- обеспечение гарантированного дозвона граждан до оператора Службы;
- балансировка загрузки оператора Службы, отвечающих за прием и обработку вызовов граждан;
- возможность перенаправления вызовов граждан на номера медицинских организаций, служб психологической поддержки и других прочих служб субъекта РФ.

У оператора Службы доступны следующие функциональные возможности:

- прием входящих вызовов из сетей общего пользования;
- исходящие голосовые вызовы в сети общего пользования;
- обратный дозвон до позвонившего в Службу в случае, если позвонивший прекратит вызов (положит трубку, даст отбой), а также в случае разрыва соединения;
- управление очередью вызовов;
- запись и хранение разговоров с возможностью прослушивания и сохранения файлов с записями;
- переключение на операторов Службы.

Служба оперативной помощи гражданам в условиях распространения новой коронавирусной инфекции предполагает огромную работу, требующую определенных материальных и физических затрат, а также кадровых, организационных и технических ресурсов. Пандемия COVID-19 стала причиной серьезных социально-экономических последствий. Создание Службы оперативной помощи – это ликвидация последствий заболевания, поэтому необходимо направлять все ресурсы на его предотвращение.

СПИСОК ЛИТЕРАТУРЫ

1. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Приказ Минцифры России №37 «Об использовании единого номера «112» на территории города федерального значения Москвы в целях обеспечения вызова экстренных оперативных служб пользователями услугами связи» https://digital.gov.ru/ru/documents/7730/
2. Правительство России. Принцип бесплатности звонков на единый номер 122 Постановление от 18 января 2021 года №11 http://government.ru/docs/41346/
3. Комитет по информатизации и связи Единая региональная информационно-справочная служба «122» https://www.gov.spb.ru/gov/otrasl/c_information/news/197737/
4. Показатель уровня обслуживания в контакт-центрах Решетникова И.В., Иевлева Д.А. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 1. С. 248-250

В.В. Стромилов

РЕАЛИЗАЦИЯ НАЦИОНАЛЬНОЙ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА» НА СОВРЕМЕННОМ ЭТАПЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: национальные программы, цифровая экономика, цифровизация экономики, информационные технологии, новые технологии.

В статье представлены задачи и принципы реализации национальной программы «Цифровая экономика» и её структура, рассмотрены результаты по её выполнению и перспективы её выполнения в будущем.

V.V. Stromilov

THE REALIZATION OF THE NATIONAL PROGRAM “DIGITAL ECOMONY” AT THE PRESENT STAGE

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

Keywords: national program, digital economy, digitalization of the economy, information technology, new technologies.

The article considers tasks and principles of the implementation of the national program "Digital Economy" and its structure, the results of its implementation and the prospects for its implementation in the future are considered.

1. Введение

Активное внедрение цифровых технологий в разнообразные сферы жизни началось ещё в конце XX века в связи с их активным развитием. Экономика не стала исключением. Цифровизация общественной жизни и государства в целом и экономики в частности на данный момент играет существенную роль не в последнюю очередь из-за пандемии COVID-19, вынудившей множество предприятий перевестись на удалённый режим работы. Цифровые сервисы смогли смягчить последствия пандемии. Меры по цифровизации экономики проводятся в большинстве развитых стран мира, и в том числе и России. Национальная программа (сокращённо – нацпрограмма) «Цифровая экономика» (она же национальный проект (сокращённо – нацпроект) «Цифровая экономика») была утверждена 24 декабря 2018 года на заседании президиума Совета при Президенте России по стратегическому развитию и национальным проектам в рамках выполнения указа президента РФ от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Данная программа входит в состав направления по нацпроектам «Экономический рост». Срок действия данной программы начался 1 октября 2018 года. Данная статья ставит целью рассмотрение национальной программы и результатов её реализации на практике.

Рисунок 1. Логотип национальной программы «Цифровая экономика»

Система управления программы была утверждена постановлением Правительства РФ от 2 марта 2019 г. №234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации».

a. Президиум Совета при Президенте Российской Федерации Российской Федерации по стратегическому развитию и национальным проектам – рассматривает и утверждает паспорт национальной программы, также рассматривая запросы на его изменения (за исключением запросов на изменение

паспорта нацпрограммы, утвержденных Президиумом комиссии) и документы мониторинга по реализации как и самой нацпрограммы, так и федеральных проектов данной программы.

b. Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности – рассматривает и утверждает предложения по новым федеральным проектам нацпрограммы;
c. Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности – рассматривает и одобряет проект паспорта национальной программы «Цифровая экономика», а также запросы на его изменение и итоговый отчет о реализации нацпрограммы
d. Куратор нацпрограммы и входящих в её состав федеральных проектов – Д. М. Чернышенко, заместитель Председателя Правительства РФ
e. Подкомиссия по развитию искусственного интеллекта Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности
f. Автономная некоммерческая организация (сокращённо – АНО) «Цифровая экономика» – обеспечивает продуктивное взаимоотношение бизнеса и государства в рамках реализации нацпрограммы
g. Центры компетенции – определяются вышеупомянутой некоммерческой организации, обеспечивают сбор предложений в проекты паспортов федеральных проектов нацпрограммы и готовят проекты паспортов в целом
h. Рабочие группы – готовят предложения и проекты и заключения на проектов паспортов федеральных проектов нацпрограммы, рассматривают итоговые отчёты о реализации нацпрограммы и выполняют её мероприятия.
i. Руководитель нацпрограммы – М. И. Шадаев, министр цифрового развития, связи и массовых коммуникаций РФ
j. Администратор нацпрограммы – Н. С. Яцеленко, заместитель министра цифрового развития, связи и массовых коммуникаций РФ

2. Федеральные проекты в составе национальной программы «Цифровая экономика». Нацпрограмма включает следующие федеральные проекты:

- «Нормативное регулирование цифровой среды»
- «Кадры для цифровой экономики»
- «Информационная инфраструктура»
- «Информационная безопасность»
- «Цифровые технологии»
- «Цифровое государственное управление»
- «Искусственный интеллект»

Федеральный проект «Нормативное регулирование цифровой среды» предусматривает поэтапную разработку и дальнейшую законодательных инициатив по правовому регулированию цифровой экономики и преодолению первоочередных барьеров, препятствующих её развитию, таким образом, благоприятствуя развитию современных технологий и ведения бизнеса с их помощью. Также проект предлагает урегулировать идентификацию субъектов правоотношения, электронного документооборота, сбора, хранения и обработки данных.

Проект «Кадры для цифровой экономики» призван содействовать увеличению уровня цифровой грамотности населения, освоению ключевых компетенций цифровой экономики.

Предполагается, что к 2024 году будет выстроена преемственная на всех уровнях система образования, включающая поддержку талантов в области информатики и математики, подготовку высококвалифицированных кадров в тех же областях, отвечающих современным требованиям; реализацию образовательных проектов и программ переподготовки по востребованным профессиям в условиях цифровой экономики. В рамках данного федерального проекта реализуются такие проекты, как «Цифровые профессии» (получение дополнительного ИТ-образования в виде 24 направлений образовательных программ от популярных ИТ-организаций и образовательных учреждений), «Готов к цифре» (сайт-агрегатор по тестированию владения цифровой грамотностью и обучению эффективной работе с цифровыми технологиями), «CDO» (образовательная программа по получению новых цифровых компетенций у представителей региональных и федеральных властей по выполнению нацпрограммы «Цифровая экономика» и заинтересованных в цифровом развитии руководителей и менеджеров крупных предприятий и представителей промышленных и научных организаций). Руководителем данного проекта является заместитель Министерства цифрового развития, связи и массовых коммуникаций Н. С. Яцеленко.

Федеральный проект «Информационная инфраструктура» ставит своей целью создание безопасной и конкурентноспособной инфраструктуры высокоскоростной передачи данных по стране, обеспечение широкополосным доступом к Интернету (в т.ч. сетей 5G) социально значимых объектов (сокращённо – СЗО), в малонаселённых и труднодоступных населённых пунктов (реализация будет осуществляться путём установки точек доступа беспроводного интернета (Wi-Fi) и сотовой связи) и эффективное и безопасное пользование онлайн-сервисами. Руководителем данного проекта является заместитель Министерства цифрового развития, связи и массовых коммуникаций Д. М. Ким.

Проект «Информационная безопасность», как уже ясно из названия, ставит своей целью обеспечение устойчивой инфраструктуры по обеспечению информационной безопасности на территории России, сокращения уровня киберпреступности, предотвращение отставания России на рынке ПО по обеспечению информационной безопасности и дальнейшее развитие конкурентоспособности отечественных разработок и технологий в мировом масштабе, обеспечение высококвалифицированными кадрами в сфере информационной безопасности. Руководителем данного проекта является заместитель Министерства цифрового развития, связи и массовых коммуникаций Д. В. Реуцкий.

Ключевой целью федерального проекта «Цифровые технологии» является обеспечение технологической независимости государства, ускорение технологического развития отечественных компаний, обеспечение конкурентоспособности отечественных разработок в области цифровых технологий на мировом рынке. Проект ставит своими задачами создание благоприятных условий для развития стартапов в области цифровых технологий, развитие перспективных высоких технологий вроде квантовых технологий и сетей 5G и поддержка отечественных компаний-лидеров в области ИТ. Руководителем проекта является заместитель Министерства цифрового развития, связи и массовых коммуникаций М. В. Паршин.

Проект «Цифровое государственное управление» ставит своей целью увеличение доли массовых услуг (как государственных услуг (сокращённо – госуслуг), так и муниципальных), доступных в электронном виде до 95% к 2030 году. Мероприятия по реализации данной цели осуществляется по трём направлениям: обеспечением граждан удовлетворённостью пользования массовых услуг в электронном виде, цифровизацией процессов предоставления массовых услуг и стимулированием граждан к пользованию массовыми услугами в электронном виде. Руководителем данной программы является заместитель Министерства цифрового развития, связи и массовых коммуникаций О. Б. Пак.

Проект «Искусственный интеллект» является одним из новейших, реализуемых в данной нацпрограмме. Его задача состоит в созданий условий для пользования гражданами сервисов и услуг, основанных на искусственном интеллекте. Проект предусматривает поддержку научных исследований в данной области, разработку и развития ПО (в т.ч.

поддержкой стартапов и пилотных внедрений технологий ИИ), создание комплексной системы правового регулирования в данной области и повышение уровня обеспечения российского рынка технологий ИИ квалифицированными специалистами. Руководителем данного проекта является заместитель Министра экономического развития РФ В. В. Федулов.

3. Реализация национальной программы «Цифровая экономика» и её федеральных проектов.

В связи с массовым распространением сетей 5G в мире распространение их в России также является целью нацпрограммы «Цифровая экономика». Впрочем, внедрение 5G отложено на потом ввиду сложностей, таких как занятость частот силовыми структурами (занимаемыми ими диапазон составляет 3,4-3,8 ГГц и по заявлению операторов связи является наиболее удобным, из-за этого предполагается, что в РФ 5G будет доступен на частотах 4,7-4,9 ГГц) и отсутствия своего оборудования. Но Правительство РФ уже заключило соглашение с Ростехом и Ростелекомом о разработке и создании отечественных базовых станций и абонентского оборудования, которое и будет использоваться на территории России. Ожидается, что к 2022 году начнётся покрытие сетями 5G десяти крупнейших российских городов-миллионников (несколько экспериментальных зон на 2020 год уже развёрнуто на территории Москвы и Санкт-Петербурга), к 2023 начнётся масштабное развёртывание сетей 5G, а доступна 5G будет в городах-миллионниках уже к 2024 году. Также, к 2024 году планируется установить порядка 10 000 базовых станций 5G в десяти городах-миллионниках, сообщает информагенство ТАСС. Уровень локализаций базовых станций для сетей 5G к тому времени должен будет составить 40% в стоимостном соотношении. Помимо базовых станций, план мероприятий по продвижению к итоговой цели проекта по производству оборудования для обеспечения 5G предусматривает опорную сеть (что наряду с базовыми станциями 5G обеспечит комплексное решение по распространению 5G), для чего будет создана технологическая кооперация отечественных компаний, обладающих соответствующими наработками и компетенцией. Причины переноса сроков пока неизвестны. Вполне возможно, что решение отложить запуск 5G на территории России может быть связано в связи урезанием трат на нацпрограмму из-за кризиса, вызванного эпидемией COVID-19.

Тем не менее, подключение к высокоскоростному и широкопотоковому Интернету осуществляется. К примеру, в Ростовской области с 2019 года осуществляется подключение к сетям передачи данных (в т. ч. Интернет) более двух тысяч социально значимых объектов, в том числе районных и поселковых администраций, школ, пожарных частей, фельдшерско-акушерских пунктов и т.д. Завершение проекта планируется уже к концу этого года. По состоянию на июль этого года, предполагается обеспечить доступ к Интернету для 964 социально значимых объектов: в т. ч. 335 культурно-досуговых учреждений, 325 образовательных учреждений и 266 фельдшерско-акушерских пунктов. А, например, Татарстан, согласно сообщению министерства цифрового развития республики, успешно прошёл основной этап создания необходимой для цифровизации инфраструктуры – уровень покрытия сотовой связью к октябрю этого года составил 99,8%, к Интернету подключены более девяти тысяч социально значимых организаций, а все социально значимые услуги будут переведены в электронный вид. В Приморском крае в рамках выполнения данной нацпрограммы до СЗО проложены волоконно-оптические линии связи (сокращённо – ВОЛС) протяжённостью 636,67 км, Интернет в данных СЗО доступен с 10 октября 2020. Из них доля подключённых к Интеренту, составила 100 % для медицинских учреждений, 58% для гос. органов власти и органов местного самоуправления (из плановых 68%), 87% для фельдшерско-акушерских пунктов (из плановых 78% (sic!)) и 38% для образовательных учреждений (из плановых 37%). В Бурятии в рамках федерального и регионального проектов «Информационная инфраструктура» с 2019 года подключено 630 СЗО: 212 фельдшерско-акушерских и акушерских пунктов, 234 образовательных учреждений, 126 гос. органов власти и органов местного самоуправления, 42 объекта МЧС и 6 объектов МВД. К 2021 году

планировалось подключение к ещё 414 СЗО, из них: 115 фельдшерско-акушерских и акушерских пунктов, 170 образовательных учреждений, 108 гос. органов власти и органов местного управления, 20 объектов МЧС и 33 объекта МВД. В Хабаровском крае в 2020 году в рамках нацпрограммы подготовлено 4633 выпускника образовательных учреждений с ключевой компетенцией цифровой экономики (по плану – 3048 чел. (sic!)). В Карачаево-Черкесии по состоянию на 2019 год предлагалось к 2024 году обеспечить более 97% жителей республики высокоскоростным Интернетом. Кроме того, по состоянию на тот же год предполагалось к 2021 году подключить к Интернету более 304 СЗО. Правительство Саратовской области в рамках осуществления нацпрограммы ставит своей целью увеличить долю домохозяйств, пользующихся Интернетом до 97%, подключить к широкополосному доступу к Интернету 100% СЗО инфраструктуры, снизить долю иностранного закупаемого и арендуемого ПО до 10% и увеличить количество выпускников по ИТ-специальностям. В Смоленской области с 2019 года в рамках нацпрограммы к Интернету были подключены 710 СЗО, среди которых оброазовательные и медицинские организации и учреждения; а также 391 населённый пункт области, в том числе труднодоступные. В Новосибирской области, по словам министра цифрового развития и связи Новосибирской области Сергея Цукаря, на 2019-2021 годы предполагалось обеспечить широкополосный доступ к Интернету в 1651 СЗО, расположенных в том числе и в малонаселённых и труднодоступных населённых пунктах, а также, в рамках выполнения нового этапа программы по ликвидации т.н. «цифрового неравенства» в 2021 году 37 населённых пункта области будет обеспечено сотовой связью формата 3G и 4G. В Краснодарском крае, по сообщениям информагенства ТАСС, в рамках реализации нацпрограммы с 2019 года было подключено к Интернету более двух тысяч СЗО (в том числе 811 за этот год): среди них 937 школ, 407 фельдшерско-акушерских пунктов и 350 культурных учреждений. В Ставропольском крае, по сообщениям информагенства ТАСС, к 2021 году планируется подключить высокоскоростной и широкополосный Интернет более к чем 400 СЗО, всего будет проложено примерно 300 км волоконно-оптических кабелей. По состоянию на 1 июня 2021 года работы по подключению Интернета завершены на 58%.

Нельзя не отметить в свете вышеописанного ухода работы множества предприятий в онлайн ввиду последствий пандемии и цифровизацию госуслуг. По сравнению с 2019 годом пользование госуслугами в онлайн режиме вырос в разы: к примеру, количество записей на приём к врачу выросло практически вдвое (с 47,9 млн до 74, 9 млн), а число обращений о состоянии индивидуальных лицевых счетов выросло с 20,7 млн до 24,8 млн. Соответственно, выросло количество человек, пользующихся госулсугами в онлайн-режиме: так, до пандемии ими пользовались лишь 28 % россиян, а уже во время пандемии госуслугами воспользовались 51%. 82% россиян считают, что онлайн-сервисы по госуслугам существенно облегчают взаимоотношение с государственными органами. Предполагается, что данный процесс будет завершён к 2023 году: к 1 января того года все наиболее значимые услуги будут доступны в онлайн-режиме. К 2024 году в новом формате (в т.ч. и в электронном виде) будет представлено около 300 госуслуг, из них 120 – федеральные и 180 – региональные и муниципальные. К примеру, централизация и завершение перевода в онлайн-режим информационных ресурсов МВД, Пенсионного фонда России, Федеральной службы госрегистрации и кадастра для оказания госуслуг должна завершиться к декабрю 2022 года. Заместитель Председателя Правительства РФ Дмитрий Чернышенко считает, что к 2024 году 85% россиян будут иметь учётную запись на сайте госуслуг gosuslugi.ru (он же «Госуслуги»). Он же подчеркнул, что на данный момент (сентябрь 2021 года) «Госуслуги» занимают четвёртое место в мире по посещаемости среди сайтов в сфере государственного управления, а мобильное приложение «Госуслуги.Авто» занимает первое место среди бесплатных приложений в магазине мобильных приложений AppStore в связи с началом тестирования цифровой копии свидетельства о регистрации транспортного средства в России. Цифровизация госуслуг влечёт к тому, что пользователь может подать полностью подать документы дистанционно, в онлайн-режиме, и таким же образом получить результат. Предполагается, что госуслуги будут

осуществляться в полностью автоматизированном режиме без участия сотрудников госорганов или вовсе в проактивном режиме – т.е. без обращения пользователя-заявителя и с использованием данных пользователя от других ведомств. К примеру, в Смоленской области, по состоянию на 19 октября 2021 года будет проведён переход в электронную версию 94 государственных и муниципальных услуг, 66 из которых уже доступны на едином портале госуслуг. Сейчас по количеству предоставляемых в электронном виде услуг Смоленская область занимает третье место среди всех регионов России. По итогам сентября этого года лидерами в сфере цифровой трансформации Липецкая, Тульская области, Ямало-Ненецкий автономный округ (ЯНАО) и Нижегородская область, говорит Чернышенко по итогам совещания с руководителями цифровой трансформации регионов. Он же назвал регионы, сильно отстающие по темпам цифровизации – это Северная Осетия (Алания), Забайкальский край, Тамбовская и Магаданская области. Проводящаяся осенью этого года перепись населения, опять же, в рамках реализации данной нацпрограммы, впервые истории также проводится и в электронном виде, онлайн. Интерактивная форма для переписи представлена на сайте «Госуслуги», время её заполнения, по словам заместителя главы Министерства цифрового развития, связи и массовых коммуникаций Олега Качанова, составляет около 15-25 минут. Что характерно, черновик переписного листа сохраняется при каждом поле ввода, что позволяет сделать перерыв и продолжить заполнение формы позднее. Чернышенко на заседании Совета по стратегическому развитию и национальным проектам в режиме видеоконференции также заявил, что планируется к 2024 году предоставлять все справки и выписки в электронном виде. Кроме того, он заявил, что к 2023 году процедура взыскания алиментов будет осуществляться преимущественно онлайн и удалённо, что позволит государству исполнять свои обязанности по защите интересов и прав ребёнка.

Одной из немаловажных целей данной госпрограммы и федерального проекта «Цифровое государственное государственное управление» в частности является массовое внедрение цифровых паспортов вместо бумажных. В цифровых паспортах будут использоваться смарт-карты, а также цифровые копии паспортов в смартфонах граждан РФ. Уже в декабре этого года в пилотном режиме в Москве будет запущен проект введения цифрового паспорта. Помимо Москвы, отметил глава Министерства цифрового развития, связи и массовых коммуникаций М. Шадаев, введение цифровых паспортах планируется по крайней мере в трёх регионах РФ (каких – не уточняется). Также он отметил, что цифровая копия паспорта будет представлять из себя приложение для мобильных устройств, которое будет считывать данные, записавнные на чип смарт-карты, а в отдельных случаях показывать не саму карту, а QR-код, который будет подтверждать право обладателя цифрового паспорта совершение определённых действий.

С 9 августа 2019 на сайте «Госуслуги» доступны прототипы так называемых суперсервисов. Это новый вид государственных услуг, позволяющий оформлять документы и осуществлять тому подобные действия в электронном режиме. Существует суперсервис в том числе и для оформления документов для поступления в ВУЗ – «Цифровые документы об образовании онлайн». В рамках реализации данного суперсервиса Министерство образования РФ разработает ФЗ «О внесении изменений в федеральный закон «Об образовании в Российской Федерации», который будет регулировать условия выдачи документов и квалификации в электронной форме.

В рамках выполнения данной нацпрограммы было введено дистанционное электронное голосование (ДЭГ), впервые осуществлённое на выборах в Городскую Думу Москвы (сокращённо – Мосгордума) 2019 года, а во время выборов в Госдуму, прошедших в сентябре этого года, вышедшее на федеральный уровень. Перед этим, с 12 по 14 мая проходило тестирование ДЭГ, оно было доступно гражданам, ранее подавшее заявку на участие через портал «Госуслуги». ДЭГ применялось на выборах в Госдуму в том числе и в Ростове-на-Дону и Ростовской области.

В целях повышения цифровой грамотности населения нацпрограмма способствует открытию и развитию образовательных проектов, интенсивов, специализированных образовательных учреждений, вебинаров и онлайн-курсов. К примеру таких образовательных проектов можно отнести «Цифровые профессии», «Урок цифры» (осуществляется при поддержке Сбербанка) и «Готов к цифре». Подобные образовательные проекты действуют не только на федеральном, но и на региональном и муниципальном уровне. Так, в Тюмени с 30 августа 2020 года действует образовательный проект «Школа цифровой трансформации», курируемый местным департаментом информатизации, организующая лекции, онлайн-курсы, семинары и вебинары, посвящённые работе за компьютером и гаджетами (планшеты, смартфоны и т.п.), и приобретения новых практических навыков в ИТ-сфере. В Ростовской области при Ростовском колледже связи и информатики (сокращённо – РКСИ), а также при поддержке правительства Ростовской области, Министерстве образования Ростовской области, Министерстве информационных технологий и связи Ростовской области, Ростелекома, МТС, банка «Центр-Инвест» и других организаций действует профориентационный летний лагерь «IT-Фабрика компьютерных гениев».

В конце 2019 года был запущен проект по созданию национального киберполигона для противодействия государства и организаций ключевых отраслей экономики России кибератакам и укрепления безопасности государства в цифровом пространстве. На нём проводятся тренировки и киберучения с симуляцией компьютерных атак по различным сценариям. Также симулируются цели кибератак, такие, как отрасли экономики, предприятия и даже города. Впоследствии цели киберполигона были расширены, и теперь он занимается комплексным подходом: помимо ключевых отраслей российской экономики (нефтегазовой, металлургической, транспортной, телекоммуникационной и т.д.) к нему будут подключаться коммерческие организации, разумеется, с соответствующей инфраструктурой.

В рамках выполнения федерального проекта «Искусственный интеллект» нацпрограммы Министерство просвещения РФ организовало Всероссийскую олимпиаду по искусственному интеллекту, участие в которой принимают школьники 8-11 классов. Участники олимпиады демонстрируют свои умения и навыки в подборке и настройке алгоритмов машинного обучения. Чернышенко сообщил ТАСС, что около 100 тысяч школьников пройдут курсы в сфере искусственного интеллекта. Также Чернышенко на первом заседание правительственной комиссии по научно-технологическому развитию (созданной по указу Президента РФ) заявил, что искусственный интеллект необходимо использовать для прогноза научно-технического прогресса. Основным вопросом данного заседания явилась подготовка государственной программы научно-технического развития РФ, реализуемой в том числе и с помощью искусственного интеллекта. 22 июля этого года был запущен конкурс среди малых предприятий на получение грантов в размере от 4 до 20 млн.? на стартапы в области развития искусственного интеллекта. Начиная с августа 2021 года в рамках реализации данного федерального проекта разрабатывается Национальный кодекс этики ИИ. Внедрение искусственного интеллекта является приоритетным в том числе и для Вооружённых сил РФ, 9 февраля этого года министр обороны РФ генерал армии С. Шойгу заявил на оперативно-мобилизационном сборе с руководящим составом ВС РФ, что «необходимо внедрение технологий искусственного интеллекта в вооружение, определяющее перспективный облик Вооруженных сил».. Глава Росстата П. Малков в интервью информагенству «РИА Новости» отметил, что перепись населения этого года проводится с применением искусственного интеллекта, а также с использованием технологии «big data» (англ. «большие данные»), с которым и будет работать ИИ. «Искусственный интеллект будет применяться при анализе тех данных, которые агрегируют операторы мобильной связи. В этот раз мы впервые будем экспериментировать с большими данными» – уточнил Малков. Данные во владении мобильных операторов о перемещении своих абонентов пойдёт в основу сведений о количестве населения муниципальных районов и городских округов. Это в том числе позволит уточнить данные перепеси ..

В рамках выполнения федерального проекта «Кадры для цифровой экономики» нацпрограммы Министерство строительства и жилищно-коммунального хозяйства РФ запустило программы по повышению квалификации кадров строительной отрасли и ЖКХ, для чего теперь необходимо получить персональный цифровой сертификат (ПЦС) и пройти бесплатное обучение по программам повышения квалификации по 22 направлениям цифровой экономики, например, по направлению BIM-технологий (информационное моделирование в строительстве). По завершению обучения будет выдано удостоверение о повышении квалификации

Одна из целей, которая ставит собой нацпрограмма – борьба с телефонным мошенничеством, которая в последние годы набирает обороты. В июле этого года, сообщает издание «РБК», представители нескольких ведомств (Ростех, Ростелеком, Росатом), а также частных компаний (среди которых Сбербанк, ВТБ, Яндекс, МТС, РЖД, Mail.ru Group и т. д.), вошедших в состав рабочей группы при АНО «Цифровая экономика», предложили включить в число целей нацпрограммы сокращение к 2024 году телефонного мошенничества в 10 раз. Список мероприятий по противодействию с телефонным мошенничеством, по предложению рабочей группы, должен был быть предоставлен сроком до 10 октября. Он включает себя регулирование IP-телефонии, ограничение на транзит трафика, признанного мошенническим и др. Для борьбы с телефонным мошенничеством также предлагается разработать единую методику сбора и подсчёта правонарушений. От себя добавлю, что уже сейчас развёрнута полномасштабная агитация по борьбе с телефонными мошенниками. Помимо этого, данная рабочая группа предложила создание единого центра кибербезопасности (англ. security operation center – SOC) для обеспечения безопасности государственных информационных систем (ГИС) в облачной инфраструктуре. Данное решение обусловлено тем, что государственная облачная инфраструктура — это единая экосистема, и соответственно, её защиту должна обеспечивать единая же экосистема кибербезопасности, а не разрозненные частные компании. Хотя представитель от МТС также отметил, что компания также поддерживает привлечение к SOC различных участников рынка, что по его словам, сократит расходы государства на обеспечение работы SOC, повысит конкуренцию и стимул к развитию данного направления, а также обеспечит наиболее безопасную и устойчивую к угрозам извне систему создания распределённого SOC. Идея по созданию SOC принадлежит Сбербанку. Кроме того, глава МВД РФ В. Колокольцев в декабре прошлого года сообщил, что в МВД будет создано отделение по борьбе с киберпреступностью, грубо говоря, киберполиция. Это решение Колокольцев аргументировал тем, что за период пандемии COVID-19 сильно вырос уровень киберпреступности. Уже в начале 2020 года сообщалось, что в следственном департаменте МВД создано отделение по борьбе с киберпреступностью ввиду возросшего уровня киберпреступлений.

Однако, стоит упомянуть и недостатки по реализации данной нацпрограммы. К 1 марта 2021 года показатели по исполнению расходов на реализацию нацпрограммы «Цифровая экономика» составили 3,4 %. К сожалению, эти показатели являются одними из самых худших, поскольку лучшие показатели нацпрограмм и нацпроектов составили около 20-25 % (среди них «Жильё и городская среда», «Здравоохранение» и «Демография»). В 2019 году (кратко – Минкомсвязь) не смогла потратить четверть из выделенных ей на развитие цифровой экономики 74,8 млрд.? (основная часть была выделена как раз на реализацию нацпрограммы «Цифровая экономика», на которую всего в 2019 году планировалось выделить 100,2 млрд.?). В числе причин данного явления представители Счётной палаты РФ, выявившей его по результатам проверки исполнения министерством закона «О федеральном бюджете за 2019 год и плановый период 2020 и 2021 годов», а также член рабочей группы АНО «Цифровая экономика» Владислав Онищенко и в едущий аналитик Российской ассоциации электронных коммуникаций Карен Казарян указывают постоянные переписывание и доработка документов нацпрограммы (в т.ч. паспорта нацпрограммы) в силу быстрого развития технологий ввиду неготовности госаппарата, а также излишняя бюрократизация и перераспределение бюджета

между задачами, заложенными в федеральных проектах. По словам Казаряна, низкое кассовое исполнение нацпрограммы может быть объяснено страхом сотрудников Минкомсвязи оказаться под следствием из-за обвинений в растрате бюджетных средств. Он же добавляет, что мероприятия нацпрограммы всё-таки реализуются на практике, хоть и с гораздо большими сроками. Помимо этого, различные проекты реализуются с различной степенью успешности: так, по состоянию на июль 2020 года в составе федерального проекта «Нормативное регулирование цифровой среды» не выполнено 9 проектов, в составе «Информационной инфраструктуры» – 11, а в составе «Цифрового государственного управления» – и вовсе из 74 проектов не выполнено 20. Эксперты Аналитического центра при Правительстве РФ ради улучшения темпов реализации нацпрограммы считают, что необходимо упростить сложную структуру управления нацпрограммой, в состав которой входят органы власти, госкорпорации, АНО и институты развития.

Подводя итоги, можно сказать, что несмотря на все трудности, данная нацпрограмма успешно выполняется, таким образом проводя масштабную цифровизацию российской экономики. Оценивая результаты, достигнутые при выполнении данной нацпрограммы на данный момент, можно заключить, что российская экономика в целом готова к восприятию новейших цифровых технологий в ближайшем будущем.

СПИСОК ЛИТЕРАТУРЫ

1. «Цифровая экономика РФ» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 23.10.2021). – Текст: электронный.
2. Цифровая экономика 2024: официальный сайт. – Москва. – URL: https://data-economy.ru/2024 (дата обращения: 23.10.2021). – Текст: электронный.
3. Национальная программа «Цифровая экономика 2024»: федеральные проекты, отрасли, структура, мероприятия, проекты и совет по цифровой экономике : официальный сайт. – Москва. – URL: https://digital.ac.gov.ru/about/ (дата обращения: 23.10.2021). – Текст: электронный
4. «Нормативное регулирование цифровой среды» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/862/ (дата обращения: 24.10.2021). – Текст: электронный.
5. «Кадры для цифровой экономики» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 23.10.2021). – Текст: электронный.
6. «Искусственный интеллект» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/1046/ (дата обращения: 24.10.2021). – Текст: электронный.
7. «Цифровое государственное управление» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/882/ (дата обращения: 24.10.2021). – Текст: электронный.
8. «Информационная инфраструктура» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/870/ (дата обращения: 24.10.2021). – Текст: электронный.

9. «Цифровые технологии» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/878/ (дата обращения: 24.10.2021). – Текст: электронный.
10. «Информационная безопасность» :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/activity/directions/874/ (дата обращения: 24.10.2021). – Текст: электронный.

Д.А. Черепанов, Н.И. Герасимов, Д.С. Предвечнов, Ю.А. Лим

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ФЛУКТУАЦИОННЫХ ОШИБОК РАДИОВЫСОТОМЕРОВ

ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина»,
г. Воронеж

Ключевые слова: флуктуационная ошибка, точность измерения высоты.

В статье рассмотрена проблема оценки флуктуационной ошибки и возможности ее учета в алгоритмах функционирования радиовысотомеров в реальном времени через усредненные значения для типовых видов подстилающих поверхностей.

D.A. Cherepanov, N.I. Gerasimov, D.S. Predvechnov, Yu.A. Lim

MODELING AND INVESTIGATION OF FLUCTUATION ERRORS OF RADIO ALTIMETERS

VUNC VVS "VVA named after Professor N.E. Zhukovsky and Yu.A. Gagarin",
Voronezh

Keywords: fluctuation error, accuracy of height measurement.

The article considers the problem of estimating the fluctuation error and the possibility of taking it into account in the algorithms of functioning of radio altimeters in real time through averaged values for typical types of underlying surfaces.

Повышение безопасности полетов авиации неразрывно связано с надежностью функционирования бортового оборудования и точностью выдаваемой экипажу информации. Это утверждение можно применять к любому из этапов выполнения полетов, однако на каждом из них указанные показатели применимы к различным группам бортового оборудования.

Анализ статистики авиационных происшествий и катастроф, как в гражданской, так и военной авиации за 20 лет, прошедших с начала XXI века показывает, что большая часть из них приходится на этапы взлета или посадки, которые зачастую выполнялись в сложных метеорологических условиях. В качестве одного из основных путей повышения безопасности полетов в данном случае целесообразно рассматривать повышение переход к их выполнению в полностью автоматическом режиме. Очевидно, что при таком подходе к бортовой аппаратуре, обеспечивающей требуемый уровень автоматизации, в том числе составляющей информационную подсистему пилотажно-навигационного комплекса, предъявляются существенно более жесткие требования по точности и надежности.

Одним из таких бортовых измерителей является радиовысотомер, обеспечивающий экипаж и бортовые системы информацией об истинной высоте полета воздушного судна [1]. При посадке летательного аппарата высоту необходимо измерять с погрешностью, не превышающей долей метра.

Не менее важно измерение высоты при выполнении таких специфических задач как бомбометание, при котором погрешность в измерении высоты должна быть меньше величины вероятного отклонения бомб от цели. Тогда ее влияние на точность бомбометания будет пренебрежительно мала. Для современных условий это соответствует измерению высоты с ошибкой, не превышающей 0,2...0,25%. Однако в ряде случаев требуется более высокая точность.

Как и любые технические устройства, радиовысотомеры измеряют высоту с ошибками и поскольку они используют сигнал, отраженный от протяженной статистически неровной поверхности, то в результате возникают специфические ошибки измерения высоты. Одной из таких ошибок является флуктуационная ошибка (погрешность).

Флуктуационная погрешность, обусловленная внешними шумами, поступающими вместе с полезным сигналом, зависит от отношения мощностей сигнала и шума на входе приемника в пределах полосы пропускания последнего и от времени усреднения сигнала в измерительных цепях. Уменьшения флуктуационной погрешности можно достигнуть сужением полосы пропускания каскадов, предшествующих измерителю, и увеличением времени усреднения до разумных пределов (0,1...1с), определяемых допустимой динамической погрешностью. Случайный характер сигнала проявляется главным образом в погрешности смещения и методической флуктуационной погрешности.

Флуктуационная ошибка, обусловленная наличием шума на входе сумматора, определяется по формуле

$$\sigma_h^2 = \frac{1}{\pi}\int_0^\infty S_h(\omega)d\omega \quad , \qquad (1)$$

где $S_h(\omega) = S_{f(\omega)}\left|W(j\omega)\right|^2$, $S_{f(\omega)} = 0.6\times10^{-6}$ – спектральная плотность входного сигнала.

Для оценки флуктуационной ошибки измерения истинной высоты полета в ходе работы была разработана модель ее определения, а также выполнено ее исследование при полете над разными типами поверхности.

Анализ процессов формирования, распространения, отражения, приема и обработки сигналов позволил разработать методику проведения исследования, на первом этапе которой осуществлялось формирование структуры подстилающей поверхности. При этом в качестве моделей поверхностей использовались фацетные модели [2] с различной высотой рельефа и структурой неоднородностей, формируемой путем задания случайным образом углового положения каждого фацета по отношению к опорной плоскости.

Использование фацетного представления достаточно часто используется при моделировании различных электрофизических сцен и является достаточно общим универсальным решением при компьютерном моделировании отраженных сигналов. При фацетном моделировании отражающие поверхности представляются совокупностью отражателей или плоских площадок, как показано на рисунке 1, которые носят название фацетов, а сигнал на входе приемной антенны равен сумме сигналов, отраженных от всех видимых, но, как правило, статистически независимых фацетов. Этот принцип позволяет заменить сложные пространственно-электрические характеристики реальных поверхностей на обобщенную характеристику – эффективную поверхность рассеяния, заданную для фиксированных поляризации, длины волны и угла облучения, зависящую от типа подстилающей поверхности, то есть диаграмму обратного рассеяния [2].

Отражение от каждого фацета происходит как от точечного отражателя. При этом каждый фацет кроме своих координат может иметь дополнительные параметры: коэффициент отражения, форму ДОР, сдвиг фазы при отражении, смещение (отклонение) по высоте относительно среднего уровня горизонтальной плоскости XOZ и углы отклонения нормали фацета (оси ДОР) от вертикали [2].

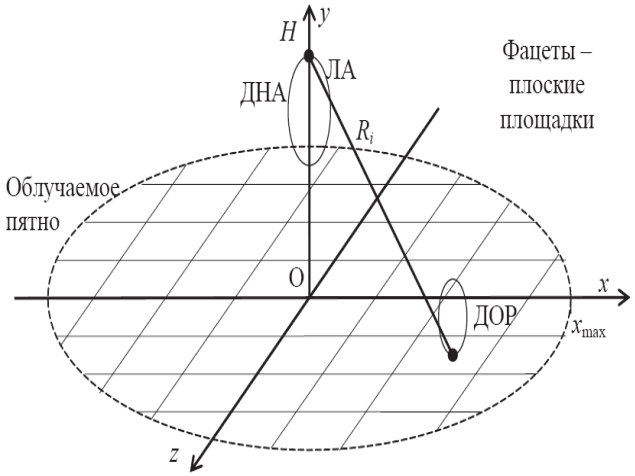
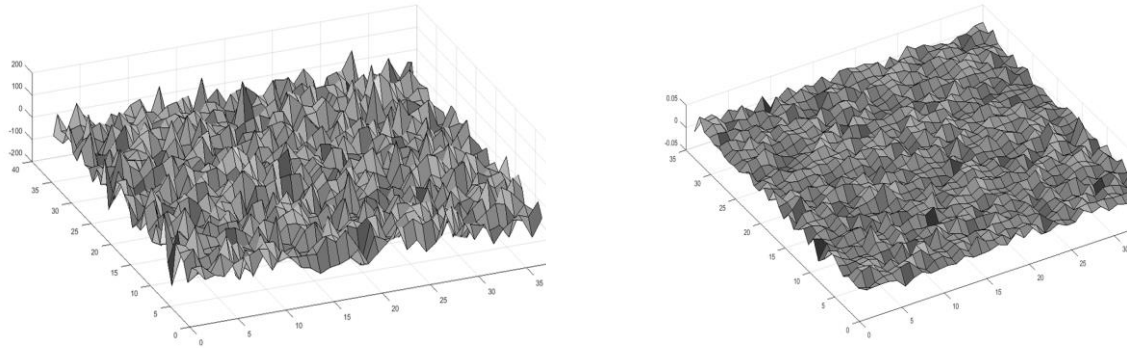


Рисунок 1. Геометрия фацетной модели подстилающей поверхности [2].

Примеры структуры подстилающей поверхности, смоделированной в работе с помощью описанного выше подхода, приведены на рисунках 2а и 2б.



а. б.

Рисунок 2. Модели подстилающей поверхности.

В ходе работы рассматривалась абсолютная ошибка, получаемая, как следует из теории измерений, как разность между истинным и измеренным значениями высоты. За истинное значение принимались показания радиовысотомера, которые фиксировались для каждых ста итераций, а за измеренное – среднее арифметическое расстояний до каждого фацета подстилающей поверхности.

Расстояния от центра антенны до фацетов вычислялись через их известные координаты в соответствии с выражением

$$R_{i,j} = \sqrt{x_{i,j}^2 + y_{i,j}^2 + (H_{ist} + z_{i,j})^2}, \quad (2)$$

где i, j – индексы координат фацета; H_{ist} – высота; $x_{i,j}$, $y_{i,j}, z_{i,j}$ – координаты фацета.

Измеренная высота вычислялась по формуле

$$H_{изм} = \frac{\sum_{m=1,n=1}^{i,j} R_{i,j}}{m \cdot n}, \quad (3)$$

где $\sum_{m=1,n=1}^{i,j} R_{i,j}$ – сумма наклонных дальностей до каждого фацета, m и n – количество фацет по координатам x и y соответственно.

График изменения мгновенного значения флуктуационной ошибки для высоты 1500 метров при полете над равниной приведен на рисунке 3.

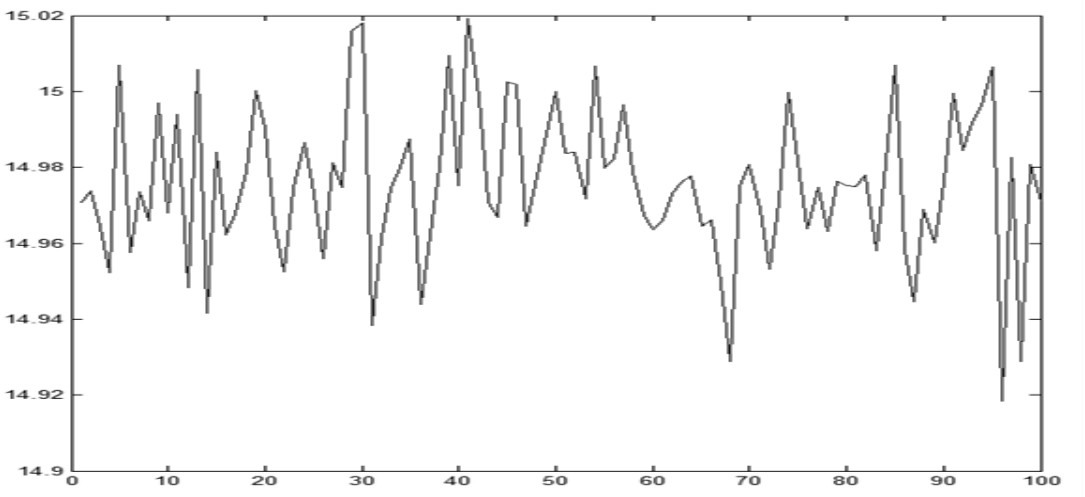


Рисунок 3. График флуктуационной ошибки для высоты 1500 метров, при средней высоте неоднородностей рельефа 10 см (равнина).

В результате проведения исследований можно сделать вывод о том, что наличие крупномасштабного рельефа поверхности в пределах пятна облучения существенно сказывается на характеристиках отраженного сигнала. Оценка флуктуационной ошибки и ее учет в алгоритмах функционирования радиовысотомеров в реальном времени или через усредненные значения для типовых видов подстилающих поверхностей позволит повысить точность измерения истинной высоты полета воздушного судна в интересах повышения эффективности функционирования пилотажно-навигационных комплексов при выполнении наиболее ответственных маневров при взлете и заходе на посадку.

СПИСОК ЛИТЕРАТУРЫ

1. *Скрыпник О.Н.* Радионавигационные системы воздушных судов. учебник. М.:Инфра-М, 2020. 352 с.
2. Полунатурное моделирование бортовых радиолокационных систем, работающих по земной поверхности: учебное пособие / Под общ. ред. *В.Г. Важенина.* Екатеринбург: Изд-во Урал. ун-та, 2015. 208 с.

О.О. Соколова, А.В. Елисеев, В.С. Лободинов, В.Н. Таран

АНАЛИЗ СТРУКТУРЫ ВТОРИЧНОЙ ОБРАБОТКИ ТРАЕКТОРНЫХ ИЗМЕРЕНИЙ И РЕАЛИЗАЦИЯ ЕЁ ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ

Донской государственный технический университет, Ростов-на-Дону, Россия
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: вторичная обработка радиолокационной информации, траектория движения объекта, фильтр Калмана.

В статье описывается структура вторичной обработки радиолокационной информации, рассматривается применение алгоритма линейной дискретной фильтрации с нечеткой модификацией структуры.

O.O. Sokolova, A.V. Eliseev, V.S. Lobodinov, V.N. Taran

ANALYSIS OF THE STRUCTURE OF SECONDARY PROCESSING OF TRAJECTORY MEASUREMENTS AND THE IMPLEMENTATION OF ITS INDIVIDUAL ELEMENTS

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

Key words: secondary processing of radar information, trajectory of object movement, Kalman filter.

The article describes the structure of secondary processing of radar information, considers the use of a linear discrete filtering algorithm with a fuzzy modification of the structure.

Основной задачей радиолокации является сбор и обработка информации относительно исследуемых объектов. В многопозиционных наземных РЛС вся обработка радиолокационной информации подразделяется на три этапа:

1. Первичная обработка заключается в обнаружении сигнала цели и измерении ее координат с соответствующими качеством или погрешностями;
2. Вторичная обработка предусматривает определение параметров траектории каждой цели по сигналам одной или ряда позиций МПРЛС, включая операции отождествления отметок целей;
3. Третичная обработка объединяет параметры траекторий целей, полученных различными приемными устройствами МПРЛС с отождествлением траекторий.

Первичная обработка радиолокационной информации (РЛИ) начинается с обнаружения полезного сигнала в шумах. Этот процесс складывается из нескольких этапов:

1. Обнаружение одиночного сигнала;
2. Обнаружение пакета сигналов;
3. Формирование полного пакета сигналов;
4. Определение дальности до цели и ее азимута.

Все эти этапы реализуются с использованием оптимальных алгоритмов, основанных на критериях минимума ошибок принятия решения и результатов измерения.

Однако на практике получение информации только о местоположении, скорости и характеристиках объекта не является достаточной для принятия окончательного решения об обнаружении (так как существует вероятность ложной тревоги) и для оценки всех интересующих получателя параметров движения цели (направление, скорость, ускорение, прогнозирование движения). Таким образом, возникает потребность в решении задачи дальнейшего анализа результатов первичной обработки РЛИ, которую решает система вторичной обработки информации.

На рисунке 1 представлена структурная схема вторичной обработки РЛИ.

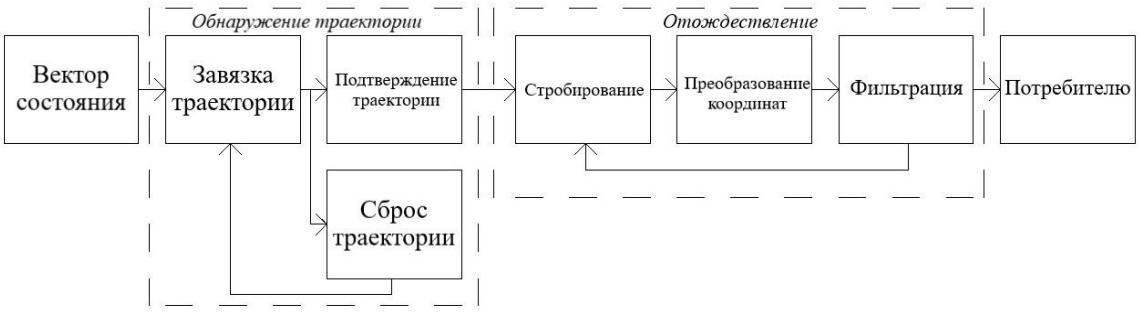


Рисунок 1. Структурная схема вторичной обработки РЛИ

Данная схема состоит из следующих элементов:

1. Вектор состояния - измерение, формируемое первичной системой обработки РЛИ. Он содержит:
   a. **β** – вектор измеренных параметров цели, включающий в себя наклонную дальность, азимут, угол места, высоту, радиальную составляющую вектора скорости, амплитуда и др.;
   b. **в** – ковариационная матрица вектора **β**. Если измерения являются независимыми, В представляет собой дисперсии погрешностей измерения составляющих вектора;
   c. t – время обнаружения цели.
2. Блок обнаружения траектории включает в себя:
   a. Завязка траектории – принимает решение о возможном наличии новой цели и оценивает первоначальные параметры ее движения;
   b. Подтверждение траектории – окончательно устанавливает наличие в определенной области пространства цели с оцененными на предыдущем этапе параметрами движения;
   c. Сброс траектории – сбрасывает завязанную траекторию, при отсутствии дальнейших отметок.
3. Блок отождествление состоит из:
   a. Стробирование – выделяет из отметок, полученных на очередном такте обновления информации, те, которые могут принадлежать той или иной сопровождаемой цели с учетом текущих оценок ее положения в пространстве и динамики движения.

Во время стробирования последнее известное положение цели предсказывается (экстраполируется) на момент прихода отметки на текущем такте, при условии, что характер ее движения неизменный на данном интервале. После этого определяется размер и ориентация в пространстве области вокруг предсказанной отметки, в которой с заданной вероятностью должна оказаться отметка от цели (строб отождествления). По результатам формируется набор полученных на обзоре отметок, которые попадают в строб отождествления данной траектории.

4. Преобразование координат – выполняет преобразование координат к единой системе, если РЛС и траекторная обработка осуществляются в разных системах координат;
5. Блок фильтрация является важной составляющей всего алгоритма сопровождения цели, он определяет отметки, которые не описывают движения какой-либо цели, поскольку во время измерений могут создаваться ложные данные, а также показывает какие из отметок являются правильными.

Существуют различные методы фильтрации траекторных измерений, рассмотрим алгоритм линейной дискретной фильтрации с нечеткой модификацией структуры.

Для уменьшения влияния погрешности измерений на результирующую оценку на практике широко используют [1-11] такие алгоритмы обработки как классический и расширенный фильтры Калмана, нелинейный фильтр, $\alpha-\beta$ -фильтр и др. Качество оценок, формируемых данными фильтрами, во многом определяется адекватностью используемых в них моделей вектора состояния. Адекватность моделей, как правило, нарушается при случайном, с точки зрения наблюдателя, маневре летательного аппарата. Использование в фильтре неадекватной модели приводит к его расходимости. Для недопущения этого в теории и практике динамической фильтрации используют следующие способы адаптации фильтра к маневру [1-3, 5, 6]: периодическое приведение коэффициента усиления фильтра к исходному значению, увеличение дисперсии формирующего шума, увеличение значений ковариационной матрицы ошибок оценивания вектора состояния, расширение вектора состояния, поочередное использование нескольких фильтров, использование многомодельных фильтров. Применение рассмотренных способов, за исключением последнего, предполагает решение задачи обнаружения маневра. По этой причине адаптивные алгоритмы фильтрации содержат три основных модуля: модуль обнаружения маневра; модуль настройки параметров фильтра; модуль фильтра [1-3]. Существующее многообразие алгоритмов динамической фильтрации обусловлено особенностями реализации перечисленных модулей. Так, например, в [6] предложен алгоритм настройки фильтра Калмана путем изменения значения элементов матрицы интенсивностей формирующих шумов. Особенностью данного алгоритма является итерационность подстройки, приводящая к возникновению динамической погрешности фильтрации. Таким образом, по-прежнему актуальной является задача разработки адаптивного к интенсивности маневра алгоритма фильтрации.

Пусть движение динамического объекта на интервале времени описывается разностным уравнением [1]

$$\mathbf{X}_j = \mathbf{\Phi}_j \mathbf{X}_{j-1} + \mathbf{\Gamma}_j \left(\mathbf{A}_{xj} + \mathbf{N}_{xj} \right), \; j = 1, 2, \ldots \tag{1}$$

а уравнение наблюдения имеет вид

$$\mathbf{Z}_j = \mathbf{H}_j \mathbf{X}_j + \mathbf{N}_{zj}, \; j = 1, 2, \ldots \tag{2}$$

где $\mathbf{X}_j = \mathbf{X}(t_j) = \left[x_{sj}, \; s = \overline{1, q} \right]^T$ – вектор параметров движения объекта $\mathbf{Z}_j = \left[z_{sj}, \; s = \overline{1, p} \right]^T$ – вектор измерений, $\mathbf{\Phi}_j = \left[\varphi_{l\,sj}, \; l, s = \overline{1, q} \right]$, $\mathbf{\Gamma}_j = \left[\gamma_{skj}, \; s = \overline{1, q}, \; k = \overline{1, m} \right]$, $\mathbf{H}_j = \left[b_{k\,sj}, \; k = \overline{1, p}, \; s = \overline{1, q} \right]$ – известные функциональные матрицы, $\mathbf{A}_{xj} = \left[a_{xsj}, \; s = \overline{1, m} \right]^T$ – вектор интенсивности маневра, элементы которого принадлежат априорно неизвестным диапазонам $a_{x\,s\,j} \in \left[a_{x\min s}, a_{x\max s} \right], \; s = \overline{1, m}$ и представляют собой ускорения объекта по соответствующей координате, $\mathbf{N}_{x\,j} = \left[n_{xsj}, \; s = \overline{1, m} \right]^T$, $\mathbf{N}_{z\,j} = \left[n_{zsj}, \; s = \overline{1, p} \right]^T$ – случайные шумы объекта (1) и канала

наблюдения (2) соответственно, имеющие нулевые математические ожидания и корреляционные матрицы $\mathbf{Q}_j = \mathrm{diag}\left[q_{ssj},\ s=\overline{1,\ m} \right]$, $\mathbf{R}_j = \mathrm{diag}\left[r_{ssj},\ s=\overline{1,\ p} \right]$.

Требуется: по результатам текущих наблюдений $\mathbf{Z}_j$ получить оптимальную в среднеквадратическом смысле оценку $\hat{\mathbf{X}}_j$ фильтрации вектора состояния (1) в условиях априорной неопределенности относительно значений элементов вектора ускорений $\mathbf{A}_{xj}$.

Пусть для формирования оценки $\hat{\mathbf{X}}_j$ вектора параметров движения динамического объекта используется конечное множество операторов $\left\{ \Re_k,\ k=\overline{1,M} \right\}$, каждый из которых представляет собой фильтр Калмана [1-6], настроенный на конкретное значение вектора ускорений $\mathbf{A}_{xj}^k \in \left\{ \mathbf{A}_x^1, \mathbf{A}_x^2, \ldots, \mathbf{A}_x^M \right\}$:

$$\hat{\mathbf{X}}_j^k = \hat{\mathbf{X}}_{j|j-1}^k + \mathbf{K}_j \left[\mathbf{Z}_j - \mathbf{H}_j \hat{\mathbf{X}}_{j|j-1}^k \right], \tag{3}$$

$$\hat{\mathbf{X}}_{j|j-1}^k = \mathbf{\Phi}_j \hat{\mathbf{X}}_{j-1}^k + \mathbf{\Gamma}_j \mathbf{A}_{xj}^k, \tag{4}$$

$$\mathbf{P}_{j|j-1} = \mathbf{\Phi}_j \mathbf{P}_{j-1} \mathbf{\Phi}_j^T + \mathbf{\Gamma}_j \mathbf{Q}_j \mathbf{\Gamma}_j^T, \tag{5}$$

$$\mathbf{K}_j = \mathbf{P}_{j|j-1} \mathbf{H}_j^T \left[\mathbf{H}_j \mathbf{P}_{j|j-1} \mathbf{H}_j^T + \mathbf{R}_j \right]^{-1}, \tag{6}$$

$$\mathbf{P}_j = \left[\mathbf{I} - \mathbf{K}_j \mathbf{H}_j \right] \mathbf{P}_{j|j-1}, \tag{7}$$

где $\hat{\mathbf{X}}_{j|j-1}^k$ – оценка прогноза вектора состояния на момент j, $\mathbf{P}_{j|j-1}$ – симметричная матрица ошибок прогнозирования, $\mathbf{P}_j$ – ковариационная матрица ошибок фильтрации $\mathbf{X}_j - \hat{\mathbf{X}}_j$, $\mathbf{K}_j$ – коэффициент усиления фильтра, $\mathbf{I}$ – единичная матрица.

При этом в каждый конкретный момент времени используется только один фильтр, то есть осуществляется переключение фильтров в зависимости от информации о значении $\mathbf{A}_{xj}^k$.

Видно, что для случая, когда в модели (1) $\mathbf{A}_{xj} \notin \left\{ \mathbf{A}_x^1, \mathbf{A}_x^2, \ldots, \mathbf{A}_x^M \right\}$ оценка на выходе фильтра $\hat{\mathbf{X}}_j^k$ будет содержать значительную динамическую ошибку из-за неадекватности модели (4) реальному процессу.

Для обеспечения устойчивости оценки $\hat{\mathbf{X}}_j$ необходима разработка адаптивного алгоритма фильтрации, учитывающего неопределенность значения $\mathbf{A}_{xj}$.

Данный алгоритм должен обнаруживать расходимость оценки $\hat{\mathbf{X}}_j$ и модифицировать структуру фильтра.

Рассмотрим последовательно возможные варианты решения указанных задач.

Задача обнаружения расходимости. Для решения данной задачи необходимо ввести показатель расходимости. Для повышения достоверности решения задачи обнаружения расходимости будем использовать одновременно два частных показателя.

Первый частный показатель. Пусть в качестве решающей статистики используется обновляющий процесс (невязка) $\boldsymbol{\varepsilon}_j = \mathbf{Z}_j - \mathbf{H}_j \hat{\mathbf{X}}_{j|j-1}$, а в качестве порога S_0 – величина [1]

$$S_{0lj} = c\sqrt{\Psi_{llj}}, \tag{8}$$

где $\Psi_{ll j}, l=\overline{1,p}$ – диагональные элементы матрицы $\mathbf{\Psi}_j = \mathbf{H}_j \mathbf{P}_{j|j-1} \mathbf{H}_j^T + \mathbf{R}_j$; c – положительная константа, значение которой определяется вероятностью $P_Д$ того, что ε_{lj} будет находиться в интервале $\left[-S_{0lj}, S_{0lj}\right]$, например, при $P_Д = 0.9973$ имеем $c=3$.

С учетом (8) факту обнаружения расходимости соответствует условие [1]

$$\left|\varepsilon_{lj}\right| > S_{0lj}. \tag{9}$$

Из (9) следует, что в качестве показателя расходимости целесообразно использовать относительное значение невязки вида

$$\left|\delta\varepsilon_{1j}\right| = \left|\varepsilon_{lj}\right| \Big/ S_{0lj}. \tag{10}$$

Второй частный показатель. Показатель (10) учитывает как аномальную случайную ошибку, так и динамическую ошибку, обусловленную неадекватностью модели (4) реальному процессу. Для учета в большей степени динамической ошибки введем, по аналогии с [6], показатель модуля среднего арифметического значения невязки $\left|\bar{\varepsilon}_j\right|$ (при этом для простоты изложения без потери общности примем, что невязка является скалярной):

$$\left|\bar{\varepsilon}_j\right| = \frac{\left|\sum_{i=0}^{n-1} \varepsilon_{j-i}\right|}{n}, \tag{11}$$

где n – количество подряд следующих измерений, используемых для обнаружения расходимости фильтра.

Вычисление показателей (11) возможно, когда $j \geq n$, т.е. когда выполнено не менее n наблюдений вида (2).

По аналогии с (10) преобразуем (11) к виду:

$$\left|\bar{\delta\varepsilon}_{2j}\right| = \frac{\left|\sum_{i=0}^{n-1} \varepsilon_{j-i}\right|}{n\sigma_{prg}}, \tag{12}$$

σ_{prg} – некоторое допустимое значение среднеквадратического отклонения (СКО) ошибки ε_j, $j \geq n$.

Задача модификации структуры фильтра. Пусть, для примера, система оценивания содержит два фильтра $\left\{\Re_k, k=\overline{1,2}\right\}$, первый из которых $(k=1)$ настроен на наименьшее значение ускорения $\mathbf{A}_{xj}^1 = \mathbf{A}_{x\min}$, а второй $(k=2)$ – на наибольшее значение ускорения $\mathbf{A}_{xj}^2 = \mathbf{A}_{x\max}$. При этом реальное значение ускорения в модели (1) может принимать любое значение из известного интервала $\mathbf{A}_{xj} \in \left[\mathbf{A}_{x\min}, \mathbf{A}_{x\max}\right]$.

Для модификации структуры фильтра будем использовать оперативно советующую экспертную систему (ОСЭС), основанную на применении нечеткого логического вывода [9]. Применение ОСЭС обусловлено неопределенностью задания значений вектора ускорений $\mathbf{A}_{xj}$. Представим процесс функционирования фильтра в виде кортежа некоторых проблемных ситуаций (ПрС) [9-11]. При этом любая ПрС описывается ситуационным вектором

$\mathbf{sv} = \left[sv_\xi, \xi = \overline{1,\Xi} \right]^T$, каждая координата которого sv_ξ является лингвистической переменной с заданным множеством термов $\mathbf{SV}_\xi = \left\{ SV_\xi^l, l = \overline{1, m_\xi} \right\}$. Полагаем, что для некоторых конкретных реализаций ситуационного вектора $\mathbf{sv}^*$ имеются прецеденты успешного решения текущей ПрС, характеризующиеся некоторым прецедентным вектором $\mathbf{pv} = \left\{ pv_m, m = \overline{1, m_{PV}} \right\}$, каждая координата которого pv_m также является лингвистической переменной с заданным множеством термов $\left\{ PV_m^p, p = \overline{1, n_m} \right\}$. Пусть для рассматриваемой системы фильтрации, состоящей из конечного множества операторов $\left\{ \Re_k, k = \overline{1,2} \right\}$ вида (3)-(7), введен ситуационный вектор $\mathbf{sv} = \left[sv_\xi, \xi = \overline{1,4} \right]^T$ с элементами: $sv_1 -$ «относительное значение невязки первого фильтра $\left|\delta\varepsilon_{1j}^1\right|$», $sv_2 -$ «значение модуля относительной ошибки первого фильтра $\left|\delta\varepsilon_{2j}^{-1}\right|$», $sv_3 -$ «относительное значение невязки второго фильтра $\left|\delta\varepsilon_{1j}^2\right|$», $sv_4 -$ «значение модуля относительной ошибки второго фильтра $\left|\delta\varepsilon_{2j}^{-2}\right|$».

Пусть переменные ситуационного вектора описываются следующими терм-множествами:

$$\mathbf{SV}_1 = \mathbf{SV}_3 = \begin{Bmatrix} "Very\ low\ \left(OH\left(\left|\delta\varepsilon_{1j}\right|\right)\right)", \\ "\ Low\left(H\left(\left|\delta\varepsilon_{1j}\right|\right)\right)", \\ "\ Average\left(CP\left(\left|\delta\varepsilon_{1j}\right|\right)\right)", \\ "\ High\left(B\left(\left|\delta\varepsilon_{1j}\right|\right)\right)" \end{Bmatrix},$$

$$\mathbf{SV}_2 = \mathbf{SV}_4 = \begin{Bmatrix} "Very\ low\ \left(OH\left(\left|\delta\bar{\varepsilon}_{2j}\right|\right)\right)", \\ "\ Low\left(H\left(\left|\delta\bar{\varepsilon}_{2j}\right|\right)\right)", \\ "\ Average\left(CP\left(\left|\delta\bar{\varepsilon}_{2j}\right|\right)\right)", \\ "\ High\left(B\left(\left|\delta\bar{\varepsilon}_{2j}\right|\right)\right)" \end{Bmatrix}.$$

Полагаем, что лингвистические переменные sv_ξ, $\xi = \overline{1,4}$ заданы на универсуме $E = [0, \infty[$ а термы описываются функциями принадлежности $\mu_{SV_\xi} \in \left\{ \mu_{SV_\xi^l}, l = \overline{1, m_{L\xi}} \right\}$, $\xi = \overline{1,\Xi}$, представленными на рисунках 2 и 3.

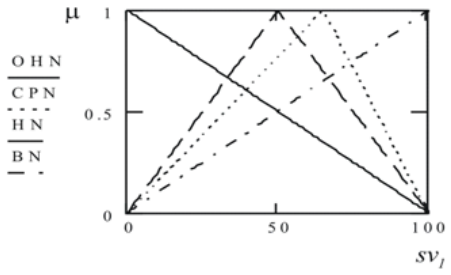


Рисунок 2. Функции принадлежности терм-множества SV_1 и SV_3: OHN – «очень низкий»; CPN – «средний»; HN – «низкий»; BN– «высокий»

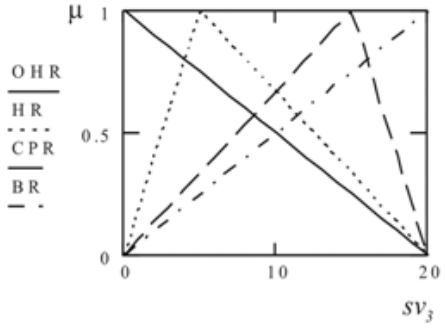


Рисунок 3. Функции принадлежности терм-множества SV_2 и SV_4: OHR – «очень низкий»; CPR –«средний»; HR –«низкий»; BR –«высокий»

Пусть для данного класса ПрС известны следующие прецеденты: $pv_1 -$ первая модель вида (4) $(k=1)$ «очень близка» к реальному процессу, целесообразно использовать оценку, формируемую первым фильтром, то есть: $\hat{\mathbf{X}}_j = \hat{\mathbf{X}}_j^1$; $pv_2 -$ первая модель вида (4) $(k=1)$ «более близка» к реальному процессу, по сравнению со второй моделью $(k=2)$, целесообразно использовать взвешенную оценку $\hat{\mathbf{X}}_j = 0,7\hat{\mathbf{X}}_j^1 + 0,3\hat{\mathbf{X}}_j^2$; $pv3 -$ вторая модель вида (4) $(k=2)$ «более близка» к реальному процессу, по сравнению с первой моделью $(k=1)$, целесообразно использовать взвешенную оценку $\hat{\mathbf{X}}_j = 0,3\hat{\mathbf{X}}_j^1 + 0,7\hat{\mathbf{X}}_j^2$; $pv_4 -$ вторая модель вида (4) $(k=2)$ «очень близка» к реальному процессу, целесообразно использовать оценку, формируемую вторым фильтром, то есть: $\hat{\mathbf{X}}_j = \hat{\mathbf{X}}_j^2$.

С учетом введенных ранее ситуационного вектора и известных прецедентов, система правил R^{mr_m}, $m=\overline{1,m_{PV}}$, $r_m=\overline{1,N_m}$, описывающих механизм решения текущей ПрС, будет иметь вид:

$$R^{mr_m}=1,1:\ \text{if}\begin{pmatrix}\left(sv_1=OH\left(\left|\delta\varepsilon_{1j}^1\right|\right)\right)\\ \text{and}\left(sv_2=OH\left(\left|\delta\varepsilon_{2j}^{-1}\right|\right)\right)\\ \text{and}\left(sv_3=B\left(\left|\delta\varepsilon_{1j}^2\right|\right)\right)\\ \text{and}\left(sv_4=B\left(\left|\delta\varepsilon_{2j}^{-2}\right|\right)\right)\end{pmatrix},\text{then}\ \left(pv_1\right),$$

$$R^{mr_m}=2,1:\ \text{if}\begin{pmatrix}\left(sv_1=H\left(\left|\delta\varepsilon_{1j}^1\right|\right)\right)\\ \text{and}\left(sv_2=H\left(\left|\delta\varepsilon_{2j}^{-1}\right|\right)\right)\\ \text{and}\left(sv_3=CP\left(\left|\delta\varepsilon_{1j}^2\right|\right)\right)\\ \text{and}\left(sv_4=CP\left(\left|\delta\varepsilon_{2j}^{-2}\right|\right)\right)\end{pmatrix},\text{then}\ \left(pv_2\right),$$

$$R^{mr_m} = 3{,}1:\ \text{if}\ \begin{pmatrix} \left(sv_1 = CP\left(\left|\delta\varepsilon_{1j}^{1}\right|\right)\right) \\ \text{and}\ \left(sv_2 = CP\left(\left|\delta\varepsilon_{2j}^{-1}\right|\right)\right) \\ \text{and}\ \left(sv_3 = H\left(\left|\delta\varepsilon_{1j}^{2}\right|\right)\right) \\ \text{and}\ \left(sv_4 = H\left(\left|\delta\varepsilon_{2j}^{-2}\right|\right)\right) \end{pmatrix}, \text{then}\ \left(pv_3\right),$$

$$R^{mr_m} = 4{,}1:\ \text{if}\ \begin{pmatrix} \left(sv_1 = B\left(\left|\delta\varepsilon_{1j}^{1}\right|\right)\right) \\ \text{and}\ \left(sv_2 = B\left(\left|\delta\varepsilon_{2j}^{-1}\right|\right)\right) \\ \text{and}\ \left(sv_3 = OH\left(\left|\delta\varepsilon_{1j}^{2}\right|\right)\right) \\ \text{and}\ \left(sv_4 = OH\left(\left|\delta\varepsilon_{2j}^{-2}\right|\right)\right) \end{pmatrix}, \text{then}\ \left(pv_4\right).$$

Для расчета функции принадлежности прецедента pv_m используем правило Мамдани-Заде [9-11]:

$$\mu_{pv_m}\left(sv_1, sv_2, \ldots, sv_\Xi,\right) = \max_{r_m} \min_{\xi} \mu_{SV_\xi\,(mr_m)}\left(sv_\xi\right), \tag{13}$$

где $\mu_{SV_\xi\,(mr_m)} \in \left\{\mu_{SV_\xi^l}, l = \overline{1, m_{L\xi}}\right\}$ – функция принадлежности лингвистической переменной sv_ξ, входящая в состав продукционного правила R^{mr_m}.

С учетом (13) наиболее предпочтительный прецедент для решения наблюдаемой ПрС может быть определен следующим образом:

$$pv_m^* = \arg\max_m \mu_{pv_m}\left(sv_1, sv_2, \ldots, sv_K,\right). \tag{14}$$

Схема ОСЭС, предназначенной для модификации структуры фильтра, представлена на рисунке 4.

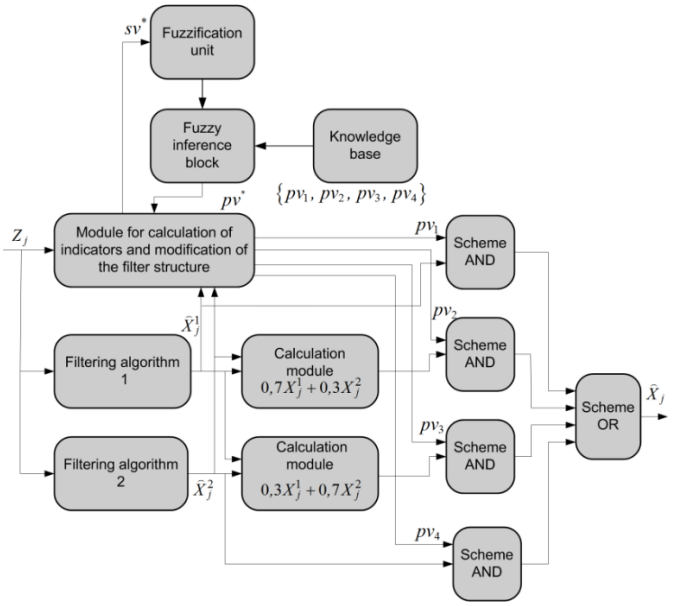


Рисунок 4. Структура интеллектуальной системы обработки измерений

Система функционирует следующим образом: конкретные значения элементов ситуационного вектора $\mathbf{sv}^*$, сформированные в модуле вычисления показателей и модификации структуры фильтра (МВПМСФ), поступают в блок фазификации, где преобразуются в нечеткие множества, полученные данные являются входными для блока нечеткого логического вывода, реализующего алгоритм выбора наиболее предпочтительного прецедента $pv^* \in \{pv_1, pv_2, pv_3, pv_4\}$ на основе выражений (13), (14), при этом используется информация из базы знаний, содержащей нечеткие продукционные правила, а также вид и параметры функций принадлежности (рисунки 1 и 2). Номер наиболее предпочтительного прецедента, выбранного для решения наблюдаемой ПрС, используется в МВПМСФ для коммутации одного из четырех рассчитанных массивов оценок $\{X_j^1\}$, $\{0{,}7X_j^1 + 0{,}3X_j^2\}$, $\{0{,}3X_j^1 + 0{,}7X_j^2\}$, $\{X_j^2\}$ на выход устройства фильтрации.

Таким образом, ОСЭС обеспечивает модификацию структуры фильтра в зависимости от изменения модели оцениваемого информационного процесса вида (1).

Для подтверждения работоспособности предложенного алгоритма было проведено математическое моделирование. Предполагалось, что модель движения маневрирующего летательного аппарата имеет вид:

$$\mathbf{X}_j = \begin{cases} \mathbf{\Phi}\,\mathbf{X}_{j-1} + \mathbf{\Gamma}\, n_{xj-1}, \; 0 \le j < 200, \\ \mathbf{\Phi}\,\mathbf{X}_{j-1} + \mathbf{\Gamma}\left(2g + n_{xj-1}\right), \; 200 \le j < 400, \\ \mathbf{\Phi}\,\mathbf{X}_{j-1} + \mathbf{\Gamma}\left(4g + n_{xj-1}\right), \; 400 \le j < 600, \end{cases} \tag{15}$$

где

$$\mathbf{\Phi} = \begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}, \quad \mathbf{\Gamma} = \begin{bmatrix} \dfrac{\tau^2}{2} \\ \tau \end{bmatrix},$$
$$\tau = t_{j+1} - t_j = 1\text{c}, \quad j = \overline{0,\,600}.$$

Для оценивания вектора состояния $\hat{\mathbf{X}}_j$ использовалась система, содержащая два фильтра $\{\Re_k, k = \overline{1,2}\}$, первый из которых $(k=1)$ был настроен на наименьшее значение ускорения $\mathbf{A}_{xj}^1 = 0$, а второй $(k=2)$ – на наибольшее значение ускорения $\mathbf{A}_{xj}^2 = 4g$, $g = 9.8$ м/с^2. При этом реальное значение ускорения в модели (1), как видно из (15), принимало три разных значения $\mathbf{A}_{xj} \in [0, 2g, 4g]$.

В результате моделирования было установлено, что применение разработанного алгоритма позволяет уменьшить динамическую погрешность оценивания на 27% по сравнению с мультиструктурным алгоритмом фильтрации, основанном на выборе в каждый момент времени только одного конкретного фильтра [1].

СПИСОК ЛИТЕРАТУРЫ

1. *Фарина А., Студер Ф.* Цифровая обработка радиолокационной информации. Сопровождение целей / Пер. с англ. М.: Радио и связь. 1993. 320 с.

2. *Бакулев П.А., Сычев М.И., Нгуен Чонг Лыу*. Многомодельный алгоритм сопровождения траектории маневрирующей цели по данным обзорной РЛС // Радиотехника. 2004. № 1. С. 26-32.
3. *Елисеев А.В., Музыченко Н.Ю.* Метод адаптивной настройки фильтра Калмана в задаче слежения за динамическим объектом с неизвестным ускорением // Радиотехника. 2014. № 8. С. 39-44.
4. *Елисеев А.В., Калашников Р.М., Тюрин Д.А*. Алгоритм обработки измерений и адаптации математического обеспечения информационно-измерительной системы в условиях изменения модели информационного процесса // Успехи современной радиоэлектроники. 2013. № 8. С. 9-17.
5. *Сычев М.И., Фесенко С.В.* Исследование многомодельных алгоритмов сопровождения воздушных судов по информации от радиолокационных средств наблюдения // Информационно-измерительные и управляющие системы. 2016. Т. 14. № 2. С. 10-17.
6. *Родкин М.М.* Адаптивный метод настройки фильтра Калмана // 6-я Всерос. конф. «Радиолокация и радиосвязь». ИРЭ им. Котельникова РАН. 19-22 ноября 2012. С. 125-128.
7. *Кузьмин С.З.* Цифровая радиолокация. Введение в теорию. Киев: Изд. КВІЦ, 2000. 428 с.
8. *Мурзова М.А., Фарбер В.Е*. Выбор коэффициентов сглаживания α-β фильтра по критерию минимума дисперсии суммарной ошибки для РЛС с ЛЧМ-сигналом // Радиотехника. 2018. № 4. С. 5-16.
9. *Гостев В.И.* Проектирование нечетких логических регуляторов для систем автоматического управления. СПб.: БХВ-Петербург. 2011. 416 с.
10. *Булычев Ю.Г., Елисеев А.В.* // Обработка измерений в условиях мультиструктурных помех // Автометрия. 2007. Т. 43. № 5. С. 26-38.
11. *Елисеев А.В*. Алгоритм линейной фильтрации, устойчивый к сингулярным ошибкам // Известия вузов. Радиоэлектроника. 2005. Т. 48. № 10. С. 20-29.

И.В. Калиенко, И.В. Решетникова, Т.В. Матвиенко, Ю.Е. Хурсенко

ИССЛЕДОВАНИЕ АКУСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ НАПРАВЛЕННОСТИ ГРОМКОГОВОРИТЕЛЯ НА ОСНОВЕ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

Донской государственный технический университет, ДГТУ,
г. Ростов-на-Дону, Россия

Ключевые слова: передача сигналов речевого диапазона, экспериментальные измерения параметров, электрические и акустические свойства громкоговорителя.

В статье рассмотрены актуальные вопросы анализа и уменьшения искажений при передаче речевых сообщений по каналам связи. Представлены результаты проведенных экспериментальных исследований акустических свойств и их влияние на электрические свойства. Получено удовлетворительное совпадение характеристик в диапазоне речевых сигналов.

I.V. Kalienko, I.V. Reshetnikova, T.V. Matvienko, Yu.E. Khursenko

INVESTIGATION OF THE ACOUSTIC CHARACTERISTICS OF THE SPEAKER DIRECTIVITY BASED ON EXPERIMENTAL DATA

Don state technical University DSTU, Rostov-on-don, Russia

Keywords: transmission of speech range signals, experimental measurements of parameters, electrical and acoustic properties of a loudspeaker.

The article deals with topical issues of analysis and reduction of distortions in the transmission of speech messages through communication channels. The results of experimental studies of acoustic properties and their effect on electrical properties are presented. A satisfactory coincidence of characteristics in the range of speech signals was obtained.

Введение.

Особенности измерения акустических волн звукового диапазона вызывают существенные трудности анализа параметров и характеристик громкоговорителей, и особенно, характеристики направленности.

Для аналитического расчета применяют различные эмпирические формулы и зависимости, которые во многом определяются интуицией исследователей, индивидуальными отличиями каждого громкоговорителя.

Нередко применение различного акустического оформления изменяет параметры и характеристики одного и того же громкоговорителя.

В результате, используемые в настоящее время аналитические зависимости, в том числе, эквивалентные схемы, требуют введения дополнительных корректировок и поправок.

С этой точки зрения представляет интерес разработка методик расчета, основных на экспериментальных данных, что дополнительно позволяет учитывать индивидуальные особенности каждого громкоговорителя и его акустического оформления.

Цель исследования – на основе экспериментальных данных разработать алгоритм аналитического описания характеристики направленности громкоговорителя в виде кусочной непрерывной сплайн – функции.

.

Для построения сплайн-аппроксимации диаграммы направленности громкоговорителя параболическим сплайном второй степени по экспериментальным данным предлагается следующий алгоритм:

a. рассчитать коэффициенты полинома для каждого интервала $S_i = a_i(x - x_i)^2 + b_i(x - x_i) + c_i$;
b. по экспериментальным данным отдельных точек зависимости эффективности громкоговорителя $L_r(\mathrm{x})$ от угла измерения, отслеживаемого от рабочей оси, для каждой точки $\mathrm{x} = \mathrm{x}_{i+1}$ $a_i h^2 + b_i h + c_i = c_{i+1} = L_r(\mathrm{x}_{i+1})$;
c. необходимо выполнить условие гладкости сигнала в углах стыковки интервалов, то есть условия непрерывности первой производной в точке $\mathrm{x} = \mathrm{x}_{i+1}$ $2a_i h + b_i = b_{i+1}$.

На основании методов построения диаграммы направленности громкоговорителя проведем расчет характеристики направленности по экспериментальным расчетам.

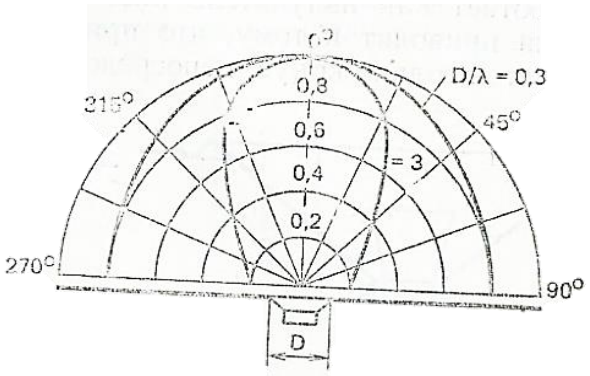


Рисунок 1. Типовые диаграммы направленности динамического диффузорного громкоговорителя

Представим экспериментальные данные в табличной форме.

Таблица 1. Характеристика направленности громкоговорителя

Угол измерено	0	22,5	45	67,5	90	$D/\lambda = 0,3$
L_r	1	0,94	0,86	0,8	0,78	
L_r	1	0,82	0,4	0,24	0,18	$D/\lambda = 3$

Поскольку диаграмма направленности симметрична относительно рабочей оси, то расчету подлежит диапазон от 0 до 90 градусов. Вторая половина диаграммы направленности строится симметрично.

Согласно справочным данным диаграмм из 5 измеренных точек разбит на 4 интервала: [0; 22,5], [22,5; 45], [45; 67,5], [67,5; 90].

Так как измерительные данные нормированы $L_r / L_{r\,max}$ так, то характеристика является безразмерной.

Для универсации математических расчетов введем обозначение

$L_r / L_{r\,max} = S$ - нормированная диаграмма направленности, угол измерения обозначим x.

Для старта расчетов определим коэффициенты сплайна на первом (начальном) шаге [0; 22,5] в начальной точке максимума

$$x = x_0 = 0;\ S_0 = c_0 = 1.$$

Поскольку в начальной точке согласно физическим условиями задачи имеется максимум, то производная в точке $x = x_0$ должна быть равна нулю

$$\frac{d}{dx} S_0(x_0) = b_0 = 0.$$

Коэффициент a_0 рассчитываем из условия стыковки сплайнов в конце интервала $x = x_1 = 22,5^0$

$$S_0(x_1) = S_1(x_1) = a_0 h^2 + b_0 h + c_0 = c_1; \quad a_0 = \frac{S_0(x_1) - b_0 h - c_0}{h^2}.$$

После расчета коэффициентов a_0, b_0, c_0 на начальном шаге $[x_0; x_1]$, [0; 22,5] рассчитываем коэффициенты a_i, b_i, c_i для остальных шагов:

Из условия непрерывности сплайна в точке x_i.

$$c_i = S_i(x_i) = S_{i-1}(x_i).$$

Из условия непрерывности первой производной

$$\frac{d}{dc} S_{i-1}(x_i) = \frac{d}{dx} S_i(x_i); \quad b_i = 2a_{i-1} h + b_{i-1}.$$

Из условия непрерывности сплайна в точке x_{i+1}

$$a_i = \frac{S_i(x_{i+1}) - b_i h - c_i}{h^2}.$$

Результаты расчета коэффициентов сплайна в программе *Matcad* по предложенной согласно таблице 1 и рисунку 1 приведены в таблицах (2 – 5).

Таблица 2. Расчет коэффициентов сплайна аппроксимированной характеристики диаграммы направленности громкоговорителя для $D/\lambda = 0,3$

	шаг	*a*	*b*	*c*
1	[0; 22,5^0]	$-1,185 \cdot 10^{-4}$	0	1
2	[22,5^0; 45^0]	$7,901 \cdot 10^{-5}$	$-5,333 \cdot 10^{-3}$	0,94
3	[45^0; 67,5^0]	$-1,083 \cdot 10^{-4}$	$-2,3 \cdot 10^{-4}$	0,86
4	[67,5^0; 90]	$-3,865 \cdot 10^{-5}$	$-1,983 \cdot 10^{-5}$	0,8

Таблица 3. Расчет коэффициентов сплайна аппроксимированной характеристики диаграммы направленности громкоговорителя для $D/\lambda = 3$

	шаг	a	b	c
1	[0; 22,5^0]	$-3,556 \cdot 10^{-4}$	0	1
2	[22,5^0; 45^0]	$1,185 \cdot 10^{-4}$	$-0,016$	0,82
3	[45^0; 67,5^0]	$-2,84 \cdot 10^{-4}$	$-7,216 \cdot 10^{-4}$	0,4
4	[67,5^0; 90]	$-1,16 \cdot 10^{-4}$	$-5,732 \cdot 10^{-5}$	0,24

Таблица 4. Значения диаграммы направленности громкоговорителя для $D/\lambda = 0,3$

Размер	$D/\lambda = 0,3$			
шаг / угол	$[0;22,5^0]$	$[22,5^0;45^0]$	$[45^0;67,5^0]$	$[67,5^0;90^0]$
x_i	1	0,94	0,86	0,8
$x_i + 2,5^0$	0,999	0,927	0,859	0,8
$x_i + 5^0$	0,997	0,915	0,856	0,799
$x_i + 7,5^0$	0,993	0,904	0,852	0,798
$x_i + 10^0$	0,988	0,897	0,847	0,796
$x_i + 12,5^0$	0,981	0,886	0,84	0,794
$x_i + 15^0$	0,973	0,878	0,832	0,791
$x_i + 17,5^0$	0,964	0,871	0,823	0,788
$x_i + 20^0$	0,953	0,865	0,812	0,784
$x_i + 22,5^0 = x_{i+1}$	0,94	0,86	0,8	0,78

Таблица 5. Значения диаграммы направленности громкоговорителя для $D/\lambda = 3$

Размер	$D/\lambda = 3$			
угол / шаг	$[0;22,5^0]$	$[22,5^0;45^0]$	$[45^0;67,5^0]$	$[67,5^0;90^0]$
1	2	3	4	5
x_i	1	0,82	0,4	0,24
$x_i + 2,5^0$	0,998	0,779	0,396	0,239
$x_i + 5^0$	0,991	0,737	0,389	0,237
$x_i + 7,5^0$	0,98	0,693	0,379	0,233
$x_i + 10^0$	0,964	0,648	0,364	0,228
$x_i + 12,5^0$	0,944	0,601	0,347	0,221
$x_i + 15^0$	0,92	0,553	0,325	0,213
$x_i + 17,5^0$	0,891	0,504	0,3	0,203
$x_i + 20^0$	0,858	0,453	0,272	0,192
$x_i + 22,5^0 = x_{i+1}$	0,82	0,4	0,24	0,18

В представленных таблицах 2 и 3 коэффициенты сплайна получим аналитическое выражение для диаграммы направленности громкоговорителя.

Соответственно, можем рассчитать значение нормированной диаграммы направленности громкоговорителя для любого значения угла.

Результаты расчетов, представленные в таблицах 4 и 5, доказывают эффективность разработанного алгоритма. Получена диаграмма направленности громкоговорителя в виде непрерывной гладкой функции, определенной на всем интервале.

Гладкость функции обеспечивается непрерывностью первой производной.

Полученная аппроксимационная формула позволяет найти значение диаграммы направленности для любого значения угла.

Выводы.

Сплайны по сравнению с другими функциями обладают лучшими аппроксимационными свойствами. Позволяют получить непрерывную гладкую функцию в виде кусочно-аналитического выражения. Гладкость аналитического выражения обеспечивается непрерывностью не только самого сплайна, но также и непрерывностью его первой производной.

Разработан алгоритм построения характеристики направленности громкоговорителя по известным экспериментальным данным в виде непрерывной гладкой функции.

Приведен пример расчета диаграммы направленности громкоговорителя по экспериментальным данным для различных случаев отношения диаметра диффузора к длине акустической волны $D/\lambda = 0,3$ и $D/\lambda = 3$.

Вычислительный эксперимент показал эффективность предложенной методики расчета характеристики направленности громкоговорителя и хорошее согласование с экспериментальными данными.

СПИСОК ЛИТЕРАТУРЫ

1. Радиовещание и электроакустика: Учебник для вузов. Под ред. М.В. Гитлица. М.: Ради о и связь, 1989. – 132 с.
2. О.В. Руденко, С.И. Солуян. Теоретические основы нелинейной акустики. М.: Наука. 1984 г 287 с
3. Сапожков М.А. Электроакустика. М.: Связь, 1978 С 192-213
4. Красильников В.А., Крылов В.В. Введение в физическую акустику. –М.: Наука. 1984 г. 403 с
5. Блацерна, П. Теория звука в приложении к музыке / П. Блацерна. - М.: Либроком, 2015. - 216 с
6. Вуд, А. Звуковые волны и их применения / А. Вуд. - М.: ЛКИ, 2008. - 146 с
7. Иофе, В. К. Электроакустика / В.К. Иофе. - М.: Государственное издательство литературы по вопросам связи и радио, 2016. - 184 с
8. Зарембо, Л. К. Введение в нелинейную акустику / Л.К. Зарембо, В.А. Красильников. - М.: Наука, 1990. - 520 с.5.
9. Н.Ю.Батурина, И.В. Калиенко, К.А.Кашуба, Н.И.Абрамова. Исследование, расчет и анализ влияния фазовых сдвигов громкоговорителя на амплитудно-частотную характеристику разделительного фильтра. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2018. С.25-30.

И.В. Калиенко, И.В. Решетникова, Т.В. Матвиенко, Ю.Е. Хурсенко

О ВОЗМОЖНОСТИ ОПРЕДЕЛЕНИЯ СИСТЕМАТИЧЕСКОЙ ОШИБКИ ПО ДАЛЬНОСТИ ПРИ ПРЯМОЛИНЕЙНОМ ДВИЖЕНИИ ОБЪЕКТА

Донской государственный технический университет, ДГТУ,
г. Ростов-на-Дону, Россия

Ключевые слова: радиолокационные измерения, систематические ошибки, прямолинейная траектория.

Проведен анализ измерительного процесса, основанный на гипотезе о прямолинейном характере движения цели на наблюдаемом участке траектории. Представлено полиномиальное уравнение второй степени, коэффициенты которого зависят от угла и дальности. На основе анализа его решений с использованием математического моделирования может быть синтезирован алгоритм компенсации систематических ошибок радиолокационных измерений по дальности.

I.V. Kalienko, I.V. Reshetnikova, T.V. Matvienko, Yu.E. Khursenko

ON THE POSSIBILITY OF DETERMINING A SYSTEMATIC ERROR IN THE RANGE OF THE RECTILINEAR MOTION OF THE OBJECT

Don state technical University DSTU, Rostov-on-don, Russia

Keywords: radar measurements, systematic errors, rectilinear trajectory.

The analysis of the measuring process based on the hypothesis of the rectilinear nature of the target movement in the observed section of the trajectory is carried out. A polynomial equation of the second degree is presented, the coefficients of which depend on the angle and range. Based on the analysis of its solutions using mathematical modeling, an algorithm for compensating I.V. Resystematic errors of radar measurements by range can be synthesized.

При проведении радиолокационных измерений возникают ошибки, которые можно представить как случайные и систематические.

Систематическая ошибка – постоянная или закономерно изменяющаяся от одного измерения к другому.

Случайные (шумовые) ошибки могут быть уменьшены до требуемого значения методами статистической обработки измерений.

Наличие систематических ошибок требует разработки и применения алгоритмов их определения и компенсации после проведения статистической обработки радиолокационных измерений.

Цель работы – разработка алгоритма определения постоянной систематической ошибки измерения дальности до объекта, движущегося по прямолинейной траектории.

Постановка задачи

Пусть объект движется по прямолинейной траектории. В этом случае координаты местонахождения объекта в различные моменты времени должны удовлетворять уравнению прямой линии. Наличие систематических ошибок приводит к тому, то линия, проходящая через измеренные точки, носит криволинейный характер. Задача состоит в том, чтобы найти поправку – постоянный параметр, при при вводе которого в результаты измерений линия становится прямолинейной.

Решение задачи

Рассмотрим плоскость, проходящую через прямую линию и точку. Прямая линия – траектория движения объекта. Точка – место расположения РЛС. Известно, что через прямую линию и точку, не принадлежащую этой прямой, можно провести одну единственную плоскость (рисунок 1).

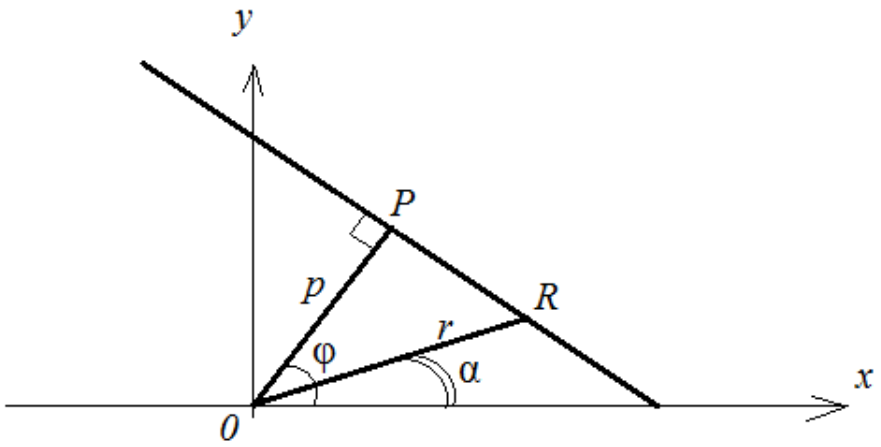


Рисунок 1. Прямолинейная траектория движения объекта

На рисунке 1 измерительное средство РЛС поместили в начало координат. Параметр P – перпендикуляр из начала координат к прямой линии. Угол φ – угол наклона этого перпендикуляра P. Точка, принадлежащая прямой, характеризуется двумя параметрами: r – длина от центра координат до точки, α – угол, между осью координат и направлением на точку. Любая точка, принадлежащая прямой линии, должна удовлетворять уравнению

$$r \cos(\varphi - \alpha) = p; \quad (1)$$

где p, φ – постоянные величины.

Тогда для двух разных точек (r1, α1) и (r2, α2) выполняется равенство:

$$r1 \cos(\varphi - \alpha1) = r2 \cos(\varphi - \alpha2). \quad (2)$$

В этом случае, если дальности r1 и r2 получены с некоторой систематической погрешностью Δr, то для удовлетворения равенства (2) необходимо учесть эту погрешность Δr.

$$r_{ист} = r_{изм} + \Delta r; \quad (3)$$

где Δ r – систематическая постоянная ошибка измерения дальности.

Тогда уравнение (2) с учетом (3) примет вид

$$(r1 + \Delta r) \cos(\varphi - \alpha1) = (r2 + \Delta r) \cos(\varphi - \alpha2) \quad (4)$$

При наличии трех измерений положения объекта, движущегося по прямолинейной траектории, уравнение (4) преобразуется к виду

$$((r1 + \Delta r) \cos (\varphi - \alpha1)) = ((r3 + \Delta r) \cos (\varphi - \alpha3)) \quad (5)$$

После преобразований из уравнения (5) получаем

$$\operatorname{tg} \varphi = ((r1 + \Delta r) \cos (\alpha1) - (r2 + \Delta r) \cos (\alpha2)) / ((r2 + \Delta r) \sin (\alpha2) - (r1 + \Delta r) \sin (\alpha1))$$
$$\operatorname{tg} \varphi = ((r1 + \Delta r) \cos (\alpha1) - (r3 + \Delta r) \cos (\alpha3)) / ((r3 + \Delta r) \sin (\alpha3) - (r1 + \Delta r) \sin (\alpha1)) \quad (6)$$

Проводим преобразования уравнения (6), учитывая, что φ – постоянная величина, характеризующая положение прямой линии. После преобразований получаем уравнение второй степени относительно искомой систематической ошибки дальности Δr.

$$A (\Delta r)^2 + B (\Delta r) + C = 0 \ ; \quad (7)$$

гле

$$A = \sin (\alpha1 - \alpha2) + \sin (\alpha2 - \alpha3) + \sin (\alpha3 - \alpha1) ; \quad (8)$$

$$B = (r1+r2) \sin (\alpha1 - \alpha2) + (r2+r3) \sin (\alpha2 - \alpha3) + (r1+r3) \sin (\alpha3 - \alpha1) ; \quad (9)$$

$$C = (r1\ r2) \sin (\alpha1 - \alpha2) + (r2\ r3) \sin (\alpha2 - \alpha3) + (r1\ r3) \sin (\alpha3 - \alpha1). \quad (10)$$

Известно, что квадратное уравнение второй степени имеет два корня. Вычислительный эксперимент показал, что правильным является то корень, когда квадратный корень из дискриминанта D входит в уравнение со знаком «минус»

$$\Delta r = (-B - \sqrt{D}) / (2A) . \quad (11)$$

Отметим, что измерения углов в предложенном алгоритме входят в коэффициенты A, B, C в виде разностей синусов. Следовательно, данный алгоритм не зависит от наличия в измерениях систематических ошибок по углу.

Таким образом, вычислительный эксперимент подтвердил правильность разработанного алгоритма определения и компенсации систематической ошибки по дальности при прямолинейном характере движения объекта.

СПИСОК ЛИТЕРАТУРЫ

1. Радиотехнические системы. Под ред. Ю.М. Казаринова. -Академия. -2008, 592 с.
2. Справочник по радиолокации. В 2-х книгах. Под ред. Сколник М.И. -2014.
3. Справочник по элементарной математике. М.Я Выгодский. 2006.
4. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся втузов. - Наука. 2008.

И.В. Калиенко, И.В. Решетникова, Т.В. Матвиенко, Ю.Е. Хурсенко

АНАЛИЗ ВОЗМОЖНОСТИ КОМПЕНСАЦИИ СИСТЕМАТИЧЕСКИХ ОШИБОК РАДИОЛОКАЦИОННЫХ ИЗМЕРЕНИЙ ПО УГЛУ МЕСТА ПРИ ЗАДАННОМ ПРЯМОЛИНЕЙНОМ ХАРАКТЕРЕ ДВИЖЕНИЯ ОБЪЕКТА

Донской государственный технический университет, ДГТУ,
г. Ростов-на-Дону, Россия

Ключевые слова: радиолокационные измерения, систематические ошибки, прямолинейная траектория.

Проведен анализ измерительного процесса, основанный на гипотезе о прямолинейном характере движения цели на наблюдаемом участке траектории. Представлено полиномиальное уравнение третьей степени, коэффициенты которого зависят от угла места и азимута. На основе анализа его решений с использованием математического моделирования может быть синтезирован алгоритм компенсации систематических ошибок радиолокационных измерений по углу места.

I.V. Kalienko, I.V. Reshetnikova, T.V. Matvienko, Yu. E. Khursenko.

ANALYSIS OF THE POSSIBILITY OF COMPENSATING SYSTEMATIC ERRORS OF RADAR MEASUREMENTS BY THE ANGLE OF THE PLACE WITH A GIVEN RECTILINEAR NATURE OF THE OBJECT MOVEMENT

Don state technical University DSTU, Rostov-on-don, Russia

Keywords: radar measurements, systematic errors, rectilinear trajectory.

The analysis of the measuring process based on the hypothesis of the rectilinear nature of the target movement in the observed section of the trajectory is carried out. A polynomial equation of the third degree is presented, the coefficients of which depend on the angle of location and azimuth. Based on the analysis of its solutions using mathematical modeling, an algorithm for compensating systematic errors of radar measurements by the angle of the place can be synthesized.

Введение. Систематическими ошибками являются постоянные или закономерно изменяющиеся ошибки при проведении многократных измерений.

Наличие постоянных систематических ошибок в радиолокационных измерениях приводит к необходимости разработки методов ее оценки и компенсации исходя из особенностей траектории и характера движения объекта, параметры которого измеряет РЛС.

Цель работы – анализ возможности определения систематических ошибок по углу места для повышения точности оценки параметров движения объекта по углу места в случае прямолинейного движения за счет компенсации постоянной систематической ошибки по углу места $\Delta\beta$.

Построение модели измерительного процесса. Рассмотрим случай прямолинейного движения радиолокационной кинематической цели на некотором участке траектории, который можно достаточно считать прямолинейным. Пусть РЛС находится в начале декартовой системы координат OXZY. Плоскость O'X'Y' параллельна плоскости OXY (рисунок 1). Тогда плоскость, проходящая через траекторию радиолокационной цели и точку O, в сечении с плоскостью O'X'Y' пересекает прямая линия A'B'C', которая описывается выражением:

$$L_{\text{П}} = \frac{h_c \cos(\alpha - \alpha_{\text{П}})}{\text{tg}\beta}, \quad (1)$$

где h_C=|OO'| – расстояние между параллельными плоскостями OXY и O'X'Y';

$L_П$ и $\alpha_П$ – длина и азимут перпендикуляра, проведенного из точки O' к прямой линии A'B'C';

α и β – азимут и угол места точек прямой ABC.

Пологая, что точка *A* – первое измерение, точка *B* второе измерение, имеем при наличии СО в измерениях РЛС по углу места Δβ

$$L_П = \frac{h_c \cos(\alpha_1 - \alpha_П)}{tg(\beta_1 - \Delta\beta)} = \frac{h_c \cos(\alpha_2 - \alpha_П)}{tg(\beta_2 - \Delta\beta)},$$

$$L_П = \frac{h_c \cos(\alpha_1 - \alpha_П)}{\mathrm{tg}(\beta_1 - \Delta\beta)} - \frac{h_c \cos(\alpha_2 - \alpha_П)}{\mathrm{tg}(\beta_2 - \Delta\beta)}, \quad (2)$$

откуда

$$\mathrm{tg}\alpha_П = \frac{\mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_2 - \mathrm{tg}(\beta_2 - \Delta\beta)\cos\alpha_1}{\mathrm{tg}(\beta_2 - \Delta\beta)\sin\alpha_1 - \mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_2}. \quad (3)$$

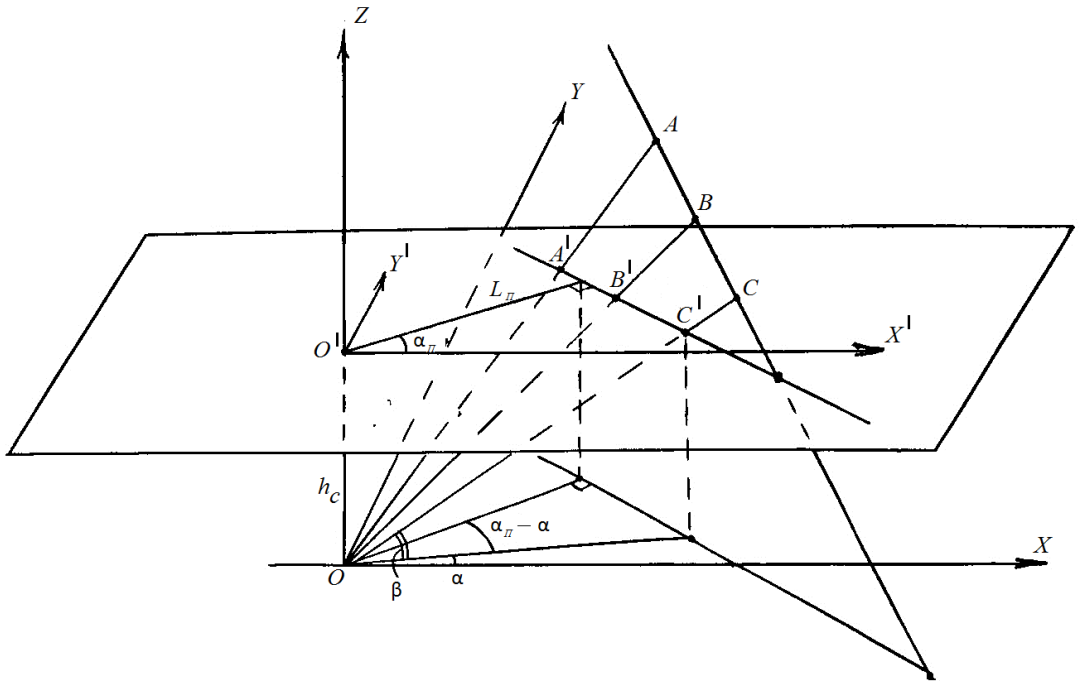


Рисунок 1. Модель измерительного процесса

Вводя третье измерение в точке *C* получим

$$\frac{\mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_2 - \mathrm{tg}(\beta_2 - \Delta\beta)\cos\alpha_1}{\mathrm{tg}(\beta_2 - \Delta\beta)\sin\alpha_1 - \mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_2} =$$

$$= \frac{\mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_3 - \mathrm{tg}(\beta_3 - \Delta\beta)\cos\alpha_1}{\mathrm{tg}(\beta_3 - \Delta\beta)\sin\alpha_1 - \mathrm{tg}(\beta_1 - \Delta\beta)\cos\alpha_3}. \quad (4)$$

В уравнениях (3) и (4) искомая ошибка по углу места Δβ присутствует единственным образом в показаниях tg(β - Δβ). Применение известных формул тригонометрического преобразования позволяет выделить систематическую постоянную ошибку по углу места в виде тангенса tg(Δβ).

Разрешая (3) и (4) относительно tg(Δβ) получаем новую модель измерительного процесса в форме полинома третьей степени

$$A\left(\mathrm{tg}\Delta\beta\right)^3 + B\left(\mathrm{tg}\Delta\beta\right)^2 + C\mathrm{tg}\Delta\beta - D = 0 \quad (5)$$

где коэффициенты *A, B, C, D* определяются сложным образом из объемных тригонометрических преобразований по углу места tg(β - Δβ) и азимуту sin α и cos α.

Решить уравнение (5) возможно, используя формулы Кардано. Получив решение кубического уравнения можно определить значение постоянных систематических ошибок по углу места Δβ в явном виде.

Отметим, что в уравнениях (3), (4), (5) отсутствуют измерения дальности, что свидетельствует о независимости предлагаемого алгоритма от наличия измерений дальности. Достаточно только применить измерения по углу места и азимут.

Выводы. Таким образом, показано, что анализ возможности позволяет определить систематические ошибки по углу места для повышения точности оценки параметров движения объекта по углу места в случае прямолинейного движения за счет компенсации постоянной систематической ошибки по углу места Δβ.

СПИСОК ЛИТЕРАТУРЫ

1. Радиотехнические системы. Под ред. Ю.М. Казаринова. -Академия. -2008, 592 с.
2. Справочник по радиолокации. В 2-х книгах. Под ред. Сколник М.И. -2014.
3. Справочник по элементарной математике. М.Я Выгодский. 2006.
4. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся втузов. - Наука. 2008.

А.В. Елисеев[1], Е.В. Землякова[1], М.П. Коваленко[1], В.И. Юхнов[2]

ОЦЕНКА КАЧЕСТВА ЦИФРОВОГО КАНАЛА СВЯЗИ НА ОСНОВЕ НЕЧЕТКОЙ ЭКСПЕРТНОЙ СИСТЕМЫ

Донской государственный технический университет,
Ростов-на-Дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: цифровой канал связи, техническая диагностика, показатели и критерии качества.

Обоснован набор частных показателей качества для радиорелейных и спутниковых каналов связи. Указана целесообразность перехода от векторного показателя качества к скалярному показателю. Предложен критерий пригодности с тремя исходами. Для решения задачи формирования интегрального показателя качества предложено использовать нечеткую экспертную систему. Рассмотрена последовательность синтеза нечеткой экспертной системы с использованием пакета Fuzzy Logic Toolbox.

A.V. Eliseev[1], E.V. Zemlyakova[1], M.P. Kovalenko[1], V.I. Yukhnov[2]

EVALUATION OF THE QUALITY OF A DIGITAL COMMUNICATION CHANNEL BASED ON A FUZZY EXPERT SYSTEM

Don State Technical University, Rostov-on-Don, Russia[1]
North-Caucasus Branch of the Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: digital communication channel, technical diagnostics, quality indicators and criteria.

A set of particular quality indicators for radio relay and satellite communication channels is substantiated. The expediency of switching from a vector quality indicator to a scalar indicator is indicated. A fitness criterion with three outcomes is proposed. To solve the problem of forming an integral quality indicator, it is proposed to use a fuzzy expert system. The sequence of synthesis of a fuzzy expert system using the Fuzzy Logic Toolbox package is considered.

При разработке и эксплуатации цифровых каналов связи (ЦКС) важным вопросом является оценка их качества. Под качеством будем понимать совокупность полезных свойств ЦКС, влияющих на способность ЦКС удовлетворять потребности абонентов в услугах связи [1]. При этом следует отметить, что качество ЦКС следует рассматривать как с позиции потребителя услуг связи – абонента сети связи, так и с позиции специалистов, занимающихся вопросами технической эксплуатации ЦКС. Иногда уровень качества ЦКС может по-разному оцениваться этими сторонами. Так, например, система связи может вполне удовлетворять абонента, так как обеспечивает еще требуемые показатели качества, но уже может не удовлетворять специалиста по эксплуатации, так как её ряд технических параметров уже приближается к предельным значениям, что может привести к нарушению связи в ближайшее время. С учетом сказанного возникает потребность в комплексном подходе к оценке качества ЦКС. Качество ЦКС различных типов, например, радиорелейных и спутниковых, существенным образом зависит от их технического состояния. По этой причине важным вопросом является создание системы технической диагностики (СТД), предназначенной для оценки технического состояния ЦКС. Существующие СТД принято делить на две большие группы: СТД с тестовым диагнозом (СТД ТД) и СТД с функциональным диагнозом (СТД ФД) [2]. Системы первого типа решают задачи диагноза с использованием специальных тестовых сигналов и требуют вывода ЦКС из эксплуатации. Системы второго типа решают задачи диагноза непосредственно в процессе применения ЦКС по функциональному назначению с использованием реальных входных воздействий. С учетом этих особенностей функционирования СТД ТД обладают большей глубиной и достоверностью диагностирования, но меньшей оперативностью, а СТД ФД – большей оперативностью, но, как правило, меньшей глубиной поиска по причине ограниченности внешних рабочих воздействий, реакции на которые и используются для оценки технического состояния ЦКС. С учетом достоинств и недостатков указанных типов СТД можно сделать вывод о целесообразности создания гибридных СДТ, способных одновременно или последовательно использовать как принцип тестового диагноза, так и принцип функционального диагноза. Таким образом, задача создания эффективной системы СТД ЦКС по-прежнему является актуальной.

Синтез СТД ЦКС должен начинаться с выбора показателей и критериев качества. При этом, как уже отмечалось выше, необходимо комплексировать различные показатели качества, учитывающие интересы как потребителей услуг связи, так и специалистов по эксплуатации.

В соответствии с [3-5] для ЦКС предлагается использовать две группы показателей качества: показатели ошибок (ER), показатели дрожания (JI) и дрейфа фазы (PDI). Для цифровых каналов спутниковых систем в [3] установлено применение пяти групп показателей:

показатели ошибок (ER); показатели дрожания (JI) и дрейфа фазы (PDI); показатели проскальзывания (TSI); показатели задержки прохождения сигнала (DI); показатель надежности (RI). Однако следует отметить, что в связи с широким внедрением адаптивных ЦКС, способных изменять свои параметры и характеристики, например, вид цифровой модуляции, следует ввести дополнительные показатели качества: относительная скорость передачи (RSI), энергетический запас линии (IERL). Данные показатели позволят учесть влияние среды распространения сигнала на общее качество ЦКС и спрогнозировать его изменение. Наличие такого прогноза позволит своевременно принять организационные и технические мероприятия, направленные на недопущение снижения качества.

Таким образом, на основе проведенного анализа были выбраны частные показатели качества обобщенного ЦКС, которые можно представить в виде векторного показателя:

$$VQI = \{ER, JI, PDI, TSI, DI, RI, RSI, IERL\} = \{vqi_k, k = \overline{1,K}\}, \quad K = 8. \tag{1}$$

Следующей задачей, которую необходимо решить при оценке качества ЦКС, является выбор критерия качества.

Для принятия решения об уровне качества ЦКС в [2] принято использовать критерий пригодности, в соответствии с которым объект считается пригодным для использования, если реальные значения частных показателей качества $\beta(t)$ удовлетворяют заданным ограничениям β^*, например:

$$K_{QoS} = \begin{cases} I_1, \text{если } (\beta_1 \le \beta_1^* \text{ и } \beta_2 \le \beta_2^* \text{ и} \ldots \text{и } \beta_N \ge \beta_N^* \ ); \\ I_0, \text{иначе;} \end{cases} \tag{2}$$

где I_1, I_0 – возможные исходы оценки качества ЦКС, соответственно, I_1 – качество ЦКП «удовлетворительное» и I_0 – качество ЦКП «неудовлетворительное».

Однако, применение критерия вида (2) нецелесообразно по двум основным причинам:

- во-первых, он не обеспечивает формирования информации о процессе деградации качества ЦКС;
- во-вторых, применение векторного показателя, состоящего из множества частных показателей, а также четких условий их сравнения с «допусками» не позволяет учесть различную степень влияния каждого частного показателя на итоговое качество.

Для устранения первой причины предлагается расширить множество возможных исходов оценки качества за счет введения нового исхода – «предельное». Данный исход предполагает такое состояние ЦКС, когда его качество еще является «удовлетворительным», но значения некоторых частных показателей приближаются к границам допусков, что может привести к скачкообразному снижению качества ЦКС до «неудовлетворительного». Наступление данного исхода свидетельствует о предотказном состоянии ЦКС и, соответственно, требует принятия управленческих решений на организацию и проведение технического обслуживания или ремонта оборудования.

Для устранения второй причины целесообразно перейти от векторного показателя качества (1) к скалярному показателю SQI, являющемуся функцией от частных показателей:

$$SQI = f(ER, JI, PDI, TSI, DI, RI, RSI, IERL), \tag{3}$$

где $f(\cdot)$ – заданная функция скаляризации векторного показателя.

Таким образом, с учетом рассмотренных выше мер, направленных на устранение недостатков критерия (2), предлагается использовать следующий критерий оценки качества ЦКС:

$$K_{QoS} = \begin{cases} I_{УК}, \text{если} \left(\beta_2 \le SQI^* \le \beta_{max} \right); \\ I_{ПРК}, \text{если} \left(\beta_1 \le SQI^* < \beta_2 \right); \\ I_{НУК}, \text{если} \left(\beta_{min} \le SQI^* < \beta_1 \right); \end{cases} \quad (4)$$

где $I_{УК}, I_{ПРК}, I_{НУК}$ – возможные исходы оценки качества ЦКС, соответственно, $I_{УК}$ – качество ЦКС «удовлетворительное», $I_{ПРК}$ – качество ЦКС «предельное» и $I_{НУК}$ – качество ЦКС «неудовлетворительное»;

SQI^* – оценка интегрального (скалярного) показателя качества;

$SQI^* \in [\beta_{min}, \beta_{max}] = [\beta_{min}, \beta_1[\cup [\beta_1, \beta_2[\cup [\beta_2, \beta_{max}]$.

В качестве функции скаляризации (3) на практике часто используют взвешенное суммирование частных показателей. Наряду с простотой данный метод скаляризации имеет два основных недостатка:

- возможна неявная взаимная компенсация частных показателей, которую сложно выявлять и контролировать при большом числе показателей;
- практически отсутствует учет нелинейной зависимости весовых коэффициентов от значений показателей, так как значения задаются один раз и остаются постоянными.

С учетом отмеченных недостатков метода скаляризации на основе взвешенного суммирования предлагается для формирования интегрального показателя качества SQI ЦКС использовать экспертную систему, основанную на применении нечеткого логического вывода [6-9].

Пример подобной системы для IP- телефонии рассмотрен в работе [9]. Для адаптации его к радиорелейным и спутниковым системам потребуется применение других показателей и критериев. Синтез экспертной системы, предназначенной для формирования скалярного показателя качества ЦКС, целесообразно реализовать с использованием пакета MatLab и его функционального расширения Fuzzy Logic Toolbox [10].

В состав Fuzzy Logic Toolbox входят следующие модули [10]:

- редактор систем нечёткого вывода FIS Editor (FIS);
- редактор функций принадлежности систем нечёткого вывода Membership Function Editor (MFE);
- редактор правил систем нечёткого вывода Rule Editor;
- программа просмотра правил системы нечёткого вывода Rule Viewer;
- программа просмотра поверхности нечёткого вывода Surface Viewer.

Синтез нечеткой экспертной системы, предназначенной для формирования скалярного показателя качества ЦКС, содержит следующие основные этапы:

1. Выбор входных лингвистических переменных и задание множества их значений (терм-множества). С учетом выбранных ранее показателей качества ЦКС введем следующие лингвистические переменные: sv_1 – «коэффициент ошибок по

секундам с ошибками **(**ESR – Errored conds)», sv_2 – «относительное значение фазового отклонения (JI)», sv_3 – «относительное значение дрейфа фазы (PDI)», sv_4 – «абсолютное значение числа событий типа «проскальзывание» (TSI), sv_5 – «задержка прохождения сигнала (DI)», sv_6 – «коэффициент готовности ($К_Г$)», sv_7 – «относительная скорость передачи (RSI)», sv_8 – «энергетический запас линии (IERL)». Для каждой переменной зададим терм-множества:

$$\mathbf{SV}_k = \left\{ SV_k^l, l = \overline{1,3} \right\} = \left\{ \begin{array}{l} SV_k^1\text{-"низкое значение показателя (НЗ)"}, \\ SV_k^2\text{-"среднее значение показателя (СРЗ)"}, \\ SV_k^3\text{-"высокое значение показателя (ВЗ)"} \end{array} \right\}, k = \overline{1,K}.$$

Пример выбора функций принадлежности и задания их параметров для входной лингвистической переменной sv_5 – «задержка прохождения сигнала (DI)» показан на рисунке 1.

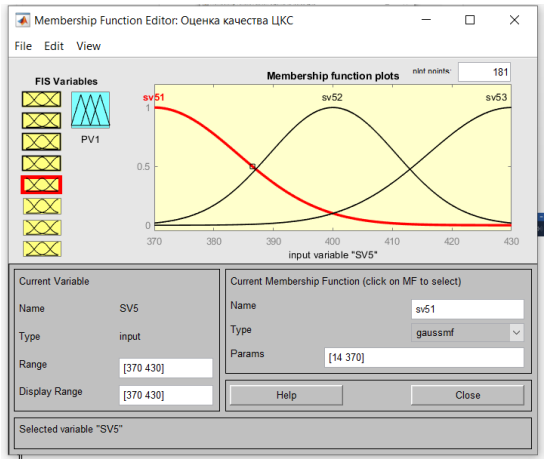


Рисунок 1. Функции принадлежности логической переменной sv_5 – «задержка прохождения сигнала (DI)»

2. Выбор выходной лингвистической переменной pv. Пусть лингвистическая переменная pv, являющаяся интегральным (скалярным) показателем качества ЦКС, задана на универсуме $E_k = [0, SQI_{max}]$ и характеризуется следующим терм-множеством:

$$\mathbf{PV} = \left\{ PV^p, p = \overline{1,4} \right\} = \left\{ \begin{array}{l} \text{"очень низкое значение (ОНЗ) "}, \\ \text{"низкое значение (НЗ) "}, \\ \text{"среднее значение (СРЗ) "}, \\ \text{"высокое значение (ВЗ) "} \end{array} \right\}.$$

3. Создание системы нечетких продукционных правил, отражающих связь значений входных и выходных переменных, например:

$$r = 1\text{: if } \begin{pmatrix} (sv_1 = B3) \\ \text{and } (sv_2 = B3) \\ \text{and } (sv_3 = B3) \\ \text{and } (sv_4 = B3) \\ \text{and } (sv_5 = B3) \\ \text{and } (sv_6 = H3) \\ \text{and } (sv_7 = H3) \\ \text{and } (sv_8 = H3) \end{pmatrix}, \text{ then } (pv = OH3)$$

.

4. Выбор правила нечеткого логического вывода и метода «дефаззификации», например, «минимаксное» правило логического вывода Мамдани-Заде и «дефаззификация» на основе метода «центра тяжести».

Результатом проведенного синтеза является нечеткая логическая система (НЛС), обеспечивающая формирование интегральной оценки качества ЦКС на основе множества входных частных показателей качества. Пример применения НЛС приведен на рисунке 2.

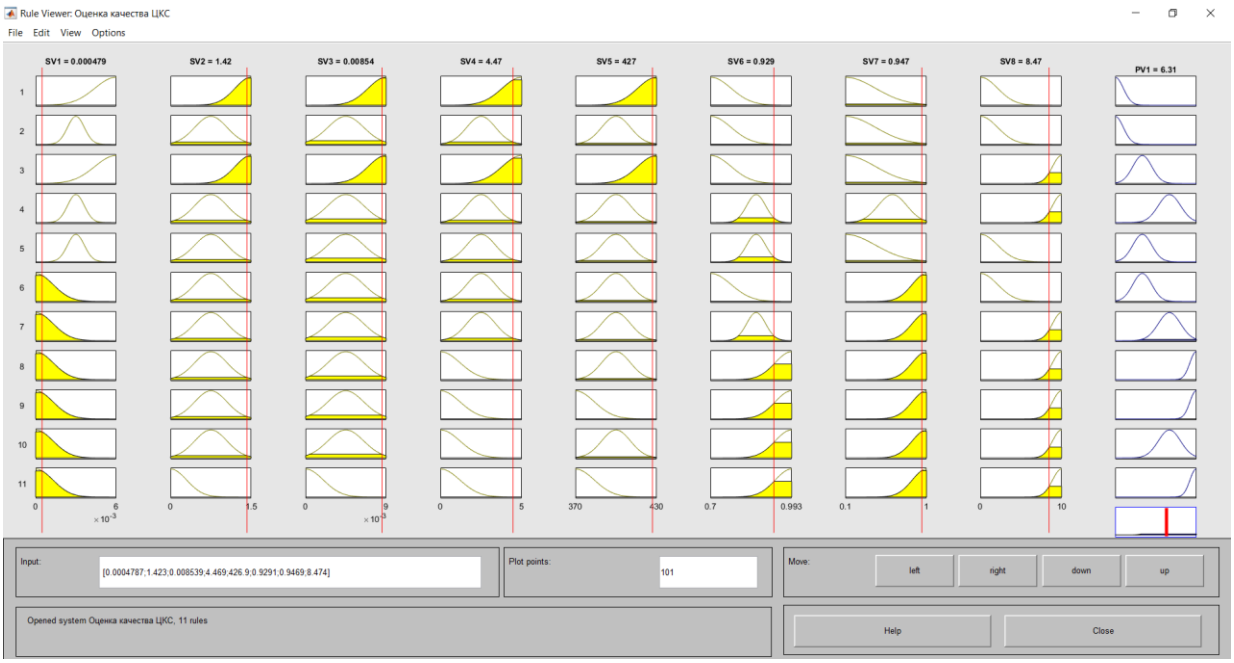


Рисунок 2. Пример вида графического интерфейса для конкретных значений входных переменных

Таким образом, в настоящей статье обоснован выбор показателей и критерия качества ЦКС, позволяющих решить задачу формирования интегральной оценки качества ЦКС на основе применения нечеткой экспертной системы. Использование предложенных результатов позволит повысить автоматизацию процедуры оценки как качества услуг, так и технического состояния ЦКС.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов А.В. Контроль соответствия в телекоммуникациях и связи. Часть 1 - М.: Компания САЙРУС СИСТЕМС, 2001. – 378с.
2. Воробьев В.Г., Константинов В.Д. Надежность и техническая диагностика авиационного оборудования: учебник. – М.: МГТУ ГА, 2010. – 448с.
3. ГОСТР 52594-2006. Магистральные каналы волоконно-оптических, радиорелейных и спутниковых систем передачи цифровых телевизионных сигналов. Основные параметры и методы измерений. – М.: Стандартинформ, 2007. – 45с.
4. Алексеев Е.Б. Эксплуатационные нормы на показатели качества функционирования каналов и трактов передачи цифровых транспортных сетей // T-Comm, – 2012. №8. С. 6-9.
5. Засецкий А.В., Иванов А.Б., Постников С.Д., Соколов И.В. Контроль качества в телекоммуникациях и связи. Часть II, под редакцией А.Б. Иванова. – М.: Компания САЙРУС СИСТЕМС, 2001. – 334с.
6. Гостев В.И. Проектирование нечетких логических регуляторов для систем автоматического управления. – СПб.: БХВ-Петербург, 2011. – 416с.
7. Елисеев А.В. Идентификация модели объекта, заданной в виде нечеткого уравнения в отношениях // Автометрия. – 2007. №1. Т43. С. 65-75.
8. Елисеев А.В., Ануфриев К.В., Погорелов Р.А., Рубайло Д.Э. Алгоритм адаптивной настройки параметров линейного дискретного фильтра с использованием нечеткой экспертной системы // Радиотехника. – 2019. –Т. 83. – № 7 (9). С. 89-102.
9. Рзаев Р.Р., Гоюшов А.И. Интеллектуальная оценка качества телекоммуникационных услуг // Информационно-управляющие системы. – 2014. – №6. С. 57-67.
10. Леоненков А.В. Нечеткое моделирование в среде MatLab и fuzzy TECH. – СПб.: БХВ-Петербург, 2003. – 736с.

Д.А. Безуглов[1], Ю.Д. Безуглов[2], В.И. Юхнов[2]

СОВРЕМЕННЫЕ ПОДХОДЫ К СОЗДАНИЮ АВТОНОМНЫХ СРЕДСТВ ИЗМЕРЕНИЙ

Ростовский филиал Российской таможенной академии,
Ростов-на-Дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: групповые эталоны единиц величин; стандарты основных единиц величин; автоматизированные поверочные комплексы.

В работе рассмотрено новое перспективное направление повышения метрологической автономности: формирование групповых эталонов единиц величин и автономных средств измерений на основе групповых эталонов, позволяющих повысить стабильность их метрологических характеристик и расширить межповерочный интервал, являющийся основным показателем метрологической автономности группового эталона.

Показано, что совершенствование технических характеристик перспективных средств измерений, предназначенных для хранения, воспроизведения и передачи размера единиц величин, возможно путём формирования принципиально новых групповых эталонов и

автономных средств измерений, реализующих идеи и принципы использования приборов с автономной поверкой, групповых эталонов и систем самоповерки, а также применение метода базовых величин и квантовой электроники при передаче размеров единиц величин.

D.A. Bezuglov[1], Y.D. Bezuglov[2], V.I. Yukhnov[2]

MODERN APPROACHES TO CREATIONAUTONOMOUS MEASURING INSTRUMENTS

Rostovsky branch of the Russian Customs Academy, Rostov-on-Don, Russia
North-Caucasus Branch of the Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: group standards of units of quantities; standards of basic units of quantities; automated verification complexes.

The paper considers a new promising direction of increasing metrological autonomy: the formation of group standards of units of quantities and autonomous measuring instruments based on group standards, which increase the stability of their metrological characteristics and expand the verification interval, which is the main indicator of metrological autonomy of a group standard.

It is shown that the improvement of the technical characteristics of promising measuring instruments intended for storing, reproducing and transmitting the size of units of quantities is possible by forming fundamentally new group standards and autonomous measuring instruments that implement the ideas and principles of using devices with autonomous verification, group standards and self-verification systems, as well as the use of the method of basic quantities and quantum electronics when transmitting the size of units of quantities.

В настоящее время выделяют следующие основные виды автономных средств хранения, воспроизведения и передачи размера единиц величин: групповые эталоны единиц величин; стандарты основных единиц величин и автоматизированные поверочные комплексы.

Стандарты основных единиц величин представляют собой отдельные исходные меры, для которых определяющим параметром является высокая точность передачи размера единицы другим мерам и средствам измерений. Существенным недостаткам стандарта, ставящим под сомнение его единоличное применение как устройства, служащего для хранения единицы величины, следует отнести достаточно большую вероятность возникновения внезапных отказов и связанное с этим увеличение риска невыполнения измерительных задач при его использовании, что недопустимо в условиях перехода к автономному принципу метрологического обеспечения.

Более надежным способом хранения единицы величины в этих условиях является создание и введение в метрологических органах групповых эталонов единиц величин. Под групповым эталоном понимается совокупность исходных и рабочих эталонов, позволяющих осуществить воспроизведение данной единицы величины, хранение и передачу ее размера другим средствам измерений с заданной точностью.

Для создания групповых эталонов, как правило, используются средства измерения одного класса точности, в исключительных случаях допускается включать и разноточные средства измерений.

На каждый групповой эталон разрабатываются методики воспроизведения единицы величины, в которых указывается его назначение, состав, порядок подготовки к работе и обработки результатов измерений и поверки средств измерений. Результаты поверки групповым методом оформляются в соответствии с действующей нормативно-технической документацией по поверке средств измерений.

Наиболее перспективным направлением повышения точности измерений при переходе от традиционного принципа иерархии метрологического обеспечения к автономному является создание автоматизированных поверочных комплексов. В основе их построения лежат идеи и принципы использования приборов с автономной поверкой, групповых эталонов и систем самоповерки, а также применение метода базовых величин и квантовой электроники при передаче размеров единиц величин. Комплексы предназначены для метрологического обеспечения единства и точности измерений на основе территориального принципа и требований автономности при удалении от центральных поверочных органов на расстояние до 8000 км.

Данные комплексы позволяют в местах эксплуатации СИ:

- обслуживать 65 % парка средств измерений, из них 99 % всех электроизмерительных и 95 % радиоизмерительных приборов;
- сократить на 40% количество средств измерений, поверяемых в вышестоящих метрологических органах Госстандарта;
- снизить на 25% количество отказов средств измерений, вызванных воздействием перегрузок при их транспортировке;
- заменить около 80% устаревшего и выработавшего свой ресурс поверочного оборудования и рабочих эталонов.
- повысить живучесть и глобальность системы передачи размеров единиц величин за счет использования сигналов ГЛОНАСС и повышения уровня метрологической автономности до 97 % (доля средств измерений, поверяемых на местах).

В практике радиотехнических и радиоэлектронных измерений массовое использование получили четыре физические величины: длина, масса, время и сила электрического тока, по которым можно оценить значение любой другой производной физической величины. Следовательно, если в комплекс ввести четыре эталонные меры длины, массы, времени и силы электрического тока, - то по ним, теоретически, могут быть поверены все приборы любого радиотехнического комплекса [1,2,3,4,5]. Физически это может быть проверено путем косвенных измерений либо на основе применения соответствующих высокостабильных преобразователей физических величин. Учитывая практическую ограниченность состава приборов комплекса, определяемую реальной потребностью решаемых измерительных задач, наиболее рациональными в качестве базовых принимаются не исходные, а производные физические величины: частота, постоянное напряжение, электрическое сопротивление постоянному току, волновое сопротивление коаксиальных трактов.

Причем, использование для передачи частоты спутниковой системы ГЛОНАСС обеспечивает глобальность ее доведения до рабочих эталонов комплекса.

Включение в состав комплекса приборов с автономной поверкой на различных его иерархических уровнях позволяет осуществлять поверку широкодиапазонных рабочих эталонов (нижний уровень иерархии) с использованием одной возимой однозначной меры (верхний уровень иерархии).

Под самоповеркой понимается совокупность операций по определению погрешностей измерительных каналов и рабочих эталонов комплекса с заданной достоверностью с использованием измерительных средств, средств автоматизации и вычислительной техники из состава комплекса. Те же операции без определения погрешностей (проверка на функционирование), либо с определением погрешностей каналов с достоверностью, ниже заданной, классифицируются как самоконтроль.

Создание системы самоповерки и самоконтроля достаточно легко реализуются, если учесть, что одной из характерных особенностей метрологических комплексов является наличие в их составе рабочих эталонов двух классов: источников стимулирующих сигналов (калибраторов) и измерителей их параметров (напряжения, частоты, мощности и т.п.). Это

позволяет, поверив рабочий эталон одного класса, использовать их затем в качестве переносчиков размеров единиц величин для поверки рабочего эталона другого класса. Между рабочими эталонами одного класса обеспечивается проведение взаимных сличений.

Наличие в составе комплекса электронно-вычислительных машин (ЭВМ) позволяет реализовать эффективные методы поверки (самоповерки, самоконтроля) при небольшом количестве измерительной информации и отказаться от трудоемких традиционных методов поверки. Это дает возможность сократить номенклатуру используемых в составе комплекса рабочих эталонов**,** существенно сократить время измерений и повысить их точность. Такое построение комплекса значительно упрощает его поверку, которая осуществляется в составе комплекса без демонтажа поверяемых рабочих эталонов**.**

Создание групповых эталонов, в основном, из рабочих эталонов верхнего уровня иерархии комплекса позволяет повысить стабильность метрологических характеристик комплекса в процессе эксплуатации и на этой основе расширить его межповерочный интервал, являющийся основным показателем метрологической автономности автоматизированных поверочных комплексов. При этом достигается высокий уровень метрологической автономности самих метрологических органов.

В настоящее время разработан ряд Методических указаний по формированию и использованию групповых мер физических величин [29], которые являются основным нормативным документом для метрологических органов и служб при организации метрологического обеспечения средств измерений.

Настоящие методические указания устанавливают порядок формирования и использования групповых эталонов единиц величин как звеньев системы передачи размера единиц измерений от государственных (ведомственных) эталонов к рабочим средствам измерений при переходе к автономному принципу иерархии метрологического обеспечения.

Анализ положений данных методик выявил ряд существенных недостатков в представленных традиционных алгоритмах проведения и обработки результатов взаимных сличений хранителей единиц величин групповых эталонов, а также оставил открытым вопрос о продолжительности времени достоверного хранения единиц величин групповыми эталонами, т.е. о межповерочном интервале групповых эталонов единиц величин.

Следуя проведённому в работе [5] анализу традиционных алгоритмов проведения и обработки результатов взаимных сличений хранителей единиц величин групповых эталонов, остановимся на наиболее существенных недостатков, присущих данным алгоритмам.

Выходные единицы групповых эталонов обычно являются аналитическими величинами, сформированными на ансамбле хранителей путем статистической обработки данных взаимных сличений между хранителями единицы величины. Поэтому стабильность группового эталона определяется не только метрологическими характеристиками, но и эффективностью статистических методов обработки данных взаимных сличений. Таким образом, задача оценивания единицы величины группового эталона по результатам взаимных сличений хранителей единицы величины является достаточно актуальной, особенно в условиях метрологической автономности.

Для реализации традиционного алгоритма формирования и оценки параметров группового эталона выбирается один наиболее стабильный и надежный хранитель, который называют опорным, и оценка единицы величины группового эталона принимается в виде относительной поправки на единицу величины опорного хранителя.

Данный алгоритм несовершенен с точки зрения устойчивости формируемой единицы величины группового эталона к изменению состава группы, так как вывод из группы или включение в её состав нового хранителя, имеющего некоторое ненулевое действительное значение погрешности единицы величины, приведет к скачкообразному изменению действительного значения единицы величины группового эталона. Чтобы избежать этого, обычно используют прогноз единицы величины хранителей относительно групповой, полученной на некотором интервале по результатам предшествующих наблюдений. Такой

алгоритм является устойчивым к изменению состава группы и составляет основу ведения большинства современных эталонов, но несмотря на то, что данный алгоритм получил широкое распространение и хорошо зарекомендовал себя в практической деятельности, он также не лишен целого ряда существенных недостатков, основными из которых являются:

- наличие явно выраженного "лидера". Несмотря на то, что в качестве опорного выбирается наиболее стабильный и надежный хранитель в случае его отказа, перевод единиц группового эталона на другую "опору" потребует значительных усилий, связанных с изменением схемы сличений, учетом задержек в кабелях, а, зачастую, и с изменением математического обеспечения, используемого в штатном цикле ведения эталона;
- жесткая схема сличений, организованная по принципу "каждый с опорным". При этом результаты других сличений (хранителей между собой, но не с опорным) используются только для дополнительного контроля и не поступают в непосредственную обработку. И наоборот, отсутствие прямых сличений какого – либо хранителя с "лидером" затрудняет возможность его использования для формирования групповой единицы величины, так как косвенный пересчет единиц величин через третий хранитель существенно снижает точность и достоверность измерений.

На ряду с этими недостатками традиционные алгоритмы проведения взаимных сличений хранителей единицы величины группового эталона не учитывает особенности в ведении аналоговых и цифровых групповых эталонов.

Таким образом, используемые в настоящее время алгоритмы проведения взаимных сличений хранителей единицы величины группового эталона, с одной стороны не обеспечивают достаточной точности при смене опорного хранителя, а с другой стороны, имеют низкий коэффициент использования измерительной информации.

Выводы

Приоритетным направлением перестройки и развития метрологического обеспечения разработки, производства, испытаний и эксплуатации современных средств измерений является оптимизация системы обеспечения единства и точности измерений на основе территориального принципа и требований автономности.

Повышение автономности региональных и территориальных систем обеспечения единства измерений может быть достигнута путем оснащения измерительных лабораторий и испытательных центров высокостабильными эталонами и установками, а также автономными многофункциональными измерительными комплексами.

Наиболее перспективным направлением повышения метрологической автономности является формирование групповых эталонов единиц величин и автономных средств измерений на основе групповых эталонов, позволяющих повысить стабильность их метрологических характеристик и расширить межповерочный интервал, являющийся основным показателем метрологической автономности группового эталона.

Совершенствование технических характеристик перспективных средств измерений, предназначенных для хранения, воспроизведения и передачи размера единиц величин, возможно путём формирования принципиально новых групповых эталонов и автономных средств измерений, реализующих идеи и принципы использования приборов с автономной поверкой, групповых эталонов и систем самоповерки, а также применение метода базовых величин и квантовой электроники при передаче размеров единиц величин.

Высокий уровень автономности как основного качественного показателя автономных средств измерений достигается за счет создания групповых эталонов, позволяющих повысить стабильность метрологических характеристик исходных мер в процессе их эксплуатации. При этом стабильность автономных средств измерений определяется не только его метрологическими характеристиками, но и эффективностью статистических методов измерений.

СПИСОК ЛИТЕРАТУРЫ

1. Донченко С.И., Блинов И.Ю., Гончаров А.С., Норец И.Б. Современное состояние и перспективы развития эталонной базы Государственной службы времени, частоты и определения параметров вращения Земли // Измерительная техника. 2015, № 1, 2015, с. 5-8.
2. Гайгеров Б.А., Сысоев В.П. Учет релятивистских эффектов при сличении шкал времени с помощью перевозимых квантовых часов // Измерительная техника. 2012, №2, с. 25-29.
3. Безуглов Д.А., Юхнов В.И. Нелинейные преобразования метрологических характеристик автономных средств измерений // Фундаментальные исследования. 2015. № 11-2. С. 232-236.
4. Безуглов Д.А., Поморцев П.М. Устройство оценки действительного значения единицы физической величины цифрового группового эталона. Патент на изобретение RU 3592141 от 3.04.2003.
5. Безуглов Д.А., Поморцев П.М. Устройство оценки действительного значения единицы физической величины аналогового группового эталона. Патент на изобретение RU 4519854 от 16.02.2004.

А.Н. Шухардин[1], А.В. Шкорина[2]

МЕТОДИКА ОПЕРАТИВНОГО ОЦЕНИВАНИЯ ВЕРОЯТНОСТЕЙ И СРОКОВ ДОСТАВКИ СООБЩЕНИЙ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Военная академия Ракетных войск стратегического назначения им. Петра Великого,
Московская обл., г. Балашиха, Россия [2]

Ключевые слова: оперативное оценивание, информационно-телекоммуникационная система, вероятность доставки сообщения, сроки доставки сообщения.

В статье рассмотрена методика, позволяющая выявить все существующие пути доставки сообщений в информационно-телекоммуникационных системах, а также оценить вероятность и сроки доставки информации до всех узлов системы при изменениях характеристик системы в процессе эксплуатации.

A.N. Shukhardin[1], A.V. Shkorina[2]

OPERATIONAL ASSESSMENT METHODOLOGY PROBABILITIES AND TIMES OF DELIVERY OF MESSAGES IN INFORMATION AND TELECOMMUNICATION SYSTEMS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Military Academy of Strategic Missile Forces, Moscow region, Balashikha, Russia[2]

Keywords: operational assessment, information and telecommunication system, probability of message delivery, probability of message delivery.

The article considers a technique that allows to identify all existing ways of message delivery in information and telecommunication systems, as well as to assess the probability and timing of information delivery to all nodes of the system with changes in the characteristics of the system during operation.

При создании современных информационно-телекоммуникационных систем (ИТС) различного назначения их структура зачастую имеет сложный территориально-распределённый иерархический характер с большим количеством дублирующих узлов и связей. Анализ возможностей передачи информации в таких системах с требуемым качеством решается различными методами на этапах проектирования и ввода в эксплуатацию, однако, в процессе эксплуатации возможно нарушение структуры ИТС, а также изменение свойств её структурных элементов, вследствие чего доставка сообщений до адресата может стать сложной задачей. Таким образом, периодически появляется необходимость провести оценку возможностей выполнения системой заданных требований, при этом в системах, обслуживающих критически значимые объекты инфраструктуры, проведение натурных исследований в процессе эксплуатации либо невозможно, либо не целесообразно по различным причинам.

В работах [1, 2] было показано, что на основе теории сетей Петри возможно создание моделей информационно-телекоммуникационных систем, позволяющие с относительно невысокими вычислительными затратами проводить моделирование функционирования таких систем.

Требуется разработать методику оценивания вероятностей и сроков доставки сообщений до каждого узла системы при изменении её структуры, характеристик её элементов, которая позволяла бы эксплуатирующему персоналу оперативно находить все возможные в заданных условиях обстановки пути доставки сообщения от пункта-источника до всех узлов в ИТС, а также рассчитать вероятность и сроки доставки сообщений для каждого пути.

В основе разработанной методики лежит моделирование функционирования информационно-телекоммуникационной системы при доведении информации основе математической модели $C_{ИТС}$, представляющей собой раскрашенную иерархическую сеть Петри с помечающей функцией

$$C_{ИТС} = (V, S, I, O, M, \Sigma), \quad (1)$$

где V – множество позиций сети;
S – множество переходов сети;
I – входная функция сети;
O – выходная функция сети;
M – множество цветов фишек;
Σ – помечающая функция.

Выполнение методики производится в четыре этапа. Порядок выполнения методики представлен на рисунке 1.

На первом этапе проводится формирование исходных данных. В качестве исходных данных при моделировании используются значения вероятностей функционирования узлов системы, времени обработки сообщения в узлах системы перед его передачей, вероятностей и времён передачи сообщений по линиям связи в каждой подсистеме, соответствующие текущей обстановке. В начальной маркировке модели $\mu^0_{ИТС}$ учитывается текущее состояние подсистем (маркировка служебных позиций модели вектором $\mu_{ИТС}$) и источник сообщения (маркировка позиции, соответствующей узлу-источнику, вектором $\mu^c_{ИТС}$, а именно фишкой, обладающей

цветом подсистемы-источника). Текущие состояния узлов системы учитываются соответствующими маркировками составных переходов μ_{ck}.

На втором этапе выполнения методики проводится моделирование функционирования ИТС при доведении информации до тех пор, пока в модели не останется ни одного активного перехода. По окончании моделирования в позициях модели будут находиться или отсутствовать фишки, окрашенные в цвета подсистем, по которым они были получены.

Каждой такой фишке соответствует массив пометок, выполненных помеченными переходами в соответствии с заданными помечающими функциями $\Sigma_{ИТС}$ и Σ_{ck}. Массив содержит информацию о пройденном пути (совокупности переходов) и характеристиках элементов пути. Каждая фишка в позиции соответствует отдельному пути доведения приказа до данной позиции. Совокупность фишек в позиции полностью определяет множество путей доставки сообщения до узла системы, соответствующего данной позиции.

Таким образом, каждой фишке в позиции $v_{упп}$ соответствует конечный массив пометок. Этот массив состоит из кортежей, содержащих метку сработавшего помеченного перехода (т.е. пройденного), значения вероятности и времени его срабатывания, и его можно представить в виде [1, 2]:

$$\left(\langle s_{u1}, p_{u1}, t_{u1}\rangle, \langle s_{u2}, p_{u2}, t_{u2}\rangle, \ldots, \left\langle s_{uZ_j}, p_{uZ_j}, t_{uZ_j}\right\rangle\right), \quad (2)$$

где s_u – переход модели $C_{ИТС}$, $s_u \in S_{ИТС}$, $S_{ИТС} = \{s_u | u = \overline{1, U}\}$;

p_u – значение вероятности срабатывания перехода s_u;

t_u – значение времени срабатывания перехода s_u;

Z_j – количество пометок помеченными переходами j-ой фишки в позиции $v_{упп}$ (количество помеченных переходов в j-ом пути до n-ого узла системы), $j = \overline{1, J_n}$;

J_n – количество фишек в позиции $v_{упп}$ (количество путей до n-ого узла).

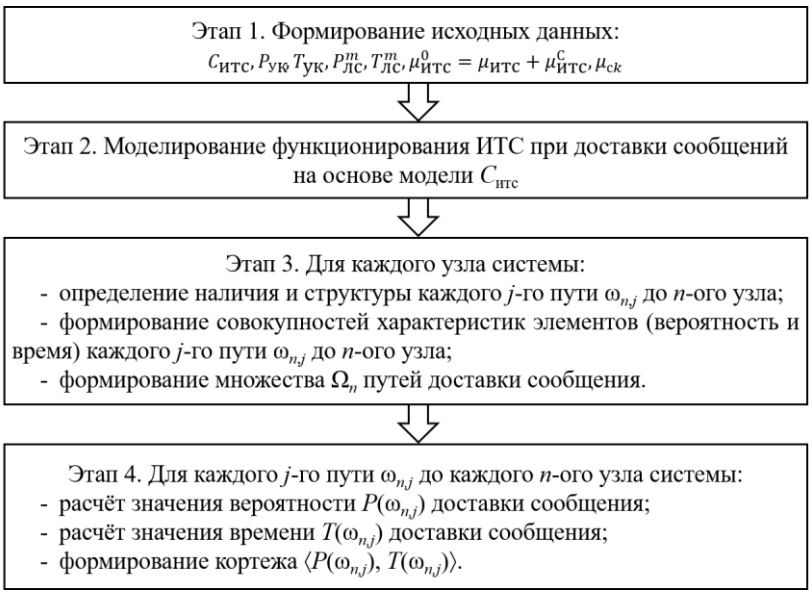


Рисунок 1. Порядок выполнения методики оценивания вероятностей и сроков доставки сообщений до каждого узла системы

На основании пометок фишек, находящихся в позициях, соответствующих узлам системы, на третьем этапе для каждого узла системы проводится:

– определение наличия и структуры каждого j-го пути $\omega_{n,j}$ до n-ого узла системы;

– формирование совокупностей характеристик элементов (вероятность и время) каждого *j*-го пути $\omega_{n,j}$ до *n*-ого узла системы;
– формирование множества Ω_n путей доставки сообщения.

Каждый *j*-й путь доставки сообщения до *n*-ого узла системы представлен последовательностью переходов:

$$\omega_{n,j} = \left(s_{u1}, s_{u2}, \ldots, s_{uZ_j}\right). \quad (3)$$

Каждый путь $\omega_{n,j}$ характеризуется совокупностями значений вероятности срабатывания переходов $\left(p_{u1}, p_{u2}, \ldots, p_{uZ_j}\right)$ и значений времени срабатывания переходов $\left(t_{u1}, t_{u2}, \ldots, t_{uZ_j}\right)$.

Множество Ω_n путей доставки сообщений до *n*-ого узла системы состоит из элементов $\omega_{n,j}$. При отсутствии фишек в позиции $v_{\text{упп}}$ $\Omega_n = \varnothing$.

На четвёртом этапе для каждого *j*-го пути $\omega_{n,j}$ до каждого *n*-ого узла системы проводится:

– расчёт значения вероятности $P(\omega_{n,j})$ доставки сообщения;
– расчёт значения времени $T(\omega_{n,j})$ доставки сообщения;
– формирование кортежа $\langle P(\omega_{n,j}), T(\omega_{n,j})\rangle$

Срабатывания переходов при прохождении фишки по каждому пути $\omega_{n,j}$ наступают совместно и являются независимыми в совокупности. Вероятность совместного появления нескольких событий, независимых в совокупности, равна произведению вероятностей этих событий. Следовательно, вероятность доставки сообщения до *n*-ого узла системы по пути $\omega_{n,j}$ определяется выражением

$$P\left(\omega_{n,j}\right) = \prod_{z=1}^{Z_j} p_{u,z}, \quad (4)$$

а сроки доставки сообщения до *n*-ого узла системы по пути $\omega_{n,j}$ –

$$T\left(\omega_{n,j}\right) = \sum_{z=1}^{Z_j} t_{u,z}. \quad (5)$$

Расчёт на основании выражений (4), (5) проводится для каждого пути из множества Ω_n для каждого узла системы. В зависимости от принадлежности перехода к множеству узлов системы или линий связи значения вероятности и времени его срабатывания есть значения вероятности функционирования узла системы и времени обработки на нём сообщения или значения вероятности передачи сообщения по линии связи и времени, необходимого для этого.

Полученные множества путей Ω_n и кортежи значений вероятности и сроков доставки сообщений по каждому из путей $\langle P(\omega_{n,j}), T(\omega_{n,j})\rangle$ являются выходными данными разработанной методики.

Порядок выполнения 2–4 этапов методики описан алгоритмом, представленным на рисунках 2, 3. Перед моделированием выполняется загрузка исходных данных (рисунок 2, блок 1).

Моделирование процесса доставки сообщения до узла системы есть выполнение сети Петри (второй этап методики), которое проводится в цикле «Моделирование ($C_{\text{ИТС}}$)» (блоки 2–7) до тех пор, пока в модели не останется ни одного активного перехода.

Для выполнения модели определяется наличие в ней активных переходов (блок 3). Если в модели есть хотя бы один активный переход (блок 4, решение «Да»), то проводится случайный выбор одного из активных переходов и его срабатывание (блок 5). Если переход является составным, то происходит выполнение соответствующей модели функционирования узла системы. В результате срабатывания перехода изменяется маркировка модели, и происходит пометка фишки (фишек) помечающей функцией $\Sigma_{\text{ИТС}}$ или Σ_{ck} (блок 6). Пометка является кортежем $\langle s_u, p_u, t_u\rangle$, содержащим метку сработавшего помеченного перехода (т.е. пройденного) s_u, значения вероятности p_u и времени t_u его срабатывания. Далее моделирование продолжается (цикл «Моделирование $C_{\text{ИТС}}$» повторяется).

Если в модели нет ни одного активного перехода (блок 4, решение «Нет»), то моделирование завершается (блок 7).

В результате моделирования $C_{ИТС}$ в позициях множества $V_{уп}$, $V_{уп} \subset V_{ИТС}$, соответствующих узлам-получателям сообщений, могут появиться фишки, соответствующие сообщениям. Количество фишек в позиции $v_{упn}$, $v_{упn} \in V_{пу}$, соответствует количеству путей доставки сообщения до n-ого узла системы. Отсутствие фишек в позиции $v_{упn}$ означает, что n-й узел системы сообщение не получил.

Проведение третьего этапа методики осуществляется в ходе выполнения цикла «Определение путей и характеристик элементов» (рисунок 3, блоки 9–13). Считывание пометок фишек из позиций $v_{упn}$ множества $V_{уп}$ модели $C_{ИТС}$ (блок 10) позволяет определить множество Ω_n путей доставки сообщения до n-ого узла системы.

Далее проводится увеличение счётчика n на 1 (блок 12), после чего цикл повторяется до перебора всех N узлов системы (блок 13).

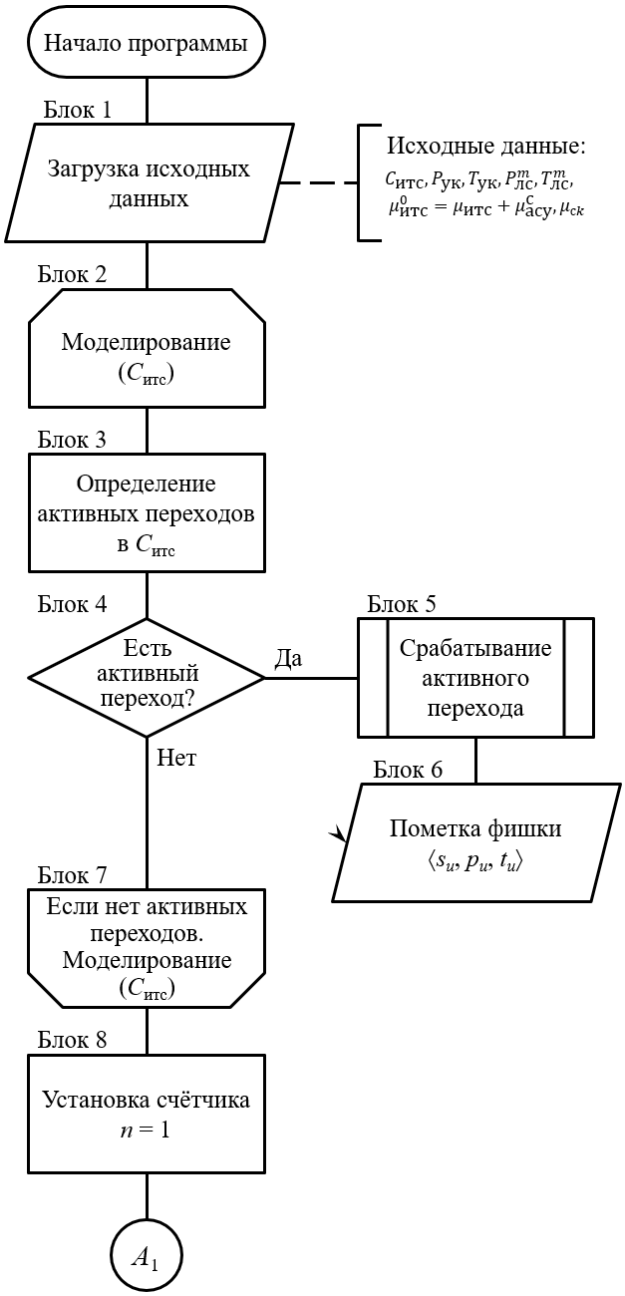


Рисунок 2. Схема алгоритма выполнения 2–4 этапов «Методики оперативного оценивания…» (часть 1)

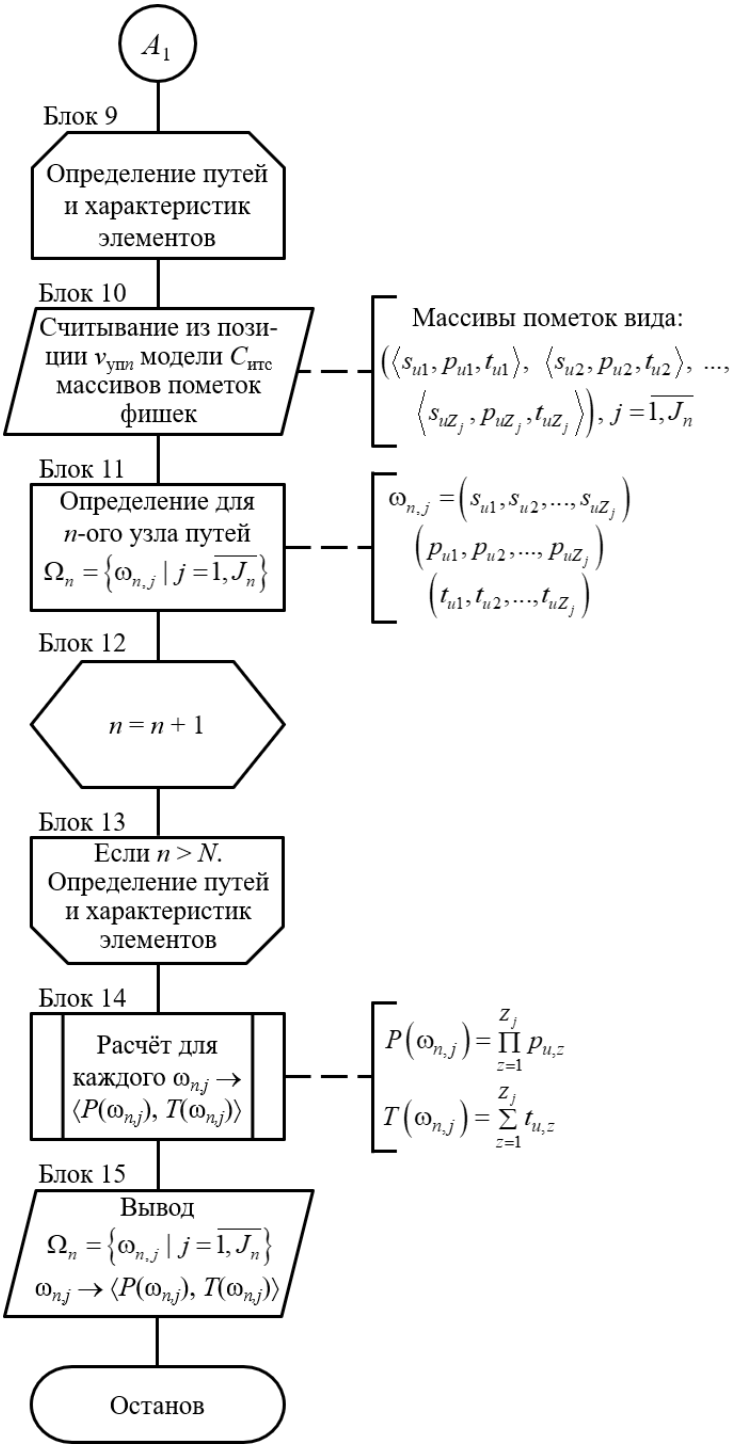


Рисунок 3. Схема алгоритма выполнения 2–4 этапов «Методики оперативного оценивания…» (часть 2)

Расчёт на основании выражений (4), (5) проводится для каждого пути из множества Ω_n для каждого узла системы (рисунок 3, блок 14). Полученные множества путей Ω_n и кортежи значений вероятности и времени доставки сообщения по каждому из путей $\langle P(\omega_{n,j}), T(\omega_{n,j})\rangle$ сохраняются в массиве данных (блок 15) для дальнейшей обработки. Выполнение блоков 14,15 соответствует четвёртому этапу методики.

Сходимость описанного алгоритма достигается конечностью циклов «Моделирование (Ситс)» (блоки 2–7) и «Определение путей и характеристик элементов» (блоки 9–13). Конечность первого достигается тем, что в модели $C_{ИТС}$ реализована блокировка циклов передачи сообщений между узлами системы. Следовательно, процесс моделирования передачи

сообщения по территориально распределённым узлам системы конечен. Конечность второго достигается последовательным изменением значения счётчика и заданием его максимального значения.

Таким образом, разработанная методика оперативного оценивания вероятностей и сроков доставки сообщений до каждого узла системы позволяет при изменении структуры информационно-телекоммуникационной системы и характеристик её элементов найти все возможные пути доставки сообщения до узлов системы в сложившейся обстановке и оценить вероятность и сроки доставки сообщения по каждому пути.

Для одного из частных случаев информационно-телекоммуникационных систем, а, именно, автоматизированной системы управления, данная методика доведена до функционирующего программного продукта, она реализована в среде Delphi 10.3.3 Community Edition, получено свидетельство о регистрации программы для ЭВМ [3].

СПИСОК ЛИТЕРАТУРЫ

1. *Шкорина А.В., Шухардин А.Н.* Оценка вероятностно-временных характеристик доведения информации в автоматизированной системе управления войсками и оружием // Вестник Ярославского высшего военного училища противовоздушной обороны. – 2019. № 4(7), С. 162-169.
2. *Шкорина А.В., Шухардин А.Н.* Модель территориально-распределенной иерархической автоматизированной системы управления // Информация и космос. – 2020. № 3, С. 94-99.
3. *Шкорина А.В.* Методика оценки вероятностно-временных характеристик доведения информации в автоматизированной системе управления // Свидетельство о регистрации программы для ЭВМ №2020616732. 22.06.2020г.

А.Н. Шухардин[1], А.В. Шкорина[2]

МОДЕЛЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ НА БАЗЕ СЕТЕЙ ПЕТРИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Военная академия Ракетных войск стратегического назначения им. Петра Великого,
Московская обл., г. Балашиха, Россия [2]

Ключевые слова: информационно-телекоммуникационная система, вероятность доведения информации, время доведения информации, сеть Петри, расширения сетей Петри.

В статье рассмотрен подход к построению на основе теории сетей Петри модели современных сложных информационно-телекоммуникационных систем (ИТС), обладающих большим количеством дублирующих узлов и связей, позволяющий определить существующие пути, а также оценить вероятность и время доведения информации до узлов системы в произвольный момент времени при деградации структуры ИТС и изменениях характеристик её элементов.

A.N. Shukhardin[1], A.V. Shkorina[2]

MODEL OF AN INFORMATION AND TELECOMMUNICATION SYSTEM BASED ON PETRI NETS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Military Academy of Strategic Missile Forces, Moscow region, Balashikha, Russia[2]

Keywords: information and telecommunication system, probability of information delivery, time of information delivery, Petri net, extensions of Petri nets.

The article considers an approach to building a model of modern complex information and telecommunication system (ITS) based on the theory of Petri nets, which has a large number of duplicating nodes and connections. This approach allows us to determine the existing paths, as well as to estimate the probability and time of bringing information to the nodes of systems at an arbitrary time when the ITS structure is degraded and the characteristics of its elements change.

В современном мире создается большое количество информационно-телекоммуникационных систем (ИТС), предназначенных для обеспечения деятельности в самых разных областях. Структура такой ИТС зачастую имеет сложный территориально-распределённый иерархический характер с большим количеством дублирующих узлов и связей. Своевременное решение задачи доведения информации до всех узлов системы в установленные сроки и с требуемым качеством для некоторых систем определяет эффективность функционирования системы в целом. Вместе с тем, в период эксплуатации возможно нарушение структуры ИТС, а также свойств её структурных элементов, вследствие чего доведение информации до узлов может стать сложной задачей.

Если при анализе вариантов доведения информации до узлов системы оценивать только время, необходимое для этого, а вероятность доведения не учитывать, это может привести к неадекватной оценке возможностей текущего состояния узлов и, в конечном итоге, к срыву доведения информации. В связи с этим при анализе вариантов доведения информации необходимо учитывать не только время, необходимое для этого, но и вероятность доведения информации [1].

В связи со сложностью и уникальностью объектов и процессов функционирования современных ИТС проведение натурных экспериментов для определения вероятности и времени доведения информации зачастую невозможно или сопряжено с высокой стоимостью. Возникает задача построения адекватной модели, позволяющей оперативно оценивать вероятность и время доведения информации до узлов системы в произвольный момент времени в конкретной сложившейся обстановке (имеющихся структуре ИТС и характеристиках её элементов).

Для решения задачи рассмотрим контур доведения распорядительной информации. Перед построением модели необходимо описать рассматриваемый контур:

информация, передаваемая в ИТС между узлами системы, формируется узлом-источником в виде сообщения;

узлы системы, которые могут передавать (ретранслировать) получаемые сообщения по линиям связи, условно называются узлами коммутации (УК);

узлы системы, которым адресованы сообщения, условно называются узлами-получателями (УП);

сообщения в ИТС передаются между УК вплоть до УП.

ИТС структурно представлена совокупностью подсистем обработки информации и связи. При наличии необходимых программно-аппаратных средств на УК и (или) полномочий

оператора УК, информация может быть передана в другую подсистему автоматически или оператором.

Необходимо построить модель ИТС, которая позволит оперативно определять множество вариантов (путей) доведения пакета до каждого узла-получателя и для каждого варианта оценивать соответствующие вероятность и время доведения пакета в любой момент времени.

Исходные данные для построения модели ИТС:

K – количество УК, задействованных в ИТС, $K \geq 1$;

N – количество УП, задействованных в ИТС, $N \geq 1$;

Q – количество подсистем, организованных в ИТС, $Q \geq 1$;

L_q – количество организованных для доведения информации линий связи (ЛС) между узлами в q-ой подсистеме, $q = \overline{1, Q}$;

$P_{\text{ук}} = \{p_{\text{ук}k} | k = \overline{1, K}\}$ – множество значений вероятностей работоспособного состояния УК;

$T_{\text{ук}} = \{T_{\text{обр}k} | k = \overline{1, K}\}$ – множество множеств значений времени обработки сообщения на УК перед его передачей по имеющимся подсистемам;

$T_{\text{обр}k} = \{t_{\text{обр}k,i} | i = \overline{1, I_k}\}$ – множество значений времени обработки сообщения, полученного на k-ом УК, перед его передачей по одной из имеющейся подсистем;

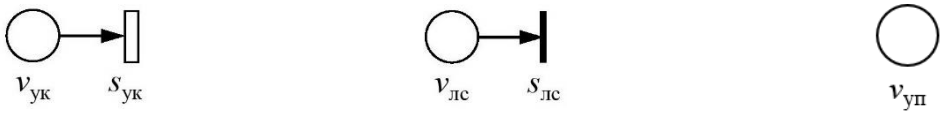
I_k – количество возможных вариантов обработки сообщения, полученных на k-ом УК, перед его передачей по имеющимся подсистемам;

$P_{\text{лс}}^q = \{p_{\text{лс}l}^q | l = \overline{1, L_q}\}$ – множество значений вероятностей передачи сообщения по ЛС в q-ой подсистеме;

$T_{\text{лс}}^q = \{t_{\text{лс}l}^q | l = \overline{1, L_q}\}$ – множество значений времени передачи сообщения по ЛС в q-ой подсистеме.

В результате проведённого анализа возможных подходов к построению необходимой модели, анализа публикаций в научных изданиях последних лет [2, 3, 4, 5] выявлено, что применение положений теории раскрашенных иерархических сетей Петри позволяет построить такую модель.

В сети Петри, как правило, условия моделируются позициями, а события – переходами. В связи с этим целесообразно УК представить совокупностью позиции $v_{\text{ук}}$ и перехода $s_{\text{ук}}$, связанных между собой дугой. Позиция представляет собой условие «получено сообщение», а переход – событие «передача сообщения». Так как на УК происходят не только процессы передачи сообщения в пределах одной подсистемы ИТС, но и трансформация сообщения для его передачи в другие подсистемы, а также блокировка возникающих циклических путей передачи сообщений, переход УК является составным (является подсетью Петри) [6]. Составной переход обозначим прямоугольником (рисунок 1, *а*). Каждая линия связи между узлами системы представляет собой совокупность позиции $v_{\text{лс}}$ и обычного перехода $s_{\text{лс}}$, связанных между собой дугой (рисунок 1, *б*). УП представляется только позицией $v_{\text{уп}}$ (рисунок 1, *в*).



а) б) в)

Рисунок 1. Графическое представление структурных элементов ИТС:
а – узел коммутации; б – линия связи; в – узел-получатель

Сообщения, передаваемые в ИТС, в модели представляются фишками. Так как ИТС может быть представлена в виде совокупности нескольких подсистем, каждая фишка имеет

свойство – цвет, соответствующий подсистеме, по которой она может быть передана. В связи с этим каждый переход каждой линии связи, в зависимости от подсистемы, в которой организована эта линия связи, получает дополнительное условие срабатывания – фишка должна быть помечена цветом, соответствующим подсистеме. Условия срабатываний переходов и правила изменения разметки сети для каждого перехода, кроме составных, задаются специальными таблицами, учитывающими цвета фишек [7].

Все УК и УП ИТС можно представить в виде множеств:

$V_{\text{ук}} = \{v_{\text{ук}k} | k = \overline{1, K}\}$ – множество позиций, соответствующих УК;

$S_{\text{ук}} = \{s_{\text{ук}k} | k = \overline{1, K}\}$ – множество переходов, соответствующих УК;

$V_{\text{уп}} = \{v_{\text{уп}n} | n = \overline{1, N}\}$ – множество позиций, соответствующих УП.

Исходя из структуры ИТС, можно утверждать, что для каждой подсистемы организованные между УК и УП линии связи будут разными и будут определяться:

наличием соответствующего оборудования в узлах системы;

правилами организации связи.

Следовательно, линии связи, организованные в q-ой подсистеме, можно представить в виде множеств:

$V_{\text{лс}}^{q} = \{v_{\text{лс}l}^{q} | l = \overline{1, L_q}\}$ – множество позиций, соответствующих линиям связи, организованным в q-ой подсистеме ИТС;

$S_{\text{лс}}^{q} = \{s_{\text{лс}l}^{q} | l = \overline{1, L_q}\}$ – множество переходов, соответствующих линиям связи, организованным в q-ой подсистеме ИТС.

В модели одной подсистемы цветом фишки и дополнительным условием срабатывания переходов $s_{\text{лс}l}^{q}$ можно пренебречь, а переходы $s_{\text{ук}k}$ считать не составными, а обыкновенными. Следовательно, модель одной подсистемы представляет собой простую (то есть без расширений) сеть Петри.

На основании выше сказанного модель q-ой подсистемы ИТС C_q будет иметь вид:

$$C_q = (V_q, S_q, I_q, O_q), \tag{1}$$

где $V_q = V_{\text{ук}} \cup V_{\text{уп}} \cup V_{\text{лс}}^{q}$ – множество позиций сети;

$S_q = S_{\text{ук}} \cup S_{\text{лс}}^{q}$ – множество переходов сети;

$I_q : S_q \rightarrow V_q$ – входная функция сети – отображение из переходов в комплекты позиций, являющихся входными позициями переходов;

$O_q : S_q \rightarrow V_q$ – выходная функция сети – отображение из переходов в комплекты позиций, являющихся выходными позициями переходов.

Следует пояснить, что УК и УП в создаваемой модели соединяются с ЛС следующим образом:

переход, соответствующий УК, соединяется одной дугой с позицией, соответствующей ЛС, – для ЛС, исходящей из УК;

переход, соответствующий ЛС, соединяется одной дугой с позицией, соответствующей УК или УП, – для ЛС, входящей в УК или УП.

Графическое представление k-го УК и n-го УП, соединённых l-ой ЛС в q-ой подсистеме, изображено на рисунке 2. Для удобства восприятия УК обозначен пунктирной линией, а ЛС – штрих-пунктирной.

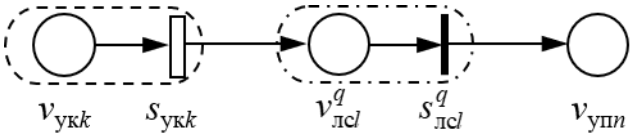


Рисунок 2. Графическое представление УК и УП, соединённых ЛС

Исходя из структуры модели C_q справедливы выражения:

$I_q(s_{\text{ук}k}) = \{v_{\text{ук}k}\}$; $I_q(s^q_{\text{лс}l}) = \{v^q_{\text{лс}l}\}$;

$O_q(s_{\text{ук}k}) \subset V^q_{\text{лс}}$; $O_q(s^q_{\text{лс}l}) = \{v_{\text{ук}k}\} \vee \{v_{\text{уп}n}\}$.

Из представленных выражений следует, что значения функций I_q и O_q не содержат повторяющиеся элементы и представляют собой множества (как частные случаи комплектов).

Модель ИТС *C* не может быть создана простым объединением подсистем, представленных моделями C_q (1), и представляется раскрашенной иерархической сетью Петри:

$$C = (V, S, I, O, M), \tag{2}$$

где $V = \bigcup_{m \in M} V_m = V_{\text{ук}} \cup V_{\text{уп}} \cup (\bigcup_{m \in M} V^m_{\text{лс}})$ – множество позиций сети;

$S = \bigcup_{m \in M} S_m = S_{\text{ук}} \cup (\bigcup_{m \in M} S^m_{\text{лс}})$ – множество переходов сети, $|S| = U$ (где $S_{\text{ук}}$ – множество составных переходов: каждый переход представлен подсетью Петри $C'_{\text{ук}k}$, $S^m_{\text{лс}}$ – множества раскрашенных переходов, которые обладают дополнительным условием срабатывания: фишка должна быть помечена цветом *m*);

$I : S \to V$ – входная функция сети – отображение из переходов в комплекты позиций, являющихся входными позициями переходов,

$$I(s_{\text{ук}k}) = I_m(s_{\text{ук}k}) = \{v_{\text{ук}k}\}, I(s^m_{\text{лс}l}) = I_m(s^m_{\text{лс}l}) = \{v^m_{\text{лс}l}\}$$

$O : S \to V$ – выходная функция сети – отображение из переходов в комплекты позиций, являющихся выходными позициями переходов,

$O(s_{\text{ук}k}) = (\bigcup_{m \in M} O_m(s_{\text{ук}k})) \subset (\bigcup_{m \in M} V^m_{\text{лс}})$, $O(s^m_{\text{лс}l}) = O_m(s^m_{\text{лс}l}) = \{v_{\text{ук}k}\} \vee \{v_{\text{уп}n}\}$;

$M = \{m | m = \overline{1, Q}\}$ – множество цветов фишек, где цвет фишки m соответствует принадлежности к *q*-ой подсистеме.

В модели *C* (2) значения функций *I* и *O* не содержат повторяющиеся элементы и представляют собой множества (как частные случаи комплектов).

Перед выполнением сети Петри *C* устанавливается начальная разметка μ_0: фишки помещаются в позиции, соответствующие узлу-источнику сообщения, и раскрашиваются цветами соответствующих подсистем. В результате выполнения сети возможно установить факт получения сообщения любым УП, а также выявить все пути, по которым это сообщение может быть получено. Каждый такой путь до *n*-го УП представляет из себя конечную последовательность запусков переходов из множества *S*:

$$\omega_{nj} = \left(s_{u1}, s_{u2}, \ldots, s_{uX_j}\right), \tag{3}$$

где X_j – количество переходов в *j*-ом пути до *n*-го УП, $j = \overline{1, Y_n}$;

Y_n – количество путей до *n*-го УП.

Совокупность всех путей доведения сообщения до *n*-го УП есть конечное множество $\Omega_n = (\omega_{n,1}, \omega_{n,2}, \ldots, \omega_{n,Y_n})$. Вычисление Ω_n возможно двумя способами:

1. Моделирование выполнения сети Петри *C*.

2. Построение и анализ дерева достижимости сети Петри *C*. Структура и алгоритм построения дерева достижимости в теории сетей Петри определены однозначно и описаны в литературе [7, 8].

Использование дерева достижимости может привести к потере информации и, возможно, к тому, что некоторые свойства сети Петри определить будет нельзя [7]. В связи с этим для вычисления Ω_n необходимо провести моделирование выполнения сети Петри *C*.

В соответствии с исходными данными каждому переходу s_u, $u = \overline{1, U}$, из множества *S* для вычисления вероятностных характеристик ставится в соответствие вероятность его

срабатывания p_u, равная: на узле коммутации – $p_{укк}$, в линии связи – $p^q_{лсl}$. Для вычисления временных характеристик в соответствии с исходными данными каждому переходу ставится в соответствие время срабатывания t_u, равное: на узле коммутации – времени обработки пакета $t_{обрk,i} \in T_{обрk}$ (вычисляется при выполнении составного перехода $s_{укк}$), в линии связи – $t^q_{лсl}$. Для учёта этих характеристик в работе сети необходимо дополнить модель (2) помечающей функцией Σ над алфавитом $A = \{a_u | u = \overline{1, U}\}$, где $a_u = \langle s_u, p_u, t_u \rangle$. То есть $\Sigma : S \rightarrow A$, $\Sigma(s_u) = a_u$, при этом [7]

$$\Sigma(\omega s_u) = \begin{cases} \Sigma(\omega)\Sigma(s_u), \text{ если } \Sigma(s_u) \text{ определено} \\ \Sigma(\omega), \text{ если } \Sigma(s_u) = \Sigma(\lambda) \end{cases},$$

где ω – последовательность переходов, запущенных непосредственно перед переходом s_u;

$\Sigma(\lambda) = \lambda$;

λ – пустое слово.

Таким образом, модель (2) принимает следующий вид:

$$C_\Sigma = (C, \Sigma) = (V, S, I, O, M, \Sigma). \quad (4)$$

Работа помечающей функции заключается в том, что каждая фишка при прохождении через переход помечается и значение помечающей функции сохраняется в соответствующий массив данных. Следовательно, для каждого искомого пути (последовательности запусков переходов) $\omega_{n,j}$ (3) фишкой фиксируется соответствующая последовательность $\left(\langle s_{u1}, p_{u1}, t_{u1}\rangle, \langle s_{u2}, p_{u2}, t_{u2}\rangle, \ldots, \left\langle s_{uX_j}, p_{uX_j}, t_{uX_j}\right\rangle\right)$.

В результате выполнения сети C_Σ (4) в позициях множества $V_{уп}$ будут находиться фишки, каждой из которых будет соответствовать последовательность меток, определяемых пройденными переходами, вероятностями и длительностями их срабатывания. Следовательно, возможно вычислить и поставить в соответствие каждому варианту прохождения сообщения ω_{nj} (3) вероятность доведения сообщения $P_{n,j}$ и время доведения сообщения $T_{n,j}$. Так как события, описанные последовательностью вероятностей $\left(p_{u1}, p_{u2}, \ldots, p_{uX_j}\right)$ срабатывания переходов независимые, то вероятность их совместного наступления есть произведение

$P_{n,j} = p_{u1} \cdot p_{u2} \cdot \ldots \cdot p_{uX_j}$.

Время доведения сообщения есть сумма

$T_{n,j} = t_{u1} + t_{u2} + \ldots + t_{uX_j}$.

Отсутствие фишек в позиции $v_{упn}$ означает не доведение сообщения до *n*-го УП.

Таким образом, предложенная модель позволяет оперативно оценивать вероятность и время доведения сообщений до узлов-получателей в информационно-телекоммуникационных системах различного назначения в произвольный момент времени при деградации структуры ИТС и изменениях характеристик её элементов.

СПИСОК ЛИТЕРАТУРЫ

1. *Шкорина А.В., Шухардин А.Н.* Оценка вероятностно-временных характеристик доведения информации в автоматизированной системе управления войсками и оружием // Вестник Ярославского высшего военного училища противовоздушной обороны. – 2019. № 4(7), С. 162-169.
2. *Кулешов И.А., Дуплинский М.А., Малахов Ю.А.* Анализ методов моделирования сетей связи // Научно-технические ведомости СПбГТУ. – 2010. № 2. С. 148–152.
3. *Тронин В.Г.* Применение раскрашенных сетей Петри в моделировании вычислительной сети // Автоматизация процессов управления. – 2007. № 2. С. 97–102.

4. *Ивутин А.Н., Дараган Е.И.* Теория сетей Петри и её расширения // Известия ТулГУ. Технические науки. – 2012. № 10. С. 211–221.
5. *Кудж С.А., Логинова А.С*. Моделирование с использованием сетей Петри // Вестник МГТУ МИРЭА. – 2015. № 1 (6). С. 10–22.
6. *Шкорина А.В., Шухардин А.Н.* Модель территориально-распределенной иерархической автоматизированной системы управления // Информация и космос. – 2020. № 3, С. 94-99.
7. *Питерсон, Дж.* Теория сетей Петри и моделирование систем / Дж. Питерсон : перевод с англ. под ред. В. А. Горбатова. – М. : Мир, 1984. – 264 с.
8. *Котов, В. Е.* Сети Петри. – М. : Мир, 1984. – 160 с.

С.В. Мухачёв, Д.А. Фараносов

О ПРЕДПОЧТЕНИЯХ В ВЫБОРЕ ЧИСЕЛ

Уральский государственный университет путей сообщения,
Екатеринбург, Россия

Ключевые слова: числа, выбор, предпочтения, распределение, пароль, криптостойкость, модель.

В статье рассмотрены предпочтения людей в выборе чисел от 0 до 9. Использованы методы статистического анализа. Полученные результаты могут быть полезны для оценки криптостойкости паролей, генерируемых человеком, а также при моделировании и объяснении общественных явлений.

S.V. Mukhachev, D.A. Faranosov

ABOUT PREFERENCES IN CHOOSING NUMBERS

Ural State University of Railway Transport,
Yekaterinburg, Russia

Keywords: numbers, choice, preferences, distribution, password, cryptographic strength, model.

The article considers people's preferences in choosing numbers from 0 to 9. Statistical analysis methods are used. The results obtained can be useful for evaluating the cryptographic strength of passwords generated by humans, as well as for modeling and explaining social phenomena.

Имеются ли у людей предпочтения при выборе чисел от 0 до 9? Казалось бы, вопрос чисто академический и имеет отношение скорее к психологии. Однако это не так. Со случайным выбором чисел приходится сталкиваться при создании пароля для доступа к устройствам и информационным ресурсам; генерации тех или иных чисел, характерных для описания сложных явлений природы и общества т.д. Поэтому вопрос интересен не только в теоретическом, но и в практическом плане: насколько устойчивы коды, созданные человеком; можно ли по сгенерированным числам определить – имеют они случайный характер, или записаны человеком. Таким образом, вопрос о предпочтении при выборе чисел интересен при обсуждении криптостойкости в информационной безопасности; при объяснении и моделировании различных, в том числе общественных явлений и т.п.

Описание попыток выяснить наличие или отсутствие таких предпочтений можно найти в публикациях. Однако они имеют либо научно-популярный характер [1], либо это – нумерологическое описание [2].

Предпринята попытка получения первичного материала и его статистической обработки с целю выявления такого рода предпочтений. Случайная выборка была сформирована из студентов 1 курса Уральского университета путей сообщения,

обучающихся по различным специальностям. Объем выборки составил 100. Каждый опрашиваемый студент независимо назвал число от 0 до 9.

В результате первичной обработки данных получена таблица 1, в которой приведены эмпирические (наблюдаемые) и теоретические частоты чисел. Теоретическая частота любого случайно выбранного чисел от 0 до 9 при объеме выборки 100 должна равняться 10 (равномерное распределение).

Принята нулевая гипотеза: распределение чисел от 0 до 9 равномерное. С помощью статистических методов оценивалась справедливость гипотезы. Для оценки статистической значимости использовался критерий Хи-квадрат. Уровень значимости был принят равным 0,01.

По приведенным в таблице 1 данным в табличном процессоре MS Excel рассчитан наблюдаемый уровень значимости (p-критерий). Для этого использовалась функция ХИ2.ТЕСТ. p-критерий оказался равен 0,002, что существенно меньше принятого уровня значимости. Гипотеза о равномерном распределении отклоняется, так как наблюдаемый уровень значимости много меньше заданного уровня значимости 0,01.

Таблица 1. Эмпирические и теоретические частоты чисел.

Число	Эмпирическая частота	Теоретическая частота
0	1	10
1	8	10
2	5	10
3	10	10
4	5	10
5	14	10
6	11	10
7	19	10
8	15	10
9	12	10
Сумма частот	100	100

Таким образом, распределение чисел от 0 до 9 следует считать не согласующимся с равномерным распределением, следовательно, при выборе чисел имеются определенные предпочтения.

Качественно характер полученного распределения приведен на рисунке 1, где темным цветом изображено распределение полученных частот. На этом же рисунке светлая гистограмма отображает распределение, полученное в [2] (при построении данные пронормированы с целью согласования масштаба).

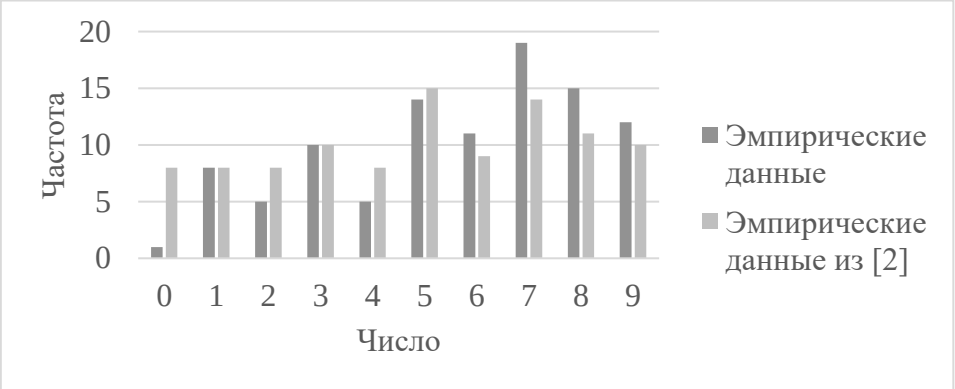


Рисунок 1. Эмпирическое распределение частот.

На основании полученных частот можно заключить, что наиболее часто выбираются числа 7, 8 и 5. Такой результат согласуется с результатами, приведенными в [1,2]. В этих публикациях также получено, что число 7, 8 и 5 выбираются чаще других.

Проведено статистическое исследование схожести полученного распределения и распределения из [2]. Пронормированные данные, полученные в [2], приведены в таблице 2. Частота числа 10 присвоена числу 0.

Была принята нулевая гипотеза H0: распределения чисел от 0 до 9 одинаковы, а различия имеют случайный характер. С помощью статистических методов оценивалась справедливость гипотезы. Для оценки статистической значимости также использовался статистический критерий Хи-квадрат. Уровень значимости был принят равным 0,01.

Таблица 2. Эмпирические и теоретические частоты чисел, полученные в [2].

Число	Эмпирическая частота
0	8
1	8
2	8
3	10
4	8
5	15
6	9
7	14
8	11
9	10

По приведенным в таблице 1 и таблице 2 данным в табличном процессоре MS Excel рассчитан наблюдаемый уровень значимости (p-критерий). Для этого использовалась функция ХИ2.ТЕСТ. p-критерий оказался равен 0,19. Гипотеза о том, что распределения одинаковы, принимается, так как наблюдаемый уровень значимости много выше заданного уровня значимости 0,01.

В результате проведенного исследования получены следующие результаты.

Числа, выбираемые человеком в диапазоне от 0 до 9, распределяются неравномерно. Об этом можно судить по наблюдаемому уровню значимости, полученному при оценке статистической значимости гипотезы о равномерном распределении: p=0,002.

Некоторые числа выбираются чаще, другие реже. Предпочтения отдаются числам 7, 8 и 5. Этот факт подтверждается в результате сравнения двух независимо полученных распределений: p-критерий, полученному при оценке статистической значимости гипотезы об одинаковости распределений оказался равен 0,19.

Полученные результаты значимы для оценки криптостойкости паролей, генерируемых пользователем без использования технических средств, так как человек склонен чаще выбирать определенные числа. Кроме того, они могут быть полезны при моделировании и объяснении различных общественных явлений, когда требуется выяснить, действительно ли те или иные числа, используемые в модели, имеют случайный характер или сгенерированы человеком.

СПИСОК ЛИТЕРАТУРЫ

1. «Seven» is world's favourite number: study /URL: https://www.business-standard.com/article/pti-stories/seven-is-world-s-favourite-number-study-114040900833_1.html (дата обращения 14.10.2021).
2. Топ 10 чисел от 1 до 10 /URL:https://medium.com/@lbrtasad/%D1%82%D0%BE%D0%BF-10%D1%87%D0%B8%D1%81%D0%B5%D0%BB-%D0%BE%D1%82-1%D0%B4%D0%BE-10-466cdaf2e07a (дата обращения 14.10.2021).

А.А. Мозоль

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ОПОЗНАВАНИЯ ВОЗДУШНЫХ ОБЪЕКТОВ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: система взаимного опознавания, ответчик, запросчик, имитостойкость.

В статье представлен краткий анализ проблемных вопросов опознавания воздушных объектов гражданского и специального назначения, а также предложены подходы к повышению эффективности опознавания.

A.A. Mozol’

IMPROVING THE EFFICIENCY OF IDENTIFICATION OF AIR OBJECTS

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

Keywords: mutual identification system, respondent, requester, imitability.

The article presents a brief analysis of problematic issues of identification of civil and special-purpose air objects, as well as approaches to improving the effectiveness of identification.

Введение. Защита информации является наиболее актуальной задачей в информационных системах и комплексах. Одним из видов таких систем является система опознавания наземных и воздушных объектов гражданского и специального назначения. В реальных условиях функционирования, характеризуемых динамичностью, стохастичностью и частичной априорной неопределенностью, возникают различные нештатные ситуации, существенно снижающие эффективность функционирования [1].

Известно [1], что ключевым свойством системы опознавания является ее имитостойкость, под которой понимается способность информационной системы противостоять вводу ложной, в том числе ранее переданной информации и навязывание ей ложных режимов работы [2]. При этом следует понимать, что снижению имитостойкости системы опознавания способствуют как активные действия, заключающиеся в имитации сигнала опознавания или провокации ответчиков на излучение, так и пассивные, являющиеся в общем случае преднамеренными или случайными и зависящие от разрешающей способности системы опознавания по угловым координатам, по декартовым координатам и их производным, по дальности, по радиальной скорости и ее производным.

Вместе с тем, повышая имитостойкость и другие показатели функциональной эффективности системы опознавания, можно обеспечить повышение достоверности формируемой ею информации относительно целевой обстановки. Достоверность, в свою очередь, характеризует степень нашего доверия результатам опознавания и является одним из наиболее важных показателей обеспечения защиты информации, циркулирующей в информационном контуре системы опознавания.

Обобщая вышесказанное, можно заключить, что достоверность информации, циркулирующей в системе опознавания в качестве результатов опознавания, можно рассматривать как один из важнейших факторов обеспечения безопасности информации в системе опознавания, а поиск эффективных способов повышения достоверности опознавания (например, посредством обеспечения имитостойкости системы), а также

повышения других качественных показателей функциональной эффективности системы опознавания (например, энергетической или спектральной эффективности, энергетической, информационной или структурной скрытности и др.) – как один из альтернативных способов реализации защиты информации в системе опознавания.

Таким образом, поиск и реализация эффективных способов обеспечения имитостойкости системы опознавания и повышения ее функциональной эффективности, обеспечивающих достоверность результатов опознавания и, как следствие, защиту информации, является актуальным направлением исследований.

Краткий анализ исследуемой предметной области. Современная система опознавания способна решать стоящие перед ней задачи в нормальных условиях функционирования. Однако реальные условия функционирования характеризуются наличием различных дестабилизирующих факторов, поэтому современный уровень тактико-технических характеристик системы опознавания не в полной мере отвечает требованиям, предъявляемым к ней в реальных условиях функционирования.

Основными дестабилизирующими факторами можно считать следующие:

- повышение уровня помех;
- совершенствование способов имитации сигналов опознавания;
- повышение плотности объектов в зоне опознавания;
- функционирование системы опознавания в плохих погодных условиях;
- расширение типажа средств, оснащаемых аппаратурой опознавания.

В качестве требований к системе опознавания можно отметить следующие:

- повышение требований к дальности опознавания;
- повышение требований к точности и достоверности определения координат и дальности (а также их производных) объектов опознавания;
- повышение помехозащищенности средств опознавания, в том числе скрытности функционирования (энергетической, структурной, информационной и др.);
- повышение имитостойкости запросчиков и ответчиков (непровокативности);
- использование избыточности формируемых координатных оценок для повышения их качественных характеристик;
- повышение требований к оперативности опознавания;
- обеспечение ситуационной осведомленности;
- повышение разрешающей способности системы опознавания.

Одним из путей повышения качественных характеристик функционирования системы опознавания является повышение избыточности за счет более полного использования различной информации с борта объекта опознавания, например, параметров движения, характеристик траектории движения и др.

Для повышения эффективности функционирования системы опознавания возможна реализация некоторых организационных и технических мероприятий, которые будут рассмотрены далее.

Предлагаемые подходы к повышению эффективности функционирования системы опознавания.

Альтернативный механизм реализации адресного запроса. Традиционный способ реализации адресного запроса может быть представлен следующим обобщенным алгоритмом:

- запросчик определяет координаты ответчика;
- запросчик передает ответчику в запросном сигнале координаты ответчика;
- ответчик производит определенные вычисления и принимает решение на ответ запросчику.

Указанный способ не лишен недостатков, связанных с имитацией запросных сигналов.

Алгоритм реализации предлагаемого способа заключается в следующем:

запросчик посылает запросный сигнал, содержащий кроме прочих параметров также значения координат запросчика, например, в декартовой системе координат $(x_з, y_з, z_з)$ и его излучаемой мощности $P_з$;

ответчик, приняв сигнал запросчика, определяет собственные координаты и вычисляет дальность до запросчика двумя способами по следующим приближенным (в виду погрешностей) аналитическим соотношениям:

$$R_{коорд.} \approx \left((x_з - x_о)^2 + (y_з - y_о)^2 + (z_з - z_о)^2 \right)^{1/2},$$

где $(x_о, y_о, z_о)$ – координаты ответчика в декартовой (той же) системе координат;

$$R_{мощн.} \approx \left(P_з \, G_\Sigma \, \lambda^{-2} \left(4 \pi \, P_{вх.} \right)^{-1} \right)^{1/2},$$

где G_Σ – результирующий коэффициент усиления антенн запросчика и ответчика; λ – длина волны; $P_{вх.}$ – мощность сигнала запросного сигнала на входе радиоприемника ответчика;

ответчик сравнивает значения дальностей $R_{коорд.}$ и $R_{мощн.}$, и принимает решение на ответ по следующему правилу:

$$\begin{cases} \textit{если } R_{мощн.} \approx R_{коорд.}, \textit{ то отвечает,} \\ \textit{иначе – не отвечает.} \end{cases}$$

Условие $R_{мощн.} \approx R_{коорд.}$ может быть переписано в виде $R_{мощн.} = R_{коорд.} \pm \Delta R$, где величина ΔR может определяться с учетом сложности помеховой обстановки, динамики движения ответчика или других факторов, влияющих на точность местоопределения запросчика и ответчика.

Указанный подход можно рассматривать, как способ повышения непровокативности ответчика. Достоинством данного подхода является отсутствие необходимости знания координат ответчика при условии широко направленной диаграммы антенны запросчика.

Синтез зоны разрешения ответа, согласованной с динамикой движения объекта опознавания. В некоторых системах опознавания в качестве области разрешения ответа используется сферическая область пространства с центром в координатах ответчика, определенных запросчиком и включенных им в запросный сигнал.

Указанный подход является не эффективным в случае существенных координатных погрешностей, высокой динамики движения ответчика или при небольших дальностях. Очевидно, что размеры и форма области разрешения ответа, должны быть согласованы с характером движения ответчика, например, с направлением и параметрами движения. При этом, если речь идет о гладких траекториях движения ответчика (что наиболее часто встречается на практике), то сферическая область должна быть преобразована в эллипсоид.

Таким образом, для повышения эффективности функционирования системы опознавания необходимо согласование формы и размеров области разрешения ответа, которая строится ответчиком после получения запросного сигнала, с параметрами движения ответчика. При этом в качестве факторов, влияющих на эффективность согласования, могут быть использованы следующие: значения координатных погрешностей, курс и скорость движения ответчика, дальность до запросчика, характер траектории движения ответчика, частота поступления запросных сигналов и др.

Согласование области разрешения ответа и указанных параметров может быть реализовано на основе следующего приближенного алгоритма:

- вспомогательное средство определяет декартовы или угловые координаты ответчика;
- запросчик в запросном сигнале (среди прочих данных) передает ответчику значения своих координат и координат ответчика, а также значения их погрешностей;
- ответчик, приняв запросный сигнал, вычисляет дальность до запросчика и строит сферическую область разрешения ответа;
- ответчик согласовывает область разрешения ответа с параметрами своего движения и другими параметрами, характеризующими систему запросчик-ответчик.

Одним из вариантов согласования может быть следующий: характер траектории движения ответчика определяет ориентацию эллипсоида (т.е. направление движения вытягивает сферическую область разрешения ответа в эллипсоид), а дальность, скорость движения и величина координатных погрешностей определяют размер этого эллипсоида.

Для определения аналитической связи параметров эллипсоида с параметрами движения ответчика необходимо задать аналитические соотношения, связывающие величину ошибки по дальности со значением координатных погрешностей, а также соотношения, связывающие параметры трансформации сферической области разрешения ответа с направлением движения ответчика, его скоростью, дальностью и другими параметрами, характеризующими систему запросчик-ответчик.

Указанный подход, состоящий в согласовании области разрешения ответа с параметрами системы опознавания и движения ответчика, может служить способом повышения разрешающей способности запросчика (и всей системы опознавания), поскольку может способствовать уменьшению (в общем случае – согласованию) размеров азимутального строба и строба по дальности, а также может способствовать повышению вероятности пребывания «своего» в зоне разрешенного ответа.

Заключение. В работе предложен подход к повышению эффективности опознавания, представляющий собой решения, способствующие повышению отдельных аспектов функциональной эффективности системы опознавания и заключающиеся в следующем:

- разработке способа согласования области разрешения ответа с параметрами движения ответчика, позволяющего ожидать повышения разрешающей способности запросчика и вероятности пребывания «своего» ответчика в зоне разрешенного ответа;
- реализации альтернативного алгоритма адресного запроса.

Предполагается, что указанные меры могут способствовать повышению качественных характеристик функциональной эффективности системы опознавания.

СПИСОК ЛИТЕРАТУРЫ

1. Панков В.А., Манежкин А.С., Мытиль В.К. Эволюция авиационных средств опознавания [Текст]. Черноголовка. Редакционно-издательский отдел ИПХФ РАН, 2016. – 160 с.
2. ГОСТ РВ 52216-2004. Связь военная. Термины и определения. Введ. 2005–01–01. М.: Стандартинформ, 2004.

А.А. Мозоль

СПОСОБ ЛОКАЛИЗАЦИИ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКА ИЗЛУЧЕНИЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: источники излучений, локализация местоположения, стационарная радиолиния, энергетические измерения.

В статье применительно к однопозиционным и многопозиционным измерительным системам излагается новый способ локализации местоположения источника излучения по энергетическим измерениям без привлечения пеленговой информации.

A.A. Mozol'

METHOD OF LOCALIZATION OF THE LOCATION OF THE RADIATION SOURCE

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

Keywords: radiation sources, location localization, stationary radio line, energy measurements.

In the article, in relation to single-position and multi-position measuring systems, a new method of localization of the location of the radiation source by energy measurements without involving direction finding information is described.

Введение. Известные способы однопозиционной и многопозиционной пеленгационной координатометрии источников излучений реализуются, как правило, на базе громоздких и дорогостоящих антенных систем, позволяющих формировать требуемый энергетический потенциал при узком (особенно в азимутальной плоскости) луче диаграммы направленности. Однако в некоторых практических задачах, связанных с определением местоположения малогабаритных радиопередатчиков, применение таких антенных систем может быть затруднительным. Примером такой задачи может быть поиск электронных устройств негласного получения информации, выполняемых органами технической защиты информации, а также иными коммерческими организациями.

В статье рассматривается альтернативный вариант способа локализации источника излучения на базе сравнительно недорогих малогабаритных энергетических измерителей (МЭИ) со слабонаправленными антеннами без привлечения пеленговой информации и с учетом частично известных параметров движения источника излучения. Актуальность такого варианта обусловлена тем, что к настоящему времени разработано большое количество теоретических и практических решений для надежной оценки уровня входного сигнала [1] и оценивания параметров движения источника излучения с использованием энергетической и угловой информации в предположении, что радиолиния является стационарной [2].

Основные соотношения метода. Предположим, что в центре декартовой системы координат XOY находится МЭИ, фиксирующий мощность или амплитуду принимаемого сигнала, движение источника излучения осуществляется по закону: $\vec{r} = \vec{r}_0 + \vec{V}t$, $t \in [0, T]$, где

$\vec{r} = [x, y]^T$, $\vec{r}_0 = [x_0, y_0]^T$, $\vec{r}_0 = \vec{r}(0)$, $\vec{V}$ – вектор скорости, $V = \|\vec{V}\|$ – величина скорости (полагается известным ее математическое ожидание $m_V = M[V]$ и дисперсия σ_V^2).

Введем временную сетку $\{t_n\}_{n=1}^N$ (где $t_n \in [0, T]$), при этом на базе МЭИ осуществляются измерения мощности $P_n = P(t_n)$ принимаемого сигнала. С учетом этого формируется вектор наблюдений $\tilde{\vec{Z}}_{ijk} = \vec{Z}_{ijk} + \Delta\vec{Z}_{ijk}$, где $\tilde{\vec{Z}}_{ijk} = \left[\tilde{V}, \tilde{P}_i, \tilde{P}_j, \tilde{P}_k\right]^T$, $\vec{Z}_{ijk} = \left[V, P_i, P_j, P_k\right]^T$, $\Delta\vec{Z}_{ijk} = \left[\Delta V, \Delta P_i, \Delta P_j, \Delta P_k\right]^T$ – вектор случайных ошибок с нулевым математическим ожиданием и корреляционной матрицей $\mathbf{K}_{\vec{Z}_{ijk}}$ соответствующей размерности. Если величина скорости V является детерминированной и известной по условию задачи, то будем принимать $m_V = V$ и $\sigma_V^2 = 0$.

Воспользуемся известным уравнением дальнометрии $P = \mu R^{-2}$ (где $R = \|\vec{r}\|$), связывающим мощность P принимаемого сигнала и дальность R до источника излучения (при этом ограничимся стационарным случаем, когда $\mu(t) = \mu = const$, $t \in [0, T]$). С учетом этого уравнения и принятой модели движения была получена формула для вычисления дальности (при выводе этого аналитического соотношения использовалась временная тройка $t_i, t_j, t_k \in \{t_n\}_{n=1}^N$, $i, j, k \in \overline{1, N}$, $i \neq j \neq k$, $t_i \neq t_j \neq t_k$, при этом $\Delta t_{ij} = |t_j - t_i| = |t_k - t_j| = \Delta t_{jk}$):

$$R_k = \left[2P_iP_jS_{ij}^2(P_iP_j + P_jP_k - 2P_iP_k)^{-1}\right]^{1/2}. \quad (1)$$

Формула (1) позволяет по трем измерениям мощности принимаемого сигнала P_i, P_j и P_k вычислить интересующую нас дальность R_k без привлечения пеленговой информации.

Для вычисления относительной погрешности оценивания дальности R_k была получена формула

$$\varepsilon_{R_k}^2 = \sigma_{R_k}^2 R_k^{-2} \leq P_k^2\varepsilon_P^2\left(P_j^2 + 4P_i^2 - 2P_iP_j\right) / \left[2\left(P_iP_j + P_jP_k - 2P_iP_k\right)^2\right] + \varepsilon_V^2, \quad (2)$$

где $\varepsilon_P^2 = \max\left\{\sigma_{P_i}^2 P_i^{-2}, \sigma_{P_j}^2 P_j^{-2}, \sigma_{P_k}^2 P_k^{-2}\right\}$ – максимальная относительная погрешность измерения мощности, $\varepsilon_V^2 = \sigma_V^2 / V^2$ – относительная погрешность задания скорости. Из (2) следует, что точностные характеристики метода существенно зависят от дальности до источника излучения, его скорости (характеризует максимально возможное приращение мощности между соседними радиоконтактами) и качества мощностных измерений. Чем больше дальность, тем выше требования к мощностному каналу.

Исходными данными для расчета дальности являются: массив мощностей $\tilde{P}_n$, измеренных в моменты времени t_n ($n = \overline{1, N}$) с погрешностью ε_{P_n}, [%], скорость V и всевозможные пары (Δt_{ij}, Δt_{jk} $\forall\, i, j, k \in \overline{1, N}$), такие, что $i \neq j \neq k$, при этом должно выполняться условие $\Delta t_{ij} = |t_j - t_i| = |t_k - t_j| = \Delta t_{jk}$.

Рассмотрим процедуру формирования результирующей оценки дальности в текущем дискретном времени t_k, при этом первичные измерения мощности сглаживаются

по выборке нарастающего объема методом наименьших квадратов (МНК). Начиная с третьего момента времени t_3, ведется расчет дальности по формуле (1). Для произвольного текущего t_k единичную оценку дальности можно получить либо с использованием последних трех замеров, положив в формуле (1) $i = k-2$ и $j = k-1$ (это первый вариант), либо с использованием всех замеров, соответствующих временной сетке $t_1, t_2 \ldots t_{k-1}, t_k$, для всевозможных пар ($\Delta t_{ij}$, Δt_{jk} $\forall\, i, j \in \overline{1, k-1}$) и усреднением единичных оценок, соответствующих этим парам (это второй вариант). В последнем варианте перебираются все тройки $\left(t_i, t_j, t_k\right)$ равноотстоящих узлов, в которых фиксирован текущий момент времени t_k ($k \geq 3$). Число таких комбинаций $L_k = \left[(k-1)/2\right]$, где $\left[\cdot\right]$ соответствует целой части вещественного числа. Единичная оценка дальности $\hat{R}_k^l$ для *l*-й тройки, где $l = \overline{1, L_k}$, рассчитывается по формуле (1), в которой необходимо осуществить замены: $i \to k-2l$, $j \to k-l$, $\Delta t_{ij} \to \Delta t_{k-2l,k-l} = \Delta t_l$, $S_{ij} \to S_l = V\Delta t_l$. Для построения результирующей оценки дальности на базе единичных оценок $\hat{R}_k^l$, $l = \overline{1, L_k}$, можно воспользоваться известным МНК для случая коррелированных измерений.

Формулы (1), (2) составляют основу алгоритмического способа локализации местоположения источника излучения по энергетическим измерениям на базе МЭИ без привлечения пеленговой информации применительно к стационарной радиолинии.

Заключение. Предложенный в статье подход может использоваться как самостоятельно, так и в комплексе с известными методами пассивной координатометрии источников излучений. Первый случай может быть актуален, когда в измерительной системе единственным источником достоверной информации является энергетический канал. Способность однопозиционной системы автономно решать задачу дальнометрии может найти широкое применение как в гражданской, так и военной областях.

СПИСОК ЛИТЕРАТУРЫ

1. Сытенький В.Д. Пассивная локация на основе амплитудных измерений // Известия ВУЗов России. Радиоэлектроника. 2011. № 1. С. 69–75.
2. Мельников Ю.П., Попов С.В. Радиотехническая разведка. Методы оценки эффективности местоопределения источников излучения. М.: Радиотехника, 2008. – 432 с.

А.И. Дубровина

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТЕХНОЛОГИЯХ «УМНОГО ДОМА»

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
Ростов-на-Дону, Россия

Ключевые слова: умный дом, модель угроз, защита информации.

В настоящей работе представлены и проанализированы три самые распространенные системы «умного дома». Выявлены возможные уязвимости при эксплуатации данных систем, построена модель угроз и составлен перечень методов, позволяющих избежать несанкционированный доступ программного и технического характера.

A.I. Dubrovina

INFORMATION SECURITY IN SMART «HOME TECHNOLOGIES»

Federal State Budgetary Educational Institution of Higher Education «Don State Technical University», Rostov-on-Don, Russia

Keywords: smart home, threat model, information protection.

In this paper three of the most common smart home systems are presented and analyzed. Possible vulnerabilities in the operation of these systems have been identified a threat model has been built and a list of methods has been compiled to avoid unauthorized access of a software and technical nature.

Системы «умного дома» являются уникальным решения для выполнения различных задач, позволяя получать информацию о состоянии территории в режиме реального времени, защищать вверенный объект как от несанкционированного доступа, так и от нештатных ситуаций: пожароопасность, нарушение работоспособности датчиков климат-контроля, утечка газа, воды и т.п. Пользуются высоким спросом вследствие разносторонней индивидуализации функций под потребности пользователя, но как и любая автоматизированная система «умный дом» имеет уязвимости в области защиты информации.

Задачей настоящей статьи является выявление и описание возможных уязвимостей компонентов системы «умного дома», анализ решений по их устранению. Посредством теоретических и эмпирических методов исследования будет реализована цель работы – разработка мер защиты информации объекта исследования.

Начальным этапом в выполнении поставленной задачи является анализ самых популярных существующих решений систем умного дома.

Классическое решение кампании ПАО «Ростелеком» с подробным описанием функций представлено на рисунке 1.

Рисунок 1. Классическое исполнение «умного дома» кампании ПАО «Ростелеком»

Представленное решение базируется на технологи объединения IOT- устройств при помощи беспроводного соединения Z-Wave. Данные о происходящих события располагаются в облачном хранилище до 1 месяца. Управление датчика организовано при помощи мобильного приложения, при возникновении экстренных ситуаций пользователю приходит смс-уведомление о случившемся с запросом о дальнейших действиях, к примеру, «организация вызова аварийной службы». Несмотря на простую установку и удобный интерфейс система имеет недостатки. Удаленное управление системой через мобильное устройство организовано не по защищенному протоколу в связи с чем злоумышленник может подключиться к каналу передачи данных, тем самым прослушать трафик и перехватить данные учетной записи пользователя, авторизоваться и скачать личные данные с устройства пользователя. В последствии возможно нарушить техническую защиту информации, переведя датчики движения и открытия в спящий режим. Злоумышленник сможет свободно проникнуть на объект и осуществить хищение персональных данных, денежных средств, документов на владение домом и пр., использовав информации в личных целях, к примеру, продав конкуренту служебную информацию о рабочих проектах. Также возможно включить газ в помещении, что приведет к отравлению владельца. Источники бесперебойного питания не установлены, что при разрядке приведет к программному сбою и вывода устройств из режима работоспособности. Система безопасности организована ненадежно [1].

К преимуществу можно отнести тип соединения, при выходе из строя одного устройства на работе остальных это не отразится.

Решение «Smart Home» кампании Xiaomi является более расширенным по наличию IoT-устройств, комплекс представлен на рисунке 2. «Умные выключатели и розетки» обеспечивают непрерывное беспроводное поступление электрозаряда к остальным устройства. Шлюз управления организует передачу информации по протоколу ZigBee, объединяя все датчику в единую защищенную сеть. Камеры видеонаблюдения позволяют непрерывно контролировать происходящее на объекте в режиме реального времени, при выводе из строя датчиков движения, открытия окна или двери видеозапись поступит на мобильное устройство владельца, данная функция также удобна при потребности отслеживать состояние родственников или времяпрепровождение детей. Наличие умного удлинителя позволяет подключиться к сети напрямую при нарушении работы в технологии ZigBee, устройства продолжат работать независимо. Наличие универсальной кнопки позволит удаленно или физически вызвать группу быстрого реагирования при возникновении опасности жизни человека (пожар, отравление газом, взлом).

Интерактивный куб является управляющим контроллером в общей сети, организующий выполнение заданных алгоритмов для домашней техники, в данном случае робота-пылесоса, также легко синхронизируется с устройствами, поддерживающими беспроводное соединение, создание сценария возможно через приложение на мобильном устройстве пользователя [2].

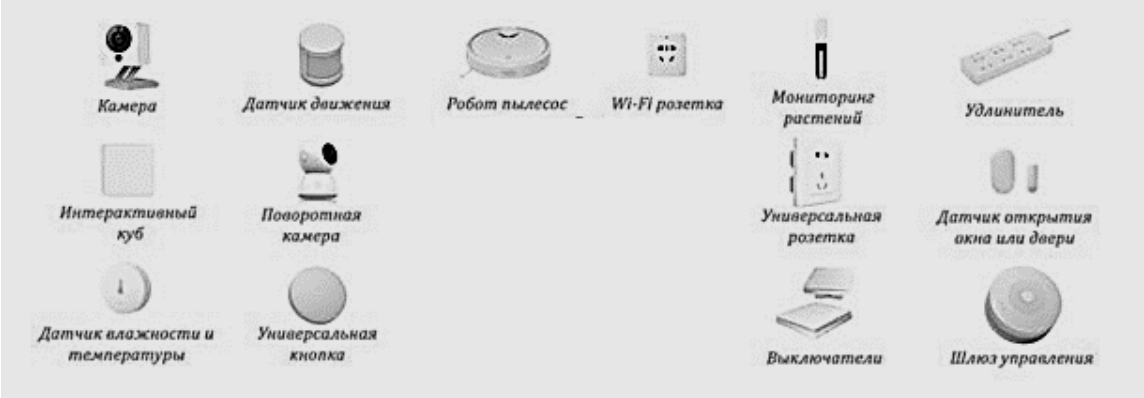


Рисунок 2. Комплект «умного дома» «Smart Home»

Данный комплект позволяет анализировать биометрические данные пользователя, контролирует питание, подбирает температуру и влажность воздуха, предупреждая об изменениях состояния организма проживающего.

Недостатком является подверженность к воздействиям метеоусловий. При влажной погоде устройства могут выходить из строя, после чего вся информация автоматически сбрасывается. Система безопасности организована ненадежно, при выходе из строя управляющего контроллера злоумышленник легко может извлечь биометрические данные пользователя и подменить алгоритм питания на иной, изменить настройки климат-контроля, контроля вскрытия. При последнем понимается также простота извлечения данных с управляющего мобильного устройства пользователя личных переписок, контактов, служебной информации, фото, телефонных переговоров. Интерактивный куб также не оснащен антивирусным программным обеспечением, что позволяет проникнуть вирусному заражению из сети «Интернет» [3].

«Умный дом» Google Home от кампании Google имеет такой же набор датчиков, как и в структуре «Smart Home» с дополнением биометрического считывателя к датчику вскрытия (умный замок). Отличительной особенностью является управление устройствами за счет использования голосового помощника. Наличие умных замков позволяет получить доступ в помещение при помощи биометрии сетчатки глаза или отпечатка пальца, что также является недостатком, так как при удачной организации несанкционированного подключения к системе злоумышленник может завладеть биометрическими данными, в дальнейшем таким образом можно обналичить средства пользователя с банковской карты.

Проведя анализ систем умного дома, пользующихся наивысшим спросом в настоящий момент, можно сделать вывод, что все они зависят от подачи электропитания, метеоусловий, управляющего контроллера и имеют незащищенный канал передачи данных, а также подвержены помехам. На основании анализа в таблице 1 представлена модель угроз.

Таблица 1. Модель угроз системы «умного дома»

Наименование атаки	Уязвимость	Нанесенный ущерб
Попытка совершить несанкционированный доступ на управляющий контроллер	В связи с тем, что взаимодействие между устройствами происходит при помощи беспроводного соединения, сеть уязвима	Выход всей системы из строя, потеря информации, перехват управления вследствие нарушения работоспособности управляющего контроллера
Воздействие вирусного программного обеспечения или программ-троянов	В связи с тем, что взаимодействие между устройствами происходит при помощи беспроводного соединения, сеть уязвима	Возникновение сбоев в программном обеспечении, что приводит к потере данных или выхода из строя оборудования (IoT-устройств)
Прослушивание трафика и перехват данных по каналу связи по беспроводному каналу связи	Недостаточная организация механизмов защиты информации, перехват радиосигнала	Искажение, нарушение конфиденциальности информации
Хищения идентифицирующих данных пользователя для управления системой	Недостаточная организация механизмов защиты информации	Искажение, нарушение конфиденциальности информации
Несанкционированный доступ к системе неавторизованных в сети пользователей	Недостаточная организация механизмов защиты информации	Искажение, нарушение конфиденциальности информации
Отсутствие или сбои в электропитании	Отсутствие автономного способа получения электропитания	Выход из строя всех датчиков системы
Выход из строя аппаратуры	Причиной может послужить неправильная эксплуатация со стороны персонала или низкокачественная техника	Нарушение целостности информации
Перехват информации по электроакустическому каналу передачи данных	Наличие акустоэлектрических преобразователей (охранных и датчиков движения)	Искажение, утечка информации
Использование наводок и электромагнитных излучений	Выход проводниковых наводок и излучений, за пределы охраняемой территории	Нарушение конфиденциальности и искажение информации, хранящейся в облаке
Несанкционированный доступ на территорию охраняемого объекта с целью хищения информации	Недостаточная организация мер по физической защите периметра	Нарушение конфиденциальности и целостности информации
Нарушители из числа проживающих на территории объекта или обслуживающего персонала	Недостаточная организация и контроль за проживающими на охраняемой территории	Нарушение конфиденциальности и целостности информации
Чрезвычайные ситуации природного характера (пожар, дождь и т.д.)	Плохая организация мер защиты от нештатных ситуаций	Выход системы из строя
Сбой работы программного обеспечения	Применение нелицензионного программного обеспечения, неправильная эксплуатация	Нарушение конфиденциальности и целостности информации

Исходя из результатов, полученных при построении модели угроз «умного дома» определен следующий перечень мер по защите информации:

- регулярное проведение обновлений системы;
- использование лицензированного программного обеспечения;
- установка антивирусного программного обеспечения;
- использование защищенного подключения по VPN-каналу;
- необходимо установить источники бесперебойного питания;
- необходимо прописать MAC-адреса устройств, которые относятся к сети «умного дома»;
- необходимо установить автономные источники электропитания;

- необходимо установить защиту на точку доступа WAN 2-го уровня;
- обеспечить защиту доступных портов подключения;
- блокировка учетной записи после попыток многоразового подбора пароля;
- ограничение лимита сетевого трафика;
- установить программное обеспечение «Kaspersky Smart Home Security» с целью отслеживания и блокировки вредоносных сетевых ссылок;
- раз в пару месяцев необходимо менять пароль к управляющему программному обеспечению и следить за его надежностью [4].

Таким образом, были проанализированы уязвимости систем «умного дома» и разработаны методы по их устранению, цель и задачи работы выполнены в полной мере. После получения результатов оценки защищенности системы «умного дома», можно сделать вывод, что к самым опасным угрозам можно отнести те, которые возникают вследствие перехвата злоумышленником контроля над управлением системой. Необходимо регулярное проведение мероприятий по обновлению, отслеживанию вредоносных ресурсов, а также организационное наблюдение за проживающими на территории охраняемого объекта. Реализация несанкционированного доступа физического или программного характера может привести к финансовым потерям, а также к риску здоровья, репутации или летальному исходу. Вследствие этого важной задачей при проектировании систем «умного дома» является детальная оценка риска при конкретных условиях и анализе потенциальных уязвимостей и угроз.

СПИСОК ЛИТЕРАТУРЫ

1. 1. «Умный дом» [Электронный ресурс] — Режим доступа: \www/ URL: http://umny dom. iev.ua/index.php?nma=catalog&fla=stat&cat_ id=3&page=1&nums=24/ — 23.10.2021 г.
2. 2. Перспективы рынка систем «Умный дом» [Электронный ресурс] / Центр инжене рных технологий CENTEC. /Режим доступа: www/ URL: http://www. centecgrou p.ru/press/artic les/18/ — 24.10.2021 г.
3. Умный дом [Электронный ресурс] – Режим доступа: URL: https://ru.wikipedia.org/wiki.
4. 4. Роберт К. Элсенпитер, Тоби Дж. Велт «Умный Дом строим сами» издатель: Кудиц-Образ 2004 г; 362 стр.

В.А. Алексеев, П.В. Лобзенко

WEB ПРИЛОЖЕНИЕ МЕНЕДЖЕРА ОТДЕЛА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: web приложение, упрощенный доступ, Visual Studio, ASP NET, базы данных.

На основе выполненного анализа программных продуктов в свободном доступе для спроектировано и реализовано приложение, обеспечивающее информационную поддержку работы менеджеров отдела технической поддержки компании. Приложение отличается удобной компоновкой и состоит только из серверной части. Клиент может воспользоваться

приложением через web браузер. В дополнение к этому, приложение снабжено базой данных, расположенной на сервере.

V.A. Alekseev, P.V. Lobzenko

WEB APP MANAGER OF TECHNICAL SUPPORT DEPARTMENT

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

Keywords: web application, easy access, Visual Studio, ASP NET, databases.

Based on the analysis of software products in the public domain, an application was designed and implemented that provides information support for the work of managers of the company's technical support department. The application has a convenient layout and consists only of the server part. The client can use the application through a web browser. In addition to this, the application is supplied with a database located on the server.

В настоящее время стало привычным использование компьютеров на рабочих местах, практически, во всех частных компаниях и государственных предприятиях.

Так, компьютеры сейчас входят в список необходимых атрибутов при организации рабочего места офисных сотрудников. Однако, еще десятилетие тому назад всего около 40% предприятий малого и среднего бизнеса использовали электронные вычислительные машины для выполнения повседневных задач [1]. Как правило, в основном, использовались текстовые редакторы для ведения отчетной и другого рода документации. Сейчас, напротив, можно сказать, что все организации офисного типа оснащены компьютерной техникой. Признаком современного этапа использования компьютеров на рабочих местах является, прежде всего то, что сейчас в организациях устанавливаются не просто отдельные компьютеры, а целостные информационные системы [2, 3]. Они служат для обеспечения всех направлений деятельности компаний. Это – коммерческая деятельность, производственные задачи и финансовое направление.

Т.о., разработка приложения для автоматизации функций менеджеров отдела сопровождения является актуальной.

На Рисунке 1 показана блок-схема работы приложения.

Видно, что приложение будет размещено на открытом ресурсе в Интернет, поэтому оно должно быть оснащено входом по логину и паролю. Следовательно, алгоритм доступа к web интерфейсу должен включать заполнение логина и пароля на стартовой форме приложения, процедуру ввода данных и сверку их с данными, записанными в базе данных приложения. После этого должен открываться доступ согласно ролей: «Администратор», «Пользователь» или «Менеджер».

База данных приложения реализована с помощью MS Sql Server, ее нормированная диаграмма данных показана на Рисунке 2.

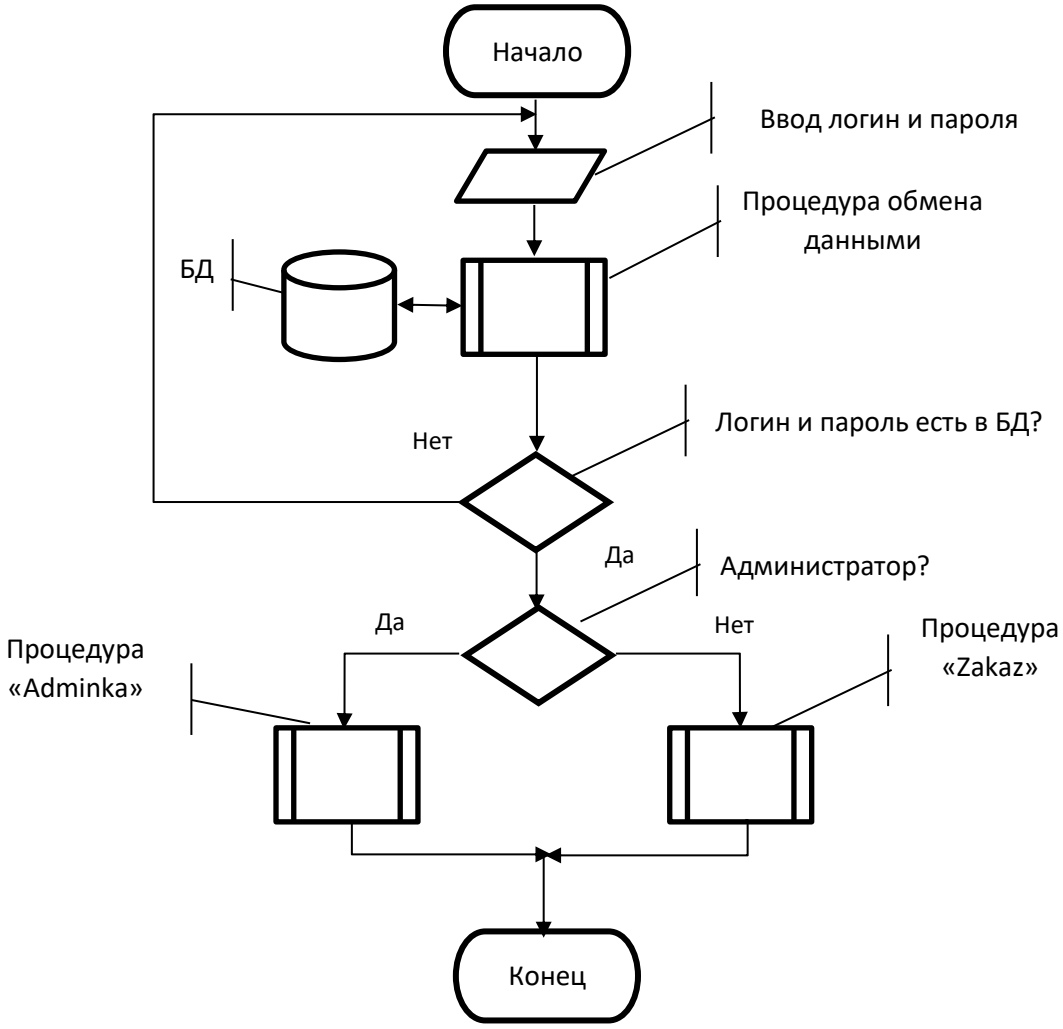


Рисунок 1. Алгоритм работы приложения

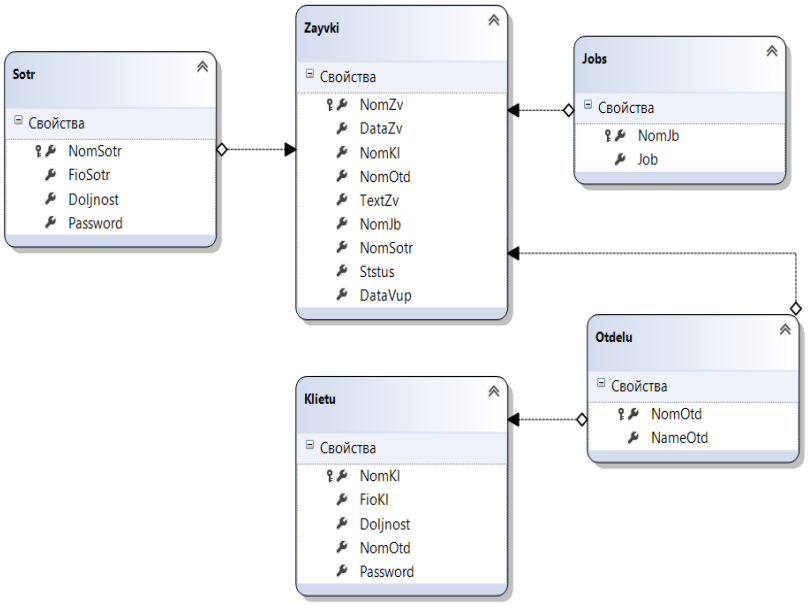


Рисунок 2. Нормированная модель логических связей базы данных

Используя схему алгоритма приложения (рисунок 1) и схему данных задачи (рисунок 2) составлена программа приложения. Проект приложения разработанный на языке C# и состоит из набора классов, каждый из которых, реализует взаимодействие с таблицами базы данных.

Платформа ASP.NET, на базе которой разработан продукт, представляет собой набор библиотек и инструментов приблизительно таких же как и FrameWork для разработки web сайтов и приложений [4]. Это удобный инструмент для использования технологии MVC (model - view — controller). Т.е., в разработке приложение делится на три компонента:

- контроллер (controller) — класс, занимающийся связью базы данных с пользователем и обработкой текущей информации из базы данных;
- представление (view) — класс, обеспечивающий пользовательский интерфейс;
- модель (model) — класс для описания логики данных приложения.

Форма для внесения и контроля исполнения заявок показана на рисунке 3.

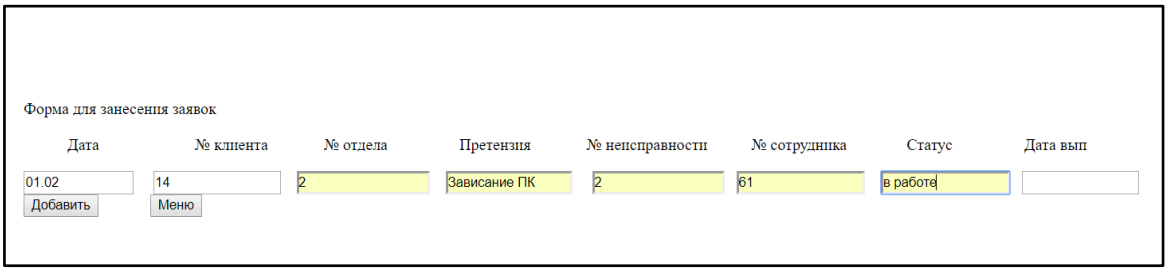


Рисунок 3. Форма для внесения и контроля заявок

Как любое приложение, содержащее интерфейсные формы, это приложение снабжено обработчиками событий. Типовой обработчик события нажатия на кнопку «Добавить» представлен в листинге 1.

Листинг 1. Типовой обработчик события нажатия на кнопку «Добавить»

```
protected void Button1_Click(object sender, EventArgs e)
      {
DataClassesSotrDataContext db = new DataClassesSotrDataC-ontext(); // создание экземпляра модели данных проекта
            Klietu kl = new Klietu();  // создание экзем-пляра таблицы Klietu БД

            //Код добавления пользователя
            do
            {
             if (TextBox1.Text != "" && TextBox2.Text != "" && TextBox3.Text != "" && TextBox4.Text != "") // ввод не-пустых данных
                {
                   kl.Doljnost = TextBox2.Text;    // заполение полей таблицы из текстовых полей
                   kl.FioKl = TextBox1.Text;
                   kl.NomOtd = int.Parse(TextBox3.Text);
                   kl.Password = TextBox4.Text;

                   db.Klietu.InsertOnSubmit(kl);    // экземпляр слушателя изменения данных в таблице Klietu БД
                   db.SubmitChanges();

                   GridView1.DataSourceID = "";
                   GridView1.DataSource = db.Klietu;   // отображение содержимого таблицы в GridView
                   GridView1.DataBind();
```

```
            //Label3.Text = "";
            Re-sponse.Redirect("/Polzovateli.aspx"); // отображение формы в Explorer
            break;
          }
      } while (true);
  }
```

Разработанное приложение обладает следующими преимуществами:

1. Реализует эффективный способ клиент-серверной системы.
2. Обладает простым, понятным и удобным пользовательским интерфейсом.
3. Реализует основные рутинные функции администратора и менеджеров.
4. Полностью реализует для пользователей алгоритм отправки заявки на техническое обслуживание аппаратуры.
5. Предоставляет исчерпывающую информацию по выполняемым заявкам.
6. Для работы с приложением достаточно первичных навыков пользователя ПК.

СПИСОК ЛИТЕРАТУРЫ

1. Использование программного обеспечения в малом бизнесе. *URL: http://www.good-reklama.ru/upravlenie/184.html.* (дата обращения: 23.09.2021).
2. Илюхин И.В. Основные направления использования информационных систем в управлении предприятиями. *URL: http://cyberleninka.ru/article/n/osnovnye-napravleniya-ispolzovaniya-informatsionnyh-sistem-v-upravlenii-predpriyatiyami*. (дата обращения: 23.09.2021).
3. Категории программных продуктов: «Раскрутка и реклама». *URL: http://www.softwizard.ru/ catalog/ categories/network-programs/advertising-software.* (дата обращения: 23.09.2021).
4. Иванова Г.С. Технология программирования: Учебник для вузов. - М.: Издательство МГТУ им. Н.Э. Баумана, 2002. - 320 с.

А.Р. Гармаш, П.В. Лобзенко

МУЛЬТИВОДОРЕГИСТРАТОР

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: Arduino, автоматизация, микроконтроллер, расходомер, I2C интерфейс.

Главной целью проекта «мультиводорегистратор» можно обозначить разработку микроконтроллерной системы мониторинга многоквартирных жилых домов, способного обеспечить введение электронных счётчиков водоснабжения в массовое использование с наименьшими затратами. Программирование линейки контроллеров Arduino на базе процессоров фирмы Atmel выполняется в среде IDE на языке программирования C++. Система состоит из необходимого количества этажных модулей (ЭМ). В свою очередь, в состав каждого ЭМ входят микроконтроллер, датчики расхода воды, блоки питания и кабельная сеть для их соединения. Имеется возможность как отправки данных на сервер, так и сохранения на SSD Flash накопитель.

A.R. Garmash, P.V. Lobzenko

MULTI - WATER RECORDER

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

Keywords: Arduino, automation, microcontroller, flow meter, I2C interface.

The main goal of the "multi-water recorder" project can be designated the development of a microcontroller monitoring system for apartment buildings that can ensure the introduction of electronic water meters into mass use at the lowest cost. Programming of the Arduino controller line based on Atmel processors is performed in the IDE in the C++ programming language. The system consists of the required number of floor modules (EM).

In turn, each EM includes a microcontroller, water flow sensors, power supplies and a cable network for connecting them. It is possible to both send data to the server and save it to an SSD Flash drive.

В современном мире большая часть повседневных задач очень упрощены или автоматизированы и с каждым днем эта тенденция возрастает. В дом к современному человеку плотно внедряются технологии мониторинга, дистанционного управления, администрирования. В этой направленности работает немало компаний. Они создают на микроконтроллерах устройства, способные автоматизировать и исполнять всевозможные цели.

В соответствии с рисунком 1 структурная схема системы включает этажные модули по количеству этажей многоквартирного дома, центральный микроконтроллер, блок передачи данных по Wi-Fi и блок резервного копирования.

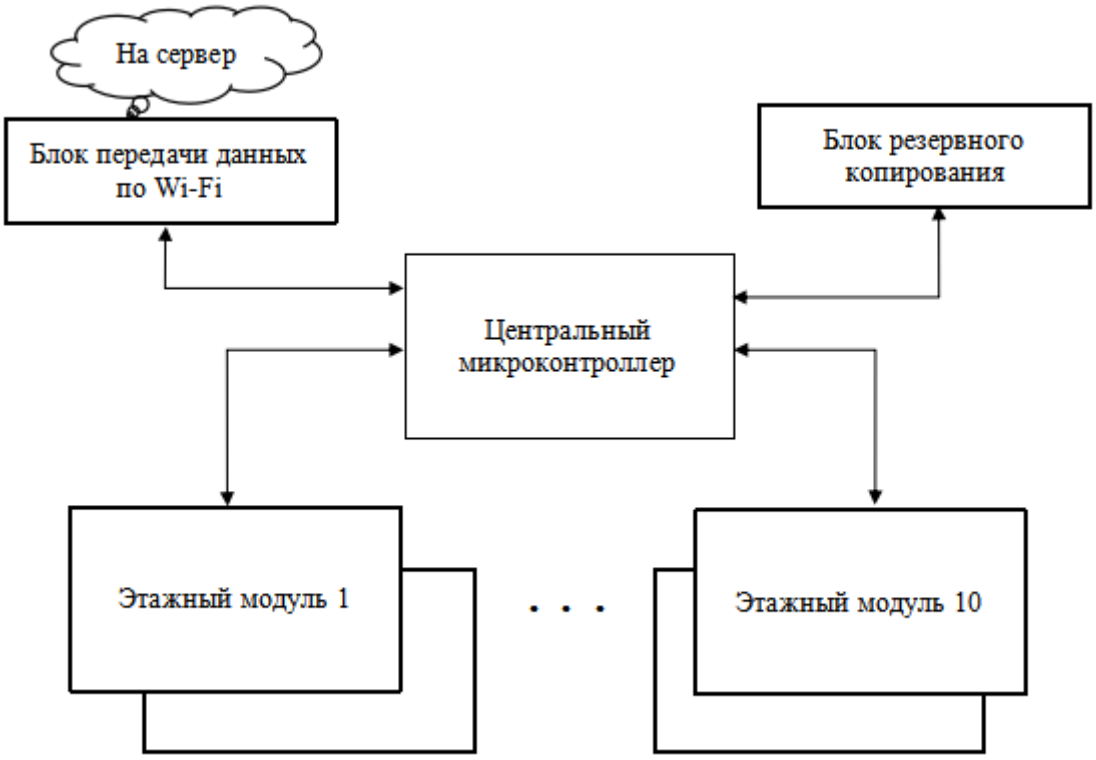


Рисунок 1. Структурная схема системы учета водоснабжения

Для типовой планировки на каждом этаже такого дома 5 квартир и, следовательно, на этаже должны подключаться к системе 20 датчиков-расходомеров (в соответствии с рисунком 2).

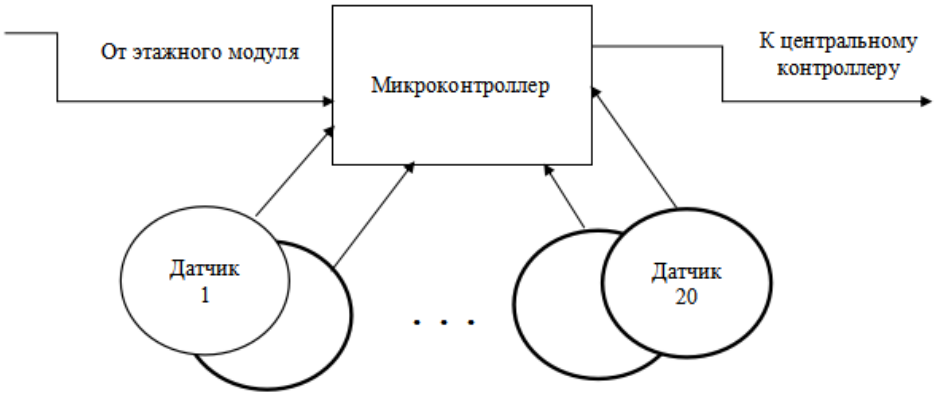


Рисунок 2. Структурная схема этажного модуля

Система состоит из необходимого количества этажных модулей (ЭМ). В свою очередь, в состав каждого ЭМ входят микроконтроллер, датчики расхода воды, блоки питания и кабельная сеть для их соединения.

Составим электрическую принципиальную схему этажного модуля системы (в соответствии с рисунком 3). Вся система состоит из нужного количества таких модулей.

В такую схему должны входить 2 Arduino, подключенные как ведомые к шине I2C, т.е. как Slave [1,2]. К цифровым контактам этих микроконтроллеров подключаются непосредственно датчики расхода воды. Причем, питание плат Arduino и датчиков осуществляется раздельно от соответствующих блоков питания.

Подключение плат Arduino к блоку питания выполняется через Vin контакт, который позволяет подключение до +24V.

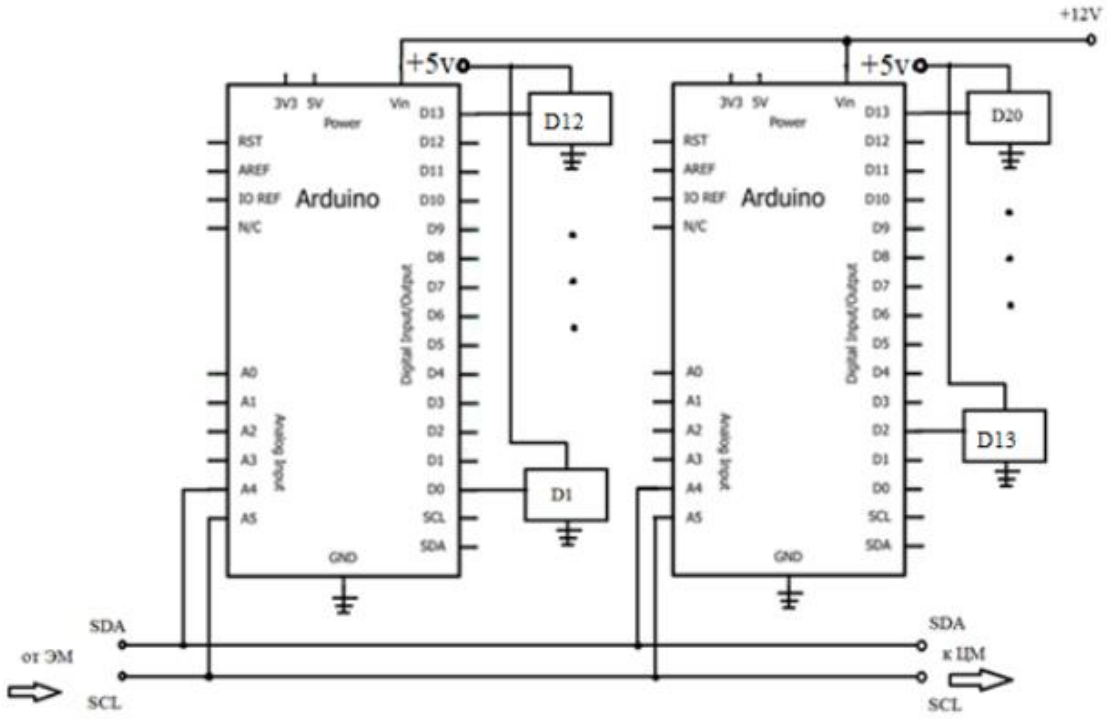


Рисунок 3. Схема электрическая принципиальная этажного модуля

В соответствии с этим рисунком к плате Arduino, которая подключена к шине I2C в качестве Master, присоединены модуль ESP 8266 для поддержания Wi-Fi соединения системы с сервером компании и модуль SD CARD для выполнения резервного копирования информации со всех датчиков расхода воды в многоквартирном доме.

Традиционно, программирование линейки контроллеров Arduino на базе процессоров фирмы Atmel выполняется в среде IDE на языке программирования C++ (в соответствии с листингом 1) [3].

Листинг 1. Фрагмент скетча платы Master: передача данных

```
void loop()
{
String cmd = "AT+CIPSTART=\"TCP\",\"";
cmd += DST_IP;
cmd += "\",8283";
Serial.println(cmd);
mySerial.println(cmd);
if(mySerial.find("Error"))
return;
for(int i=0;i<4;i++){

for(int j=0;j<3;j++){
cmd = "#A0:F3:C1:70:AA:99\n#2881C4BA0200099B1#"+
String(kv[i][j])+"\n##";}}
delay(3000);
mySerial.print("AT+CIPSEND=");
mySerial.println(cmd.length());
delay(1000);
Serial.println(">");
mySerial.print(cmd);
Serial.println(cmd);
delay(3000);
mySerial.println("AT+CIPCLOSE");
delay(300000);}
```

Разработанная система обладает следующими преимуществами:

- контроллером системы является микроконтроллер или их группа;
- система в автоматическом режиме регистрирует потребление воды на каждом установленном датчике в заданные промежутки времени;
- показания аккумулируются совокупно по холодной и горячей воде для каждой квартиры дома;
- система передает данные на сервер обслуживающей компании каждый час, используя Wi-Fi Интернет-соединение;
- параллельно с передачей данных на сервер, организовано резервное копирование на стороннем носителе информации, входящем в состав системы;
- реализована возможность масштабирования системы для заданного количества квартир (этажей);
- система имеет низкую стоимость относительно схожих решений от других производителей.

СПИСОК ЛИТЕРАТУРЫ

1. Датчик расхода воды и Arduino. URL: https://arduino-diy.com/arduino-datchik-rashoda-vodi. (дата обращения 14.10.2021).

2. Arduino или Raspberry Pi: какая платформа лучше? URL: http://edurobots.ru/2014/09/arduino-ili-raspberry-pi-kakaya-platforma-luchshe/ (дата обращения 14.10.2021).
3. Как настроить I2C-связь на Arduino. URL: https://arduinoplus.ru/i2c-svyaz-arduino/ (дата обращения 14.10.2021).

С.В. Горбаенко, П.В. Лобзенко

ВИЗУАЛЬНЫЙ UNITY ПЛАНИРОВЩИК ЗАДАЧ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: Unity приложение, элементы игровой логики, Visual Studio, язык C#, базы данных.

В статье описано приложение, реализующее планировщик задач для руководителя отдела малого бизнеса. Приложение создано в среде программирования Visual Studio и в редакторе Unity. Отличительными особенностями программного продукта, в первую очередь, является игровой сценарий регистрации и контроля исполнения проектных задач, а также их игровая визуализация.

S.V. Gorbaenko, P. V. Lobzenko

VISUAL UNITY TASK PLAN

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

Keywords: Unity application, game logic elements, Visual Studio, C # language, databases.

This article describes an application that implements a task planner for a head of a small business department. The application was created in the Visual Studio programming environment and in the Unity editor. Distinctive features of the software product, first of all, is a game script for registration and control over the execution of project tasks, as well as their game visualization.

Статья посвящена решению задачи планирования работы руководителя в организации малого бизнеса.

Такие задачи возникают в организациях, где есть наемные работники, которые должны выполнять свои обязанности согласно инструкциям и технологическому процессу бизнеса.

В самом широком понимании планирование – это неотъемлемая часть любого руководства, когда нужно выполнить что-то в коллективе к поставленному сроку.

Еще одним направлением, где очень важно планирование и контроль за выполнением поставленных задач, это совместное выполнение проектов. Когда в проекте много задач и подзадач, то в дополнение к планированию, необходимы средства наглядного отображения состояния решаемых задач.

Не для кого ни секрет, что люди мыслят образами или картинками [1]. Тогда проще и легче контролировать выполнение задач, анализировать полученные результаты и принимать решения.

В известных сейчас подходах к планированию и визуализации процессов выполнения задач отсутствуют средства и методы, стимулирующие рабочий процесс по реализации планов. Одним из таких способов является игровой момент, когда сам процесс планирования представляется в виде игры, где за выполнение задач начисляются баллы. Очевидно, что использование игровых ситуаций, привычных пользователю, в обучении и повседневной деятельности значительно повышает эффективность выполнения решаемых задач [2].

Т.о., разработка приложения для автоматизации процесса планирования является актуальной.

Разработка любого программного продукта состоит из двух основных этапов – проектирования структуры и его составных частей, и непосредственно его программирование, т.е. написание программного кода. Необходимо, так же, спроектировать базу данных, как основу приложения. Далее, для конкретной базы данных программируются управляющая оболочка и пользовательский интерфейс. В заключение, нужно разработать модуль визуализации планирования в организации.

Логическую схем данных всей базы данных решаемой задачи в формате MS Access показана на рисунке 1.

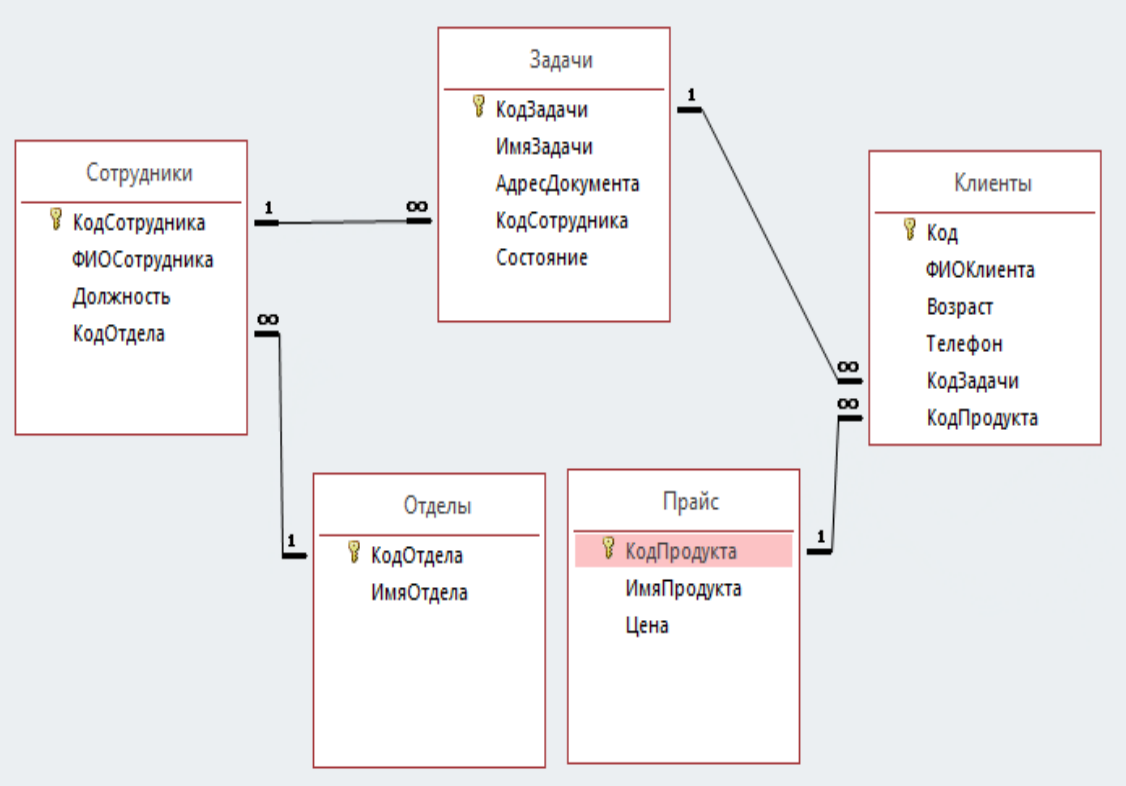


Рисунок 1. Схема данных в формате MS Access

Первый модуль приложения должен управлять базой данных. Значит его состав должен полностью повторять все таблицы базы данных (в соответствии с рисунком 1).

В дополнение к этому, нужны компоненты, с помощью которых можно вносить изменения в таблицы базы данных.

Поэтому, проект выполнен на языке программирования C#, вариант - Windows Form и его состав показан в соответствии с рисунком 2.

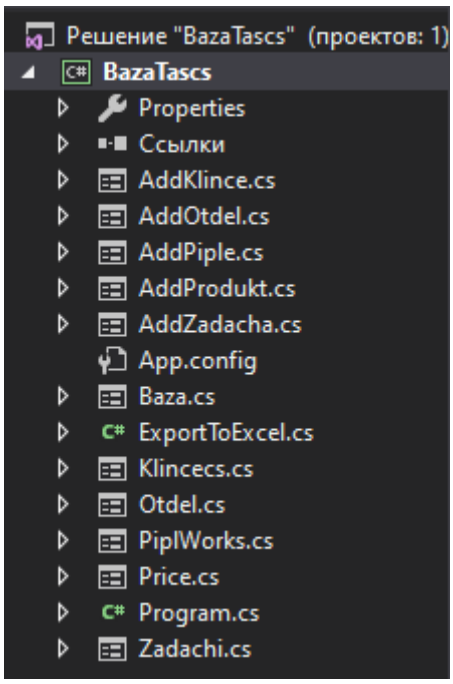


Рисунок 2. Состав модуля для управления базой данных

Внешний вид формы для управления базой данных показан в соответствии с рисунком 3.

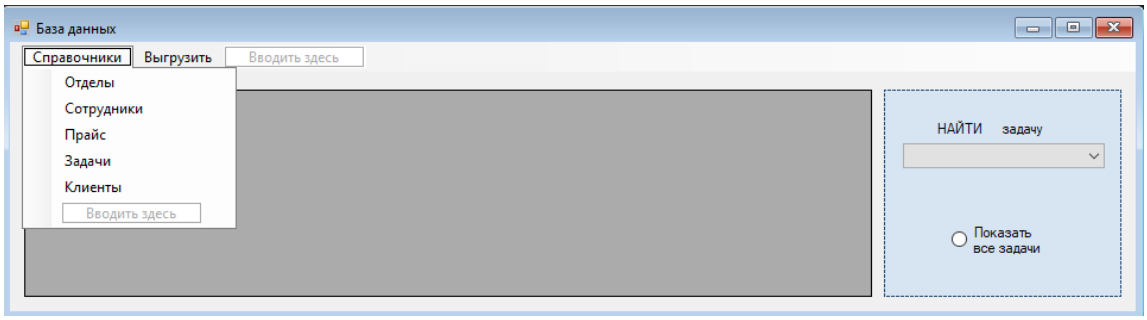


Рисунок 3. Главная форма модуля приложения

Идея создания этой формы состоит в том, чтобы при запуске модуля приложения отрывалась бы эта форма со списком всех задач отдела организации. Поэтому на эту форму помещен элемент управления radioButton1, который блокирует comboBox2 и отображает все задачи, а не одну из них (в соответствии с рисунком 3). Еще одной функцией этой формы является обращение к остальным формам приложения через выпадающее меню (ToolStripMenuItem), поэтому код этой формы содержит, в основном, операторы с объектами других форм приложения (в соответствии с листингом 1).

Листинг 1. Фрагмент кода формы Baza

```
private void организацииToolStripMenuItem_Click(object sender, EventArgs e)
      {
         Otdel ob = new Otdel();
         ob.Show();
      }
```

Листинг 1 – Продолжение

```
private void сотрудникиToolStripMenuItem_Click(object sender, EventArgs e)
      {
         PiplWorks ob = new PiplWorks();
```

```
            ob.Show();
        }
    private void товарыToolStripMenuItem_Click(object sender, EventArgs e)
        {
            Price ob = new Price();
            ob.Show();
        }

        private void услугиToolStripMenuItem_Click(object sender, EventArgs e)
        {
            Zadachi ob = new Zadachi();

    ob.Show();
        }
    private void категорииToolStripMenuItem_Click(object sender, EventArgs e)
        {
            Klincecs ob = new Klincecs();
            ob.Show();
        }
```

Визуализирующий модуль приложения реализовывает принцип планирования, использующийся в компании Toyota [3]. Основным здесь является постоянный контроль за исполнением задач. Согласно нему, менеджеры этой компании наклеивали стикеры на настенную доску и писали на них номера или названия заданий (задач). На такой доске визуализации было, обычно, 3 раздела: «Текущие задачи», «Выполненные» и «Перешедшие с предыдущих дней». Итоги подводились ежедневно с перераспределением всех задач законченного дня по указанным категориям. Т.о., все задачи всегда находились в фокусе внимания без потерь.

Согласно этому принципу, общая логика работы приложения будет в соответствии с рисунком 4, когда вначале запускается блок визуализации, а уже из него можно будет открыть модуль управления базой данных.

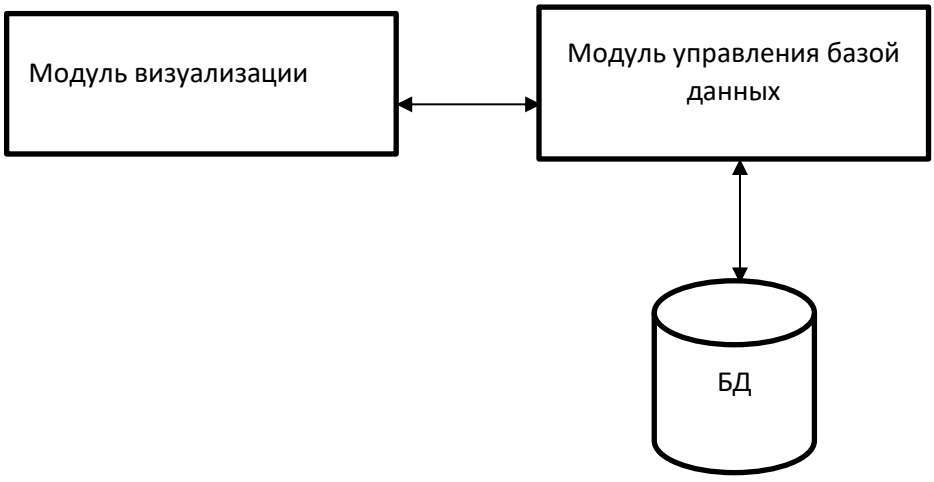


Рисунок 4. Логика работы приложения в целом

Далее, в известном игровом редакторе Unity создается игровая сцена, отображающая недельное планирование (в соответствии с рисунком 5).

Рисунок 5. Вид игрового интерфейса

Разработанный программный продукт обладает следующими преимуществами:

1. Реализует эффективный способ визуализации планирования.
2. Воплощает игровой элемент поощрения выполнения поставленных задач.
3. Обладает дружественным пользовательским интерфейсом.
4. Предоставляет исчерпывающую информацию по выполняемым проектам.

СПИСОК ЛИТЕРАТУРЫ

1. Наглядно-образное мышление. URL: https://www.psychologos.ru/articles/view/naglyadno-obraznoe-myshlenie. (дата обращения: 21.10.2021).
2. Применение обучающих программ на игровых платформах для повышения эффективности образования. URL: https://cyberleninka.ru/article/n/primenenie-obuchayuschih-programm-na-igrovyh-platformah-dlya-povysheniya-effektivnosti-obrazovaniya. (дата обращения: 21.10.2021).
3. Четырнадцать Принципов Дао Toyota. URL: https://www.cfin.ru/management/practice/14_principles.shtml. (дата обращения: 21.10.2021).

А.Е. Дмитриев, П.В. Лобзенко

РАБОЧЕЕ МЕСТО МЕНЕДЖЕРА ОПТОВЫХ ПОСТАВОК

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: база данных Access, Visual Studio, язык C#, автоматизированное рабочее место.

В статье разработано приложение для автоматизации рабочего места менеджера коммерческой организации. Приложение состоит из базы данных, созданной в СУБД Access, и управляющего кода, написанного на языке программирования C#.

A.E. Dmitriev, P. V. Lobzenko

WORKPLACE OF WHOLESALE MANAGER

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

Keywords: Access database, Visual Studio, C #, workstation.

The article has developed an application for automating the workplace of a manager of a commercial organization. The application consists of a database created in the Access DBMS and control code written in the C # programming language.

Признаком современного этапа использования компьютеров на рабочих местах является, прежде всего то, что сейчас в организациях устанавливаются не просто отдельные компьютеры, а целостные информационные системы. Они служат для обеспечения всех направлений деятельности предприятий. Это – коммерческая деятельность, производственные задачи и финансовое направление.

В настоящее время, специализированные приложения для автоматизации рабочих мест создаются в 2-х вариантах- одно или многопользовательские, а также основанные на клиент-серверных структурах баз данных (БД) или на использовании БД, встроенных в офисные пакеты (например Access от Microsoft Office) [1].

Традиционно, приложения для автоматизации рабочих мест состоят из базы данных и управляющей ее оболочки.

В разработанном приложении база данных реализована с помощью СУБД Access. Причины выбора Microsoft Access для разработки базы данных заключаются в следующем:

- для работы программы не требуется BDE или InterBase, или дополнительные серверные среды разработки;
- такое решение обладает большей гибкостью: в него легко можно внести дополнения и изменения;
- вся база данных находится всего в одном файле.

Access обеспечивает все возможности определения, обработки и управления данными для работы с большими объемами информации. Может так же использоваться для создания файла проекта, подключаемого к серверу SQL Server, что позволит совместно использовать данные сервера другими приложениями или пользователями по сети. При создании файла проекта в качестве системы управления базами данных выступает SQL Server (или Microsoft SQL Server Desktop Engine, MSDE).

Физическая диаграмма созданной базы данных показана на рисунке 1.

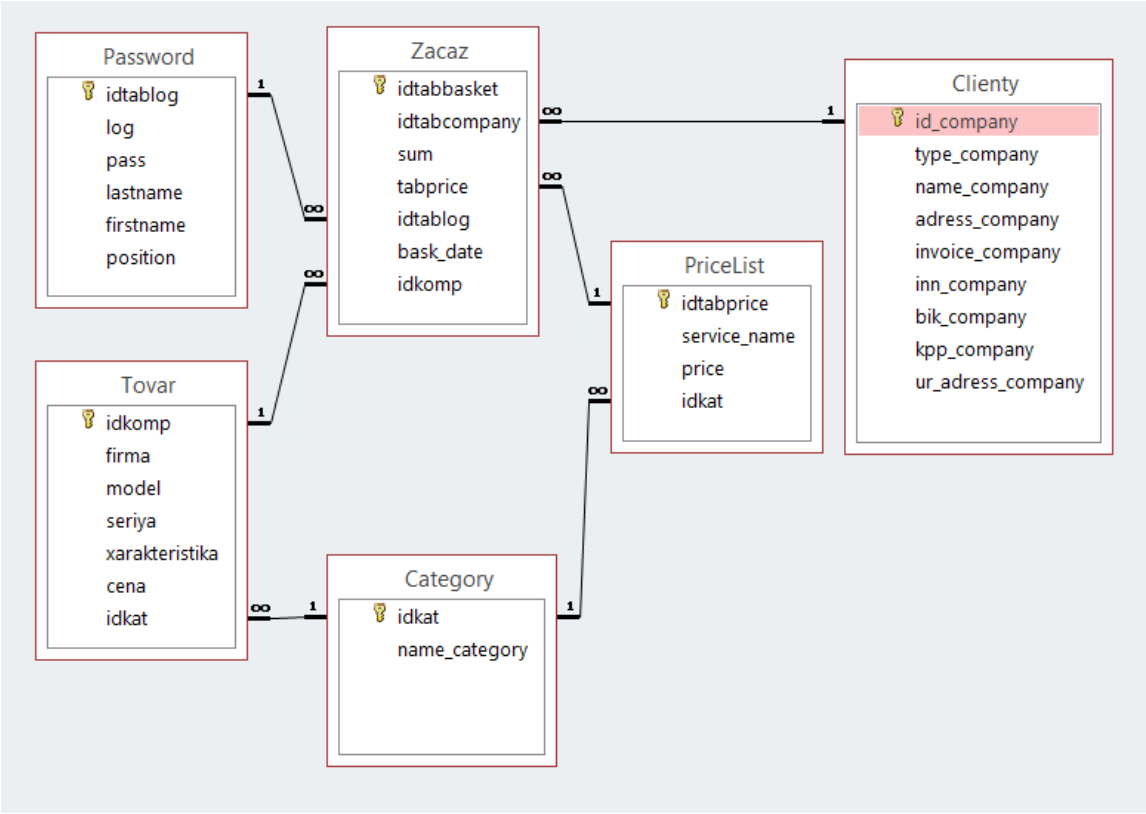


Рисунок 1. «Физическая» диаграмма базы данных

Управляющая оболочка приложения выполнена на языке программирования C# в редакторе Visual Studio [2,3].

Наиболее популярной средой разработки для C# является мультиплика-тивная универсальная среда Visual Studio.

В настоящее время, C# включен в семейство продуктов этой среды разработки ПО на различных языках высокого уровня – мощной интегрированной среды разработки приложений различного уровня сложности и назначения. В этом пакете используется единая интегрированная среда разработки (IDE), состоящая из нескольких элементов: строки меню, панели инструментов, различных закрепленных или автоматически скрываемых окон инструментов в левой, нижней или правой областях, а также области редакторов.

Проект приложения, разработанный в C# состоит из набора классов, каждый из которых, реализует взаимодействие с таблицами базы данных (рисунок 2).

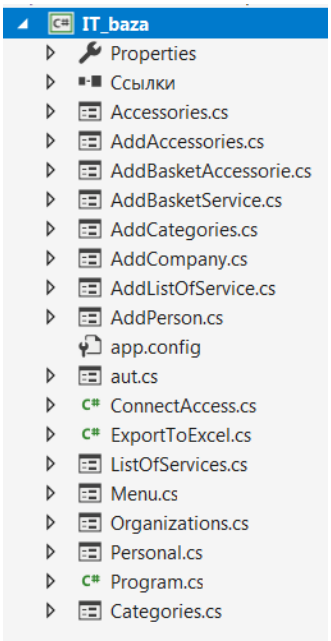


Рисунок 2. Состав проекта приложения

Основной класс, запускающий главную форму приложения, это Program, содержащий главную функцию проекта - void Main() (листинг 1).

Листинг 1. Класс для запуска проекта

```
using System;
using System.Collections.Generic;
using System.Windows.Forms;
namespace IT_Baza
{
   static class Program
   {
      /// <summary>
/// Главная точка входа для приложения.
      /// </summary>
      [STAThread]
      static void Main()
      {
         Application.EnableVisualStyles();
         Application.SetCompatibleTextRenderingDefault(false);
         Application.Run(new aut());
      }
   }
}
```

Как видно, здесь запускается начальная форма приложения. Она служит для аутентификации пользователя приложения, а также для запуска формы Menu.

В классе Menu описывается состав формы и всплывающих окон и списков.

Здесь же задается вид таблиц главной формы приложения. Классы, например, Accessories и Accessories.Designer задают и разворачивают форму для задания таблицы «Tovar», помещая на нем управляющие клавиши. Под одноименными названиями классы создают формы для списков клиентов, сотрудников, услуг и товаров.

В дополнение к этому, классы, названия которых начинается с приставки «Add» необходимы для задания форм с которых можно заполнять все таблицы базы данных. Это, можно сказать, сервисные классы, с помощью которых заполняются таблицы базы данных.

В отличие от них, в классе Menu, как это было указано выше, формируется форма «Журнал заказов и услуг».

Главная форма приложения показана на рисунке 3.

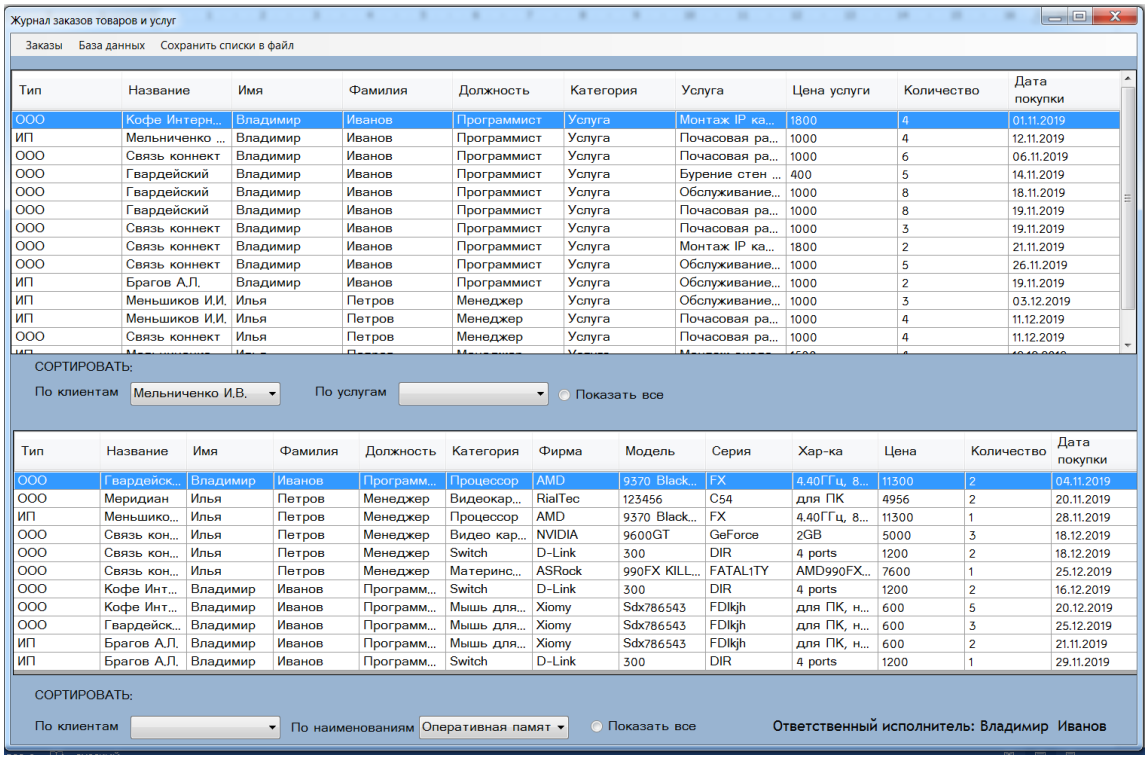


Рисунок 3. Главная форма приложения

Разработанное приложение обладает следующими преимуществами:

1. Реализует эффективный способ управления базой данных.
2. Обладает простым, понятным и удобным пользовательским интерфейсом.
3. Реализует основные рутинные функции менеджеров.
4. Полностью реализует алгоритм отправки заявки на оптовые поставки.
5. Предоставляет исчерпывающую информацию по выполняемым заявкам.

СПИСОК ЛИТЕРАТУРЫ

1. Технические статьи по Access. *URL: http://msdn.microsoft.com.* (дата обращения: 25.09.2021).
2. Краткое описание Visual Studio. *URL: URL: http://habrahabr.ru.* (дата обращения: 25.09.2021).
3. Джесс Либерти Программирование на C#. - Изд-во Символ – плюс: Москва, 2012.- 863 с.

О.Ю. Траленко, П.В. Лобзенко

ИГРОВОЕ ОБУЧЕНИЕ ПРОГРАММИРОВАНИЮ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: Unity приложение, элементы игровой логики, Visual Studio, язык C#, обучение программированию.

В статье описано приложение, реализующее игровой метод обучения. Приложение создано в среде программирования Visual Studio и в редакторе Unity. Отличительными особенностями программного продукта, в первую очередь, является использование вовлеченности и заинтересованности пользователей в игровых ситуациях, что обеспечивает быстрое и качественное восприятие нового материала при обучении программированию.

O.Yu. Tralenko, P.V. Lobzenko

GAME LEARNING PROGRAMMING

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

Keywords: Unity application, game logic elements, Visual Studio, C # language, programming training.

The article describes an application that implements a game learning method. The application was created in the Visual Studio programming environment and in the Unity editor. Distinctive features of the software product, first of all, is the use of the involvement and interest of users in game situations, which ensures fast and high-quality perception of new material when teaching programming.

Созданное приложение соединяет в себе две сильных стороны современных способов обучения: визуализацию и использование Интернет- технологий размещения и хранения контента.

Вообще в современном мире, можно сказать, что, практически ни одна из сторон жизни и деятельности человека не обходится без использования Интернет-разработок или с помощью того, что в нем расположено. В том числе, и обучающие приложения, использующие силу Интернета, имеют большую популярность.

Сейчас в Интернете представлено множество обучающих ресурсов различного назначения:

- различного рода тестирующие и программные средства для контроля и измерения уровня знаний, умений и навыков обучающихся;
- электронные учебники;
- электронные практикумы;
- экспертные обучающие системы.

И тем не менее, возникает необходимость в разработке приложения для обучения программированию посредством метода визуализации. Тем более, что пользователи в процессе самостоятельной работы получают доступ к материалам, подобранным оптимально с точки зрения освоения программирования на выбранном машинном языке.

Необходимо отдельно остановиться на методе визуализации в изучении программирования. Визуализация — общее название приёмов представления числовой

информации или физического явления в виде, удобном для зрительного наблюдения и анализа [8]. Другими словами, существуют доказательства того, что наш мозг не различает разницы между действительным и воображаемым.

Вот почему имея в распоряжении визуальные образы – предметы, помещенные в 3-х мерном пространстве, пользователь имея задачу передвинуть их с помощью программы, или еще как-то организовать их взаимодействие, увлекается этим процессом и осваивает значительно больше материала, по сравнению с чисто математическими задачами. Это как раз и реализовывает приложение.

Приложение состоит из обучающих материалов и управляющей оболочки. Логика работы электронной оболочки следующая. После запуска приложения в стартовом окне можно перейти либо к практикуму и к теории, а также к шаблонам решения заданий, либо закрыть каждую из вкладок. Т.е., обучающийся может выбрать форму изучения материала. При этом, он может использовать теоретические материалы, темы и задания к ним, которые размещаются на Интернет - ресурсах. Шаблоны решений практических заданий отображаются в отдельных окнах приложения.

Самый простой и удобный вариант – это скомпоновать приложение из отдельных сцен в редакторе Unity [2].

Сценой называется контекст или исходное расположение всего, что участвует в игре. Это могут быть персонажи, или просто обстановка, которая соответствует чему-либо.

В нашем случае, это будут элементы интерфейса (UI-user interface): кнопки для переключения сцен и обучающих материалов, а также текст для вывода на форму приложения описательной информации.

Для размещения элементов управления используется панель выбранного цвета. Первая стартовая сцена приложения показана на рисунке 1.

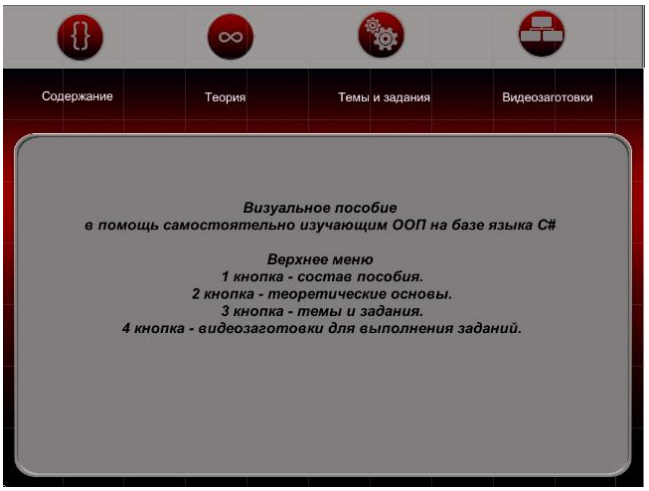


Рисунок 1. Стартовая сцена приложения

Здесь кнопки управления реализованы в слоях, которые невидимы до нажатия на кнопку «Содержание».

«Невидимость» можно сделать программно или с помощью свойств объектов, составляющих стартовую сцену приложения (рисунок 2).

Рисунок 2. Состав стартовой сцены приложения

Для того, чтобы объекты, находящиеся в любой из сцен проекта выполняли требуемые действия (при нажатии на кнопки что-то происходило) нужно в редакторе Visual Studio на языке C# составить скрипт и прикрепить его к одному из объектов на сцене [3]. Управляющие скрипты, в свою очередь, представляют собой классы, наследующие свойства самого большого класса MonoBehavior. В их состав входят библиотеки, глобальные переменные и методы для реализации логики интерфеса.

Так, например, для перехода к требуемой сцене проекта используется метод запуска определенного объекта, в данном случае, сцены.

Листинг 1. Фрагмент кода управляющего скрипта

```
public void Button2()
   {
      Application.LoadLevel("Sc1");
   }
   public void Button3()
   {
      Application.LoadLevel("Sc2");
   }
   public void Button4()
   {
      Application.LoadLevel("Sc3");
   }
```

В соответствии с этим листингом нужная сцена, например, Sc2 открывается с помощью метода LoadLevel("Sc2"), который находится в классе Application.

Т.о., сцены составляются как отдельные проекты в Unity. В них помещаются трехмерные графические фигуры – примитивы (куб, цилиндр, сфера и т.д.) (рисунок 3).

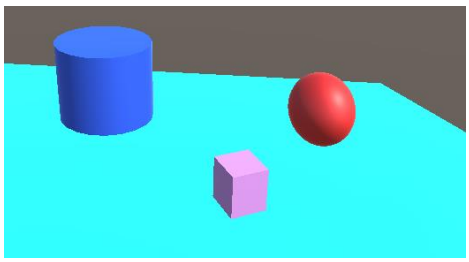


Рисунок 3. Визуальный шаблон для выполнения заданий

Перейдя в третий раздел приложения можно запустить одну из видео-заготовок (рисунок 4).

Рисунок 4. Раздел видео-заготовок

Т.о., используя готовые шаблоны, обучающиеся решают определенные игровые задачи и вовлекаясь в этот процесс более глубоко осваивают учебный материал.

Разработанный программный продукт снабжен:

- простым и понятным пользовательским интерфейсом с наглядными кнопками навигации;
- возможностью использования в любой операционной системе и на мобильных устройствах;
- возможностью оперативного внесения изменений в имеющийся материал контента;
- удобством и наглядностью навигации по учебным ресурсам, быстрым доступом к искомым разделам, объектам электронного пособия;
- возможностью разработки собственных игровых приложений, используя видео-заготовки пособия;
- реализацией метода визуализации посредством готовых визуальных моделей, которые программирует пользователь самостоятельно.

СПИСОК ЛИТЕРАТУРЫ

1. Метод визуализации: раскрываем все секреты работы. 3 важных момента. URL: https://omkling.com/metod-vizualizacii-2/. (дата обращения: 06.10.2021).
2. Хокинг Дж. Unity в действии. Мультиплатформенная разработка на C# / Пер. с англ. И. Рузмайкиной. — СПб.: Питер, 2016. — 336 с.
3. Краткое описание Visual Studio URL: http://habrahabr.ru. (дата обращения: 06.10.2021).

О.Н. Шкумат, П.В. Лобзенко

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ПРОДАВЦА-ТОВАРОВЕДА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: мобильное приложение, клиент-серверное приложение, Visual Studio, ASP NET, базы данных.

На основе выполненного анализа программных продуктов в свободном доступе для спроектировано и реализовано приложение, информационно обеспечивающее рабочее место продавца-товароведа торговых точек малого бизнеса. Приложение отличается удобным доступом через web браузер с любого мобильного устройства, подключенного к сети Интернет. В дополнение к этому, приложение снабжено базой данных, расположенной на сервере.

O.N. Shkumat, P.V. Lobzenko

MOBILE APP OF THE SELLER-COMMANDER

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

Keywords: mobile application, client-server application, Visual Studio, ASP NET, databases.

On the basis of the analysis of software products in the public domain, an application was designed and implemented that provides informational support to the workplace of a merchandiser at small business outlets. The application is easily accessible via a web browser from any mobile device connected to the Internet. In addition to this, the application is supplied with a database located on the server.

Автоматизация повседневной деятельности организаций направлена, как правило, либо на весь процесс бизнес-процесс в целом, либо на отдельные его составляющие.

Обычно, в первую очередь, это касается документооборота или бухгалтерской отчетности. Однако, большинство, представленных на рынке программных продуктов (ПП) такой направленности, содержат множество функций, которые на конкретных предприятиях, как правило, в дальнейшем не используются. Это приводит к удорожанию ПП для конечных пользователей. Поэтому, в настоящее время предприятия малого и среднего бизнеса предпочитают ПП локального использования, например, для конкретного рабочего места, которые либо заказывают, либо разрабатывают сами.

Сейчас, специализированные приложения для автоматизации рабочих мест создаются в 2-х вариантах- одно или многопользовательские, а также основанные на клиент-серверных структурах баз данных (БД) или на использовании БД, встроенных в офисные пакеты (например, MS Access).

ПП, использующее сторонние базы данных, где, как обычно, присутствуют серверная и клиентская части, стоят, обычно, дороже из-за необходимости иметь на рабочих местах дополнительное программное обеспечение (ПО) (в данном случае, необходимы системы управления базами данных (СУБД)).

Конечно, использование предустановленного ПО в качестве СУБД является сейчас все чаще избираемым путем экономного оснащения рабочих мест, что значительно снижает затраты на их оснащение.

Одной из основных характеристик используемого ПО сейчас рассматриваются его сетевые качества, т.е. на сколько оно используется в сети Интернет.

В этом отношении приложения разрабатываются и устанавливаются либо для мобильных устройств, либо имеют сайтовый вариант применения. Ко второму типу ПП относятся те, которые не требуют предустановки клиентской части на устройствах пользователей. Т.е., имея в распоряжении Интернет – соединение и любой из эксплореров можно использовать такое приложение, запущенное на определенном Интернет – ресурсе.

В торговых организациях малого бизнеса, как правило, продавцы одновременно и заказывают товары. Это означает, что бизнес – процесс предусматривает реализацию товаров по схеме поставок на реализацию. Т.е., продавец-товаровед делает заказ на реализацию продукции с отсроченным платежом.

Т.о., возникает необходимость в автоматизации указанного бизнес – процесса, чтобы все данные хранились в общей сетевой базе и были доступны для совместного использования.

В качестве инструмента разработки используется язык C# и платформа ASP.NET, а редактором является Visual Syudio [1,2]. Это удобные инструменты для использования технологии MVC (model - view — controller). Т.е., в разработке приложение делится на три компонента:

- контроллер (controller) — класс, занимающийся связью базы данных с пользователем и обработкой текущей информации из базы данных;
- представление (view) — класс, обеспечивающий пользовательский интерфейс;
- модель (model) — класс для описания логики данных приложения.

Реляционная база данных приложения представляет собой взаимосвязанные таблицы и реализована на встроенном Sql Server [3]. Состав ее модели показан на рисунке 1.

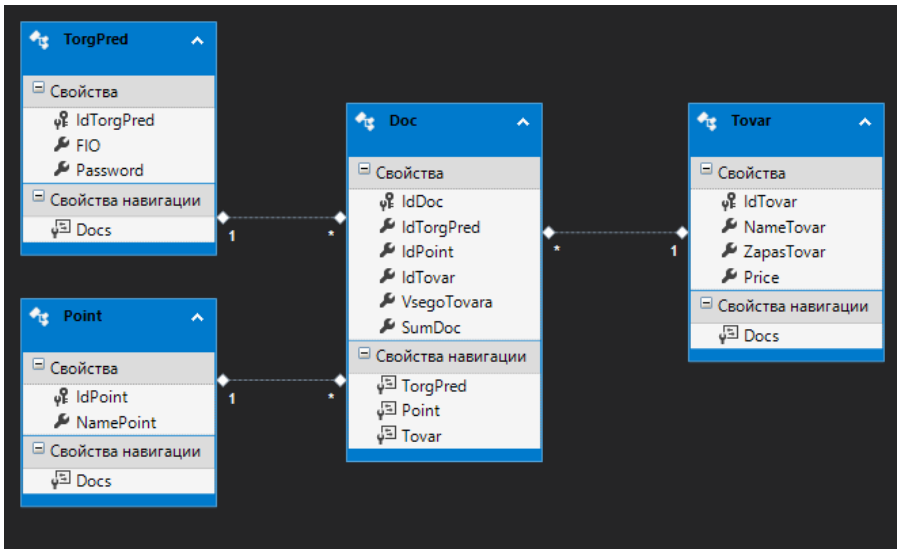


Рисунок 1. Модель базы данных.

Для того, чтобы начать разработку программы приложения необходимо связать модель базы данных с формами, которые будут создаваться. Для этого воспользуемся классом Linq to Sql, который для этого и предназначен.

Добавляем (по правой клавиши мыши) в проект этот компонент (в соответствии с рисунком 2).

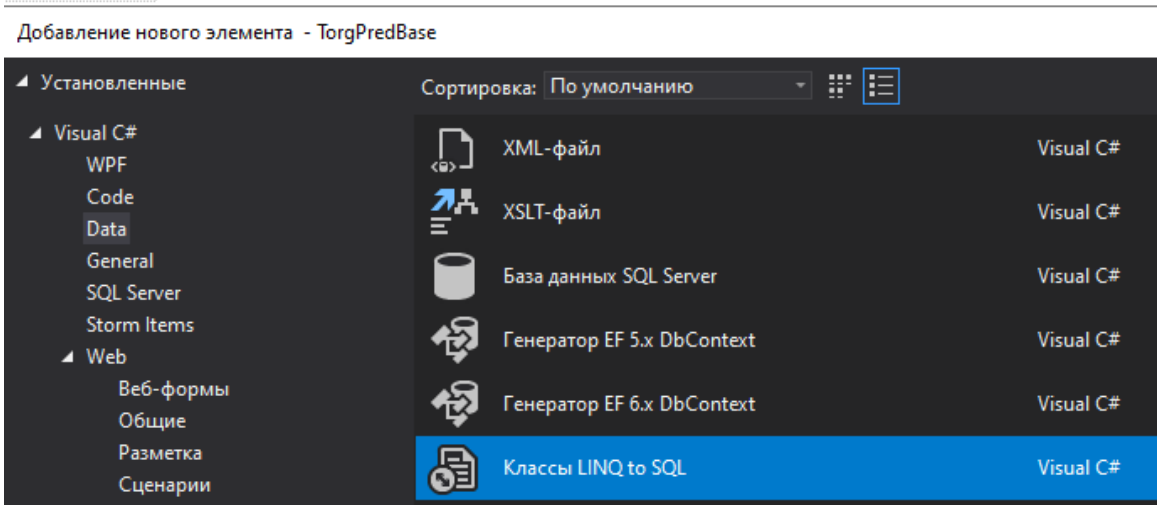


Рисунок 2. Добавление компонента для связи с БД

Далее, в отрывшейся конструктор «перетаскиваем» созданную базу данных в соответствии с рисунком 3.

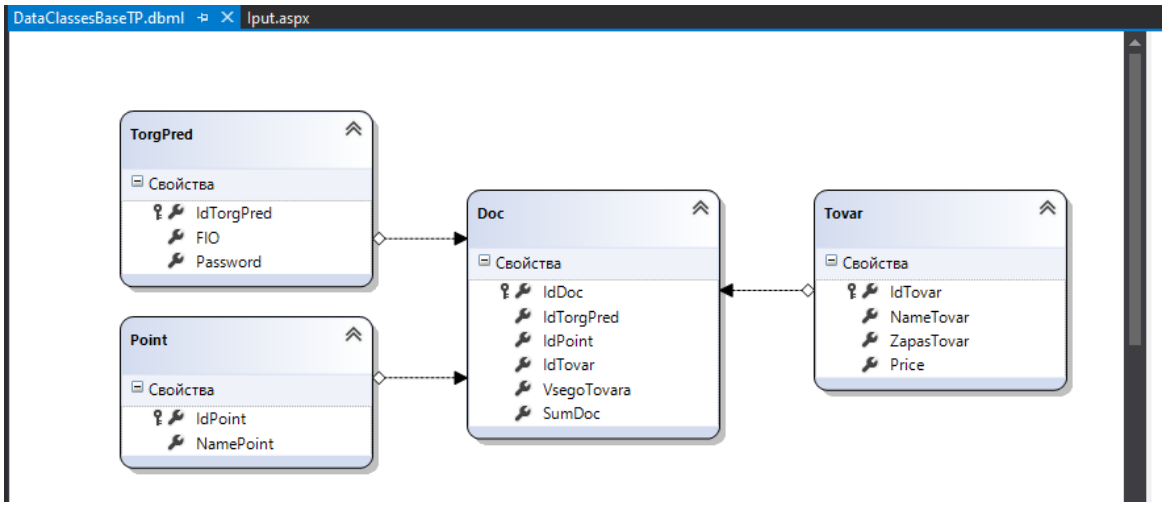


Рисунок 3. Состав базы данных приложения

Созданное приложение включает несколько форм для выполнения заказа и для заполнения таблиц базы данных.

Рабочая форма продавца содержит необходимые данные для создания накладной на поставку товара (рисунок 4).

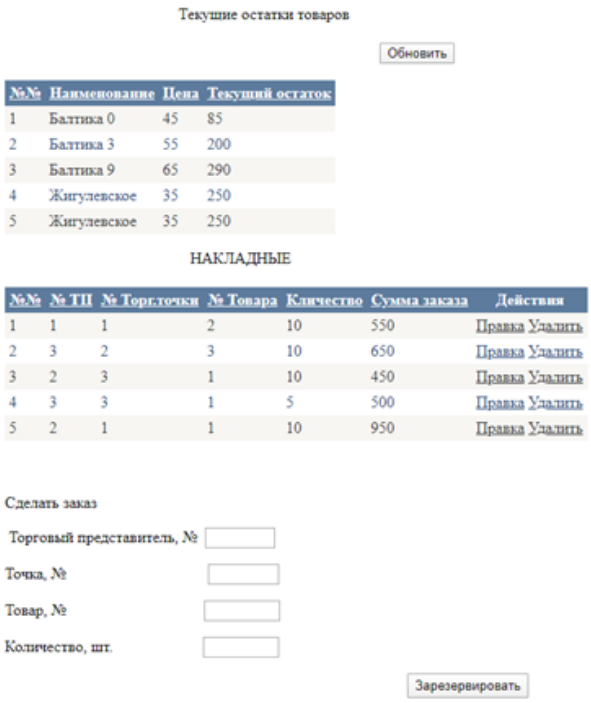


Рисунок 4. Форма для заказа

Разработанное приложение обладает следующими преимуществами:

1. Реализует эффективный способ клиент-серверной системы.
2. Обладает простым, понятным и удобным пользовательским интерфейсом.
3. Реализует основные рутинные функции продавца-товароведа.
4. Полностью реализует алгоритм отправки заявки на доставку товаров.
5. Предоставляет исчерпывающую информацию по выполняемым заявкам.

СПИСОК ЛИТЕРАТУРЫ

1. Джесс Либерти Программирование на C#. - Изд-во Символ – плюс: Москва, 2012.- 863 с.
2. Краткое описание Visual Studio. URL: http://habrahabr.ru. (дата обращения: 21.09.2021).
3. Справочное руководство по MySQL. URL: http://www.mysql.ru/docs/man/Features.html. (дата обращения: 21.09.2021).

Г.В. Мельников, В.Д. Дрокин, О.В. Куликова

МЕТОДЫ ОБРАБОТКИ И ОТСЛЕЖИВАНИЯ ПРЕРЫВАНИЙ В ОС WINDOWS И ОС LINUX

Донской государственный технический университет,
Ростов-на-Дону, Россия

Ключевые слова: система прерываний, обработчик прерываний, приоритет прерываний, время прерываний, сигналы.

В статье представлен обзор принципов работы прерываний и их методы обработки и перехвата в операционных системах Windows и Linux. Были изучены и проанализированы области в которых выполняются системы и обрабатываются компоненты, а также устройства их взаимодействия, а именно система прерываний, время выполнения прерываний и отслеживание прерываний, путем установки их обработчика.

G.V. Melnikov, V.D. Drokin, O.V. Kulikova

INTERRUPTION HANDLING AND TRACKING METHODS IN OS WINDOWS AND OS LINUX

Don State Technical University, Rostov-on-Don, Russia

Keywords: interrupt system, interrupt handler, interrupt priority, interrupt time, signals.

The article provides an overview of the principles of interrupt operation and their methods of handling and interception in Windows and Linux operating systems. The areas in which systems are executed and components are processed, as well as the devices of their interaction, namely the interrupt system, interrupt execution time and interrupt tracking, were studied and analyzed by installing their handler.

Введение

На сегодняшний день, большинство пользователей даже не задумывается, как программа будет взаимодействовать с процессором, памятью и устройствами ввода-вывода. Это вопрос, которым озадачиваются разработчики при проектировании любого ПО. Данная процесс по большей части отдается операционной системе. Операционная система связывает программное обеспечение с аппаратным обеспечением и именно поэтому является основой для функционирования остальных программ. Более того, если возникает необходимость в решении специфических задач, таких как создание и управление процессами и потоками, управление элементами файловых систем и т.п., то ОС предоставляет разработчику все необходимые инструменты, реализованные в виде различных библиотек системных функций.

Фундаментом любой операционной системы является набор системных вызовов. Системные вызовы используются операционной системой для выполнения всех своих функций. Более того часть системных вызовов доступна для каждого разработчика, что позволяет ему использовать возможности операционной системы при проектировании работы собственных прикладных программ и приложений, а также возможность дополнять существующий набор системного программного обеспечения новой функциональностью.

Объектом нашего исследования стали методы отслеживания прерываний в операционных системах Windowsи Linux.

Программные прерывания представлены сигналами, обеспечивающие асинхронную обработку событий, а аппаратные прерывания называются IRQ (сокращенно от

InterruptReQuests - Запросы на Прерывание) и делятся на два подвида: “короткие” и “длинные”.

1 Отслеживания прерываний в ОС Windows

1.1 Реализация прерываний, в ОС Windows

Прерывания и исключения - это состояния операционной системы, которые отвлекают процессор от выполнения кода, выходящего за рамки обычного потока управления. Обнаружить их может как оборудование, так и программное обеспечение. Термин «ловушка» относится к механизму процессора для захвата выполняемого потока при возникновении исключения или прерывания и передачи управления в фиксированное место в операционной системе. В Windows процессор передает управление обработчику прерывания, который является функцией, специфичной для определенного прерывания или исключения.

Общим для реализации рассматриваемых основных механизмов является необходимость сохранения состояния текущего потока с его последующим восстановлением. Для этого в ОС Windows используется механизм ловушек

В случае возникновения требующего обработки события (прерывания, исключения или вызова системного сервиса) процессор переходит в привилегированный режим и передает управление обработчику ловушек, входящему в состав ядра.

Обработчик ловушек создает в стеке ядра (о стеке ядра см. «Реализация процессов и потоков») прерываемого потока фрейм ловушки, содержащий часть контекста потока для последующего восстановления его состояния, и в свою очередь передает управление определенной части ОС, отвечающей за первичную обработку произошедшего события [1].

То же самое происходит в случае возникновения исключений и прерываний. Простые исключения могут быть обработаны диспетчером ловушек, а более сложные обрабатываются диспетчером исключений, который может в случае возникновения исключения вернуть управление вызвавшему это исключение приложению.

Аппаратные прерывания обычно исходят от устройств ввода-вывода, которые должны уведомлять процессор, когда им требуется обслуживание. Устройства, управляемые прерываниями, позволяют операционной системе максимально использовать возможности процессора, перекрывая центральную обработку с операциями ввода-вывода. Поток начинает передачу ввода-вывода на устройство или с устройства, а затем может выполнять другую полезную работу, пока устройство завершит передачу. Когда устройство завершает работу, он прерывает работу процессора для обслуживания. Указывающие устройства, принтеры, клавиатуры, дисководы и сетевые карты обычно управляются прерываниями.

Ядро устанавливает обработчики прерываний для ответа на прерывания устройства. Обработчики прерываний передают управление либо внешней программе (ISR), которая обрабатывает прерывание, либо внутренней программе ядра, которая реагирует на прерывание. Драйверы устройств предоставляют ISR для обслуживания прерываний устройств, а ядро предоставляет процедуры обработки прерываний для других типов прерываний.

В большинстве операционных систем аппаратные прерывания имеют приоритеты, которые определяются контроллерами прерываний. Однако ОС Windows имеет свою аппаратно-независимую шкалу приоритетов, которые называются уровни запросов прерываний (interruptrequestlevels, IRQL), и охватывает не только прерывания, а все события, требующие системной обработки. На рисунке 1 представлена таблица значений IRQL уровней для x86 систем [2].

Уровень	Значение	Номер
High	Наивысший уровень	31
Power fail	Отказ электропитания	30
Inter-process interrupt	Межпроцессорный сигнал	29
Clock	Системные часы	28
Profile	Контроль производительности ядра	27
Device n	Прерывание от устройства	26
...	Прерывания от устройств	...
Device 1	Прерывание от устройства	3
DPC /dispatch	Отложенные операции и планирование	2
APC	Асинхронные вызовы процедур	1
Passive	Нормальное выполнение потоков	

Рисунок 1. Таблица значений IRQL

1.2 Время прерываний в ОС Windows

Для отслеживания времени исполнения прерывания в ОС Windows, можно обратится к системному таймеру.

Время прерываний — это время, прошедшее с момента последнего запуска системы.Таймер в Windows является устройством ввода информации,которое периодически извещает приложение о том, что истек заданный интервалвремени. При решении некоторых задач программа должна отслеживатьтекущее время или выполнять какие-либо действия с определенной периодичностью.Например, эта проблема возникает в приложениях, имитирующих аппаратуру,работающую в реальном масштабе времени, в игровых или мультимедийныхприложениях, а также при проведении различных тестов. Кроме того, иногдатребуется отладить критичные по времени исполнения фрагменты кода, для чегонужен «хронометр» с высокой разрешающей способностью.

Win32 API содержит как функции для измерения текущеговремени, так и функции для создания виртуальных таймеров - устройств,оповещающих приложение об истечении заданного интервала времени. Для успешногоприменения этих программных средств необходимо учитывать разрешающуюспособность и потенциальную точность измерения.

Для получения счетчика времени прерывания можно использовать функции QueryInterruptTime(),QueryInterruptTimePrecise(),QueryUnbiasedInterruptTime(),QueryUnbiasedInterruptTimePrecise().

QueryInterruptTime()-Получает текущий счетчик времени прерывания.

QueryInterruptTimePrecise()-Получает текущий счетчик времени прерывания в более точной форме.

QueryUnbiasedInterruptTime()-Получает текущий несмещенный счетчик времени прерывания в единицах по 100 наносекунд.

QueryUnbiasedInterruptTimePrecise()-Получает текущее несмещенное количество времени прерывания в более точной форме.

Несмещенное время прерывания означает, что учитывается только время, в течение которого система находится в рабочем состоянии, поэтому счетчик времени прерывания не «смещен» по времени, которое система проводит в спящем или спящем режиме [3].

2 Отслеживания прерываний в ОС Linux

2.1 Прерывания и их обработка в ОС Linux

2.1.1 Программные прерывания. Сигналы

Сигналы - это программные прерывания, обеспечивающие асинхронную обработку событий. Эти события могут приходить из-за пределов системы; например, пользователь

может сгенерировать символ прерывания, нажав Ctrl+C. Другие источники прерываний - действия программы или ядра; например, сигнал возникнет, если процесс выполнит код, в котором происходит деление на нуль. В качестве примитивной формы межпроцессной коммуникации (IPC) один процесс также может послать сигнал другому процессу [4].

Ядро Linux реализует около 30 разновидностей сигналов (точное количество зависит от конкретной архитектуры). Каждый сигнал представлен числовой константой и текстовым названием. Например, сигнал SIGHUP используется, чтобы сообщить о зависании терминала. В архитектуре x86-64 этот сигнал имеет значение 1.

Сигналы прерывают исполнение работающего процесса. В результате процесс откладывает любую текущую задачу и немедленно выполняет заранее определенное действие. Все сигналы, за исключением SIGKILL (всегда завершает процесс) и SIGSTOP (всегда останавливает процесс), оставляют процессам возможность выбора того, что должно произойти после получения конкретного сигнала. Так, процесс может совершить действие, заданное по умолчанию (в частности, завершение процесса, завершение процесса с созданием дампа, остановка процесса или отсутствие действия), — в зависимости от полученного сигнала. Кроме того, процессы могут явно выбирать, будут они обрабатывать сигнал или проигнорируют его.

Проигнорированные сигналы бесшумно удаляются. Если сигнал решено обработать, выполняется предоставляемая пользователем функция, которая называется обработчиком сигнала. Программа переходит к выполнению этой функции, как только получит сигнал. Когда обработчик сигнала возвращается, контроль над программой передается обратно инструкции, работа которой была прервана. Сигналы являются асинхронными, поэтому обработчики сигналов не должны срывать выполнение прерванного кода. Таким образом, речь идет о выполнении только функций, которые безопасны для выполнения в асинхронной среде, они также называются сигналобезопасными.

Основная черта сигналов заключается в том, что не только события происходят асинхронно - например, пользователь может нажать Ctrl+C в любой момент работы программы, - но и обработка сигналов в программе выполняется асинхронно. Функции обработки сигналов регистрируются в ядре, которое асинхронно вызывает функции из остальной части программы, когда программа получает тот или иной сигнал.

Сигналы обладают очень строгим жизненным циклом. Сначала сигнал *порождается*. Затем ядро *сохраняет* сигнал до тех пор, пока не сможет его доставить. Наконец, как только появляется такая возможность, ядро *обрабатывает* сигнал требуемым образом. В зависимости от требований процесса ядро может выполнить одно из трех действий: *Игнорировать сигнал; Перехватить сигнал и обработать его; Выполнение действия, задаваемого по умолчанию.*

В настоящее время ядро может предоставлять заинтересованному программисту широкий контекст происходящего. Сигналы могут передавать даже данные, определяемые пользователем.

У каждого сигнала есть символьное имя, начинающееся с префикса SIG. Например, SIGINT отсылается, если пользователь нажал Ctrl+C. Сигнал SIGABRT генерируется, когда процесс вызывает функцию abort(). Наконец, сигнал SIGKILL посылается при принудительном завершении процесса.

2.1.2 Аппаратные прерывания. Обработка прерываний

Так как сигналы в ОС Linux являются программными прерываниями и были уже рассмотрены. То необходимо рассмотреть аппаратные прерывания и их обработку.

Аппаратные устройства обычно имеют весьма ограниченный объем ОЗУ, и если не считать поставляемую ими информацию немедленно, то она может потеряться.

В Linux аппаратные прерывания называются IRQ (сокращенно от InterruptReQuests - Запросы на Прерывание). Имеется два типа IRQ: "короткие" и "длинные". "Короткие" IRQ занимают очень короткий период времени, в течение которого работа операционной

системы будет заблокирована, а также будет невозможна обработка других прерываний. "Длинные" IRQ могут занять довольно продолжительное время, в течение которого могут обрабатываться и другие прерывания (но не прерывания из того же самого устройства). Поэтому, иногда бывает благоразумным разбить выполнение работы на исполняемую внутри обработчика прерываний (т.е. подтверждение прерывания, изменение состояния и пр.) и работу, которая может быть отложена на некоторое время (например, постобработка данных, активизация процессов, ожидающих эти данные и т.п.). Если это возможно, лучше объявлять обработчики прерывания "длинными".

Когда CPU получает прерывание, он останавливает любые процессы (если это не более приоритетное прерывание, тогда обработка пришедшего прерывания произойдет только тогда, когда более приоритетное будет завершено), сохраняет некоторые параметры в стеке и вызывает обработчик прерывания. Это означает, что не все действия допустимы внутри обработчика прерывания, потому что система находится в неизвестном состоянии. Решение проблемы: обработчик прерывания определяет - что должно быть сделано немедленно (обычно что-то прочитать из устройства или что-то послать ему), а затем запланировать обработку поступившей информации на более позднее время (это называется "bottomhalves" - "нижние половины") и вернуть управление. Ядро гарантирует вызов "нижней половины" так быстро, насколько это возможно. Когда это произойдет, то наш обработчик - "нижняя половина", уже не будет стеснен какими-то рамками и ему будет доступно все то, что доступно обычным модулям ядра [5].

Устанавливается обработчик прерывания вызовом request_irq. Ей передаются номер IRQ, имя функции-обработчика, флаги, имя для /proc/interrupts и дополнительный параметр для обработчика прерываний. Флаги могут включать SA_SHIRQ, чтобы указать, что прерывание может обслуживаться несколькими обработчиками (обычно, по той простой причине, что на одном IRQ может "сидеть" несколько устройств) и SA_INTERRUPT, чтобы указать, что это "короткое" прерывание. Эта функция установит обработчик только в том случае, если на заданном IRQ еще нет обработчика прерывания, или если существующий обработчик зарегистрировал совместную обработку прерывания флагом SA_SHIRQ.

Во время обработки прерывания, из функции-обработчика прерывания, мы можем получить данные от устройства и затем, с помощью queue_task_irq, tq_immediate и mark_bh(BH_IMMEDIATE), запланировать "нижнюю половину". В ранних версиях Linux имелся массив только из 32 "нижних половин", теперь же, одна из них (а именно BH_IMMEDIATE) используется для обслуживания целого списка "нижних половин" драйверов. Вызов mark_bh(BH_IMMEDIATE) как раз и вставляет "нижнюю половину" драйвера в этот список, планируя таким образом ее исполнение.

/proc/interrupts содержит статистику прерываний: номер прерывания, число прерываний этого типа, полученных каждым процессорным ядром, тип прерывания и список драйверов, обрабатывающих это прерывание. Подробную информацию можно найти на справочной странице man 5 proc.

2.2 Установка обработчика прерываний

Для того, чтобы отслеживать прерывания, простого подключения к аппаратному устройству недостаточно; в системе должен быть настроен программный обработчик. Если ядру Linux не было сказано ожидать прерывания, оно просто получит и проигнорирует его.

Линии прерываний являются ценным и часто ограниченным ресурсом, особенно когда есть только 15 или 16 из них. Ядро ведёт реестр линий прерываний, похожий на реестр портов ввода/вывода. Как ожидается, модуль запрашивает канал прерывания (или IRQ, для запроса прерывания), прежде чем использовать его и освобождает его, когда заканчивает работу. Во многих ситуациях также ожидается, что модули будут способны делить линии прерывания с другими драйверами. Функции, объявленные в <linux/interrupt.h>, реализуют интерфейс регистрации прерывания.

Обработчик прерывания может быть установлен либо при инициализации драйвера, либо при первом открытии устройства. Хотя установка обработчика прерывания в функции инициализации модуля может звучать как хорошая идея, часто это не так, особенно если устройство не разделяет прерывания. Из-за ограниченного числа линий прерывания растрачивать их нецелесообразно. Можно легко выключить больше устройств на компьютере, чем существует прерываний. Если модуль запрашивает прерывание при инициализации, он запрещает любым другим драйверам использовать прерывание, даже если удерживающее его устройство никогда не используется. С другой стороны, запрос прерывания при открытии устройства позволяет некоторое совместное использование ресурсов.

Можно, например, запускать захват кадров на том же прерывании, как и модем до тех пор, пока не используются два устройства одновременно. Весьма распространённая практика для пользователей - загрузить модуль для специального устройства при загрузке системы, даже если устройство используется редко. Приспособление сбора данных может использовать те же прерывания, как второй последовательный порт.

Правильным местом для вызова request_irq является первое открытие устройства перед поручением оборудованию генерировать прерывания. Местом для вызова free_irq является закрытие устройства последний раз, после указания оборудованию больше не прерывать процессор. Недостатком этого метода является то, что нужно сохранять счётчик открытий каждого устройства, чтобы знать, когда прерывания могут быть отключены.

Несмотря на это, short запрашивает свою линию прерывания во время загрузки. Этот нужно для того, чтобы можно было запускать тестовые программы без запуска дополнительных процессов, держащих устройство открытым. short, таким образом, запрашивает прерывание внутри своей функции инициализации (short_init), а не делает это в short_open, как бы сделал реальный драйвер устройства [6].

Прерыванием является short_irq. short_base является базовым адресом ввода/вывода используемого параллельного интерфейса; для разрешения подтверждающих прерываний делается запись в регистр 2.

Устанавливаемый обработчик является быстрым обработчиком (SA_INTERRUPT), не поддерживает совместное использование прерывания (SA_SHIRQ отсутствует) и не способствует энтропии системы (SA_SAMPLE_RANDOM тоже отсутствует). Следующий затем вызов outb разрешает подтверждающие прерывания для параллельного порта.

Для архитектур i386 и x86_64 определена функция для запроса наличия линии прерывания, can_request_irq() с передаваемыми атрибутами прерывания irq и флагов flags. Эта функция возвращает ненулевое значение, если попытка получить данное прерывание успешна. Однако, следует отметить, что между вызовами can_request_irq и request_irq всё может в любой момент измениться [7].

Заключение

Таким образом, в ходе исследования были рассмотрены принципы работы прерываний и их методы обработки и перехвата в операционных системах Windows и Linux. На основе чего, были выбраны оптимальные языки программирования для реализации дальнейшей программы по статистическому анализу времени исполнения прерываний - язык программирования C++ и C, как наиболее подходящие для системного программирования.

СПИСОК ЛИТЕРАТУРЫ

1. Подольская Н.А Прерывания Учебное пособие / Н.А Подольская : Москва 2016 - 50 с
2. Системные прерывания Аппаратное прерывание Обработка прерываний — URL:http://life-prog.ru/view_os.php?id=16

3. Время прерываний - URL:https://docs.microsoft.com/ru-ru/windows/win32/sysinfo/interrupt-time
4. Лав Р., Linux. Системное программирование / Роберт Лав – СПб.: Питер, 2014. – 448 с. – ISBN 978-5-496-00747-4.
5. Interrupt Handling Contexts — URL: https://0x657573.wordpress.com/2010/11/29/the–crisp–boundary–between–hardirq–context–softirq–context–and–user–context/
6. Jonathan Corbet, Linux Device Drivers / Jonathan Corbet, Alessandro Rubini, and Greg Kroah-Hartman – Third Edition – O'Relly, 2005. – 615 p. – ISBN 978-0-59600-590-0.
7. William Shotts., The Linux Command Line / William Shotts – 2nd Edition – San Francisco: no starch press, 2019. – 474 p. – ISBN 978-1-59327-389-7.

В.А. Митрофанов, С.С. Коротков

ПРИМЕНЕНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСАХ

Краснодарское высшее военное училище, г. Краснодар, Россия

Ключевые слова: робототехнический комплекс, средства криптографической защиты информации, командно-программная информация, телеметрическая информация.

В статье представлен обзор основных методов и средств, применяемых для защиты информации, передаваемой по радиоканалам робототехнических комплексов различного назначения.

V.A. Mitrofanov, S.S. Korotkov

THE USE OF CRYPTOGRAPHIC PROTECTION OF INFORMATION IN ROBOTIC COMPLEXES

Krasnodar Higher Military School, Krasnodar, Russia

Keywords: robotic complex, means of cryptographic protection of information, command and program information, telemetry information.

The article presents an overview of the main methods and tools used to protect information transmitted via radio channels of robotic complexes for various purposes.

В настоящие время ведется активное развитие теории и практики построения робототехнических комплексов (РТК) и уже существует множество различных систем, имеющих в своем составе РТК и решающих разные по своей природе задачи: от выполнения наиболее трудоемких процессов в сельскохозяйственной деятельности до работы в условиях, при которых создается опасность для жизни и здоровья человека. На рисунке 1 показана динамика процентного роста объемов разработки РТК в России.

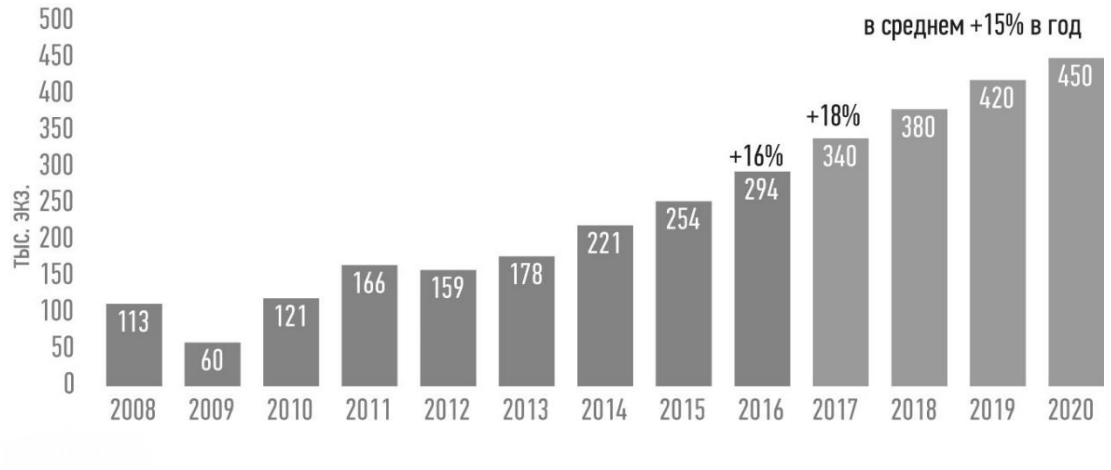


Рисунок 1. Статистика разработки РТК в России

Самым перспективным направлением использования РТК является их применение в условиях терроризма или ведения боевых действий, когда имеется прямая угроза для жизни людей [1].

Для управления РТК необходимо обеспечение устойчивого канала обмена телеметрической и командно-программной информацией. Для обеспечения безопасности передачи указанных видов информации по радиоканалам применяются средства криптографической защиты информации (СКЗИ). Чем важнее задача, выполняемая РТК и чем больший объем информации циркулирует в его информационном контуре, тем выше требования по скорости передачи и, главное, обеспечению безопасности передаваемой информации. Современные РТК способны находиться на большом удалении от оператора, выполнять сбор требуемой информации и передавать ее с требуемым качеством по защищенным каналам связи. В этой связи существует проблема применения СКЗИ для обеспечения безопасности, достоверности и устойчивости передачи больших объемов разнородной по своей физической природе информации.

Под СКЗИ в статье понимаются средства защиты информации, реализующие алгоритмы криптографического преобразования информации [2]. СКЗИ могут применяться к различным видам информации (телеметрическая информация, данные обстановки вокруг РТК, командно-программная информация, фото- и видеосъемка и другие виды информации). При этом для обеспечения необходимого быстродействия внутренних систем для каждого конкретного РТК характерно применение конкретного вида СКЗИ для защиты как потоковой информации, так и информации разделенной на блоки. Большое количество различных способов применения СКЗИ позволяет сделать вывод, что в каждом конкретном случае должна быть решена оптимизационная задача относительно тактико-технических параметров СКЗИ и требуемых качественных характеристик решения задачи обеспечения безопасности и эффективности передаваемой информации.

На данный момент существует единый алгоритм криптографического преобразования информации, который обязателен для применения в организациях, предприятиях и учреждениях применяющих криптографическую защиту данных. По данному стандарту предусмотрено четыре вида работ [3]:

1. Зашифрование (расшифрование) данных в режиме простой замены;
2. Зашифрование (расшифрование) данных в режиме гаммирования;
3. Зашифрование (расшифрование) данных в режиме гаммирования с обратной связью;
4. Режим выработки имитовставки.

Каждый из представленных выше видов работ криптографических средств обработки информации обладает своим набором параметров и характеристик, эффективных в тех или иных ситуациях. Однако некоторые государственные и

коммерческие организации легкомысленно относятся к реализации криптографической защиты информации, тем самым подвергая ее высоким рискам. Как говорилось ранее, перспективным направлением применения РТК является их использование для решения задач государственной важности, в том числе ведения боевых действий [4]. Если злоумышленник сможет перехватить важную информацию РТК, то это может привести к срыву всей операции или даже к человеческим жертвам.

Кроме перехвата информации и использования ее для подмены передаваемых управляющих сигналов, злоумышленником могут быть использованы средства радиоэлектронного воздействия. Для защиты и противодействия данным средствам в РТК должны применяться такие алгоритмы работы, при использовании которых обеспечивается также проверка наличия и исправление искажений, возникающих при передаче информации по каналам связи с непреднамеренными или преднамеренными помехами. Очень успешно для этого применяются современные реализации методов помехоустойчивого кодирования, обеспечивающих целостность передаваемой и хранимой в памяти информации. Особую актуальность приобрели нелинейные коды. Это обусловлено развитием быстродействия современных электронно-вычислительных машин и реализацией принципа параллельных вычислений. Получение искаженных сигналов может восприниматься РТК как отсутствие управляющего сигнала, или получение случайного сигнала из набора предопределенных. Чтобы защититься от получения случайного управляющего сигнала, в РТК применяются системы контроля и подтверждения входящих сигналов, в том числе с применением имитовставок, вырабатываемых СКЗИ.

Таким образом, применение СКЗИ является одной из самых важных задач по защите информации, а выбор конкретного типа СКЗИ, отвечающего предъявляемым требованиям к качественным характеристикам защищенности информации, и тактики его применения является нетривиальной практической задачей, требующей разрешения в оптимальной постановке с позиции теории криптографических преобразований, передачи сигналов, оптимального управления с элементами нечетной логики и искусственного интеллекта. Указанные теоретические аспекты являются предметом дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Кравченко А.Ю. Проблемы и перспективы создания робототехнических комплексов военного назначения / А.Ю. Кравченко, Ю.Е. Стукало // Материалы VIII Всероссийской научно-практической конференции «Перспективные системы и задачи управления», 2013. С. 22-48.
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
3. ГОСТ 34.13-2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
4. Леонов А.В., Тюлькин М.В., Трущенков В.В. Критерии оценки целесообразности и эффективности использования робототехнических комплексов военного назначения // Вооружение и экономика. 2019. № 1 (47). С. 23-29.

А.Н. Иванов, Д.Л. Устименко

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: вирусы, виды вирусов, защита от вирусов.

В этой статье рассмотрены вирусы и также рассмотрены антивирусы которые защищают компьютер или другое устройство.

A.N. Ivanov, D.L. Ustimenko

INFORMATION SECURITY IN THE MODERN WORLD

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

Keywords: viruses, types of viruses, protection against viruses.

This article discusses viruses and also discusses antiviruses that protect a computer or other device.

Считается неоспоримым, что информационные данные являются «одним из самых ценных ресурсов, именно поэтому хранение, защита и обеспечение их целостности – одни из наиболее важных задач в современной ИТ-индустрии»[2]

В современном мире немаловажно иметь знания о мерах безопасности, применяемых для вычислительных устройств и компьютерных сетей. Так как в данное время мы живем в компьютерном, информационном мире. Большинство людей имеют несколько электронно-вычислительных машин (компьютеры, планшеты, телефоны и т. д.). И множество из этих устройств имеют подключение к компьютерной сети (системы связи компьютеров или вычислительного оборудования, включая Интернет), что и заставляет нас в большей мере задуматься о безопасности каждого, имеющего данный доступ. Тем более, что интернет путь новому направлению преступности – «компьютерным преступлениям, которые в настоящее время являются актуальной проблемой и решение которых должно быть комплексным и всесторонним. Преступления данной направленности в своем разнообразии многогранны: интернет-мошенничество, DDoS-атаки, создание вредоносного программного обеспечения, нарушение авторских прав и многое другое» [3]. Что и кто угрожает нашей безопасности в компьютерном мире.

Всегда были, и будут существовать злоумышленники, которые будут взламывать и совершать кражи. В компьютерной сфере можно завладеть незаконным путем информациями, которые имеются на вычислительных устройствах, а также в компьютерных сетях. Кроме информации также можно портить различные устройства и установки. Основной угрозой компьютерной безопасности являются вредоносные программные обеспечения, написанные человеком. Такие программы называются компьютерными вирусами, попадающие в устройство несанкционированно обманным путем или по неосторожности пользователя.

Вирусы способны самостоятельно размножаться (создавать копии) и распространяться по всему устройству, а также передавать свои копии по разным каналам связи. Большая угроза существует при соединении вычислительных устройств к сети или же к внешним носителям. Рассмотрим известное вредоносное программное обеспечение под названием Stuxnet. Stuxnet – это чрезвычайно высокотехнологичное вредоносное

программное обеспечение во всех его проявлениях, поражающий компьютеры. Данный червь внедряется в электронно-вычислительные машины при помощи USB-flash накопителей. Он считается самым разрушительным, открывшим эру кибернетического оружия. Это был первый боевой вирус, который действуя в рамках виртуального пространства нанес физический урон крупной инфраструктуре. В ходе анализа кода, попавшего в руки специалистов, постепенно раскрывались суть и предназначение Stuxnet. Он распространялся не через Интернет, а через обычные флешки. Это дало ему возможность заражать сети, отключенные от Интернета. Попадая внутрь защищенных сетей, он находил системы, управляющие технологическими процессами на производстве, заражал их, но атаковал лишь устройства, отвечающие за одну операцию: контроль скорости вращения некой установки. Попав в компьютеры, управляющие центрифугами для обогащения урана, Stuxnet заставлял их раскручиваться до запредельных скоростей. В результате центрифуги взрывались, в то время как на компьютерах операторов все было нормально. Секретный завод, который был неуязвим даже для прямого ядерного удара всего за один день потерял более тысячи центрифуг для обогащения урана. Это привело к серьезному радиационному заражению подземных цехов завода и срыву Иранской ядерной программы. Когда начали искать способ передачи данного червя, то обнаружилось, что это оборудование – специфическое, поставленное в Иран, используется оно для обогащения урана. Таким образом, можно сказать, что Stuxnet был создан для того, чтобы саботировать ядерную программу Ирана.

Шеф военной разведки Израиля генерал Амос Ядлин считает, что сегодня киберпространство представляет собой пятое измерение ведения войны — наряду с сушей, морем, воздухом и космическим пространством. Война в киберизмерении имеет такое же большое значение, как и война в воздухе в XX веке. Киберпространство играет все более важную роль в международных конфликтах. Это новое поле боя, но боя не на традиционном оружии, а основанного на совершенно новых принципах. Компьютерные вирусы – они, подобно тонкой, изящной рапире, поражают противника внезапно в самую неожиданную точку, казалось бы, защищённую идеально.

Защищает от подобных вторжений антивирусные программы. «Антивирусная программа использует различные методы обнаружения. Поскольку характеристики вирусов различны, отличаются и методы их обнаружения. Все типы атак не могут быть выявлены каким-либо одним методом. Популярные методы, используемые антивирусными программами для их обнаружения, заключаются в следующем:

- сканирование сигнатур;
- проверка целостности;
- эвристическое сканирование;
- эмуляция;
- мониторинг активности» [1].

Как же бороться с такими угрозами, как вредоносные программные обеспечения? Идеально защититься от данной проблемы невозможно. Но можно снизить риск заражения и повысить уровень безопасности. Для этого нам могут помочь антивирусные программные обеспечения, которых в данное время немало и их выбор велик. Такие как: Антивирус Касперского, AVAST, Dr.Web, NOD32 и т. п. Также есть отличная возможность, сначала испробовать пробную версию, а потом установить уже лицензионную версию программы на свой вкус, желание, т. к. у каждого антивируса есть множество видов.

Данный вид защиты помогает: обнаружить и защитить ПК от всех типов вирусов, включая макро-вирусы, вирусы загрузочных секторов, вирусы резидента памяти и троянских коней, червей и других вредоносных вирусов.

Кроме антивирусных программных обеспечений мы можем защитить компьютеры и электронно-вычислительные машины, а вернее снизить их заражение вирусами следующими способами: общими средствами защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или

ошибочных действий пользователей; профилактическими мерами, позволяющие уменьшить вероятность заражения вирусом; специализированными программами для защиты от вирусов. Общие средства защиты информации полезны не только для защиты от вирусов.

Имеются две основные разновидности этих методов защиты: 1. резервное копирование информации, т. е. создание копий файлов и системных областей дисков на дополнительном носителе; 2. разграничение доступа, предотвращающее несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Шифровальщики и инструменты шантажа – еще две стратегии атаки на системы. В течение всего 2020 года росло число атак шифровальщиков – вредоносного ПО, которое шифрует данные, блокирует работу и нередко требует выкуп. С первый по третий квартал количество такого рода атак удвоилось. Причем в качестве цели их создатели выбирают как правило не абстрактное множество пользователей, а конкретных представителей крупных компаний, которые могут заплатить большой выкуп и для которых жизненно важно продолжать работать.

Также популярность приобрел шантаж украденными приватными данными. Примеры ПО для шантажа: Maze, Sodinokibi, DoppelPaymer, NetWalker, Ako, Nefilim, Clop. Это превратилось в полноценную индустрию: злоумышленники даже создали собственные сайты и аукционы для продажи похищенной информации.

Еще одна вариация такой активности – злоумышленники похищают компрометирующие данные активности в интернет-магазине (например, о покупках в секс-шопе) и предлагают заплатить, чтобы информацию не продали третьим лицам. По некоторым прогнозам, вымогатели смогут добраться даже до облачных репозиториев.

Возникают новые киберкартели. Как следствие, скоро появится множество новых хакерских объединений и площадок в теневом интернете. Мотивация проста – совместно атаковать привлекательную цель и заработать на этом хорошие деньги. Их, как и прежде, будут требовать за восстановление работоспособности системы и сохранность украденной информации. Угроза публикацией чувствительных данных по-прежнему в почете у злоумышленников.

Поставщики и промышленный сектор как излюбленная цель хакеров. Сегодня в зоне особого внимания хакеров поставщики услуг и сервисов. В 2020 году было совершено около 200 атак на энергетические и промышленные компании, когда как годом ранее их было 125. Также есть растущий тренд атак на поставщиков. Так как крупные компании становятся все более сложной целью, в зоне риска разработчики ПО и средств защиты, ИТ-интеграторы, подрядчики ИТ-компаний.

Для защиты от хорошо спланированной атаки нужны высококлассные ИБ-специалисты, а их могут себе позволить далеко не все эти компании. И это повышает вероятность успеха для хакеров. Остановка производства – желанная цель для злоумышленников, ведь в таком случае жертва сильно мотивирована заплатить деньги. По этой причине выросли и суммы выкупов. В июне компании Honda и Enel Group стали жертвой нового шифровальщика Snake, созданного специально для остановки важных процессов в промышленных системах управления.

Один из вариантов избежать этого – потратить время и ресурсы на детальное исследование всей цепочки поставок вендора, чтобы понимать последствия в случае взлома.

Логические уязвимости в банковских приложениях. Крупные банки хорошо поработали над безопасностью своих приложений: повысили отказоустойчивость, перейдя на микросервисную архитектуру и уменьшили количество стандартных веб-уязвимостей (XSS, SQLi, RCE).

Однако выросло количество логических уязвимостей, которые в конечном итоге могут привести к краже денег, получению хакерами чувствительной информации и, как итог, отказу в обслуживании со стороны банка. Цель хакеров на сегодняшний день – даже не полная компрометация системы банковских приложений, а эксплуатация логических уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. Земляная Д.А., Болдырихин Н.В., Шипшова Е.М. Анализ методов обнаружения вирусных сигнатур // Информационная Безопасность. Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2020)» стр.336-342
2. Гадасин Д.В., Кольцова А.В., Полякова А.Н. Модель построения кластера для пограничных вычислений // Состояние и перспективы развитие инфокоммуникаций. Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2020)» стр.98-104
3. Файсханов И.Ф., Комарова А.Н. Анализ и обзор преступлений, совершенных с использованием информационных технологий // Информационная Безопасность. Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2020)» стр. 322-328

Е.А. Щерба, Д.Л. Устименко

ЗНАЧИМОСТЬ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: кибербезопасность, защита, данные, значение кибербезопасности, кибератаки, сеть, злоумышленники.

В статье рассмотрена значимость кибербезопасности в наши дни, представлены главные кибератаки десятилетий, возможные пути решения проблемы риска возникновения киберпреступлений.

E.A. Shcherba D.L. Ustimenko

THE IMPORTANCE OF CYBER SECURITY IN THE MODERN WORLD

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

Keywords: cybersecurity, protection, data, value of cybersecurity, cyber attacks, network, attackers.

The article discusses the importance of cybersecurity today, presents the main cyber attacks of decades, possible ways to solve the problem of the risk of cybercrime.

Введение.

Цифровые технологии плотно вошли в нашу жизнь. Современную реальность невозможно представить без компьютеров. Каждый человек более или менее часто, но

сталкивается с компьютерными технологиями. Роботы, криптовалюты, беспилотные устройства, автоматизированные системы, медицинское цифровое оборудование. Новые технологии улучшают нашу жизнь, но вместе с ними появляются и новые угрозы.

Киберпреступления создают множество проблем на разных уровнях. От личных до глобальных государственных киберугроз. Главным оружием скоро могут стать не ракеты и танки, а компьютер, при помощи которого можно будет перенаправлять транспортную систему, отключать электричество.

Кибербезопасность в современном мире.

Киберпреступления затрагивают различные сферы жизни. Они могут быть социальные, связанные с вторжением в личную жизнь (шпионаж, отслеживание, подбор паролей, кража персональной и личной информации с различными целями). Финансовоориентированные преступления – атаки с целью получения коммерческий выгоды. Ещё один тип преступлений в сети - политические - попытки влиять на настроения населения, а также могут иметь экстремистские и террористские задачи.

«В 2016 г. также получила широкую известность волна атак, когда компания «CrowdStrike» сообщила, что идентифицировала двух отдельных противников, связанных с российской разведкой, присутствующих в сети Демократического национального комитета США (DNC). Согласно отчету, компания обнаружила доказательства того, что в сети DNC были две русские хакерские группы: Cozy Bear (также классифицированная как APT29) и Fancy Bear (APT28). Cozy Bear не был новым субъектом в этом типе атаки, т. к. доказательства показали, что в 2015 г. они стояли за атакой на систему электронной почты Пентагона посредством фишинговых атак. Этот тип сценария называется кибератаками, спонсируемыми правительством, но некоторые специалисты предпочитают изъясняться более общими терминами и называют их данными, используемыми в качестве оружия, поскольку их цель состоит в том, чтобы украсть информацию, которая может быть использована против скомпрометированной стороны» [1, с. 25].

Кибератаки в наше время.

В начале декабря 2019 года Москва и Санкт-Петербург пережили очередную атаку «телефонных террористов». Практически ежедневно «минировались» торговые центры, школы, аэропорты. Однако под самый мощный «шквал» попали суды: их эвакуировали во многих районах и не по одному разу.

За 2017 – девять месяцев 2019 года прирост преступлений в сфере информационных технологий составил 165 %. В 2017 году их было совершено 66 тысяч, в 2018 – 175 тысяч, за девять месяцев 2019 года – более 200 тысяч. Около 50 % данных деяний – различные виды мошенничества. В 2019 году их количество увеличилось на 40 %. Более половины подобных преступлений совершается с помощью интернета, более трети – средств мобильной связи, каждое десятое – с использованием банковских карт.

Как же совершаются киберпреспупления. Начиналось все с безобидного хулиганства – простых вирусов, которые тешили самолюбие создателей. Сегодня вирусы создаются командами высококлассных специалистов и имеют глобальные цели.

Вредоносное ПО – действуют по принципу вируса биологического – внедряются в организм компьютера и изменяют код установленных на нем программ. Вредоносные программы могут снижать функциональность аппаратных и программных структур вычислительных устройств: удалять файлы, повреждать данные, блокировать работу пользователя. Воздействие инфекций может быть не только разрушительным, но и раздражающим, так как они тормозят работу операционной системы, ведут к сбоям и внезапным перезагрузкам, сокращают свободный объем памяти. Они способны распространять свои копии по различным каналам связи на другие цифровые устройства.

Видов вредоносного ПО много. «Вирусы - самораспаковывающийся программный код – заражает файлы, обычно направлены на причинение вреда операционной системе»

[3]. Червь – саморазмножающаяся программа, просто кочует с одного компьютера на другой, ему не требуется участие пользователя. Он поселяется в системе, ищет уязвимости и выполняет команды хакеров. Трояны устанавливаются самим пользователем под видом законной программы и делают то, что хочет злоумышленник (шантаж, шпионаж и т.п.). Программы-блокеры, шифрующих файлы пользователя и требующих деньги за восстановление данных. SMS-блокеры, блокирующие вход в операционную систему. Причем в последнее время все чаще прикрывающиеся «законными» способами – штрафами за нарушения пользователем различных правил.

Важность угроз.

«На сегодняшний день практически у каждого человека есть мобильное устройство для осуществления связи или взаимодействия через социальные сети, а также другие различные средства. С одной стороны гаджеты позволяют легко общаться друг с другом, находить новые знакомства, но с другой стороны их повсеместность создает для государственных и негосударственных субъектов ряд неотъемлемых уязвимостей и возможные векторы атак. Применение таких уязвимостей обычно приводит к глобальным проблемам для национальной безопасности путем намеренных действий таких, как шпионаж, неэффективное командование и управление объектами, кража интеллектуальной собственности и информации личного характера, нарушение предоставления услуг и работы очень важной инфраструктуры или нанесение ущербов экономике и промышленности» [4, с. 1].

Избежание кибератак.

Взломы случаются благодаря ошибкам и уязвимостям в программном обеспечении, но значительно чаще они случаются по причине неправильных и безответственных действий людей, пользующихся этими программами. Очень часто на помощь хакеру приходит сам пользователь ПК. Социальная инженерия – это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств, основанный на использовании слабостей человеческого фактора и является очень эффективным. Попросту – обман, сбор информации из открытых источников и социальных сетей, ложные письма, представление работником компании незаслуженное доверие.

«Настоящая проблема состоит в том, что обычно взломы связаны с человеческими ошибками. Все может начинаться с фишингового сообщения по электронной почте, использующего социальную инженерию, чтобы заставить сотрудника щелкнуть ссылку, которая может загрузить вирус, вредоносное ПО или троян» [1, с. 24]. Фишинг (рыбалка) – форма мошенничества, при которой рассылаются мошеннические электронные письма, похожие на электронные письма из надежных источников. Однако целью этих писем является кража конфиденциальных данных, например, с кредитной карты или логин и пароль для входа в систему. Интернет-попрашайничество от имени благотворительных фондов, родителей тяжелобольных детей и т.п. Особенно получило распространение с развитием социальных сетей. Вообще, социальная инженерия – это очень мощный инструмент, при правильном умении вести разговор (вспомните разведчика Штирлица) собеседник сам расскажет вам обо всем, что нужно [2, с. 23].

Чтобы значительно уменьшить риски кибератак обычным пользователям необходимо выполнять ряд несложных правил:

1. Вовремя обновлять программное обеспечение и операционную систему.
2. Использовать антивирусное программное обеспечение.
3. Использовать надежные пароли, которые нелегко угадать.
4. Не открывать вложения электронной почты от неизвестных отправителей, возможно заражённые вредоносным ПО.
5. Не переходить по ссылкам в электронных письмах от неизвестных отправителей или с незнакомых веб-сайтов.

6. Избегать использования незащищенных сетей Wi-Fi в общественных местах.

Следующий этап эволюции киберопасностей – DDoS-атаки. Они используются для одновременного направления на требуемый сайт огромного количества запросов из различных источников, в результате перегрузки сайт может быть выведен из строя (недоступен для реальных пользователей Интернета). Для этого создаются большие сети (известные как ботнеты) из устройств пользователей, зараженных вредоносными программами. DDoS-атаки всё активнее используют как инструмент конкурентных войн. Эксперты «Лаборатории Касперского» провели исследование и выяснили, что в 2015 году DDoS-атаке подверглась каждая шестая российская компания.

Заключение.

Безопасность в сети – это постоянно изменяющая и совершенствующаяся система. По мере появления новых технологий и их использования по-новому, появляются и новые способы атак. Кибербезопасность сегодня – это комплексный подход и многоступенчатая защита организаций и государственных служб. «Все больше развитых стран стремятся защититься путем создания особых подразделений, действующих в составе спецслужб, внедрения системы сертификаций программного обеспечения и устройств, разработка инструкций и политик безопасности. 12 декабря 2019 года был подписан Кодекс этики использования данных» [6], подготовленный Институтом развития интернета и Ассоциацией больших данных.

СПИСОК ЛИТЕРАТУРЫ

1. Д. А. Беликова Кибербезопасность: стратегии атак и обороны / пер. с анг. – М.: ДМК Пресс, 2020. – 326 с.
2. Бирюков А. А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012. - 474 с.
3. Лаборатория Касперского. Блокеры всех времен и народов. // [Электронный ресурс] URL: http://habrahabr.ru/company/ kaspersky/blog/
4. Азимкова К. А. Важность обеспечения кибербезопасности // Инновационная наука (журнал), 2021 г. № 7 с. 29-31.
5. Пешева П. А., Смирнов В. М. Кибербезопасность в сети // журнал Student. Том 4 № 7. М., Московский университет МВД, 2021 г. – 109 с.
6. Кодекс этики использования данных. [электронный ресурс] // URL: https://ac.gov.ru/files/content/25949/kodeks-etiki-pdf.pdf

С.М. Бейбутян, С.А. Швидченко

АНАЛИЗ И ПОИСК РЕШЕНИЯ ЗАДАЧИ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ ОТ ВЗЛОМОВ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: телефон, мобильное устройство, мошенники, хакеры, программное обеспечение, взлом.

В статье проведен анализ проблемы взлома смартфонов, рассматриваются различные виды хакерского программного обеспечения и способы, посредством которых

хакер может проникнуть в телефон и украсть личную и важную информацию. Рассмотрен Пример восстановления работы смартфона посредством сброса пароля.

S.M. Beybutyan, S.A. Shvidchenko

ANALYSIS AND SEARCH FOR SOLUTIONS TO THE PROBLEM OF PROTECTING MOBILE DEVICES FROM HACKING

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

Keywords: phone, mobile device, scammers, hackers, software, hacking.

The article analyzes the problem of smartphone hacking, discusses various types of hacking software and ways by which a hacker can get into a phone and steal personal and important information. An example of restoring the operation of a smartphone by resetting a password is considered.

Введение

Угроза взлома телефона стала обычным и рациональным страхом. Теперь взломать можно любой телефон. С развитием технологий, когда открытие знаний и информации способствует пониманию технологий, хакеры могут взламывать даже самое сложное программное обеспечение для телефонов [1,2].

Анализ программного обеспечения для взлома

Существует программа для взлома Android и других мобильных устройств. В интернете есть бесчисленное множество бесплатных программ для взлома. Программное обеспечение для взлома - это метод, используемый хакерами для получения информации с телефона.

Серьезные хакеры могут купить хакерское программное обеспечение где угодно, например, телефонное шпионское приложение, которое должно быть установлено на целевом телефоне. Не всем хакерам необходимо физически обращаться с телефоном, чтобы установить программу для взлома, но в некоторых случаях это необходимо.

1. Кейлоггинг - это подход, который включает загрузку шпионского приложения для нацеливания на телефон и получения данных с телефона перед шифрованием. Этот тип программного обеспечения можно использовать, получив физический доступ к телефону.

2. Троян - это тип вредоносного ПО, которое может быть замаскировано в телефоне для извлечения важных данных, таких как данные учетной записи кредитной карты или личная информация. Чтобы установить вредоносные троянские программы, хакеры используют такие методы, как фишинг, чтобы загнать в ловушку.

3. Фишинг - это метод, используемый хакерами, когда они выдают себя за компанию или доверенного лица для получения конфиденциальных данных. Хакеры используют этот метод, отправляя коды, изображения и сообщения официального вида, которые чаще всего встречаются в электронной почте и текстовых сообщениях. При нажатии на этот вредоносный контент URL-адреса могут взломать телефон, потому что ссылка была заражена хакерским вирусом или программным обеспечением, которое может забрать вашу личную информацию.

4. Взлом по номеру телефона.

Чтобы иметь возможность взломать, используя только номер телефона, вы должны знать и понимать технические аспекты взлома телефона. Сигнализация SS7 - это система, используемая для соединения сетей сотовых телефонов друг с другом, но для того, чтобы использовать эту систему в качестве метода взлома телефонов, необходимо иметь к ней доступ. Запись звонков, переадресация звонков, чтение сообщений и поиск

местоположения определенного устройства могут быть выполнены с доступом к системе SS7. Хотя из-за уровня сложности маловероятно, что обычный человек сможет взломать телефон таким образом.

5. Взлом SIM-карты.

В августе 2019 года у генерального директора Twitter была взломана его SIM-карта путем подмены SIM-карты методом фишинга. Замена SIM-карты выполняется, когда хакер связывается с оператором связи, притворяется вами, а затем просит заменить SIM-карту. Как только провайдер отправит хакеру новую SIM-карту, старая SIM-карта будет деактивирована, а номер телефона украден. Это означает, что хакер перехватил телефонные звонки, сообщения и т. д. Этот метод взлома относительно прост, если хакер может убедить провайдера в том, что это вы. Хранение личных данных при себе - важная часть гарантии того, что хакеры не смогут притвориться вами.

6. Adaptive Mobile Security обнаружила новый способ проникновения хакеров в телефоны с помощью SIM-карты - метод, который они называют Simjacker. Этот способ взлома более сложен, чем фишинг, поскольку он нацелен на SIM-карту, отправляя сигнал на целевое устройство. Если открыть сообщение и щелкнуть по нему, хакеры могут шпионить за взломанным устройством и даже узнать его местонахождение.

7. Взлом Bluetooth.

Профессиональные хакеры могут использовать специальные программные продукты для поиска уязвимых мобильных устройств с работающим Bluetooth-соединением. Эти типы взломов выполняются, когда хакер находится в зоне досягаемости телефона, обычно в густонаселенном районе. Когда хакеры подключены к Bluetooth, у них есть доступ ко всей доступной информации и подключение к Интернету для доступа в Интернет, но данные должны быть загружены, пока телефон находится в пределах досягаемости.

Есть много разных способов, которыми хакер может проникнуть в телефон и украсть личную и важную информацию. Чтобы не допустить этого, необходимо следовать основным рекомендациям:

1. Необходимо добавить дополнительную защиту с помощью лица, пальца, рисунка или PIN-кода.

Во-первых, основы. Блокировка телефона с помощью идентификатора лица, отпечатка пальца, рисунка или булавки - основная форма защиты, особенно в случае потери или кражи. Возможные варианты зависят от устройства, операционной системы и производителя. Необходимо защищать учетные записи на телефоне надежными паролями и использовать двухфакторную аутентификацию в приложениях, которые ее предлагают, что удвоит линию защиты.

2. Необходимо использовать VPN.

Нельзя подключиться к общедоступным сетям Wi-Fi без защиты. VPN маскирует соединение от хакеров, позволяя подключаться конфиденциально, когда вы находитесь в незащищенных общедоступных сетях в аэропортах, кафе, отелях и т.д. Благодаря VPN-подключению пользователь будет знать, что его конфиденциальные данные, документы и действия, которые он делает, защищены от слежки, что очень важно, учитывая объем личного и профессионального бизнеса, которым пользователи управляют с помощью своих смартфонов.

3. Необходимо приобрести приложения в официальных магазинах приложений.

И в Google Play, и в Apple App Store приняты меры по предотвращению попадания потенциально опасных приложений в их магазины. Вредоносные приложения часто находятся за пределами магазинов приложений, которые могут работать в фоновом режиме и ставить под угрозу личные данные, такие как пароли, номера кредитных карт и т. д. - практически все, что храниться на телефоне. Кроме того, когда вы находитесь в магазинах приложений, нужно внимательно изучать описания и обзоры приложений, прежде чем загружать их. Вредоносные приложения и подделки по-прежнему могут попадать в

магазины, и вот несколько способов предотвратить попадание этих вредоносных приложений на телефон:

4. Необходимо сделать резервную копию данных на телефоне.

Резервное копирование телефона всегда полезно по двум причинам:

Во-первых, он упрощает процесс перехода на новый телефон за счет переноса данных из резервной копии со старого телефона на новый.

Во-вторых, он гарантирует, что данные останутся с вами, если телефон потерян или украден, что позволяет удаленно стереть данные на потерянном или украденном телефоне, сохраняя при этом защищенную копию этих данных, хранящуюся в облаке.

И iPhone, и телефоны Android имеют простые способы регулярного резервного копирования данных с телефона.

5. Необходимо узнать, как удаленно заблокировать или стереть данные с телефона в экстренных случаях.

В худшем случае - телефона нет. На самом деле либо безнадежно потеряно, либо украдено. Нужно заблокировать его удаленно или даже полностью удалить все данные. Хотя последнее о стирании данных с телефона кажется радикальным шагом, если будете регулярно выполнять резервное копирование, как упомянуто выше, данные будут в безопасности в облаке и готовы к восстановлению. В целом это означает, что хакеры не смогут получить доступ к конфиденциальной информации, что может уберечь от неприятностей и защитить профессиональный бизнес. Apple предоставляет пользователям iOS пошаговое руководство по удаленной очистке данных с устройств, а Google также предлагает руководство для пользователей Android.

6. Необходимо избавляться от старых приложений и обновлять те, которые остались.

Многие пользователи загружают приложения, используют их один раз, а потом забывают, что они есть в телефоне. Нужно потратить несколько минут, чтобы провести по экрану и посмотреть, с какими из них действительно закончили и удалить их вместе с данными. С некоторыми приложениями связана учетная запись, которая также может хранить данные с телефона. Необходимо сделать дополнительный шаг и удалить эти учетные записи, чтобы все данные вне телефона были удалены [3,4].

Причина этого в том, что каждое дополнительное приложение - это другое приложение, которое требует обновления или с которым может быть связана проблема безопасности [1]. Во время утечки данных и уязвимостей удаление старых приложений - разумный шаг. Что касается тех, которые пользователь сохраняет, их необходимо обновлять регулярно и включать автоматические обновления, если это возможно. Обновления не только вводят новые функции в приложения, но также часто решают проблемы безопасности.

7. Необходимо защищать телефон.

Установка программного обеспечения безопасности может защитить телефон и хранилище телефона. Независимо от того, является ли пользователь владельцем Android или iOS, программа для обеспечения безопасности мобильных устройств обеспечит безопасность данных, покупок и платежей.

Обращение к пониманию того, как работает взлом, может помочь практиковать безопасность в повседневной жизни [2]. Необходимо знать, как подготовиться к взлому, чтобы, когда это произойдет, вы знали, как с этим справиться.

Пример восстановления работы смартфона посредством сброса пароля

Для восстановления работоспособности или получения доступа к функционалу мобильного устройства производители предусмотрели функцию жесткого сброса настроек и возврата к заводским параметрам. Если пароль был благополучно забыт, а хранящаяся в телефоне информация никакой ценности не представляет, можно смело использовать данный вариант. Чтобы сбросить пароль через Recovery (функция), понадобится проделать следующие манипуляции:

Во-первых, необходимо выключить смартфон, как показано на рисунке 1.

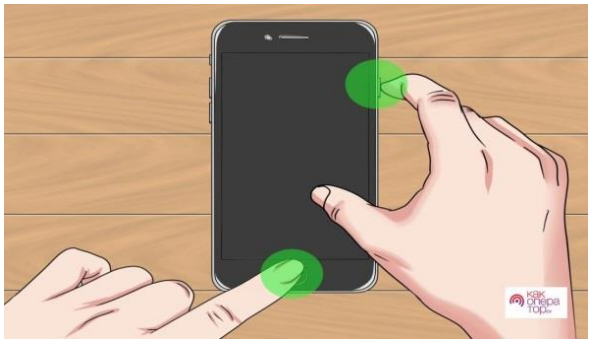


Рисунок 1. Выключение смартфона

После того, как потухнет экран, необходимо одновременно зажать и удерживать две кнопки: питания и регулятора громкости (неважно вниз или вверх).

Когда появится меню загрузчика «Bootloader», необходимо выбрать режим «Recovery mode», как показано на рисунке 2.

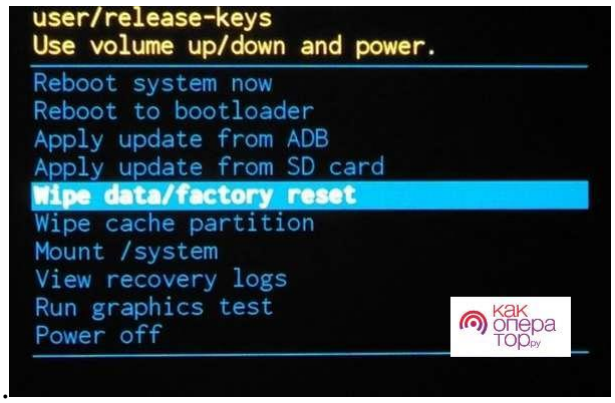


Рисунок 2. Выключение смартфона

В списке доступных операций необходимо выбрать функцию «wipe data/factory reset», как показано на рисунке 3.

Рисунок 3. Выключение смартфона

Попав на следующий экран, необходимо отыскать команду «Yes delete all user data» и запустить удаление действующих параметров системы, как показано на рисунке 4.

Рисунок 4. Выключение смартфона

Для завершения процесса необходимо активировать опцию перезагрузки, кликнув по строке «reboot system now».

В результате этих действий смартфон выполнит резервное восстановление системы и сбросит все настройки до заводских параметров. Пользователь же получит устройство в том виде, в каком он приобрел его в магазине.

Заключение

Можно взломать телефон по номеру, через СМС или установив программу для взлома, эти действия могут сделать обычные пользователи, есть различные программы для взлома телефона, они предоставят в конечном итоге разную информацию. Поэтому, необходимо помнить, что повсеместное использование информационных технологий с соответствующим программным обеспечением дает большие возможности, но при этом необходимо обеспечивать безопасность этих систем обработки данных [1,2,3].

СПИСОК ЛИТЕРАТУРЫ

1. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство проектирования однозоновой сети транкинговой связи для ее оперативного развертывания. Свидетельство о регистрации программы для ЭВМ 2021610521, 14.01.2021. Заявка № 2020665716 от 03.12.2020.
2. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.
3. *Безуглов Д.А.,* Швидченко С.А. Синтез общей модели обеспечения безопасности для неоднородной системы обработки данных. В сборнике: Системный анализ, управление и обработка информации. труды X Международной научной конференции. 2020. С. 109-114.
4. *Швидченко С.А.* Анализ обеспечения безопасности информации в АСУ. - В сборнике: Актуальные аспекты развития воздушного транспорта (Авиатранс-2018). Материалы международной научно-практической конференции. 2018. С. 257-262.

М.М. Фролова, С.А. Швидченко

АНАЛИЗ ТИПОВ УЯЗВИМОСТЕЙ ВЕБ-САЙТОВ И СПОСОБЫ ИХ ЗАЩИТЫ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: уязвимости веб-сайтов, внедрение кода, вредоносный код, методы защиты веб-сайтов.

В статье рассмотрены основные типы уязвимостей веб-сайтов и методы борьбы с ними.

M.M. Frolova, S.A. Shvidchenko

ANALYSIS OF TYPES OF VULNERABILITIES OF WEBSITES AND WAYS TO PROTECT THEM

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

Keywords: vulnerabilities of websites, code injection, harmful code, methods of protecting websites.

The article discusses the main types of vulnerabilities of websites and methods of dealing with them.

Введение

В XXI веке человека повсюду окружает информация. В настоящее время почти все аспекты нашей жизни оцифрованы: банковские системы, медицина, образование, промышленность, индивидуальное предпринимательство, государственные организации, сферы услуг и т.д. С каждым годом вырастает количество пользователей Интернета, а следовательно проблема информационной безопасности становится все более актуальной. Любая информация, попавшая в Интернет подвержена утечке или взлому. По статистике, кибератакам подвергается каждая третья мелкая компания и каждая шестая крупная. Но меньше половины организаций стремятся обезопасить информацию на своих сайтах, и лишь немногие регулярно занимаются обновлением системы безопасности. В результате это приводит к серьезным материальным потерям [1]. Также мы регулярно слышим, что веб-сайты общего пользования, такие как социальные сети, куда мы добровольно отдаем часть информации о себе, сайты банков и т.д. становятся недоступными из-за совершенных на них атак. В более серьезных случаях утекает конфиденциальная информация их пользователей: миллионы паролей, адреса электронных почт, данные кредитных карт – всё это подвергает людей очень серьезным рискам. По этой причине каждый пользователь, а тем более разработчик, должен быть грамотным в вопросе безопасности веб-сайтов. Чтобы сохранить свою конфиденциальность и безопасность в Интернете, важно знать о различных типах интернет-атак [2, 3, 4].

Цель работы: исследование методов взлома и защиты веб-сайтов [5].

Задача работы: разобраться в структуре HTTP-запросов и их методов, рассмотреть следующие типы уязвимостей – Open Redirect, засорение HTTP-параметров, межсайтовая подделка запросов, внедрение SQL, межсайтовый скриптинг [1].

Что происходит, когда пользователь заходит на веб-сайт

1 этап. Браузер вычленяет из URL-адреса доменное имя. Например:

У URL-адреса http://www.skf-mtusi.ru/ доменное имя будет www.skf-mtusi.ru

2 этап. Используя DNS(domain name system – система доменных имен), браузер получает IP-адрес сайта. IP адреса существуют двух версий – IPv4 и IPv6.

IPv4 состоит из 4 чисел в диапазоне от 0 до 255, разделенных точкой.

IPv6 – состоит из 8 шестнадцатеричных цифр, разделенных двоеточиями. Эта версия была разработана из-за нехватки IPv4.

В данном примере сайту www.skf-mtusi.ru соответствует IP-адрес 5.181.108.69.

3 этап. Дальше используется TCP(transmission control protocol – протокол управления передачей). Говоря простыми словами, этот прокол обеспечивает двунаправленное взаимодействие компьютеров(сервера и клиента).

4 этап. После установки соединения браузер отправляет сайту HTTP-запрос следующего вида:

```
GET http://www.skf-mtusi.ru/sveden/common HTTP/ 1.1
HOST: www.skf-mtusi.com
Connection: keep-alive
User-Agent: Chrome/72.0.3626.109
Accept: application/html, */*
```

1) в первой строке указывается тип запроса, URL-адрес и версия HTTP-запроса;

2) Connection: keep-alive – оставляет соединение с сервером открытым, чтобы не приходилось его устанавливать в следующий раз;

3) заголовок Accept означает формат ожидаемого ответа;

4) User-Agent передает серверу информацию о браузере, который отправил запрос.

5 этап. Сервер отправляет ответ в виде:

```
HTTP/1.1 200 OK
Content-Type: text/html
<html>
    <head>
        <title>Основные сведения : Северо-Кавказский филиал МТУСИ</title>
    </head>
    <body>
        ...
    </body>
</html>
```

В первой строке указан код состояния – 200. Коды вида 2** обозначают, что запрос прошел удачно. Также существуют и другие коды:

- 1** - коды, информирующие о процессе передачи;
- 3** - перенаправляющие коды;
- 4** - коды, сигнализирующие о пользовательской ошибке;
- 5** - коды, сигнализирующие об ошибке со стороны сервера.

6 этап. На последнем этапе браузер отображает ответ в виде сайта, который он получил от сервера.

Методы HTTP-запросов

- GET – получает информацию от сервера и не способен ее изменять;
- POST – используется для редактирования данных на сервере, с помощью этого метода можно зарегистрировать нового пользователя на сайте, добавить комментарий к статье или написать новую;
- PUT – обращается к уже существующим записям на сервере и изменяет их;
- TRACE – возвращает запрос тому, кто его отправил, может использоваться для тестирования сайта;

- OPTIONS – определяет возможности сервера(узнает, принимает ли сервер GET, POST, PUT, DELETE и OPTIONS вызовы);
- DELETE – запрашивает удаление ресурса идентификатором URI(uniform resource identifier; по сути URL это вариация URI);
- CONNECT – работает с прокси-сервером, который перенаправляет запросы другим серверам [6].

Уязвимость Open Redirect

Уязвимость Open Redirect позволяет сайту перенаправлять пользователя на другие URL-адреса, возможно, даже на другом домене. Это позволяет перенаправить пользователя на вредоносные или фишинговые сайты. Многие разработчики игнорируют эту уязвимость и не выплачивают награду за ее обнаружение, т.к. она не наносит прямой ущерб сайту.

Эта уязвимость возникает, если разработчик разрешает перенаправлять браузер к другим сайтам [4]. Обычно для этого используются параметры URL-адреса. Если предположить, что веб-сайт www.site.com может перенаправить на другой с помощью параметра redirect, тогда HTTP-запрос будет выглядеть следующим образом: http://www.site.com/?redirect=http://www.site2.com.

При переходе по ссылке сервер получит GET запрос и проанализирует значение параметра redirect, чтобы определить, куда перенаправлять пользователя.. Если разработчики сайта не предусматривают возможность перенаправления только на сайты своего сервиса, то злоумышленники могут воспользоваться этой уязвимостью и сделать перенаправление на свои вредоносные сайты.

При переходе на подозрительные ссылки всегда стоит обращать внимание на атрибуты, похожие на *redirect_to=, redirect=, r=, url=, next=* и т.д.

Лучший способ избежать Open Redirect – это избегать перенаправления по параметру, зависящему от пользователя или проходящего через GET-запрос. Если перенаправление неизбежно, можно проверять конечные сайты и добавлять их в «белый список» подтвержденных URL-адресов [8, 9].

Засорение HTTP-параметров

Засорение HTTP-параметров(HTTP parameter pollution, или HPP) происходит, когда злоумышленник вставляет в HTTP-запрос дополнительные параметры. HPP бывают серверными и клиентскими.

Серверные HPP могут произойти тогда, когда веб-сайт принимает параметры, вписанные злоумышленниками. Например: сайт принимает параметр *value*. Рассчитано получить только один параметр. Засорение запроса в данном примере будет выглядеть следующим образом: https://www.site.com/main?value=12345&value=5000.

Получая несколько одинаковых параметров сервер может обработать их по-разному, в зависимости от самой серверной технологии [7, 8].

Клиентские засорения параметров дают возможность злоумышленникам влиять на работу компьютера пользователя. Рассмотрим конкретный пример. Допустим, что в теле сайта у нас есть данный серверный код:

<? $val=htmlspecialchars($_GET['par'],ENT_QUOTES); ?>

<a href=”/page.php?action=view&par=’.<?=$val?>.’”>View Me!

С помощью параметра *par* мы можем реализовать уязвимость используя следующий URL-адрес: https://host/page.php?par=123%26action=edit

В данном примере мы присваиваем *par* значение *123%26action=edit.* При анализе URL-адреса *%26* преобразовывается в строку *&*(что означает символ *&*). Преобразованное значение сохраняется в атрибут ссылки – *href*. Получается следующая ссылка: *<a href=”/page.php?action=view&par=123&action=edit”*>[1].

Таким образом получилось два параметра *action*, это может стать причиной уязвимости, если серверная технология будет использовать последний записанный

параметр. Из этого всего можно сделать вывод: если сайт принимает какой-то контент, взаимодействует с другими веб-сервисами и генерирует результат на основе текущего URL-адреса, значит, потенциально он содержит уязвимости [10].

Межсайтовая подделка запросов

При межсайтовой подделке запросов(cross-site forgery, или CSRF) злоумышленник заставляет браузер жертвы отправить HTTP запрос на другой сайт, чтобы он выполнил какое-то определенное действие. Обычно предполагается, что жертва будет аутентифицирована на атакуемом сайте. В этом злоумышленникам могут помочь Cookie-файлы браузера, которые отправляют сохраненные данные пользователя вместе с HTTP-запросом.

Cookies – небольшие файлы, которые веб-сайты создают и хранят внутри браузера пользователя.

CSRF подвержены все веб-приложения, которые автоматически добавляют аутентификационные данные пользователя к запросу.

Существует несколько способов защиты от подделки запросов:

1. Anti-CSRF токены. Для этого сервер должен будет сгенерировать случайный уникальный токен для браузера пользователя и проверять его для каждого запроса;
2. Выбор защищенных фреймворков;
3. Использование двух токенов или Double submit cookie: один токен сохраняется в cookie-файлах, а второй – в одной из параметров ответа. Защита обеспечивается сравнением обоих токенов;
4. Флаг Same-site: в cookie устанавливается дополнительный атрибут – same-site, у которого может быть два значения lax и strict. Браузер не отправляет cookies, если запрос осуществляется с другого домена [11].

Внедрение SQL-инъекций

Внедрение SQL-инъекций позволяет злоумышленнику обращаться к БД на атакуемом сайте с помощью языка структурированных запросов(structured query language, или SQL).

Уязвимые точки для атаки находятся в местах, где происходит запрос к БД: форма аутентификации, поисковая строка, каталог и URL.

Классическим примером SQL-инъекции является внедрение комментария через форму аутентификации. Это может позволить игнорировать часть запроса к базе данных. Например: введя в поле для логина строку *admin'--* , мы закомментируем остальную часть запроса, который будет выглядеть следующим образом

*SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'*

Запрос на ввод пароля проигнорируется и таким образом мы сможем войти на сайт через учетную запись администратора.

Также существуют и другие способы внедрений SQL:

1. Сворачивание условия WHERE к истинностному результату при любых значениях параметров;
2. Присоединение к запросу результатов другого запроса через оператор UNION.

Существует несколько методов по предотвращению атак с использованием SQL-инъекций [12]:

1. Заранее подготовленные инструкции.
2. Утвержденный список - прием заведомо действительных входных значений и отказ в случае ввода других.
3. Приведение типов – преобразование пользовательского ввода в более безопасный тип данных.

4. Чистка - шифрование или удаление спецсимволов, способных вмешаться в работу логики SQL.

Межсайтовый скриптинг

Межсайтовый скриптинг(или cross-site scripting, XSS) возникает, когда сайт не проверяет и не обрабатывает должным образом выводимые символы, которые позволяют запустить вредоносный код на JavaScript. Одними из таких символов являются кавычки (“), одинарные кавыки(‘) и угловые скобки(< >).

Сайт особенно подвержен уязвимости XSS, если не содержит флаг *httponly* для конфиденциальных cookie-файлов. Доступ к значениям cookies может позволить злоумышленнику получить контроль над учетной записью жертвы.

Самым элементарным примером XSS может послужить следующий код[1]:

<input type=”text” name=”username” value=”hacker” width=50px>

Если у злоумышленника будет доступ к значению value, он может закрыть существующую кавычку и внедрить код на JavaScript. Достаточно будет поменять значение атрибута на следующее: *name” onfocus=alert(document.cookie) autofocus”*

В результате получится код:

<input type=”text” name=”username” value=”hacker” onfocus=alert(document.cookie) autofocus “” width=50px>

Атрибут *onfocus* заставит сработать скрипты сразу после потери фокуса в поле username. При выполнении кода выведется диалоговове окно с *document.cookie* . Такими же махинациями – вводом закрывающей кавычки – возможно внедрить сторонний код с помощью тега <script>, если он содержит переменную, доступ к значению которой имеет злоумышленник.

XSS делятся на два вида: хранимые и отраженные. Отраженные XSS возникают, когда внедряемый код выполняет и доставляет один и тот же HTTP-запрос, который не сохраняется на сайте. Хранимые атаки XSS – напротив, сохраняются на сайте и выводятся без предварительной обработки в разных местах.

Также атаки межсайтового скриптинга можно разделить на три подкатегории: основанные на DOM, слепые и локальные.

Атаки XSS, основанные на DOM подразумевают манипулирование JavaScript кодом, который есть на самом сайте. Они могут быть как отраженными, так и хранимыми.

Слепая XSS атака является хранимой и подразумевает, что вредоносный код будет виден всем пользователям сайта, кроме администратора и злоумышленника, внедрившего код.

Локальные XSS атаки затрагивают только самого пользователя, который внедряет свой код, т. е. злоумышленника.

Для защиты от межсайтового скриптинга стоит прогонять введенные пользователем данные через фильтры, которые будут обрабатывать все специальные символы.

Выводы: для наилучшей защиты веб-ресурса стоит максимально уделять внимание разделам сайта, которые могут наполняться или редактироваться непосредственно с помощью пользовательского ввода. Любые данные, введенные пользователем должны проходить определенную проверку и обработку.

СПИСОК ЛИТЕРАТУРЫ

1. *Яворски П.* Ловушка для багов. Полевое руководство по веб-хакингу / Питер Яворски. – Санкт-Петербург: Питер, 2021. – 272 с.
2. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство проектирования однозоновой сети транкинговой связи для ее оперативного

развертывания. Свидетельство о регистрации программы для ЭВМ 2021610521, 14.01.2021. Заявка № 2020665716 от 03.12.2020.
3. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.
4. *Безуглов Д.А.,* Швидченко С.А. Синтез общей модели обеспечения безопасности для неоднородной системы обработки данных. В сборнике: Системный анализ, управление и обработка информации. труды X Международной научной конференции. 2020. С. 109-114.
5. *Швидченко С.А.* Анализ обеспечения безопасности информации в АСУ. - В сборнике: Актуальные аспекты развития воздушного транспорта (Авиатранс-2018). Материалы международной научно-практической конференции. 2018. С. 257-262.
6. Carettoni Luca, di Paola Stefano. HTTP Parameter Pollution. – URL: www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf (дата обращения 22.10.2021)
7. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство опроса и сбора программно-аппаратных характеристик персональных компьютеров. Свидетельство о регистрации программы для ЭВМ RU 2020613849, 23.03.2020. Заявка № 2020612910 от 16.03.2020.
8. *Николаева, В*. Атака HTTP request smuggling: механизм, разновидности и защита / В. Николаева // Tproger. – URL: https://tproger.ru/translations/http-request-smuggling/ (22.10.2021)
9. Лобанов, Н. Спидран по 13 уязвимостям на сайтах. Основные понятия, и средства защиты / Н. Лобанов // Хабр. – URL: https://habr.com/ru/post/226321/ (дата обращения 22.10.2021)
10. Борисенков, О. Межсайтовая подделка запроса: защита от CSRF атак / О. Борисенков // Tproger. – URL: https://tproger.ru/articles/mezhsajtovaja-poddelka-zaprosa-zashhita-ot-csrf-atak/ (дата обращения 22.10.2021)
11. Мишанин, Д. CSRF-уязвимости все еще актуальны / Д. Мишанин // Хабр. – URL: https://habr.com/ru/company/oleg-bunin/blog/412855/ (дата обращения 22.10.2021)
12. Silver. Взламываем сайты: шпаргалка по SQL инъекциям / Silver // proglib. – URL: https://proglib.io/p/vzlamyvaem-sayty-shpargalka-po-sql-inekciyam-2019-12-21 (дата обращения 22.10.2021)

В.И. Юхнов, А.А. Бородина

АНАЛИЗ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ CISCO ДЛЯ ОБЕСПЕЧЕНИЯ ВНУТРЕННЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: обеспечение безопасности, внешние и внутренние угрозы, защита, сетевая безопасность, Cisco Security Agent, Cisco NAC Appliance , Cisco MARS, списки контроля доступа и протокол IP Security.

В статье рассмотрены следующие вопросы: безопасность конечность хоста на базе Cisco Security Agent, контроль доступа к сети на основе Cisco Network Admission Control,

сбор и преобразование предоставляемых сетевыми устройствами, сетевыми и узловыми сенсорами данных о злонамеренной активности с помощью аппаратно-программного решения Cisco MARS.

V.I. Yukhnov, A.A. Borodina

ANALYSIS OF CISCO HARDWARE AND SOFTWARE TO ENSURE INTERNAL INFORMATION SECURITY OF THE COMPANY

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

Keywords: security, external and internal threats, protection, network security, Cisco Security Agent, Cisco NAC Appliance, Cisco MARS, access control lists and IP Security Protocol.

The following issues are considered in the article: security of the host limb based on Cisco Security Agent, network access control based on Cisco Network Admission Control, collection and transformation of malicious activity data provided by network devices, network and node sensors using the Cisco MARS hardware and software solution.

Одним из ведущих производителей продуктов информационной безопасности является компания Cisco.

Цель работы - провести анализ использования Cisco Security Agent, Cisco NAC Appliance и Cisco MARS для обеспечения внутренней информационной безопасности компании.

Перед информационной безопасностью современной компании стоят задачи – поддержка защищенных каналов связи компании, поддержка подсистемы контроля доступа пользователей, обеспечение антивирусной защиты, защиты от спама, контроль утечек информации, мониторинг событий информационной безопасности, происходящих в сети, и другие задачи.

Эффективная защита от известных угроз безопасности обеспечивается хорошо продуманной и развитой инфраструктурой безопасности, которая включает в себя такие компоненты, как предотвращение вторжений, антивирусные программы, средства фильтрации контента и межсетевой экран традиционного и нового поколения.

Любая система информационной безопасности строится на основе предполагаемой модели угроз. При планировании системы защиты необходимо учитывать две категории угроз: внешние и внутренние.

Внешние угрозы легко предсказуемы, поскольку компания располагает полной информацией о том, какие услуги доступны извне, какие программные и аппаратные ресурсы обеспечивают связь между этой услугой и Интернетом.

Гораздо сложнее бороться с внутренними угрозами, поскольку пользователи, работающие в компании, имеют разные уровни доступа и строят разные отношения внутри компании. Для обеспечения защиты необходимо подходить к данному вопросу комплексно, а не ограничиваться только техническими средствами.

Безопасность конечность хоста – Cisco Security Agent.

Решение Cisco Security Agent (CSA) представляет собой систему безопасности для конечного хоста и в сочетании с другими системами позволяет решать более сложные задачи.

CSA состоит из двух основных частей: центра управления (Management Center) и агентов (Agents). CSA использует агентов для применения настроенных на центральном сервере политик информационной безопасности.

CSA обеспечивает защиту серверных систем и настольных компьютеров. Возможности Cisco Security Agent превосходят возможности стандартных решений для защиты оконечных узлов, сочетая в себе расширенные функции защиты от целевых атак, шпионских программ, программ скрытого удаленного управления, антивирусную защиту, защиту от утечек информации и многих других видов нарушения компьютерной безопасности.

Cisco Security Agent предоставляет ряд функций, среди которых:

- мониторинг соответствия состояния сетевых объектов требованиям политики безопасности;
- профилактическая защита от целенаправленных атак;
- контроль USB, CD-ROM и т.д.;
- возможность обнаружения и изоляции вредоносных программ для скрытого удаленного управления;
- контроль утечки информации;
- расширенные функции для предотвращения вторжений на сетевые узлы, персонального межсетевого экрана и защиты от новых атак;
- создание замкнутой программной среды;
- мониторинг и предотвращение загрузок с несанкционированных носителей;
- маркировка сетевого трафика;
- обеспечение доступности важных приложений «клиент-сервер» и проведения транзакций;
- оптимизация использования полосы пропускания Wi-Fi;
- интеграции с системами предотвращения вторжений (Cisco IPS),с системой управления безопасностью (Cisco MARS) и с системой контроля доступа к сети (Cisco NAC).

Контроль доступа к сети – Cisco Network Admission Control (NAC).

Cisco NAC Appliance (Cisco Clean Access) - решение, предназначенное для автоматического обнаружения, изоляции и лечения зараженных, уязвимых или не соответствующих требованиям безопасности узлов, которые предоставляют проводной или беспроводной доступ к корпоративным ресурсам.

Основные особенности решения Cisco NAC:

- интеграция с Kerberos, LDAP, RADIUS и другими методами аутентификации;
- поддержка ОС Windows, macOS, Linux, принтеров, IP-телефонов и т.д.;
- поддержка антивирусов и других продуктов для защиты компьютеров;
- централизованное веб-управление;
- независимость от производителя сетевого оборудования;
- изолирование неподходящего узла путем применения списков управления доступом;
- автоматическая установка обновлений, новых версий средств безопасности или обновление антивирусных баз;
- наличие русского языка;
- проведение прозрачного аудита.

Cisco NAC - это аппаратно-программный комплекс для внутренней безопасности информации, использующий сетевую инфраструктуру, применяющий политики информационной безопасности и ограничивающий доступ к сети для тех устройств, которые не соответствуют требованиям политик информационной безопасности.

Cisco Security Monitoring, Analysis and Response System (MARS).

Cisco MARS - это аппаратно-программное решение в серверном исполнении. Программное обеспечение системы основано на операционной системе Linux. Основным компонентом системы является база данных Oracle, используемая для хранения информации.

Одна из основных задач Cisco MARS – централизованный сбор и преобразование предоставляемых сетевыми устройствами, сетевыми и узловыми сенсорами данных о злонамеренной активности в удобную для анализа форму с целью устранения подтвержденных нарушений политики безопасности с учетом их приоритетов.

В качестве источников данных Cisco MARS могут выступать:

- сетевые устройства (маршрутизаторы и коммутаторы);
- сетевые узлы (серверы под управлением ОС Windows, Solaris и Linux);
- средства защиты информации (межсетевые экраны, системы обнаружения атак, сканеры уязвимостей и антивирусные программы);
- серверы приложений (базы данных, серверы аутентификации и Web-серверы);
- программы обработки сетевого трафика (Cisco NetFlow).

MARS поддерживает оборудование различных производителей. Логика системы Cisco MARS основана на запросах к базе данных. Вы можете выбрать информацию и уточнить ее по IP-адресу источника, IP-адресу получателя, портам, типам событий, устройствам, ключевым словам и так далее.

Cisco MARS обеспечивает преобразование необработанных данных о вредоносной активности, предоставленных сетью и системой безопасности, в понятную информацию, которая используется для устранения нарушений безопасности с использованием оборудования, уже существующего в сети.

Не стоит забывать и о традиционных способах обеспечения безопасности, таких как защита службы системы доменных имен, списки контроля доступа, туннелирование, шифрование данных, IP Security и т.д.

Списки контроля доступа.

Одним из наиболее важных навыков сетевого администратора является управление списками контроля доступа, которые предоставляют возможности фильтрации пакетов для управления потоком трафика.

Сетевые разработчики используют межсетевые экраны для защиты сети от несанкционированного использования. Межсетевые экраны или брандмауэры – это программные или аппаратные решения, предназначенные для повышения степени защищенности сети. На маршрутизаторе Cisco можно настроить простой брандмауэр, который позволяет фильтровать трафик на базовом уровне с помощью списков контроля доступа, использование которых позволяет администраторам фильтровать трафик, допуская или блокируя в сеть только определенные пакеты.[1]

Протокол IP Security.

Протокол IPSec (IP Security Protocol) представляет собой набор открытых стандартов, обеспечивающий конфиденциальность данных и их целостность при передаче, а также процедуры аутентификации между принимающими участие в связи одноранговыми устройствами на уровне протокола IP.

Протокол IPSec позволяет системе выбирать протоколы и алгоритмы безопасности, а также устанавливать криптографические ключи

Сетевая безопасность современной сети - это не только классический набор из межсетевого экрана, системы предотвращения вторжений и фильтрации контента. Современные угрозы могут проникать во внутреннюю сеть многими другими способами - от проникновения через незащищенный Wi-Fi или 3G/4G-модем, до заражения с USB-накопителя или в рамках синхронизации с мобильным устройством. Поэтому перед службами информационной безопасности стоит задача защитить сеть не только от внешних, но и от внутренних угроз. В то же время установить сенсор системы обнаружения атак на каждый порт коммутатора невозможно как по финансовым, так и по техническим причинам.

СПИСОК ЛИТЕРАТУРЫ

1. *Юхнов В.И. Бородина А.А.* ВЫБОР СРЕДСТВ CISCO ДЛЯ РЕШЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. С. 300-303.
2. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие/ *А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков*; под общ. ред. *Н.И. Синадского*. – Екатеринбург: Изд-во Урал. Ун-та, 2014. – 180 с.
3. Программа Сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. : Пер. с англ. – М. : ООО “И.Д. Вильямс”, 2007, с. 843-862
4. Научный журнал Jet Info №1-2 (275) / 2017 / Обнаружение аномалий на сетевом уровне с Cisco StealthWatch /https://www.jetinfo.ru/obnaruzhenie-anomalij-na-setevom-urovne-s-cisco-stealthwatch /
5. https://habr.com/ru/company/cisco/blog/348532/

С.Е. Топорков[1], Н.В. Болдырихин[2]

ОБЗОР БЕЗОПАСНОСТИ УМНОГО ДОМА

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: умный дом, безопасность, защита, уязвимости, бэкдоры, беспроводные сети.

В статье проанализированы основные уязвимости современных умных домов и риски при их использовании. Показаны особенности реализации систем умных домов, выявлены недостатки и даны рекомендации к их максимальному устранению.

S.E. Toporkov[1], N.V. Boldyrikhin[2]

SMART HOME SAFETY OVERVIEW

Don State Technical University, Rostov-on-Don, Russia[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: smart home, security, protection, vulnerabilities, backdoors, wireless networks.

The article analyzes the main vulnerabilities of modern smart homes and the risks associated with their use. The features of the implementation of smart home systems are shown, shortcomings are identified and recommendations for their maximum elimination are given.

Умный дом, это система управления и контроля всеми системами, включёнными в качестве комплектующих, и подключёнными к сети, в том числе системы управления комфортом и безопасностью самого дома и прилегающей территории. Неисправности внутренних систем дома, а в частности системы безопасности, могут стать причинами серьёзных материальных потерь, но при должном уровне осторожности владельца вполне решаемы. Однако с точки зрения информационной безопасности «умный дом» - крайне рискованное предприятие для владельцев. В этой статье будут рассмотрены причины потенциальной опасности умного дома с точки зрения безопасности информации.

В начале следует рассмотреть стандартные системы безопасности – система охраны, обнаружения вторжений, методы обезвреживания злоумышленников – встроенные в саму концепцию умного дома по умолчанию [1-4].

Система безопасности – самый важный и самый дорогой элемент умного дома. Строится он по принципу постановки нескольких «линий защиты».

Первая линия защиты – это средства обнаружения, включающая в себя камеры наружного и внутреннего наблюдения, а также датчики на основе различных физических признаков (движение, тепло, вес, звук и прочие).

Вторая линия подразумевает обеспечение беспрепятственного прохода в охраняемую зону владельца дома и ряда обозначенных им лиц – членов семьи, друзей и других. Также эта линия защиты ограничивает доступ посторонним лицам на охраняемую территорию.

Третья линия защиты блокирует передвижение потенциальных злоумышленников внутри охраняемой зоны и воздействует на его психическое и физическое состояния (задымление, газ, световые вспышки, воздействие электричеством) с целью нейтрализации потенциальной угрозы.

Четвёртая – последняя – линия защиты предназначается для охраны особо ценных вещей в доме (сейфы, хранилища), а также для предоставления убежища жителям дома.

Эти физические линии защиты обладают своими известными сильными и слабыми сторонами, но умный дом – это не только стены и крыша, но и множество программных и программно-аппаратных средств, подключённых к локальной и глобальной сети. Такой подход из-за своей новизны имеет массу уязвимостей при недостатке опыта защиты и корректного использования.

Владелец умного дома в любое время может связаться напрямую как с самим домом, так и с любым устройством внутри него по телефону или посредством сети для выполнения определённых задач [4-6]. Все эти «удобства» умных домов, как по отдельности, так и в своей совокупности являются ахиллесовой пятой в первую очередь для их владельцев из-за бескрайних возможностей для перехвата управления ими.

Пока люди с развитым воображением рисуют разной степени убедительности картины о восстании машин и других «умных» устройств, а также применении смарт-дома как орудия убийства или терроризма, специалисты по кибербезопасности и хакеры выходят на новую линию соприкосновения. И речь идёт о реальных и уже (относительно) массово применяемых устройствах, реальных уязвимостях в них и испытанных способах использовать эти уязвимости в недобрых целях.

В ходе исследования умного дома, проведённого в университете Мичигана, к сети было подключено 18 различных устройств. Основная задача исследования – выявить основные уязвимости беспроводных интеллектуальных систем управления. Кроме того, были протестированы продукты компании под названием SmartThings.

В ходе исследования было проведено множество различных атак на комплектующие устройства умного дома. По итогам проверок выявлены две основные уязвимости – избыточные разрешения и небезопасные сообщения.

В плане избыточных разрешений и прав выяснилось, что большая часть установленных приложений имеет доступ к гораздо большему объёму информации, чем им достаточно для корректной и эффективной работы. Кроме того, приложения и физические устройства обменивались при взаимодействии сообщениями, содержащими конфиденциальные сведения без должной защиты. А иногда вообще без защиты, что совершенно некорректно с точки зрения информационной безопасности [1-3].

Так, например, приложение, контролирующее уровень заряда автоматического кодового замка, содержало код его разблокировки, а программные средства генерировали ряд сообщений, идентичных реальным сигналам физических устройств. Этот подход даёт злоумышленникам возможность для получения фактически любую информацию путём банального перехвата или прослушивания каналов связи, а также для передачи в локальную сеть умного дома недостоверной информации с потенциальными бэкдорами для взломщиков, призванные для дальнейшего несанкционированного входа и управления системами.

Помимо явно лишних разрешений и совершенно небезопасных сообщений, была выявлена очередная проблема, заключающаяся в том, что устройства и приложения передают проходящую через них информацию, в том числе конфиденциальную, на серверы компаний-производителей, которые занимаются поддержкой этих устройств. Умный дом и его компоненты следят за своими пользователями каждую минуту и отправляют полученную информацию обо всех взаимодействиях на сервера. Имея эту информацию, есть все возможности для восстановления распорядка дня жильцов, их предпочтений, рода деятельности, заработка, информации о членах семей, местах работы и ещё множестве параметров. В нечистых руках вся эта информация может быть (и обязательно будет) использована как в целенаправленных атаках, так и в массовых противозаконных и противоправных действиях.

Кроме этого, не обошлось и без самых обычных бэкдоров, оставляемых разработчиками ради возможности получения полного контроля над устройствами пользователей. Производители оправдывают свои действия необходимостью оказания технической поддержки и поддержки нормальной работы приложений и устройств, однако даже сама возможность наличия бэкдоров в системах безопасности заставляет усомниться не только в собственной безопасности внутри умных домов, но и о необходимости покупки таких потенциальных ловушек. Целенаправленное наличие подобных уязвимостей противоречит всем нормам и доктринам информационной безопасности, даже не учитывая множества злоумышленников. Это не говоря уже о потенциальных злоумышленниках как со стороны, так и внутри компании-производителя, желающих воспользоваться данной информацией.

Как можно убедиться, при комплектации умного дома необходима предельная внимательность ко всем компонентам и их существующим и потенциальным уязвимостям, потому как абсолютно все устройства так или иначе подвержены риску взлома.

Основные рекомендации для пользователей умных домов:

- отключение ненужного функционала;
- внимательное изучение возможностей устройств и приложений;
- использование сложных паролей и двухфакторной аутентификации;
- защита умных устройств или кодов доступа к ним от посторонних.

Главный вывод в том, что на сегодняшний день «умные» дома, несущие в себе множество удобств для жизни простого пользователя, являются троянскими конями, которые в обмен на комфорт крадут информацию, но могут украсть и жизнь. Поэтому лучше повременить с покупкой таких сомнительных удобств, учитывая их стоимость и незащищённость. А лучше – вообще воздержаться от их использования.

СПИСОК ЛИТЕРАТУРЫ

1. *Буковшин В.А., Болдырихин Н.В.* Современные проблемы информационной безопасности // Современные материалы, техника и технология. Сборник научных статей 8-й Международной научно-практической конференции. 2018. С. 47-51.
2. *Буковшин В.А., Болдырихин Н.В.* Кибербезопасность как неотъемлемая часть информационного мира // Современные материалы, техника и технология. Сборник научных статей 8-й Международной научно-практической конференции. 2018. С. 52-54.
3. *Короченцев Д.А., Черкесова Л.В., Ревякина Е.А., Болдырихин Н.В., Сафарьян О.А.* Импортозамещающие технологии обеспечения информационной безопасности и защиты данных / Учебное пособие / Министерство науки и высшего образования Российской Федерации, Донской государственный технический университет. Ростов-на-Дону, 2021.335 с.
4. *Шарифов П.М.З., Кияшова З.В., Болдырихин Н.В.* Анализ безопасности технологий интернета вещей // Информационные технологии в управлении, автоматизации и мехатронике. сборник научных трудов 2-й Международной научно-технической конференции. Курск, 2020. С. 219-223.
5. *Бодров С.А., Журавлёв А.В., Ерпелев А.В.* Умный дом: история, принцип работы, устройства умного дома, протоколы // Технические науки: проблемы и решения. Сборник статей по материалам XLIV международной научно-практической конференции. Москва, 2021. С. 29-32.
6. *Аль-Обайди А.Т., Болдырихин Н.В., Решетникова И.В., Рыбалко И.П.* Принципы построения IOT-сетей // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 208-210.
7. *Аль-Обайди А.Т., Болдырихин Н.В.* Управление мониторингом IOT-сетей // Актуальные проблемы науки и техники. 2021. Материалы Всероссийской (национальной) научно-практической конференции. Ростов-на-Дону, 2021. С. 378-379.

С.Е. Топорков[1], Н.В. Болдырихин[2], И.В. Решетникова[3]

ОБЗОР ЗАЩИЩЁННОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

Донской государственный технический университет, Ростов-на-дону, Россия[1]
Ростовский государственный университет путей сообщения,
Ростов-на-Дону, Россия[2]
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[3]

Ключевые слова: операционные системы, безопасность, защита, Astra Linux, KasperskyOS, Fedora Silverblue.

В статье проанализированы современные операционные системы и методики, используемые в их защите. Показаны особенности реализации данных методов, выявлены достоинства и недостатки.

S.E. Toporkov[1], N.V. Boldyrikhin[2], I.V. Reshetnikova[3]

OPERATING SYSTEM SECURITY OVERVIEW

Don State Technical University, Rostov-on-Don, Russia[1]
Rostov State Transport University Rostov-on-Don, Russia [2]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[3]

Keywords: operating systems, security, protection, Astra Linux, Kaspersky OS, Fedora Silverblue.

The article analyzes modern operating systems and techniques used in their protection. The features of the implementation of these methods are shown, the advantages and disadvantages are revealed.

Операционная система (ОС) – важнейшая составляющая любого программно-аппаратного средства, которая обеспечивает управление всеми ресурсами, такими как память, устройства ввода вывода, процессорное время и т.д. От нее во многом зависит эффективность работы любого компьютера [1-7]. Вместе с тем, именно с операционной системой связано большое количество уязвимостей информационной безопасности. Рассмотрим далее несколько операционных систем, позиционируемых как системы повышенной защищенности.

Astra Linux — операционная система специального назначения, созданная на базе ядра Linux. Данная система предназначена для комплексной защиты информации и построения защищённых автоматизированных систем [6]. Astra Linux так же может использоваться для нужд спецслужб, армии России и государственных органов. Для снижения порога вхождения пользователей в новую систему, а также для её популяризации, итоговую операционную систему разделили на две отдельные версии:

- Astra Linux Common Edition (Орёл);
- Astra Linux Special Edition (Смоленск).

Первая версия предназначена для пользователей и разработчиков, которые хотели бы попробовать новую систему, а также защитить свои данные. Вторая версия является «военной» ОС и соответствует всем необходимым стандартам безопасности.

Важной особенностью Astra Linux стала отличная защищённость как самой ОС, так и пользовательских программ и данных. Новая система обеспечивает крайне высокую степень защиты обрабатываемой информации вплоть до уровня «особой важности» включительно, что подтверждает наличие сертификатов Минобороны, ФСТЭК и ФСБ России.

Одна из новейших операционных систем, она уже включена в Единый реестр российских программ Минкомсвязи России, поэтому может быть использована для исполнения приказа о переходе на отечественное программное обеспечение в коммерческих и некоммерческих организациях.

Astra Linux среди массы защищенных российских дистрибутивов оказалась самым популярным продуктом – именно она станет основной для Министерства обороны России.

Защита в Astra Linux Special Edition рассматривает одного и того же пользователя как нескольких разных пользователей в зависимости от его действий и создаёт для всех этих пользователей отдельные домашние каталоги, к которым невозможен одновременный прямой доступ нескольких пользователей.

Всего новая система использует 256 уровней доступа (от 0 до 255) и 64 категории доступа, которые разграничивают допуск к различным операциям с файлами, стеком TCP/IP, файловой системой и многое другое.

На основе типа операции или взаимодействия, а также шаблонного эталона безопасности, принимается решение о запрете или же разрешении доступа пользователя или программы к файлу.

Уникальная иерархия позволяет точно отличить действия пользователя от результата работы зловредного кода или несанкционированного управления системой извне. За счёт этого операционная система самостоятельно определяет скомпрометированные (несоответствующие правилам доступа) ресурсы и препятствует доступу этих ресурсов к дистрибутиву и файловой системе.

В Astra Linux отсутствует большая часть известных уязвимостей, которым подвержено абсолютное большинство операционных систем: зловредные программы не могут работать с памятью, встраиваться в код ОС или запускаться напрямую из сети.

Если исполняемый код скачивается извне, его запуск осуществляется в защищенной области памяти, который ограничивает доступ к данным и системе на всех уровнях.

Другие функции операционной системы: очистка внешней оперативной памяти, гарантированное удаление файлов, механизмы защиты информации в графической подсистеме, маркировка всех документов, механизм контроля замкнутости программной среды, регистрация событий, контроль целостности, двухфакторная аутентификация. Так же в ОС Реализованы механизмы мандатного и дискреционного разграничения доступа, кроме того, включён набор изменений PaX, обеспечивающий защиту от использования различных уязвимостей. Системные файлы Astra Linux, и отдельные элементы хэшируются, заносятся в протокол и сравниваются с эталоном, что исключает изменение или подмену кода.

KasperskyOS — это микроядерная проприетарная операционная система, разработка которой ведётся «Лабораторией Касперского» [7]. Целью данной разработки является создание защищённой операционной системы, которая предназначена для промышленных систем критической важности. Ядро KasperskyOS не основано на каких-либо существующих проектах и является собственной разработкой «Лаборатории Касперского».

Данная операционная система построена на концепции «множественных независимых уровней защиты/безопасности», которая определяет строгую изоляцию системных процессов и политик управления потоками информации.

Модуль контроля доступа, который отслеживает все взаимодействия между процессорами и исключает доступ приложений к защищаемым областям памяти с критически важными данными и процессами, является одним из наиболее важных компонентов KasperskyOS. Этот модуль исполняется только в привилегированном режиме: он поддерживает обширный набор политик и правил доступа, а также может быть настроен в соответствии с требованиями заказчика. Любое действие, не предусмотренное политиками безопасности, по умолчанию считается запрещённым.

KasperskyOS —новый продукт «Лаборатории Касперского», в который заложены основные функции и методики безопасности информации и превентивной защиты на уровне архитектуры.

В схему работы модуля контроля доступа входит обязательная маркировка и идентификация ресурсов. Также все приложения ОС имеют безопасную конфигурацию, без которой их установка невозможна, а все ресурсы уровня приложений и аппаратное обеспечение имеют маркировки безопасности. Это позволяет пресечь попытки доступа к ресурсам, которые не имеют этой маркировки, из-за чего исключаются возможности доступа для непроверенных программных и аппаратных средств.

Помимо этого, KasperskyOS поддерживает виртуализацию – для этого она содержит встроенный гипервизор, поддерживающий операционные системы Linux и Windows в качестве гостевых. Виртуализация позволяет изолировать потенциально опасные и недоверенные гостевые ОС как друг от друга, так и от критически важных программно-аппаратных средств, которые физически находятся на одной платформе. Это позволяет

минимизировать или даже исключить проникновение зловредного исполняемого кода или пути для получения информации потенциальными злоумышленниками.

Fedora Silverblue — является неизменяемой десктопной операционной системой, в которой все приложения запускаются в изолированных контейнерах, а различные обновления устанавливаются исключительно атомарно.

Термин «неизменяемая операционная система» означает режим «только для чтения» для корневой и пользовательской директорий. Все изменяемые данные размещены в каталоге /var. Такой подход повышает защищенность ОС и не дает удалить системные файлы по ошибке или по злому умыслу. Кроме того, это упрощает установку обновлений, потому что для этого нужно лишь перезагрузить систему с нового образа.

Операционная система проста и интуитивно понятна в настройке, много дополнений на основе Linux, а также имеет встроенный файервол, однако часть пакетов приходится скачивать со сторонних репозиториев. Fedora имеет встроенный механизм *SELinux*. Этот механизм встроен в ядро Linux и по умолчанию включен в Fedora, CentOS, RHEL и некоторых другие дистрибутивах Linux. SELinux позволяет администратору сервера определять различные разрешения для всех процессов работы. Он определяет, как все процессы взаимодействуют с другими частями сервера. SELinux также устанавливает ограничения и инструктирует серверные программы: к каким файлам им обращаться и какие действия предпринимать, определяя политику безопасности. Другими словами, ущерб теперь может быть ограничен конкретным сервером и файлами. Взломщик не сможет получить оболочку на сервере через распространенные демоны (процессы, работающие в фоновом режиме), такие как Apache / BIND / Sendmail, поскольку SELinux предлагает следующие функции безопасности:

- защита данных пользователей от несанкционированного доступа;
- защита сетевых портов от несанкционированного доступа;
- другие программы, защищающие от несанкционированного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. *Половинченко М.И., Елисеев В.С., Болдырихин Н.В., Рыбалко И.П.* Сравнительный анализ современных операционных систем // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2018. № 1. С. 258-261.
2. *Короченцев Д.А., Черкесова Л.В., Ревякина Е.А., Болдырихин Н.В., Сафарьян О.А.* Импортозамещающие технологии обеспечения информационной безопасности и защиты данных / Учебное пособие / Министерство науки и высшего образования Российской Федерации, Донской государственный технический университет. Ростов-на-Дону, 2021.335 с
3. *Бакланов В. В.* Защитные механизмы в операционной системе Linux; Москва, 2013.
4. *Мельников В. Ю., Пугачёв В. К.* Методы защиты операционных систем и данных, 2015.
5. *Проскурин В.* Защита в операционных системах, 2014.
6. Сайт ГК Astra Linux [электронный ресурс] URL: https://astralinux.ru/ (дата обращения 23.10.21)
7. Сайт KasperskyOS [электронный ресурс] URL: https://os.kaspersky.ru/ (дата обращения 23.10.21)

Б.П. Борисов, А.Е. Евсикова, Е.О. Владимирова, В.А. Уварова

ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: локальная сеть, защита информации, проводные и беспроводные сети связи, программная защита.

В статье рассмотрены основные принципы защиты информации в беспроводных и проводных сетях, а также подробнее рассмотрены программные средства защиты.

B.P. Borisov, A.E. Evsikova, E.O. Vladimirova, V.A. Uvarova

INFORMATION PROTECTION IN LOCAL COMMUNICATION NETWORKS

North Caucasus Branch Moscow Technical University of Communication and
Information Technology, Rostov-on-don, Russia

Keywords: local area network, information protection, wired and wireless communication networks, software protection.

The article discusses the basic principles of information security in wireless and wired networks, and also discusses in more detail software protection tools.

Введение.

Рассмотрим локальную сеть как это взаимодействия нескольких устройств между собой. Сеть часто используется в офисах, в учебных заведениях, а также небольших организациях или отделениях крупных компаний. По локальной связи можно передавать различные сообщения, начиная от текстовых и электронных писем и заканчивая видеофайлами и базами данных.

При реализации мер, направленных на защиту информации, предусматривается комплекс мероприятий, который направлен на предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Также, исходя из того, что утечка информации может произойти по каким-либо неумышленным причинам, а также по техническим или объективным, то в состав мероприятий, указанных выше, необходимо включить те, целью которых будет повышение надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Сегодня имеет место рост компаний профессиональная деятельность которых, направлена на защиту сообщений в инфокоммуникационных сетях связи. Это говорит о том, что защите информации передаваемой по сетям связи стало уделяться больше внимания.

Проводная связь

Проводная связь – это связь, осуществляемая по проводным линиям связи, где в качестве направляющей среды электросвязи используются электрические и волоконно-оптические кабели.

В проводных сетях связи электрический и оптический сигнал передает по направляющей среде электросвязи большое количество различных сообщений. В автоматизированных системах управления для передачи данных в основном используются

стандартизованные каналы связи для передачи как аналоговой, так и дискретной информации (телеграфные и телефонные широкополосные каналы связи), отвечающие предъявляемым к ним требованиям. Средства проводной связи отличаются высоким качеством каналов, простотой организации связи, относительно большой скрытностью по сравнению с радиосвязью, а при использовании оптики практически не подвержены воздействию преднамеренных помех.

Проводная линия связи является одним из основных элементов системы связи. В настоящее время телефонные сети используют коммутируемую сеть (switched network), в которой каждый телефонный аппарат с помощью линии связи соединяется с АТС, которая обеспечивает связь, доступную только на период времени соединения двух сторон. Как только разговор/передача сигнала завершается, связь разрывается. Основным принципом разработки сети является обеспечение качественного уровня обслуживания абонентов при наименьших расходах. Работа коммутируемой сети рассчитана на то, что в одно и то же время не будут разговаривать сразу все ее пользователи. Дальность и качество телефонной связи зависит от конструктивных особенностей и электрических параметров линий связи.

Соответственно очень важным является такое свойство связи, как ее безопасность. Необходимо обеспечить конфиденциальность. Безопасность характеризует способность связи противостоять несанкционированному подключению и изменению информации, передаваемой (принимаемой, хранимой, обрабатываемой) в системе связи, скрытию содержания передаваемых сообщений, а также вводу ложных сообщений.

В качестве устройств противодействия снятия информации широко используют:

- блокираторы телефонов;
- устройства защиты от высокочастотного-навязывания и микрофонного эффекта;
- анализаторы телефонных линий;
- устройства активной защиты телефонных линий;
- скремблеры;
- универсальные устройства защиты телефонной связи;
- выжигатели средств съема.

Блокираторы телефонов предотвращают попытки применения платных сервисов доступных через данную телефонную линию, а также прослушивания разговора с помощью параллельно включенного телефонного аппарата. Следовательно, блокираторы защищают телефон от пиратских покушений на защищаемую линию.

Защита от методов снятия конфиденциальной информации путем ВЧ-навязывания и за счет микрофонного эффекта сейчас не очень актуальна.

Анализаторы телефонных линий считают подключение к линии средств съема информации по следующим признакам:

- отклонению напряжения в линии от стандартного значения;
- изменению характера комплексного сопротивления линии (дополнительная нелинейность);
- появлению новых неоднородностей в линии.

Анализаторы телефонных линий делятся на индивидуальные сигнализаторы и тестовые комплекты. Индивидуальные сигнализаторы устанавливаются на заранее проверенную линию и применяются для контроля параметров телефонной пары. Тестовые комплекты предназначены для проверки линии специалистами.

Устройства постановки маскирующей помехи (УПМП) работает двумя способами:

- синусоидальный сигнал с диапазоном частот 20—70 кГц и амплитудой 12-50 В подается в телефонную линию при разговоре и нарушает работу телефонных передатчиков, « разрушая» спектр передаваемого сигнала и нарушая режим работы выходного каскада передатчика;

- шумовой сигнал с диапазоном частот 6—10 кГц и амплитудой ~ 5 В (метод высокочастотной маскирующей помехи);
- шумовой сигнал с диапазоном частот 300—3400 Гц и амплитудой ~ 2 В (метод низкочастотной маскирующей помехи). Данный сигнал подается в телефонную линию при положенной трубке и, влияя на систему активации записи диктофонов, стимулирует их записывать только шум в интервалах между переговорами. Так же мешает работе выносных микрофонов, использующих телефонную линию для передачи информации при положенной трубке, скрывает сигналы, возникающие из-за микрофонного эффекта. Телефонный подавитель организовывает зашумление верхнего звукового диапазона, ухудшая тем самым соотношение сигнал/шум на входе устройств съема информации.

Наиболее важно отметить аппаратуру криптографической защиты (скремблеры).

Все рассмотренные выше устройства могут обеспечить защиту телефонных переговоров только в диапазоне от абонента до АТС. Для обеспечения секретности на всем пути прохождения речевого сигнала применяются специальные устройства скремблеры.

Под криптографической защитой понимается преобразование свойств речевого сигнала таким образом, чтобы речевой сигнал, переданный в канал связи, был расплывчатым и занимал такую же полосу частот спектра, что и исходный открытый сигнал в речепреобразующем устройстве.

Можно выделить два основных метода закрытия речевого сигнала: дискретизация и аналоговое засекречивание, или выделение параметров речевого сигнала, представленных в цифровом виде, с последующим шифрованием.

В первом случае в канале связи — сигнал с фрагментами речевого сигнала, во втором — сигнал с выхода модема, использующего один из стандартных видов модуляции и скорости передачи 2400, 4800, 7200 или 9600 бит/с.

Цифровой способ кодирования информации более устойчив к рассекречиванию. Сигнал заранее преобразуется в цифровой вид, а затем кодируется с использованием специальных криптографических алгоритмов. Главная проблема с аппаратами данного класса, состоит в достижении высокого качества синтезированного Р.С. при реальных скоростях его передачи по каналу связи, составляющих 2400-9600 бит/с.

Так же существует метод физической защиты информации, включающие в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации.

Помеха создается вне полосы речевого сигнала и превышает его номинальный уровень на несколько порядков. Наличие мощной помехи выводит из линейного режима все простейшие устройства контактного и бесконтактного подключения к телефонной линии (появляется шум в звуковом диапазоне, речь становится неразличима).

Комплексное использование различных устройств защиты сигналов значительно повышает безопасность проводной связи.

Беспроводные сети связи

Беспроводные сети связи уступают в вопросах безопасности проводным сетям связи. Это в первую очередь обусловлено средой, где передается сигнал. Защитой информации называют комплекс мероприятий, проводимых для предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования и блокирования информации.

Беспроводные каналы связи используют различные диапазоны электромагнитных излучений:

- радиочастотный (3 – 3000000) кГц;
- инфракрасное излучение (0,75-1,4) мкм;
- инфракрасные лазеры.

Остановимся несколько подробнее на радиосвязи, которая использует технологию Wi-Fi. Технология Wi-Fi это технология передачи данных, которая в настоящее время широко используется для передачи мультитрафика в локальных сетях и в абонентском доступе.

Две главные уязвимости беспроводных сетей: удаленный бесконтактный доступ и радиоэфир как широковещательная среда передачи данных, где любой приемник сигнала может прослушивать эфир, а любой передатчик может вставить в сеть ненужные передачи и радиопомехи. Все это ухудшает безопасность беспроводной сети связи.

Начало проблемы.

Когда были созданы Wi-Fi сети, в начале использовали простой алгоритм: в центре периметра ставили одну точку доступа для наибольшего покрытия. Если для удаленных участков мощности сигнала не хватало, к точке доступа добавляли усиливающую антенну. Такой подход имел разумное объяснение. Изначально оборудование для создания беспроводных сетей имело большую стоимость, поэтому устанавливать большое количество точек доступа не было возможности.

Следующая проблема.

Чтобы осуществить атаку, злоумышленнику необходимо было как-то незаметно подкрадываться поближе, чтобы перехватить относительно слабый сигнал "с улицы" или другого приближенного места. Для этого надо вплотную подойти к строению от куда исходит сигнал, либо пытаться проникнуть внутрь здания. В любом случае это повышает риск быть замеченным. При этом значительно сокращается временной интервал для атаки. Это уже трудно назвать "идеальными условиями для взлома".

Разумеется, остается ещё одна изначальная проблема: беспроводные сети вещают в доступном диапазоне, который могут перехватить все клиенты. Действительно, сеть WiFi можно сравнить с Ethernet-HUB, где сигнал передается сразу на все порты. Чтобы этого избежать, в идеале каждая пара устройств должна общаться на своем частотном канале, в который не должен встревать никто другой.

Идеальной защиты добиться в любом случае не получится. Но можно значительно затруднить проведение атаки, сделав результат нерентабельным по отношению к затраченным усилиям.

Для защиты информации используются прямые и косвенные средства защиты.

Условно средства защиты можно разделить на две основные группы:

1. Технологии прямой защиты трафика, такие как шифрование или фильтрация по MAC;
2. Технологии, изначально предназначенные для других целей, например, для повышения скорости, но при этом косвенным образом усложняющие жизнь злоумышленнику.

Увеличение числа точек доступа позволит снизить уровень сигнала и сделать равномерной зону покрытия, а это значительно усложнит задачу злоумышленнику.

Так же повышение скорости передачи данных упрощает применение дополнительных мер безопасности. Например, если на каждый компьютер установить VPN клиент и передавать данные даже внутри локальной сети по зашифрованным каналам. Это потребует ресурсов, в том числе и аппаратных, но уровень защиты при этом значительно повышается.

Ниже приведем кратко технологии, которые позволяют улучшить работу сети и косвенным образом повысить степень защиты.

Косвенные средства улучшения защиты.

Client Steering. Функция Client Steering устанавливает несколько точек доступа на более близком расстоянии, что позволяет снизить мощность, при том даже улучшив скорость передачи данных. Так как точек несколько, это усложняет взлом сети.

Auto Healing. Auto Healing настраивает мощность, не теряя надежности и быстроту передачи данных. Контроллер анализирует исправность и функциональность точек

доступа. Если какая-то из них не работает, то ближайшие получают команду, увеличить мощность сигнала, чтобы заполнить белое пятно. Как только точка доступа вновь заработала, рядом стоящие точки принимают команду уменьшить мощность сигнала, чтобы уровень взаимных помех стал меньше.

Технология WiFi также использует и программные средства защита информации.

Это совокупность различных специализированных устройств, программ и приборов используемые для защиты информации от актуальных угроз.

Средства защита информации в зависимости от способа осуществления защиты можно разделить на группы, которые представлены на рисунке 1.

Рисунок 1. Группы средств защиты информации

Остановимся на одной из групп средств защиты информации, а именно – «Программные средства защиты».

Программные средства защиты информации представляют собой программы, основная цель которых представляет собой выполнение функций по обеспечению защиты информации.

Хочется отметить, что рассматриваемая группа средств защиты информации является ведущей по степени распространения и доступности, остальные же применяются в случая необходимости дополнительной защиты.

Среди программных средств защиты информации в локальных сетях можно выделить следующие типы, которые представлены на рисунке 2.

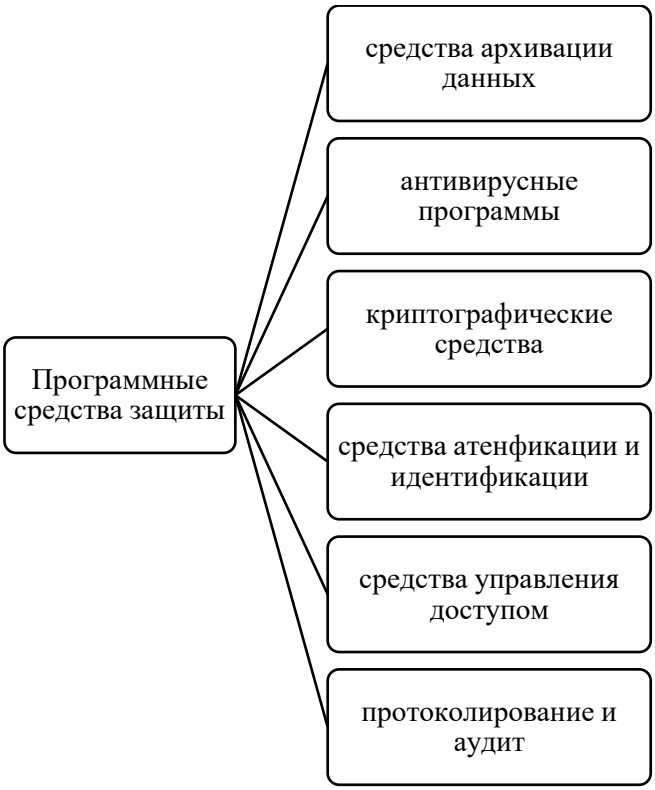


Рисунок 2. Типы программных средств защиты информации

Средства архивации данных – это средства, которые осуществляют соединение нескольких файлов или каталогов в единый файл, то есть в архив. В основном они используются при совершении действий с файлами больших размеров (для их передачи и прочего), так как помогают уменьшить объем данных файлов, при этом не искажая информацию.

Антивирусные программы представляют собой программы, разработанные для защиты цифровой информации от вирусов.

Криптографические средства – это средства, которые включают в себя способы обеспечения конфиденциальности информации, в том числе с помощью шифрования и аутентификации.

Средства идентификации и аутентификации пользователей.

Аутентификация – это процедура проверки принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. А идентификация – это процедура, которая определяет пользователя и полномочия субъекта в автоматизированной системе, контролирует установленные полномочия в процессе сеанса работы, регистрации действий и др.

Средства управления доступом — это совокупность технических средств, которые направлены на ограничения и контроль входа-выхода объектов на заданной территории через «точки прохода» с целью обеспечения безопасности.

Протоколирование и аудит:

- протоколирование обеспечивает сбор и накопление информации о событиях, происходящих в информационной системе.
- аудит – это процесс анализа накопленной информации. Целью компьютерного аудита является контроль соответствия системы или сети требуемым правилам безопасности, принципам или индустриальным стандартам. Аудит обеспечивает анализ всего, что может относиться к проблемам безопасности, или всего, что может привести к проблемам защиты.

Вывод:

Главной проблемой локальной системы безопасности является, необходимость локального соединения большого количества серверов и компьютеров. Поэтому при выборе сетевой топологии необходимо подобрать правильную, что бы не потратить лишних средств и ресурсов.

Сетевой топологии необходимо тратить на обработку информации управляющей сетью, минимальное количество сил и ресурсов, при это делать это быстро. Основной проблемой становится то, что скорость процессов становится куда важнее, чем надежная защита. Поэтому решение принимается чаще всего в сторону устаревших быстрых, но ненадежных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы/В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2002. –672с.
2. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации – Юниор, Москва, 2003. -476с.
3. Лагутин В.С. Утечка и защита информации в телефонных каналах.— 2-е изд., испр. и доп. / В.С. Лагутин, А.В. Петраков.— М.: Энергоатомиздат, 1997.— 298 с.

И.А. Сосновский, А.М. Коршун, А.И. Сосновский, С.В. Коробенко[1]

ПОДХОД К ПОСТРОЕНИЮ ЗАЩИЩЁННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия
Государственное бюджетное профессиональное образовательное учреждение
Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий», Ростов-на-Дону, Россия[1]

Ключевые слова: инфокоммуникационные сети, it-риск, ущерб, безопасность функционирования инфокоммуникационной сети.

В статье рассматривается подход к оценке безопасности данных в инфокоммуникационных сетях, основанный на том, что центральным элементом возможных угроз безопасности информации является текущее функциональное состояние человека, имеющего доступ к её обработке. Для определения опасности, возникающей при работе человека в инфокоммуникационных сетях, предложено использовать новое выражение для оценки it-риска, основанное на определении текущей эффективности деятельности.

I.A. Sosnovskiy, A.M. Korshun, A.I. Sosnovsky, S.V. Korobenko[1]

APPROACH TO THE CONSTRUCTION OF SECURE INFOCOMMUNICATION COMMUNICATION NETWORKS

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia
State Budgetary Professional Educational Institution of the Rostov Region "Rostov-on-Don College of Radioelectronics, Information and Industrial Technologies", Rostov-on-Don, Russia[1]

Keywords: infocommunication networks, it-risk, damage, safety of functioning of infocommunication network.

The article considers the approach to assessing the security of data in infocommunication networks, based on the fact that the central element of possible threats to information security is the current functional state of a person who has access to its processing. To determine the danger that arises when a person works in infocommunication networks, it is suggested to use a new expression for assessing it-risk, based on determining the current performance of the activity.

Проблема обеспечения безопасности информации является достаточно многогранной. Её рассматривают с различных точек зрения, однако, в данной статье, безопасность информации при эксплуатации инфокоммуникационных сетей (ИКС) будет рассматриваться в контексте работы пользователя, который в текущий момент времени выполняет действия по обработке данных. Его текущая деятельность будет в значительной степени зависеть от двух факторов.

Первым является совокупность знаний и навыков пользователя, необходимых для безопасного выполнения необходимых операций с обрабатываемой информацией. В данной статье, в качестве ограничения, будем считать, что пользователь обладает необходимыми знаниями и навыками по технологии безопасной обработки данных.

Вторым является текущее состояние функциональное состояние (ФС) пользователя. Под ФС понимается текущее психофизиологическое состояние пользователя при выполнении действий по обработке информации. Именно функциональное состояние пользователей, производящих обработку информации в ИКС, является одной из основных причин изменения безопасной технологии работ (выполнения последовательности действий, позволяющей обрабатывать информацию без допущения возможности разглашения информации, её несанкционированного изменения или нарушения её целостности), что приводит к разглашению конфиденциальных данных.

Поскольку раскрытие информации может привести к определённому уровню ущерба, то можно утверждать, что эксплуатация ИКС, сопряжена с определённой долей технологического it-риска.

Рассмотрим одну из возможностей определения технологического it-риска.

В общем случае ИКС можно представить как человеко-машинную систему, в которой в качестве системы выступает оборудование ИКС, находящееся под управлением пользователя. Далее будем придерживаться этой терминологии.

Предположим, что поле деятельности пользователя может быть представлено в виде конечной совокупности последовательностей действий, реализуемых им при обработке информации. В этом случае безопасная работа пользователем ИКС возможна только при наличии у него устойчивых навыков выполнения конечного множества типовых алгоритмов *S*, каждый из которых может быть представлен в виде последовательности $p_j = \{ i_1, i_2, ..., i_l, ..., i_{k_j} \}$ $(j = \overline{1,S})$ типовых действий, набранной из *M* множества типовых действий ($i = \overline{1,m}$), где m - его мощность. При этом любое типовое действие в последовательности p_j характеризуется:

τ_{ji} – максимально допустимой продолжительностью выполнения;

c_{ji} – коэффициентом, запрещающим пропуск и изменение очередности выполнения;

b_{ji} – коэффициентом запрета пропуска при произвольном размещении в очередности;

u_{ji} – коэффициентом, отражающим возможность перестановки или пропуска действия в очередности.

Данные последовательности действий определены технологией проведения работ.

На рисунке 1 представлена в общем виде последовательность действий пользователя ИКС в виде сетевой модели со следующими характеристиками:

n_i^q – номер события в *j*-ой последовательности, где ($n = \overline{1,k_j}$);

q_{ji} – код события из множества Q_j;

$t_{n_i^q}$ – время наступления события.

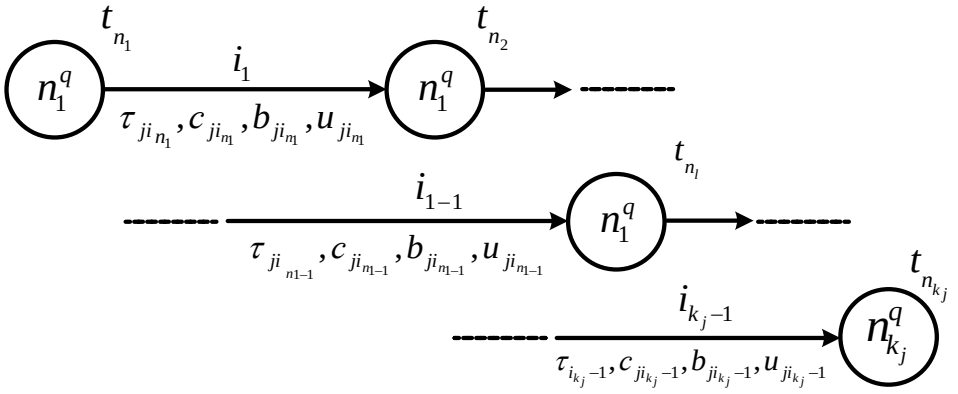


Рисунок 1. Модель оптимальных действий оператора в виде сетевого графа

Модель действий пользователя может быть сформирована при известных исходных данных о последовательностях p_j действий оператора, путем присвоения каждому действию коэффициентов c_{ji}, b_{ji}, u_{ji} и назначения максимально допустимых величин времени на их выполнение τ_{in}, с учетом средней скорости рабочих движений, совершаемых оператором и удовлетворяющих сложившимся требованиям к общему времени выполнения учебной задачи [1-3].

Наличие модели действий, а также назначение коэффициентов τ_{ji}, c_{ji}, b_{ji}, u_{ji} позволяет при реализации пользователем последовательности p_j выявлять отклонения фактических действий от модели действий и на этой основе проводить оценку эффективности действий пользователя в реальном времени по выражению:

$$w(t,\delta) = W^* - \Delta w(t,\delta), \tag{1}$$

где

$$\Delta w(t,\delta) = \max\left[\Delta w_{c_{ji}}, \Delta w_{b_{ji}}, \Delta w_{u_{ji}}\right]. \tag{2}$$

$$\Delta w_{c_{ji}} = \begin{cases} 0, \ при\ n_{c_{ji}} = 0\ ; \\ h_{c_{ji}} W^{\max}, \ при\ n_{c_{ji}} = 1\ ; \end{cases}$$

$$\Delta w_{b_{ji}} = \begin{cases} 0, \ при\ n_{b_{ji}} = 0\ ; \\ h_{b_{ji}} W^{\max}, \ при\ n_{b_{ji}} = 1\ ; \end{cases}$$

$$\Delta w_{u_{ji}} = \begin{cases} 0, \ при\ n_{u_{ji}} = 0\ ; \\ h_{u_{ji}} W^{\max}, \ при\ n_{u_{ji}} = 1\ . \end{cases}$$

В представленных выражениях коэффициенты $h_{c_{ji}}$, $h_{b_{ji}}$, $h_{u_{ji}}$ являются значениями штрафов за допущенные оператором отклонения от модели действий и назначаются с учетом важности *i*-го действия в последовательности p_j, а коэффициенты $n_{c_{ji}}$, $n_{b_{ji}}$, $n_{u_{ji}}$ указывают количество отклонений оператора от модели оптимальных действий.

Таким образом, наличие модели действий пользователя и контроля текущих действий позволяет оценить правильность действий пользователя и определять мгновенную эффективность действий. С учётом допущения о том, что пользователь обладает необходимыми знаниями и умениями работы можно утверждать, что отклонение от модели действий происходит в виду динамики ФС.

Отклонение от модели действий однозначно связано с определённой величиной технологического it-риска. Это обстоятельство позволяет рассматривать величину технологического it-риска как величину, пропорциональную интегралу отклонения в действиях оператора от требуемых по времени функционирования, и зависящую от реализуемого в системе управления состоянием оператора [1,3]

$$R(\delta) = \frac{C}{t_1 - t_0} \int_{t_0}^{t_1} \left[W^* - w(t,\delta)\right] dt \xrightarrow[\delta^*]{} \min, \tag{3}$$

где W^*– максимальное значение показателя эффективности действий оператора;

$w(t,\delta)$ – мгновенная оценка эффективности действий пользователя;

$[t_0,t_1]$ – период функционирования пользователя;

C – максимальная стоимость ущерба от происшествия;

δ – реализуемое в системе управление состоянием пользователя.

Определение величины технологического it-риска возможно на основе мгновенной оценки эффективности.

Таким образом, наличие модели действий делает возможным автоматический расчет мгновенной оценки эффективности каждого действия оператора по выражению (2), подсчет числа отклонений в действиях оператора при реализации одной вводной, а также расчет величины технологического it-риска (3) при ее выполнении.

Рассчитанное значение риска будет отражать текущий уровень опасности при работе пользователя с определённой информацией, посредством доступа к ней через инфокоммуникационную сеть.

Наличие значения риска открывает возможность приступить к построению автоматизированных систем, позволяющих на основе заданных правил принимать решение о прекращении доступа к запрашиваемой оператором информации, а также формировать различные стратегии управления ФС оператора, посредством подбора управляющего воздействия δ.

СПИСОК ЛИТЕРАТУРЫ

1. Сосновский И.А., Манин А.А., Болдырихин Н.В., Коробенко С.В. Подход к оценке IT-рика в инфокоммуникационных сетях связи // Труды Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики». «ИНФОКОМ-2018». - 2018. - № 1. - С. 518-522.
2. Коробенко С.В., Сосновский И.А., Собко В.П. Методика адаптации автоматизированных обучающих систем к индивидуальным особенностям операторов минимуму эксплуатационного технологического риска. Известия Волгоградского государственного технического университета. Серия Актуальные проблемы управления, вычислительной техники и информатики в технических системах. Выпуск №8. 2010 г. №6. С. 56-61.
3. 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. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. «ИНФОКОМ-2017». - 2017. - № 1. - С. 328-335.

В.В. Соболев

ОБЗОР ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ВНЕДРЕНИЯ В НОВЫЕ СФЕРЫ

Краснодарское высшее военное училище, Краснодар, Россия
sobolev.ele.21@yandex.ru

Ключевые слова: распознавание лиц, разграничение доступа, идентификация, биометрические данные.

В данной статье рассматривается достаточно актуальная проблематика – системы по распознаванию лиц. Проанализирована технология распознавания биометрических данных лица и возможность ее внедрения в новые сферы человеческой деятельности.

V.V. Sobolev

REVIEW OF FACIAL RECOGNITION TECHNOLOGIES IN THE FIELD OF INFORMATION SECURITY AND THEIR IMPLEMENTATION IN NEW AREAS

Krasnodar Higher Military School, Krasnodar, Russia
sobolev.ele.21@yandex.ru

Keywords: face recognition, access control, identification, biometric data.

This article discusses a rather topical issue – face recognition systems. The technology of facial biometric data recognition and the possibility of its introduction into new spheres of human activity are analyzed.

Объектом исследования в данной статье является технология распознавания лица. В современном мире технология распознавания лица применяется в различных сферах жизни. Одно из основных применений эта технология получила в области защиты информации. На основе биометрических данных лица, полученных с различных видеокамер, осуществляется разграничение доступа. Многие организации применяют распознавание лица для защиты данных от злоумышленников, которые пытаются их похитить, однако несмотря на это остаются организации в которых данный метод не применяется. Цель данной работы – анализ практики применения метода защиты информации с помощью биометрических данных лица.

Задачи данной статьи:

1. Проанализировать технологию распознавания биометрических данных лица.
2. Рассмотреть практику применения данной технологии.
3. Рассмотреть возможность внедрения данной технологии в инные сферы человеческой деятельности.

В данной работе применяется теоретический метод исследования, состоящий в сборе информации с различных источников и анализе полученной информации.

Распознавание лиц – это одни из наиболее перспективных методов биометрической бесконтактной идентификации человека по лицу. Первые системы распознавания лиц были реализованы как программы, устанавливаемые на компьютер. В наше время технология распознавания лиц наиболее часто используется в системах видеонаблюдения и контроля доступа. Журнал Массачусетского технологического института – MIT Technology Review – включил технологию распознавания лиц в список «10 прорывных технологий 2017 года» [1, 2]. Сегодня функция распознавания лиц используется для обеспечения безопасности информации в телефонах, ноутбуках и других различных информационных объектах. В современном мире технология распознавания лица развивается стремительными темпами. Система распознавания все больше усложняется и совершенствуется. Ряд разработчиков программ утверждают, что уже появились алгоритмы, которые способны даже читать эмоции человека и анализировать эмоциональное состояние. Впервые разработки данной технологии появились еще в 1960-х годах, но именно в последние годы она получила широкое распространение в связи с развитием в области компьютерного зрения и искусственного интеллекта [3].

Система распознавания лиц может быть описана как процесс сопоставления лиц, попавших в объектив камеры, с базой данных ранее сохраненных и идентифицированных изображений лиц эталонов. Если совпадение происходит с определенной точностью, то объект получает доступ к данным. Изображения могут поступать из любых источников, даже из учетных записей в социальных сетях. В целом технология распознавания лица работает следующим образом:

Шаг 1. Обнаружение лица. Камера обнаруживает и фиксирует положение изображения лица. На изображении может быть человек, смотрящий в анфас или в профиль.

Шаг 2. Анализ лица. Выполняется снимок и проводится анализ изображения лица. Большинство технологий распознавания лиц используют 2D, а не 3D-изображения, поскольку 2D-изображения удобнее сопоставлять с общедоступными фотографиями или фотографиями в базе данных. Программа считывает геометрию лица. Ключевые факторы включают расстояние между глазами, глубину глазниц, расстояние от лба до подбородка, форму скул и контуры губ, ушей и подбородка. Цель состоит в том, чтобы определить черты, отличающие данное конкретное лицо.

Шаг 3. Преобразование изображения в данные. В процессе анализа аналоговая информация (лицо) преобразуется в набор цифровой информации (данных) на основе черт лица человека. По сути, анализ лица представляет собой математическую формулу. Цифровой код называется «отпечатком лица». У каждого человека есть свой уникальный отпечаток лица, так же как и отпечатки пальцев.

Шаг 4. Поиск совпадения. Отпечаток лица сравнивается с данными в базе известных лиц. Из всех биометрических систем идентификации распознавание лиц считается наиболее естественным [4].

Технология распознавания лиц используется для самых разных целей, а именно:

1. Разблокировка телефонов. Различные телефоны, включая последние модели iPhone, используют технологию распознавания лиц для разблокировки устройств. Эта технология обеспечивает мощный способ защиты личных данных и гарантирует недоступность конфиденциальных данных в случае кражи телефона.
2. Получение доступа к личным аккаунтам в различных информационных ресурсах. В наше время можно получить доступ к аккаунту, не мучаясь с паролями, логинами и прочими данными.
3. Получение доступа в личные кабинеты. Например, с помощью распознавания лица можно получить доступ к личному кабинету Сбербанк, в котором хранится большое количество конфиденциальной информации.
4. Для подтверждения какого-либо действия. Программа удостоверяется, что действие совершает объект, получивший доступ [5].

Преимущества данного метода состоят в следующем:

- повышенная безопасность – распознавание лиц с помощью биометрии вполне может повышать уровень безопасности. Лицо каждого человека, который приближается или уже находится в определенной (контролируемой зоне), захватывается фиксирующим устройством, таким образом, быстро и эффективно обнаруживается любая личность, которой запрещен доступ в обозначенную зону. В этом случае, распознавание лиц может значительно уменьшить расходы на общую безопасность.
- высокая точность – совокупность применения всех доступных методов (традиционный, трехмерный и текстовый анализ кожи) делает распознавание лиц более точным и результативным.
- полная автоматизация – в настоящее время распознавание лиц является полностью автоматизированным высокоскоростным процессом.
- минимизация компрометации ключевых данных – современные методы делают практически невозможным шанс обмануть систему.
- более высокая надежность в сравнении с другими методами разграничения доступа – на данном этапе развития не один метод не может обеспечить столь высокую надежность разграничения доступа.
- упрощение процесса получения доступа – не надо вводить личные данные (логин и пароль).

Недостатки данного метода состоят в следующем:

- трудности хранения данных – для хранения данных требуется много места. Это означает, что для эффективной работы систем распознавания лиц можно обработать только около 10-25% собранных ими данных. Многие компании вынуждены задействовать большое количество компьютеров для того, чтобы максимально быстро обрабатывать полученные данные. Пока специалистами не найдено оптимальное решение для хранения и обработки таких объемов данных.
- сложность технологии – слишком большие алгоритмы работы, которые очень сложно описать, а также технологии на основе нейронной сети.
- дороговизна комплектующих – технология требует уникальных дефицитных комплектующих.
- идентификация близнецов – из-за слишком большой схожести лиц близнецов система может их путать [6].

Вопросы разграничения доступа наиболее важны в наше время. Злоумышленник может получить информацию о любом человеке, в том числе о первых лицах государства, получить доступ к управлению критически важной инфраструктурой. В мире информационных технологий при получении злоумышленником доступа могут возникнуть проблемы государственных масштабов.

Например, в Вооруженных Силах Российской Федерации вопросы доступа наиболее актуальны, нежели в любой другой сфере. При получении доступа к критически важным объектам информатизации злоумышленник может получить контроль над вооружением, управлением связью, управлением ракетами и прочим. Данный инцидент может повлечь за собой катастрофические последствия. Внедрение данной технологии, как дополнительного контролирующего звена, безусловно, повысит информационную и, как следствие, государственную безопасность. При этом внедрение данной технологии создаст ряд трудностей, а именно:

1. Дороговизна. Внедрение данной технологии требует больших затрат. Начиная с закупок самого программного обеспечения, заканчивая закупкой новых аппаратных частей, которые смогут обеспечить работу данной технологии.
2. Аппаратная составляющая. Не все объекты имеют достаточную производственную мощность.

Таким образом, внедрение данной технологии во многом повысит безопасность данных и упростит контроль доступа: технология распознавания лица после аутентификации будет сама предоставлять доступ и полную информацию, взятую из базы данных. Благодаря распространению технологий распознавания лиц совершенствуется и модернизируется сбор данных, что снижает процент вероятности ошибки информационной системы. Данная технология может значительно повысить надежность разграничения доступа в различных сферах человеческой деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. «10 Breakthrough Technologies2017»[Электронный ресурс]. – Режим доступа: https://www.technologyreview.com/10-breakthrough-technologies/2017/ – Дата доступа: 22.10.2021.
2. «Технология распознавания лиц «А» до Я» [Электронный ресурс]. – Режим доступа: https://securityrussia.com/blog/face-recognition.html – Дата доступа: 22.10.2021.
3. «Технология распознавания лиц: тайная история» [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/netologyru/blog/515090/ – Дата доступа: 22.10.2021.

4. «Что такое распознавание лиц – определение и описание» [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-facial-recognition – Дата доступа: 22.10.2021.
5. «Лицо как ID: 5 примеров использования технологии распознавания лиц» [Электронный ресурс]. – Режим доступа: https://news.rambler.ru/other/38401094-litso-kak-id-5-primerov-ispolzovaniya-tehnologii-raspoznavaniya-lits/ – Дата доступа: 22.10.2021.
6. «Распознавание лиц: как это влияет на вашу конфиденциальность» [Электронный ресурс]. – Режим доступа: https://le-vpn.com/ru/face-recognition-privacy/ – Дата доступа: 22.10.2021.

В.А. Головской[1], М.Ю. Завальцев[2]

К ВОПРОСУ АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСУРСОВ РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище им. генерала армии С.М. Штеменко», Краснодар, Россия[2]

Ключевые слова: робототехнический комплекс, информационный конфликт, конфликтная устойчивость, информационное взаимодействие, безопасность информации.

В работе рассмотрено влияние составляющих сложного информационного конфликта на информационную безопасность защищаемых ресурсов робототехнического комплекса, а также предложены плоскости умозрительного рассечения объекта исследования для проведения всестороннего анализа.

V.A. Golovskoy[1], M.Yu. Zavaltsev[2]

TO THE QUESTION OF ANALYSIS OF INFORMATION SECURITY OF RESOURCES OF A ROBOTECHNICAL COMPLEX

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia
Krasnodar Higher Military School named after S.M. Shtemenko, Krasnodar, Russia

Keywords: robotic complex, information conflict. conflict stability, information interaction, information security.

The paper considers the influence of the components of a complex information conflict on the information security of the protected resources of a robotic complex, and also proposes planes of speculative dissection of the research object for a comprehensive analysis.

ВВЕДЕНИЕ

Актуальной тенденцией развития средств и способов ведения вооруженной борьбы является интенсификация использования робототехнических комплексов специального

назначения (РТК) в вооруженных конфликтах [1]. Под РТК в настоящей статье понимается киберфизическая система, состоящая из следующих подсистем [2]:

- группа выполняющих специальные задачи робототехнических средств (РТС), в общем случае гетерогенных;
- пункт управления, осуществляющий управление и обработку информации;
- система передачи данных (СПД) РТК;
- подсистема обеспечения (информационной безопасности, транспортировки, запуска и т.д.).

В настоящее время вопросы создания интеллектуализированных образцов вооружения и их подсистем активно обсуждаются с различных позиций [3-7]. При этом, как правило, все такие позиции имеют общее место – представление о необходимости учета вопросов информационной безопасности объектов разработки с начальных этапов создания этих объектов. Однако работа [8], показавшая наличие уязвимости в универсальной машине Тьюринга, актуализировала вопрос, о том, на каком этапе создания вычислительной системы необходимо внедрять в неё функции безопасности. Вследствие этого обеспечение информационной безопасности ресурсов РТК в любых условиях обстановки является актуальной научной проблемой. В связи с указанным, целью настоящей работы является анализ взаимосвязи информационной безопасности защищаемых ресурсов РТК и конфликтной устойчивости СПД указанного комплекса, а также выработка предложений по методологии осуществления комплексного анализа предметной области.

Будем полагать, что СПД РТК обеспечивает:

- обмен разнородными данными (информационными, командными и телеметрическими) между РТС и пунктом управления, а также между РТС в РТК;
- ретрансляцию сигналов как для нужд РТК, так и для коалиционных систем и средств, т.е. объединенных в условную «коалицию» согласованными целями функционирования;
- использование своих элементов в качестве датчиков, в том числе, источников информации для других взаимодействующих коалиционных систем.

Анализ литературы [7, 9, 10 и др.] также показывает, что особенностями функционирования РТС в настоящее время являются и будут таковыми оставаться в будущем следующие факторы:

- технологическая ограниченность предприятий промышленности РФ по производству отечественных вычислительных средств;
- наличие этических ограничений;
- наличие жестких ресурсных ограничений (энергетических, структурных и др.), обусловленных автономностью РТС;
- высокая степень интеграции информационных и физических ресурсов РТС.

Последний из рассмотренных выше факторов обуславливает зависимость обеспеченности информационной безопасности ресурсов РТК от такой характеристики СПД как конфликтная устойчивость. При этом необходимо отметить, что СПД РТК при функционировании нельзя отнести ни к открытым системам, ни к замкнутым системам [2].

В условиях активного информационного противоборства будут предъявляться повышенные требования к обеспечению информационной безопасности (ИБ) ресурсов R РТС [2]. Подлежащими защите типами ресурсов РТС являются $R^Z \subseteq R$:

аппаратные $R_{HW}^Z \subseteq R_{HW}$ (средства обработки и накопления информации, средства обеспечения ИБ, датчики и др.);

программные $R_{SW}^Z = R_{SW}$ (средства управления различными системами, средства обработки информации, средства обеспечения ИБ и др.):

информационные $R_{Inf}^{Z} \subseteq R_{Inf}$ (навигационные данные, данные целевой нагрузки, обрабатываемые СПД данные и др.).

Таким образом множество защищаемых ресурсов РТК может быть описано как

$$R^{Z} = \left\{ R_{HW}^{Z}, R_{SW}^{Z}, R_{Inf}^{Z} \right\} \subseteq R \,. \tag{1}$$

В работе [2] было показано, что перспективные РТК будут функционировать в условиях сложного информационного конфликта, под которым понимается одновременное наличие антагонистического $\left(\mathrm{K}_{ant}\right)$, коалиционного $\left(\mathrm{K}_{coal}\right)$ и индифферентного $\left(\mathrm{K}_{ind}\right)$ конфликтов:

$$\mathrm{K}_{comp} = \left\{ \mathrm{K}_{ant}, \mathrm{K}_{coal}, \mathrm{K}_{ind} \right\}, \tag{2}$$

где $\mathrm{K}_{ant} \neq \varnothing$, $\mathrm{K}_{coal} \neq \varnothing$, $\mathrm{K}_{ind} \neq \varnothing$, т.е. каждый тип характеризуется непустым множеством вариантов конфликтных воздействий, имеющих цель нарушить конфиденциальность, доступность и целостность защищаемых ресурсов, т.е.

$$\left\{ \overline{I}(R_{Inf}^{Z}) \cup \overline{A}(R_{Inf}^{Z}) \cup \overline{C}(R_{Inf}^{Z}) \cup \overline{I}(R_{SW}^{Z}) \cup \overline{A}(R_{SW}^{Z}) \right\} \neq \varnothing \,, \tag{3}$$

где $\overline{I}(R_{x}^{Z})$, $\overline{A}(R_{x}^{Z})$ и $\overline{C}(R_{x}^{Z})$ – множество вариантов воздействий, нарушающих целостность, доступность и конфиденциальность защищаемых ресурсов группы x соответственно. Выражение (2) описывает условия формирования сложного информационного конфликта применительно к задачам обеспечения информационной безопасности ресурсов РТС, а выражение (3) ситуацию, при которой были нарушена информационная безопасность ресурсов РТС. Таким образом, сложный информационный конфликт K_{comp}, может быть описан как отношение

$$\mathrm{K}_{comp} : \begin{cases} I(R_{Inf}^{Z}) \to \overline{I}(R_{Inf}^{Z}), \\ A(R_{Inf}^{Z}) \to \overline{A}(R_{Inf}^{Z}), \\ C(R_{Inf}^{Z}) \to \overline{C}(R_{Inf}^{Z}), \\ I(R_{SW}^{Z}) \to \overline{I}(R_{SW}^{Z}), \\ A(R_{SW}^{Z}) \to \overline{A}(R_{SW}^{Z}). \end{cases} \tag{4}$$

В работах [2] были также рассмотрены различные аспекты информационного взаимодействия (ИВ) между СПД РТК, коалиционными и антагонистическими системами, а также средой функционирования СПД РТК, в результате чего был выявлен новый для рассматриваемой области тип информационного взаимодействия – индифферентный, что иллюстрирует рисунок 1.

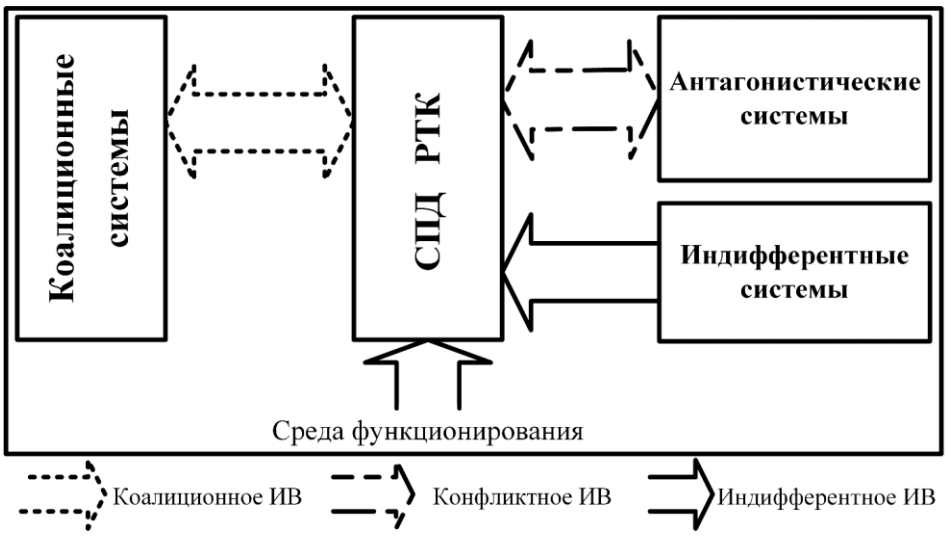


Рисунок 1. Схема информационного взаимодействия

Однако в работе [2] недостаточно внимания было уделено рассмотрению направленности указанных типов информационных взаимодействий. Таблица 1 иллюстрирует предлагаемое описание схемы ИВ между объектами ИВ. В представленной таблице ИВ направлено от объекта в первом столбце (выделенного жирным) к остальным объектам, приведенным в заголовках столбцов со второго по пятый.

Информационные процессы, которые будут возникать при ИВ рассматриваемых объектов с СПД РТК, обуславливают её структурные характеристики. Наличие большого количества ИВ конфликтного типа выводит на первый план такую характеристику СПД РТК, как конфликтная устойчивость. В связи с указанным выше предлагается рассматривать проблематику функционирования РТК в условиях сложного информационного конфликта в нескольких проекциях.

Таблица 1. Схема информационного взаимодействия

Объекты ИВ	СПД	Антагонистические системы	Коалиционные системы	Среда
СПД		Конфликт.	Коалиц.	Индифф.
Антагонистические системы	Конфликт.		Конфликт.	Конфликт.
Коалиционные системы	Коалиц.	Конфликтное		
Среда	Индифф.	Индифф.	Индифф.	

Для обеспечения всестороннего и полного анализа предметной области предлагается умозрительное рассечение анализируемого объекта – СПД РТК – различными плоскостями. В зависимости от рассматриваемой плоскости рассечения может быть использован тот или иной подход к моделированию интересующей стороны, и соответственно, будут выбраны соответствующие указанному подходу средства.

Применительно к рассматриваемому объекту могут быть рассмотрены следующие варианты плоскостей:

1. Плоскость конфликтных взаимодействий, предусматривающая рассмотрение электромагнитной совместимости технических средств, радиоэлектронные борьбу и разведку, криптоанализ, кибернетические воздействия и т.д.
2. Радиоэлектронная плоскость, предусматривающая рассмотрение электромагнитной совместимости как радиоэлектронных, так и технических

средств, радиоэлектронные борьбу и разведку, распространение радиоволн, теорию сигналов, радиолокационные методы обнаружения и др.

3. Информационная плоскость, предусматривающая использование теоретико-информационных подходов – построение энтропийных и информационных моделей, систем массового обслуживания, киберфизическое управление и т.д.
4. Плоскость управления, предусматривающая рассмотрение элементов теорий принятия решений, оптимального управления, автоматического управления, элементы искусственного интеллекта (базы знаний, экспертные системы).

Поскольку любое умозрительное рассечение суть научная абстракция, указанные плоскости могут быть достаточно близки и иметь различные по размеру линии пересечения.

ЗАКЛЮЧЕНИЕ

Разработка эффективной подсистемы информационной безопасности РТК возможна только в комплексе с разработкой информационной системы РТС и СПД РТК. Представленные результаты имеют теоретическую значимость для исследования вопросов построения конфликтно-устойчивых СПД РТК, однако при дальнейших развитии могут быть полезны и для практики при создании рассматриваемых СПД.

СПИСОК ЛИТЕРАТУРЫ

1. *Зарудницкий В. Б.* Факторы достижения победы в военных конфликтах будущего. // Военная мысль. – 2021, №8. – с. 34-47.
2. *Головской В.А., Чернуха Ю.В., Семенюк Д.Б.* Формализация задачи построения системы передачи данных робототехнического комплекса, функционирующего в условиях антагонистической киберэлектромагнитной деятельности. // Вопросы кибербезопасности. – 2019, № 6(34), с.113-122.
3. *Тарасенко С.А.* Формализованная методология исследования специальной техники. - М.: Красная Звезда, 2017. - 367 с.
4. *Чипко В.М., Орлов С.Д., Перцев С.Ф., Тарасенко С.А., Фисенко И.Д.* Формализованная методология при разработке методов исследований технических объектов. / Технологии электромагнитной совместимости. – 2020, № 1 (72), с. 7-17.
5. *Жидков И.В., Зубарев И.В., Хабибуллин И.В.* Выбор рациональной модели разработки безопасного программного обеспечения. // Вопросы кибербезопасности. – 2021, № 5 (45, с. 21-29.
6. *Грибунин В.Г., Кондаков С.Е.* К вопросу о защите информации в интеллектуализированных образцах вооружения. // Вопросы кибербезопасности. – 2021, № 5 (45), с. 5-11.
7. *Кирхеев А. Г., Головской В. А., Мазур Е.В.* Предложения по выбору оптимальной программной конфигурации специальных робототехнических комплексов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть I. – Ростов-на-Дону: СКФ МТУСИ, 2019. – С. 473-477.
8. *Johnson P.* Intrinsic Propensity for Vulnerability in Computers? Arbitrary Code Execution in the Universal Turing Machine [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/2105.02124v1.pdf (дата обращения: 23.10.2021)
9. *Хрипунов С.П., Васильев С.В., Благодарящев И.В.* Методический подход к синтезу интеллектуальной информационно-управляющей системы группового применения робототехнических комплексов военного назначения. // Информационно-измерительные и управляющие системы. – 2017, т.15, № 2, с.16-25.
10. *Макаренко С.И.* Робототехнические комплексы военного назначения – современное состояние и перспективы развития. // Системы управления, связи и безопасности. – 2016, №2, с. 73-132.

Д.А. Жуковский[1], О.А. Решетникова[2]

ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Южный федеральный университет, Ростов-на-Дону, Россия[2]

Ключевые слова: информация, безопасность, конфиденциальность, защита информации.

В статье рассматривается защита информационной безопасности и методы защиты от несанкционированного доступа.

D.A. Zhukovskiy[1], O.A. Reshetnikova[2]

INFORMATION SECURITY PROTECTION

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Southern Federal University, Rostov-on-Don, Russia[2]

Keywords: information, security, confidentiality, information protection.

The article discusses the protection of information security and methods of protection against unauthorized access.

В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

Конфиденциальность – это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

Целостность – имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

Доступность – обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации,

и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней.

Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

Логические средства управления базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

Физический это контроль среды рабочего места и вычислительных средств.

Средства защиты информации делятся на:

Организационные – это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых средств.

Программные – те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.

Технические – это технические виды устройств, которые защищают информацию от проникновения и утечки.

Смешанные аппаратно-программные – это те, которые выполняют функции как аппаратных, так и программных средств.

Виды средств защиты информации:

Антивирусные программы — программы, которые борятся с компьютерными вирусами и возобновляют зараженные файлы.

Облачный антивирус – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

DLP Data Leak Prevention решения – это защита от утечки информации. Предотвращение утечки данных представляет собой набор технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру. Успешная реализация этой технологии требует значительной подготовки и тщательного технического обслуживания. Предприятия, желающие интегрировать и внедрять DLP, должны быть готовы к значительным усилиям, которые, если они будут выполнены правильно, могут значительно снизить риск для организации.

Криптографические системы – преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров Криптография обеспечивает защиту информации и другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Старые, менее безопасные приложения, например, Telnet и протокол передачи файлов, медленно заменяются более безопасными приложениями, такими как Secure Shell, которые используют зашифрованные сетевые коммуникации. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый. Проводные коммуникации защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.

Информация очень важна для успешного развития бизнеса, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое информационная безопасность https://habr.com/ru/post/527094/ (дата обращения 20.10.2021).
2. Контроль информационной безопасности https://pirit.biz/reshenija/informacionnaja-bezopasnost (дата обращения 21.10.2021).
3. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.
4. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.
5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.
6. Бабаш, А.В. Криптографические методы защиты информации: Учебное пособие: Т.1 / А.В. Бабаш. - М.: Риор, 2018. - 48 с.

Д.А. Жуковский, И.А. Казачанский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: ПО, угрозы, безопасность, мобильные устройства, данные, приложение.

В статье рассматривается мобильные угрозы и методы борьбы с ними.

D.A. Zhukovskiy, I.A. Kazachanskiy

MOBILE OYSTERS INFORMATION SECURITY

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

Keywords: software, threats, security, mobile devices, data, application.

The article discusses mobile threats and methods of combating them.

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий. В связи с этим возникает задача систематизировать основные угрозы и уязвимости мобильных приложений для последующего формирования методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

Рынок вирусов для мобильных устройств вырос и усложнился. Мобильным устройствам угрожают уже не только относительно безобидные трояны-кликеры, но и полноценные вирусы и шпионское ПО. Большинство вирусных исследовательских компаний выделяют следующие виды угроз.

Для данного вида угроз как Adware и кликеры используется термин Madware. Основная цель этого класса ВПО – показ пользователю нерелевантной рекламы и генерирование искусственных переходов на сайты рекламодателей. С помощью Madware злоумышленники зарабатывают клики и демонстрируют оплачивающим их компаниям иллюзию интереса пользователей.

Spyware – ПО, осуществляющее кражу персональных данных или слежку за своим носителем. Фактически, мобильное устройство может превратиться в полноценное устройство слежки, передавая злоумышленникам данные о сетевой активности, геолокации, истории перемещений, а также фото и видеоинформацию, данные о покупках, кредитных картах и др.

Дроппер – ВПО, целью которого является скачивание другого вредоносного ПО.

Вирус – ПО, которое наносит явный вред, например, выводит из строя конкретное приложение или одну из функций устройства.

Бот – агент бот-сетей, ВПО, которое по команде C&C-сервера осуществляет требуемую злоумышленнику сетевую активность.

Мобильные устройства также подвержены и традиционным атакам, так как используют те же базовые пользовательские сервисы, что и персональные ПК.

На основе анализа описанных примеров мобильного ВПО, а также каналов проникновения других образцов ВПО можно выделить следующие основные пути компрометации устройства:

Установка пакета приложений APK из неофициальных маркетов.

Установка зараженного приложения из официального магазина. В данном случае, после обнаружения зараженного приложения службой безопасности магазина, оно будет оперативно удалено, а установленное пользователями приложение будет обновлено на безопасную версию.

Фишинг и социальная инженерия – SMS, MMS с привлекательными для жертвы вредоносным контентом или ссылкой. Или звонок от ложного оператора связи или служащего банка с требованием передать учетные данные. Известны несколько нашумевших случаев добровольной установки пользователями программы удаленного управления TeamViewer. После установки программы пользователи передавали злоумышленникам учетные данные для удаленного управления, что равнозначно передаче разблокированного телефона в чужие руки.

Для снижения риска заражения мобильного устройства и утечки конфиденциальной информации необходимо реализовать следующие методы защиты: Шифрование данных на устройстве.

Шифровать можно отдельные папки, данные приложений или все устройство целиком. По возможности, необходимо использовать аппаратные платы шифрования и хранения ключевой информации.

Защита сетевого трафика: шифрование канала передачи данных, использование внешних фильтрующих решений для очистки трафика. Использование корпоративного

шлюза, сканирующего web и email-трафик, или использование облачных решений очистки трафика от ВПО.

Обнуление данных на скомпрометированном устройстве. Уничтожение всех данных или данных отдельного корпоративного приложения при утере или краже мобильного устройства.

Обнуление может быть реализовано по удаленной команде или после нескольких неудачных попыток аутентификации.

Использование приложения с изолированным контейнером для хранения данных, которое, как правило, выполняет шифрование данных, контроль их целостности, изоляцию данных приложения в оперативной памяти, запрет копирования данных, удаленное уничтожение данных.

Контроль установленных приложений, вплоть до составления белого списка разрешенных приложений, контроль их целостности. Контроль целостности приложений при запуске устройства.

Использование двухфакторной аутентификации: желательно использовать дополнительные средства аутентификации, в частности, сканирование отпечатка пальца. Необходимо иметь в виду, что некоторые биометрические способы аутентификации пока не очень надежны, например, распознавание лиц. Аутентификация путем ввода кода из СМС в современных условиях многими экспертами также признается недостаточно ненадежной.

Своевременная регулярная установка обновлений ОС, приложений, драйверов. При этом важно использовать официальные источники ПО.

Антивирусная защита: регулярное сканирование системы, файлов, приложений. Сканирование приложений перед их установкой. Вслед за развитием мобильных технологий, растет количество и разнообразие ВПО, нацеленного на мобильные устройства. Для снижения риска заражения вредоносным ПО, обеспечения защиты от утечек конфиденциальных данных и минимизации ущерба в случае потери физического контроля над устройством рекомендуется также использовать специализированные средства защиты – антивирусы, решения класса MTM, а также корпоративные решения классов UEM, MDM, EMM

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. - СПб.: СПбГУ ИТМО, 2010. - 98 с.
2. Безопасность мобильных приложений https://cyberleninka.ru/article/n/bezopasnost-mobilnyh-prilozheniy (дата обращения 22.10.2021).
3. Безопасное использование мобильных приложений https://www.securitylab.ru/blog/personal/bezmaly/351037.php (дата обращения 23.10.2021).
4. Мобильные угрозы и методы борьбы с ними https://www.securitylab.ru/analytics/501302.php (дата обращения 23.10.2021).
5. Проблемы защиты информации в приложениях для мобильных систем https://cyberleninka.ru/article/n/problemy-zaschity-informatsii-v-prilozheniyah-dlya-mobilnyh-sistem (дата обращения 23.10.2021).
6. Михайлов Д. М., Жуков И. Ю. Защита мобильных телефонов от атак; Фойлис - Москва, 2011. - 192 с.

А.Н. Иванов, С.А. Швидченко

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ ВУЗА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: вирусы, Операционная система (ОС), антивирусы, Kaspersky, взломы.

В этой статье мы рассматриваем антивирусы и почему нужны нам антивирус в той или иной системе, которая используется и рассматриваем антивирус, установленный на ОС в университете.

A.N. Ivanov, S.A. Shvidchenko

ANALYSIS OF INFORMATION SECURITY OF UNIVERSITY OPERATING SYSTEMS

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

Keywords: viruses, Operating system (OS), antiviruses, Kaspersky, hacking..

In this article we are considering antiviruses and why we need an antivirus in a particular system that is used and we are considering an antivirus installed on the OS in the university

“Одной из важнейших функций антивирусной программы является обнаружение угрозы в компьютерной системе. Как только вирус найден, программное обеспечение обычно информирует пользователя об его выявлении.”[1]

В университете установлены три ОС Windows 7,XP и для сервера Windows Server 2019.На данный момент современная ОС является Windows 10 на которую на данный момент вышло и будет выходить обновления,так как используется Windows 7 и XP то требуется для безопасного использования антивирусы, например:

Kaspersky (имеет разные вариации например для бизнеса Kaspersky Security Center)

Dr.Web (тоже имеет разные вариации и каждый по свойму работает есть переносная версия а есть версия для обычного пользователя и для компании)

ESET NOD32 (имеет разные вариации в качестве антивируса используют в основном его)

В каждой ОС установленных в университете есть антивирус Kaspersky Security Center- централизованная консоль управления, которая позволяет управлять безопасностью устройств в сети и автоматизировать защиту рабочих мест.В Kaspersky Security Center установлен свой протокол безопасности GPO позволяющее защитит от вирусов сервер и компьтеры в кабинете так же и защитить сервер от внешних атак.

Kaspersky используется в различных учебных учереждения например:ДГТУ или СКФ МТУСИ. Kaspersky был создан в России и входит в русское ПО как основной антивирус для обезопашивания ОС в разных Российских учереждениях.Так же есть закон об обязательном русском ПО на разных устройства таких как компьютер, смартфон, телевизор и тд. Kaspersky делает персональное предложение для каждого учреждения по другой цене отличающееся на сайте. Kaspersky имеет обширную базу данных про вирусов или как их искать по коду или другим проявлениям.

Многие учереждения сталкивались с атаками ради получений личных данных или других инных вещей например: поставили плохую оценку и эта оценка отправляется на сервер где хранятся и другие данные пароли и тд. и надо проникнуть в систему но неизвестно каких либо данных от системы и не известно как туда проникнуть и подключиться и приходится пользоваться различными программами или пользоваться другой ОС для взлома например можно взломать сеть Wifi через Linux,Linux имеет открытый код чтоб сделать сборку нужного для взлома или для работы, для взлома использовать могут VPN чтоб сбить где след и так же используется специальное программное обеспечение для взлома. Так же пытаются взламывать компьютера через смартфон который используется всегда, есть множество программ но через программы обычно взламывают только Wifi чтоб получить доступ к данным и удалённо передать их или просто чтоб что-то закачать. Из-за чего многим учереждением приходится устанавливать антивирусное программное обеспечение чтоб обезопасить от взлома из вне. И учебные учереждения предпочитают Kaspersky в виде основного и главного антивирусного программного обеспечение. Бывают взломы извнутри попадают на флешку и заражают компьютер и от заражённого пк идёт по всей сети если не обеспечить во время защиту то могут взломать и оставить дыру в системе через которую будут утекать различные данные.

Бывают вирусы, которые могут не улавливать или устанавливать на компьютер вместе с программой, например майнер. В основном вирусы передаются через заражённые файлы или программы, которые находятся на флешке и чтоб защитить используется антивирус. Kaspersky используется от вирусов например: вирусов, черви, программы-вымогатели, шпионское по, руткитов, троянов, шпионских программ и тд.

“Угроза вредоносного кода на вычислительное устройство пользователя при работе с ресурсами сети Интернет, в большей степени, проявляется «слабым звеном» механизмов как внутреннего, так и внешнего сетевого трафика, а также ослаблением антивирусного мониторинга пользователя (как в индивидуальном (личном) аспекте), так и организации пользователя в целом.”[2]

Вирус-Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах.Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты.

Червь-В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы, и затем процесс начинается снова. Помимо того, что многие черви просто «съедают» системные ресурсы, снижая тем самым производительность компьютера, большинство из них теперь содержит вредоносные «составляющие», предназначенные для кражи или удаления файлов.Есть червь которые на данный момент представляет угрозу.

Троян-Более известные как троянцы, эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

Майнер-Криптовалютная лихорадка стала настоящей проблемой для пользователей компьютеров. Во-первых, майнинг истощил рынок видеокарт, игровых приставок и даже некоторых компонентов для сборки автомобилей. Во-вторых, компьютеры теперь страдают из-за нового типа атак — криптовалюта добывается не только на специальных фермах, но и на системах обычных пользователей.Из-за чего страдают обычные пользователи. К троянскому сорту компьютерных вирусов также относятся и майнеры. В отличие от

классических троянов, новые зловреды рассчитаны на распространение среди систем частных пользователей — им не нужна информация, пароли и данные кредитных карт. Эти вирусы интересуются только аппаратными возможностями компьютера — они майнят криптовалюту. Несмотря на то, что вирусы-майнеры не занимаются кражей информации и паролей, вред от них может быть куда более масштабным, чем от обычных вирусов. Для эффективной добычи криптовалюты компьютеру необходимо задействовать как можно больше мощности, поэтому «зараженный» работает одновременно на двух фронтах — например, добывает валюту на процессоре и видеокарте, а также с помощью накопителя. И даже непродолжительная работа системы в таком режиме может привести к перегреву компьютера или выходу комплектующих из строя [3,4]. Это может сказаться на результат вычислительных операций, проводимых при обработке данных, например обработке сигналов и изображений на базе вейлет-преобразований [5,7] и при обеспечении безопасности в неоднородных системах обработки данных [6].

На данный момент создаются большее количество вирусов и из-за чего постоянно обновляется база вирусов. От некоторых вирусов не может быстро среагировать так как вирус встраивается в систему и становится нейтральной для антивируса, и он не может обнаружить, например, как майнер. “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” [3]

Самые опасные вирусы:

- ILOVEYOU – 2000 год;(присылал сообщение в виде ILOVEYOU, при его открытие рассылал всем из контактного листа);
- Nimda – 2001 год;(он поражал не только компьютеры обычных пользователей, но даже и серверные части под управлением Windows NT и 2000, которые на тот момент обладали достаточно мощной защитой. Он проникал на жесткий диск посредством рассылки через электронные почты. Объектами заражения становились порталы в Интернете, которые не обладали необходимой системой защиты);
- SQL Slammer/Sapphire – 2003 год (результате его атаки отключились сети экстренных служб, обрушились многие хосты, а также исчез доступ к Интернету на атомной электростанции в штате Огайо, США);
- Sasser – 2004 год (после инфицирования одного устройства червь получал доступ к Интернету и искал компьютеры с уязвимостью, через которую мог попасть туда. Особого вреда и пакостей вирус не причинял – он всего лишь пускал компьютер в бесконечный цикл перезагрузок);
- Storm Trojan – 2007 год (создавал свою сеть для совершение мощных атак на сервера);
- Conficker – 2008 год (использовал уязвимости операционных систем и отключал множество служб, в их числе и безопасности);
- Wannacry – 2017 (шифрует подавляющее большинство хранящихся на жестком диске файлов, после чего блокирует компьютер и выводит окно с требованием выкупа);
- Petya – 2017 (похож на Wannacry не блокирует отдельные файлы а блокирует целый диск).

Это самые опасные вирусы, которые встречались и, которые принесли много проблем пользователям ПК, но на каждого из них нашли способ защиты, в связи с чем необходимо обновлять антивирусное программное обеспечение.

СПИСОК ЛИТЕРАТУРЫ

1. *Д.А. Земляная,* Н.В. Болдырихин, Е.М. Шипшова Анализ методов обнаружения вирусных сигнатур // Информационная Безопасность. Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2020) » стр.336-342
2. *М.Г. Гизатуллин,* В.А. Цепаев Некоторые аспекты реализации вредоносного кода на вычислительное устройство пользователя при работе с ресурсами в сети интернет // Информационная Безопасность. . Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2019) » стр.478-481
3. Б.П. Борисов, А.И. Янкина Анализ аппаратных средств защиты информации в сетях передачи данных // Состояние и перспективы развития инфокоммуникаций. Сборник «Труды Северо-Кавказского филиала Московского технического университета связи и информатики (2017) » часть 1 стр.39-43.
4. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство проектирования однозоновой сети транкинговой связи для ее оперативного развертывания. Свидетельство о регистрации программы для ЭВМ 2021610521, 14.01.2021. Заявка № 2020665716 от 03.12.2020.
5. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.
6. *Безуглов Д.А.,* Швидченко С.А. Синтез общей модели обеспечения безопасности для неоднородной системы обработки данных. В сборнике: Системный анализ, управление и обработка информации. труды X Международной научной конференции. 2020. С. 109-114.
7. *Швидченко С.А.* Анализ обеспечения безопасности информации в АСУ. - В сборнике: Актуальные аспекты развития воздушного транспорта (Авиатранс-2018). Материалы международной научно-практической конференции. 2018. С. 257-262.

В.А. Ландышев[1,2], О.Н. Ландышева[3]

ВОПРОСЫ ОБЕСПЕЧЕНИЯ УДАЛЕННОГО ДОСТУПА СОТРУДНИКОВ К ИНФОРМАЦИОННЫМ СИСТЕМАМ ВУЗА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет», Ростов-на-Дону, Россия[2]
Институт водного транспорта имени Г.Я. Седова - филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный морской университет имени адмирала Ф.Ф. Ушакова» Ростов-на-дону, Россия[3]

Ключевые слова: Удаленная работа, работа в режиме самоизоляции, QOVID 19.

В настоящей работе рассмотрена реализация защищенного удаленного доступа учебного и учебно-вспомогательного персонала к локальным вычислительным ресурсам ВУЗа в период пандемии QOVID 19.

V.A. Landyshev[1,2], O.N. Landysheva[3]

ISSUES OF PROVIDING REMOTE ACCESS OF EMPLOYEES TO THE INFORMATION SYSTEMS OF THE UNIVERSITY

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Federal State Budgetary Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia [2]
Institute of Water Transport named after G.Ya. Sedov - a branch of the Federal State Budgetary Educational Institution of Higher Education “State Maritime University named after Admiral F.F. Ushakova »Rostov-on-Don, Russia [3]

Keywords: Remote work, self-isolation mode, QOVID 19.

This paper considers the implementation of secure remote access of educational and educational support personnel to the local computing resources of the university during the QOVID 19 pandemic in accordance with the requirements of the legislation of the Russian Federation.

Учебный процесс в высших учебных заведениях в 2020 году столкнулся с новым неожиданным вызовом, а именно пандемией короновирусной инфекции, в связи с чем в организациях Минобрнауки с 16 марта 2020 г. введены следующие меры борьбы с распространением новой инфекции:

- контроль температуры при входе в здания;
- установка в зданиях средств дезинфекции;
- ограничение проведения очных совещаний и направления работников в служебные командировки;
- перевод работников на удаленный режим работы при необходимости [1].

Наиболее сложной с точки зрения информационной безопасности задачей явилось массовое подключение пользователей, находящихся на удаленном режиме работы к ресурсам локально вычислительной сети ВУЗа.

Если в предыдущие периоды времени доступ к ресурсам локальной вычислительной сети извне требовался ограниченному количеству сотрудников, то после массового ухода сотрудников на “удаленку” задача стала актуальна для десятков и сотен сотрудников, относящихся как к учебному, так и учебно-вспомогательному персоналу.

К основным проблемам реализации удаленного подключения в текущих условиях следует отнести:

- Фактическое отсутствие сотрудников в организации, невозможность личной передачи парольной ключевой информации;
- Сложность установки клиентского программного обеспечении в связи с тем, что установка планировалась с использованием разнородных программно-аппаратных платформ;
- Различный уровень технической подготовки пользователей от гуманитариев до технических специалистов.

Значительные технические трудности составляет необходимость соблюдения требований регуляторов в применении сертифицированных средств криптографической защиты информации данное требование определено в [2]. Актуальность этого обусловлено тем что практически все системы управления учебным процессом могут быть классифицированы как информационные системы персональных данных.

В настоящее время основные клиентские операционные системы не содержат встроенных крипто провайдеров, поддерживающих алгоритмы ГОСТ Р 34.11-2012 их надо приобретать отдельно или использовать специализированные программные клиенты

самостоятельная установка которых пользователями представляет из себя достаточно сложный процесс.

Выводы:

1. Реализация удаленного доступа для большого количества сотрудников в короткий промежуток времени является сложной административно технической задачей.
2. Реализация удаленного доступа требует наличия альтернативного канала передачи парольной-ключевой информации использовались группы в мессенджерах и электронная почта сотрудников.
3. Реализация защищенного подключения с использованием сертифицированного оборудования требует дополнительных финансовых затрат и настроек оборудования у конечного пользователя А при отсутствии необходимых средств делает требование регулятора нереализуемым в настоящих условиях.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Министерства науки и высшего образования РФ от 14 марта 2020 г. № 398 “О деятельности организаций, находящихся в ведении Министерства науки и высшего образования Российской Федерации, в условиях предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации”
2. "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности" (утв. ФСБ России 31.03.2015 N 149/7/2/6-432)

Л.В. Черкесова, А.И. Ревякин, Е.А. Ревякина

АНАЛИЗ ВОЗМОЖНЫХ РЕШЕНИЙ ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОМУ КОНТЕНТУ

Донской государственный технический университет,
Ростов-на-дону, Россия

Ключевые слова: информационная безопасность, Деструктивный сайт, кибербуллинг, деструктивный текстовый контент, информационная защищённость детей и подростков, Web–программирование, браузер.

В статье рассмотрены основные возрастные особенности использования сети Интернет детьми и подростками. Всё большее распространение получает подключение к сети по высокоскоростным каналам, что позволяет им проводить в сети Интернет почти всё своё свободное время. Все острее встает проблема обеспечения их безопасности в Web–пространстве.

L.V. Cherkesova, A.I. Revyakin, E.A. Revyakina

ANALYSIS OF POSSIBLE SOLUTIONS TO COUNTER DESTRUCTIVE CONTENT

Don State Technical University, Rostov-on-Don, Russia

Keywords: information security, Destructive website, cyberbullying, destructive text content, information security of children and adolescents, Web programming, browser.

The article discusses the main age-related features of the use of the Internet by children and adolescents. Connection to the network via high-speed channels is becoming increasingly widespread, which allows them to spend almost all their free time on the Internet. The problem of ensuring their security in the Web space is becoming more acute.

В современных условиях развития информационных технологий, а также их интеграции с повседневной жизнью каждого человека возрастает важность такого направления государственной политики, как противодействие негативному влиянию на население в информационной сфере.

Информационная сфера – это совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [1].

Главная цель информационного воздействия является подрыв духовного мира человека, их ценностей и нравственности. Для этого предпринимаются меры по изменению ценностных установок личности и их замене, создается атмосфера бездуховности и безнравственности. Применяются различные приемы – от манипулирования общественным мнением до пропаганды чуждой идеологии. Больше всего информационному влиянию подвержены молодые люди в связи с их неопытностью.

Молодежь – социально-возрастная группа, которой присуще неполное включение в социально-экономические отношения. Она отличается высокой мобильностью, инициативностью и интеллектуальной активностью.

Антироссийским содержанием наполняются различного рода развлекательные программы, реклама, ток-шоу, контенты в социальных сетях, блоги и даже онлайн-игры. К сожалению, именно это сфера – сфера формирующегося сознания молодого поколения – долгое время оставалась без внимания государственных и общественных структур и была, по сути, отдана на откуп различного рода антироссийским организациям как внутри страны, так и за ее пределами. Наши же отечественные информационные ресурсы далеко не всегда эффективно противодействуют негативному информационному воздействию. Особенно это касается компаний и структур кинопроката и телевещания, руководство которых в погоне за рентабельностью фактически перестали исполнять миссию общественно-полезного блага, что противоречит не только интересам государства и общества, но и опыту ведущих зарубежных стран.

В результате игнорирования контроля развлекательной сферы государством у молодого поколения происходит размывание традиционных российских духовно-нравственных ценностей, нарушается способность к эмпатии. В следствии чего начали происходит инциденты, которые раньше невозможно было представить - нападение учеников на школу. Первый случай стрельбы в школе, которую устроил ученик, был зафиксирован 3 февраля 2014 года. С этого дня и до 19 января 2018 года в России зафиксировано минимум 15 случаев стрельбы и семь конфликтов с использованием колюще – режущих предметов [2]. Данные преступления опасны тем, что эти они являются

довольно редкими, вследствие чего правоохранительные органы не в силах предугадать, где и когда может произойти подобный инцидент.

Помимо этого, информационным воздействием подвергается история. Так происходит фальсификация значимых исторических событий для России. Данное влияние происходит путём исключения каких-либо позитивных ассоциаций, связанных с историей своей страны, ее современным состоянием, целями и задачами эффективного развития. Наиболее отчетливо это прослеживается в попытках фальсификации истории и итогов Великой Отечественной и Второй мировой войн, целью которых является не только принижение роли СССР в победе над нацистской Германией, но и фактическое уравнивание его в ответственности за жертвы этих войн. Стоит напомнить, что советский союз понес самые большие потери среди стран участников Второй мировой войны, более 25 миллионов человек. Так же происходит навязывание исторических стереотипов, таких как поголовное пьянство населения, варварство России, отставание от развитых стран. Данные действия совершаются с целью принуждения к забвению исторической памяти, формирования образа страны-агрессора, навязывания безразличия к интересам общества и государства [3].

Наиболее значимое направление негативного информационного воздействия на сознание российской молодежи заключается в дискредитации органов государственной власти; противопоставлении общества и государства, граждан – институтам государства; воздействии на политическую ориентацию активных гражданских слоёв в интересах создания напряженности в политической обстановке; дестабилизации политических отношений между объединениями, движениями и партиями с целью провокации конфликтов, разжигании атмосферы недоверия и подозрительности; провоцировании репрессий и насильственных действий против оппозиции; дискредитации органов управления в глазах населения, подрыв их авторитета; дезинформации населения и инициировании забастовок, массовых беспорядков и других протестных акций; провоцировании социальных, политических, национальных и религиозных столкновений, развязывании в обществе гражданской войны [4].

Наиболее ярким примером такого воздействия являются события, получившие название «арабской весны» и приведшие к смене политических режимов в Египте и Тунисе. С помощью дезинформации в социальных сетях удалось собрать критическую массу людей и направить её против действующего режима. Такой же сценарий произошёл на Украине, где в результате массовых беспорядков было свергнуто законное правительство, вследствие чего в стране наступила разруха и война. Подобные методы воздействия на массы применяют и в России с целью её дестабилизации и смены власти. Правительством применяются необходимые меры по защите целостности государства. На данным момент политическая обстановка держится под контролем.

Так в феврале 2020 года Пензенский суд вынес приговор о дело об террористической организации под названием «Сеть», ячейки которой существовали в Москве, Санкт-Петербурге, Пензе, Омске и Белоруссии. Семь обвиняемых были приговорены к наказаниям от 6 до 18 лет лишения свободы [5]. Данная организация собиралась провести теракты, приуроченные к выборам президента и чемпионату мира по футболу, — и тем самым дестабилизировать обстановку в стране. Несмотря на все собранные доказательства и признание вины самих обвиняемых правозащитники и журналисты настаивают на их невиновности. Стоит обратить внимание на расследование издании «Медуза» связанное с возможным убийством фигурантами дела «Сети» [6]. Оно только подтверждает радикальность данной организации. Другим примером негативного влияния на политическую обстановку является дело «Нового величия» - дело о создании экстремистского сообщества, целью которого было захватить власть в России путём государственного переворота [7]. Помимо создания террористических организаций информационные атаки в политическом направлении влекут за собой массовые беспорядки. Примером этого может служить «Московское дело», где несогласованный митинг в центре

Москвы перерос в массовые беспорядки и насилие в отношении представителей органов власти.

Более опасным способом информационного воздействия на граждан являются радикальные экстремистские структуры, то есть террористы. Терроризм представляет собой систематическое социально или политически мотивированное, идеологически обоснованное применение насилия либо угрозы применения такового, посредством которого через устрашение физических лиц осуществляется управление их поведением в выгодных для террористов направлении и достигаются преследуемые террористами цели.

Террористически организации используют Интернет в связи с легкой доступностью к аудитории, обеспечения анонимности общения и отсутствия контроля на государственном уровне. За счёт психологического воздействия через дезинформацию, запугивание, манипуляцию общественным сознанием оказывает сильное воздействие на личность, ломая ее под влиянием столь неожиданной информации. Вербовщиками навязывается простая система взглядов, обещающая быстрый результат, достигнутый своими агрессивными действиями. Происходит подмена примитивными призывами к полному разрушению существующих устоев.

Среди всех террористических организаций наибольшую активность в этом плане проявляет ИГИЛ (запрещенная в России террористическая организация). Исламское государство занимающегося вовлечением в свои ряды российских граждан мусульманского вероисповедания, с тем чтобы в последующем с их помощью инициировать вооруженные мятежи уже на территории РФ. Несмотря на антитеррористическую работу ФСБ, данные инциденты всё равно происходят с некой периодичностью. Так 23 октября произошёл захват заложников на Дубровке в Москве. В здание Театрального центра, где шло представление популярного мюзикла "Норд-Ост", ворвалась вооруженная группа из 40 боевиков и взяла в заложники 912 человек, в том числе женщин и детей. На четвёртый день удержания заложников произошёл штурм, в результате которого были ликвидированы все террористы. Жертвами теракта стали 130 заложников. Более кровавый теракт произошёл 1 сентября 2004 года. В результате захвата террористами бесланской школы № 1 в заложниках оказались более 1200 человек. Погибли и позднее скончались от ранений 334 человека, 186 из них - дети. Инвалидами стали 126 бывших заложников, 70 из которых - дети [9].

Это далеко не весь список терактов, выше приведены только самые известные. Он показывает, насколько важна информационная безопасность и какие последствия ожидают за игнорированием данного направления.

Для защиты от информационной агрессии граждан, и особенно молодежи, используется цензура, блокировка сайтов, так же принят закон Яровой и закон о «суверенном интернете». Несмотря на все попытки обезопасить население от негативного информационного влияния в России до сих пор не отлажено правовое регулирование информационной безопасности детей и молодежи. В связи с этим обеспечение информационной безопасности данной группы наиболее значимая задача.

Исходя из опасностей можно выделить следующие риски онлайн–среды. Они разделяются на четыре типа: контентные, коммуникационные, электронные и потребительские.

Контентные риски – это различные материалы (тексты, картинки, аудио и видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. Столкнуться с ними можно практически везде: социальные сети, блоги, торренты, персональные сайты, видеохостинги и др.

Коммуникационные риски связаны с общением и межличностными отношениями интернет-пользователей. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, груминг), знакомства в сети, встречи с опасными интернет–знакомыми и др.

Электронные риски – это вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ. Вредоносные программы представляют собой различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации.

Потребительские риски – это злоупотребление в интернете правами потребителя. Они включают в себя риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию, потерю денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества и др.

В наших силах разработать интеллектуальные информационные системы – мониторинги безопасности, которые смогут контролировать деструктивный контент, выкладываемый в сеть.

Обеспечение безопасности детей и подростков является задачей повышенной актуальности. Для её решения необходимо разработать специальное программное обеспечение, а именно монитор безопасности, позволяющий просматривать, анализировать и блокировать деструктивный Web–сайт с вредоносным контентом ещё до его загрузки на компьютер юного пользователя, а также помогающий родителям контролировать увлечения своих детей.

Задачу анализа текста на Web–сайтах рассматривали многие российские и зарубежные авторы, среди которых Barakhnin V.B., Mukhamedyev R.I. (в работе «Methods to identify the destructive information»), Воронина И.Е., Гончаров В. А. (в работе «Анализ эмоциональной окраски сообщений в социальных сетях (на примере сети «В_Контакте») , Gostyunina V.A., Davidyuk N.V. (в работе «The combined method of textual information analysis for the content of destructive indicators»), Байдулова Д.Р., Гостюнина В.А., Давидюк Н.В. (в работе «Применение машинного обучения в процессе поиска деструктивной информации в web-контенте»), Браницкий А.А., Дойникова Е.В., Котенко И.В. (в работе «Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям») и многие другие авторы [8].

Целью данного исследования является разработка программного обеспечения – монитора безопасности, предназначенного для родителей детей и несовершеннолетних подростков, способного защитить юных пользователей от деструктивного влияния Web–сайтов с вредоносным контентом, представляющих угрозу их психологической защищённости.

Объектом исследования является Интернет–ресурсы, содержащие деструктивный текстовый контент, угрожающий психологической безопасности детей и несовершеннолетних подростков. Предметом исследования является алгоритмы анализа текстового контента Web–сайтов и методы блокирования таких сайтов до из загрузки на компьютер юного пользователя. Подобные программные средства в мире существуют. Среди них нужно прежде всего назвать программные продукты: KinderGate, KidShell, Kaspersky и другие.

В процессе работы, авторами этой статьи были изучены возрастные особенности использования Интернета детьми и несовершеннолетними подростками, выявлено негативное влияние социальных сетей на психику детей и подростков, исследована классификация рисков и угроз, возможных при отсутствии родительского контроля, проведен анализ защиты детей и подростков на правовой основе. Существующие Интернет–риски способны принести непоправимый ущерб эмоциональному благополучию и психологическому здоровью ребенка или несовершеннолетнего подростка, и поэтому требуют со стороны родителей тщательного анализа и нивелирования.

На основе этого анализа была выбрана технология разработки программного средства в виде браузерного расширения, разработаны основные модули и алгоритмы для работы с сетевыми ресурсами, и создано ПО для осуществления родительского контроля за

поведением детей и несовершеннолетних подростков в сети Интернет, с целью их защиты от деструктивного и опасного влияния Web–сайтов, представляющих угрозу их психологической, нравственной и моральной защищённости.

Выяснено, что существующие программные приложения, в основном, созданы за рубежом, и могут использоваться в России только при подключении платных версий. Кроме того, они, как правило, имеют англоязычный интерфейс и трудный в настройке функционал, непонятный многим российским родителям, тем более, не связанным по своей профессии с информационными технологиями. В то же время, импортозамещающий монитор безопасности, планируемый для разработки, является совершенно бесплатным и очень простым в использовании.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 31.07.2020) "О защите детей от информации, причиняющей вред их здоровью и развитию".
2. *Атагимова Э.И.* Проблемы отрицательного влияния Интернета на нравственное воспитание подростков в информационном пространстве и пути решения // Правовая информатика. 2013. № 1. С. 21–24.
3. *Barakhnin V., Mukhamedyev R., Mussabaev R., Kozhemyakina O., Issayeva A.,* et al. Methods to identify the destructive information // Journal of Physics: Conference Series, 2019.
4. *Воронина И. Е., Гончаров В. А.* Анализ эмоциональной окраски сообщений в социальных сетях (на примере сети «В_Контакте») // Компьютерная лингвистика и обработка естественного языка. 2015. № 4. С. 151 –158.
5. *Gostyunina V.A., Davidyuk N.V.* The combined method of textual information analysis for the content of destructive indicators // Journal of Physics: Conference Series. 2019. DOI: 10.1088/1742-6596/1399/3/033109.
6. *Байдулова Д.Р., Гостюнина В.А., Давидюк Н.В.* Применение машинного обучения в процессе поиска деструктивной информации в web–контенте // Вопросы информационной безопасности. 2019. С. 62–68.
7. *Браницкий А.А., Дойникова Е.В., Котенко И.В.* Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям // Информационно-управляющие системы. 2020. № 104. С. 24-33. DOI: 10.31799/1684-8853-2020-1-24-33.
8. *Сидорова Е.А., Кононенко И.С., Загорулько Ю.А.* Подход к фильтрации запрещенного контента в веб-пространстве // Аналитика и управление данными в областях с интенсивным использованием данных: сборник научных трудов XIX Международной конференции DAMDID/RCDL’2017. 2017. С. 94–101.

А.И. Ревякин, Е.А. Ревякина

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ РАСПОЗНАВАНИЯ РЕЧИ

Донской государственный технический университет,
Ростов-на-дону, Россия

Ключевые слова: информационная безопасность, распознавание речи, скрытые маркосовские модели, нейронные сети, динамическое программирование.

В данной статье приведена терминология в распознавании речи. Проведен анализ алгоритмов распознавания речи.

A.I. Revyakin, E.A. Revyakina

ANALYTICAL REVIEW OF SPEECH RECOGNITION METHODS

Don State Technical University, Rostov-on-Don, Russia

Keywords: speech, speech recognition, hidden Markov models, neural networks, dynamic programming.

This article describes the terminology in speech recognition. The analysis of speech recognition algorithms is carried out.

Основой распознавания речи является звуковой сигнал, передающийся от распознаваемого объекта к распознающему субъекту. Звуковой сигнал в теории распознавания является речью в простом понимании этого слова [1]

Речь – исторически сложившаяся форма передачи сообщения от одного объекта к другому. Для передачи информации от одного объекта к другому используется воздушная среда, принимающая и передающая колебания звука, которые имеют амплитуду и частоту. Данные колебания передают нужную информацию и по своей сути являются сигналом.

Процесс распознавания речи можно упрощенно представить, как алгоритм, состоящий из получения сигнала, цифровой обработки, отчистки, подавления шумов или с их использованием при обучении некоторой модели для получения достоверных результатов и сравнения с эталонами [2].

При преобразовании некоторого входного голосового сигнала пользуются разбиением речи на большое количество фреймов одинаковой длины с последующим преобразованием в частотную область с использованием дискретного преобразования Фурье.

Распознавание речи – задача преобразования речевого сигнала в орфографическое представление, а в данном случае цифровое, для ее дальнейшего использования. Системы распознавания речи могут быть классифицированы по потребительским качествам, а именно распознающие отдельные слова, в данном случае команды, либо слитную речь [3]. Для решений, основанных на первом типе хорошо подходят методы распознавания, основанные на сравнениях с эталоном, словарем данных. Для работы со слитной речью подходят скрытые Марковские модели. Помимо этого, существуют как дикторозависимые системы, требующие от пользователя тренировки до ее непосредственного использования для достижения результатов с малым процентом ошибок, так и независимые.

На рисунке 1 приведена схема распознавания речи на верхних уровнях.

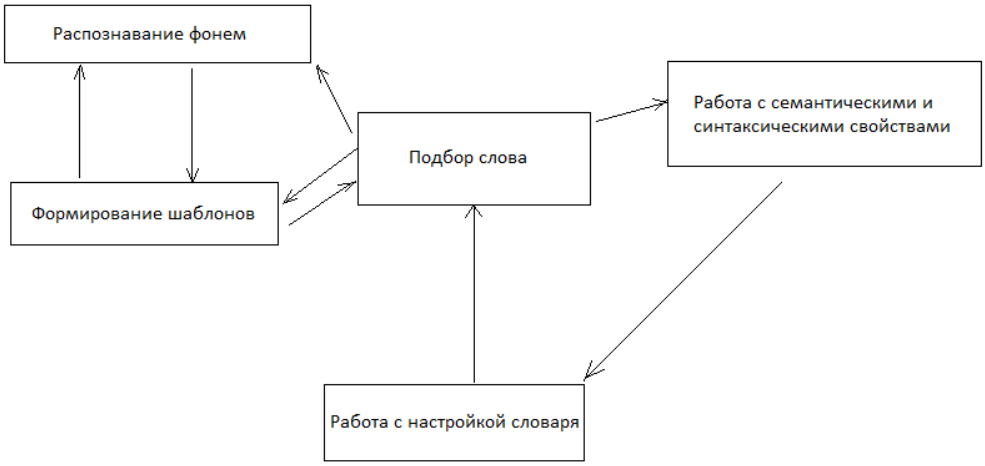


Рисунок 1. Процесс распознавания речи

В настоящее время системы распознавания речи строятся на основе принципов признания форм распознавания [4]. Методы и алгоритмы, которые использовались до сих пор, могут быть разделены на следующие большие классы:

1. Динамическое программирование - временные динамические алгоритмы (Dynamic Time Warping).
2. Скрытые Марковские модели.
3. Нейронные сети.

Выбор метода, в основном, основывается на том, какой тип системы распознавания речи выбран.

Одним из самых ранних алгоритмов является алгоритм распознавания речи на основе (DTW – Dynamic Time Warping). В анализе временных рядов динамическое временное деформирование является одним из алгоритмов для измерения сходства между двумя временными последовательностями. В общем случае, DTW - это метод, который вычисляет оптимальное соответствие между двумя заданными последовательностями с определенными ограничениями и правилами

Альтернативный метод для DTW основан на функциональном анализе данных, в котором временные ряды рассматриваются как дискретизация гладких (дифференцируемых) функций времени и, следовательно, применяется непрерывная математика.

Другим связанным подходом являются скрытые модели Маркова (HMM), и было показано, что алгоритм Витерби эквивалентен стохастическому DTW.

Достоинства DTW:

- быстродействие алгоритма;
- простота обучения;
- существуют эффективные аппаратные реализации.

Недостатки DTW:

- не подходит для непрерывного распознавания речи;
- нет очевидного выравнивания двух рядов, если точки не совпали.

Скрытая марковская модель (HMM) — это статистическая марковская модель, в которой моделируемая система считается марковским процессом с скрытыми состояниями.

Для оптимизации алгоритма HMM часто используют нейронные сети, которые предварительно обрабатывают речевой сигнала, например, преобразование объектов или уменьшение размерности.

В настоящее время разработаны эффективные алгоритмы СММ, которые имеют потенциал к распараллеливанию, чем пользуются специалисты при аппаратной реализации.

В основе, Скрытой Марковской Модели лежит конечный автомат, состоящий из N-состояний, называемых скрытыми. Переходы между состояниями в каждый дискретный момент времени t не являются детерминированными, а происходят в соответствии с вероятностным законом и описываются матрицей вероятностей переходов ANN [5]. Схематическое изображение диаграммы переходов между состояниями СММ приведено на рисунке 2.

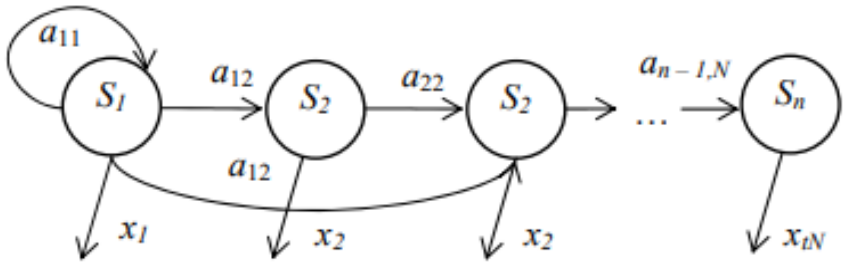


Рисунок 2. Схематическое изображение диаграммы

Работа со Скрытыми Марковскими Моделями, как и с любой другой адаптивной экспертной системой, осуществляется в три этапа:

1. Обучение – определение параметров модели – алгоритм Баума-Велча (forward-backward, BaumWelch re-estemation);
2. Определение – какова вероятность того, что наблюдаемая последовательность векторов [({x)]1, x2, ..., xT} была сгенерирована данной моделью – алгоритм максимума правдоподобия (Витерби). Далее приводится краткое описание вышеперечисленных алгоритмов.
3. Обучение скрытой марковской модели. Процесс обучения скрытой марковской модели заключается в определении с помощью набора обучающих образцов следующих параметров:
   - матрицы вероятностей переходов между состояниями ANN;
   - параметров гауссовых смесей (математическое ожидание, матрица ковариации и веса) для каждого состояния.

Преимуществом Скрытых Марковских Моделей перед остальными методами является естественное встраивание времени в модель λ, что позволяет учесть вариативность произнесений по длине и скорости, а также перейти к распознаванию слитной речи. Еще одним преимуществом является способность сегментировать распознаваемый объект.

Недостатком СММ является отсутствие различающей способности, т.е. алгоритм обучения только максимизирует отклик каждой модели на свои классы, но не минимизирует отклик на другие классы [6].

Самым распространенным методом в теории распознавания и машинного обучения является распознавание с помощью нейронных сетей. Нейронная сеть – это совокупность соединенных и взаимосвязанных между собой искусственных нейронов, аккумулирующих входные значения и генерирующих выходной сигнал при помощи функции активации. Нейронную сеть часто ассоциируют с головным мозгом, сети нервных клеток живого организма.

В последнее время в системах распознавания речи все чаще используются искусственные нейронные сети (ИНС), которые позволяют повысить точность распознавания речи по сравнению с базовыми моделями (скрытые Марковские модели— в качестве акустических моделей; и n-граммы — в качестве моделей языка).

Искусственные нейронные сети могут применяться как для акустического, так и для языкового моделирования, позволяя повысить точность распознавания. При акустическом моделировании, в зависимости от способа объединения Скрытых Марковских Моделей (СММ) и Искусственных Нейронных Сетей, различают тандемные и гибридные нейросетевые модели. Такая модель позволяет объединять преимущества СММ и ИНС, при этом длительные временные зависимости моделируются с помощью СММ, поэтому для акустического моделирования ИНС прямого распространения являются достаточно эффективными. Поскольку нейронные сети не могут идентифицировать динамические объекты, для сравнения моделей с сигналом по-прежнему используется формализм Марковских Моделей, однако теперь в качестве вектора признаков используется набор апостериорных вероятностей трифонов, полученный на выходе нейронной сети. Такой метод использования нейронных сетей одним из первых предложил для монофонов Х. Германский с соавторами.

Существует достаточно много разновидностей ИНС, среди которых можно выделить основные виды: персептроны, автоэнкодеры, сверточные ИНС, ИНС с временными задержками, глубокие нейронные сети доверия, ИНС с длительной кратковременной памятью [7].

Важным моментом при проектировании и реализации нейронных сетей является обучение. Различают алгоритмы обучения с учителем и без учителя.

Процесс обучения с учителем представляет собой предъявление сети выборки обучающих примеров. Каждый образец подается на входы сети, затем проходит обработку внутри структуры НС, вычисляется выходной сигнал сети, который сравнивается с соответствующим значением целевого вектора, представляющего собой требуемый выход сети. Затем по определенному правилу вычисляется ошибка, и происходит изменение весовых коэффициентов связей внутри сети в зависимости от выбранного алгоритма. Векторы обучающего множества предъявляются последовательно, вычисляются ошибки и веса подстраиваются для каждого вектора до тех пор, пока ошибка по всему обучающему массиву не достигнет приемлемо низкого уровня.

При обучении без учителя обучающее множество состоит лишь из входных векторов. Обучающий алгоритм подстраивает веса сети так, чтобы получались согласованные выходные векторы, т.е. чтобы предъявление достаточно близких входных векторов давало одинаковые выходы. Процесс обучения, следовательно, выделяет статистические свойства обучающего множества и группирует сходные векторы в классы. Предъявление на вход вектора из данного класса даст определенный выходной вектор, но до обучения невозможно предсказать, какой выход будет производиться данным классом входных векторов. Следовательно, выходы подобной сети должны трансформироваться в некоторую понятную форму, обусловленную процессом обучения. Это не является серьезной проблемой. Обычно не сложно идентифицировать связь между входом и выходом, установленную сетью. Для обучения нейронных сетей без учителя применяются сигнальные метод обучения Хебба и Ойа [8].

Появление технологий глубокого обучения и развитие рекуррентных нейронных сетей для обработки текстов позволили существенно улучшить качество лингвистической модели за счет учета контекста и отсутствия ограничений на использование только N предыдущих слов. В результате получилось еще больше повысить точность итогового распознавания речи — на слух могут распознаваться не все слова, и пропущенные элементы важно угадывать по контексту, как это делает человек. Лингвистические модели на основе рекуррентных нейронных сетей, которые позволяют эффективно реализовать такое поведение, сейчас повсеместно применяются в индустрии.

На базе нейронных сетей можно создавать обучаемые и самообучающиеся системы. К самообучающимся системам предъявляют следующие требования:

- разработка системы заключается только в построении архитектуры системы (основную часть информации система получает в процессе обучения);

- возможность контроля своих действий с последующей коррекцией;
- возможность накопления знаний об объектах рабочей области;
- автономность системы.

Возможность создания на базе ИНС самообучающихся систем является важным условием для их применения в системах распознавания речи. Преимущества нейронных сетей: устойчивость к шумам входных данных; адаптация к изменениям; отказоустойчивость; сверхвысокое быстродействие. Недостатки нейронных сетей: ответ всегда приблизительный.; принятие решений в несколько этапов.

Распознавание речи очень перспективная технология и занимает отдельное большое место в науке информационных процессов и в настоящее время повсеместно активно применяется. Данная функция позволяет упростить многие процессы, связанные с ручным вводом, сделать их более автоматизированными. Например, различные сервисы по бронированию билетов, очередей, общению с роботизированными программными продуктами. Находит применение и в повседневной жизни, как способ общения с близкими без использования виртуальной или физической клавиатуры. Многим людям с ограниченными возможностями распознавание речи облегчило некоторые жизненные или рабочие ситуации.

Прогресс не стоит на месте, и данная технология используется как одна из основных при построении огромных вычислительных систем, например, крупная поисковая система, умный дом, медиа-центр, управляющий многими гаджетами в большинстве домов, которые каждый год становится более комплексными.

Помимо вопросов о облегчении жизни, данная технология затрагивает такие аспекты, как защита конфиденциальной информации и других ценностей. В этом случае распознавание речи не является ведущей технологией, но как одной из важнейших. Примером может являться идентификация человека при запросе доступа к какой-либо информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Фролов А.В., Фролов Г.В., Курейчик В. М.* Синтез и распознавание речи. Современные решения. — 1-е изд, 2003. — 150 с.
2. *Сапунов Г.В.,* Система автоматического распознавания речевых команд для параллельных архитектур / Диссертация, — 2005. — 129 с.
3. *Хеин М.З.* Алгоритмы динамического программирования в распознавании речи / Труды Курского государственного университета – 2017, с. 5
4. *Авсентьев А.О.*, Лукьянов А.С. Применение скрытых Марковских моделей для распознавания речи диктора / Труды Воронежского института МВД России – 7 с.
5. *Вишнякова О. А., Лавров Д. Н.* Применение преобразования Гильберта-хуанга к задаче сегментации речи / Математические структуры и моделирование. 2011. вып. 24. С. 12–18
6. *Васенков, Д.В.* Методы обучения искусственных нейронных сетей / Компьютерные инструменты в образовании, 2007. – С. 20–29
7. *Грибачев, В.П.* Элементная база аппаратных реализаций нейронных сетей / Компоненты и технологии, №8, 2006. – С. 72-75.
8. *Amato, F., López, A., Peña-Méndez, E.M., Vaňhara, P., Hampl, A., Havel J.* Artificial neural networks in medical diagnosis / Journal of Applied Biomedicine, Vol. 11, pp. 47–58, 2013.
9. *Brester, C., Semenkin, E., Sidorov, M.* Speech-based emotion recognition: Application of collective decision making concepts / International Conference on Computer Science and Artificial Intelligence (ICCSAI2014), pp. 216–220, 2014.

А.А. Мержвинский[1], А.А. Нерсесянц[2], Н.Н. Будник[1]

ИНФОРМАЦИОННЫЕ МОДЕЛИ В КЛАССИФИКАЦИИ ЗНАНИЙ

Институт кибернетики им. В.М. Глушкова, г. Киев, Украина[1],
merzh3@ukr.net
Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[2]

Ключевые слова: *коммуникэт*, объект-отражение, модели объектов, общая теория информации.

Приведены различия в сути определений информационных моделей, как адекватных отражений реального мира (РМ) и моделей представления знаний, как целенаправленных отражений РМ.

Исходные аналоговые отражения прототипов, формируемые сенсорами устройств ввода, - эмпирические образы РМ – целесообразно определять как компоненты информационных моделей РМ и как важнейшие компоненты моделей представления знаний.

Понятие информация предпочтительнее определять не на основе созданной сознанием естественно-языковой картины мира, а на основе явлений материального мира.

A.A. Mierzvinskyi[1], A.A. Nersesyants[2], N.N. Budnyk[1]

INFORMATION MODELS IN THE CLASSIFICATION OF KNOWLEDGE

Glushkov Institute of Cybernetics, Kiev, Ukraine[1]
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[2]

Keywords: *communicat*, models of objects and subject areas, general theory of information

The differences in the essence of the definitions of information models, as adequate reflections of the real world (RM) and models of knowledge representation, as purposeful reflections of RM are given.

The initial analog reflections of prototypes, formed by the sensors of input devices - empirical images of RM - it is advisable to define as components of RM information models and as the most important components of knowledge representation models. It is preferable to define the concept of information not on the basis of the natural-language picture of the world created by consciousness, but on the basis of the phenomena of the material world.

Введение.

Развитие теории информации, начавшееся с книгопечатания и разработки средств связи, выходит на новый этап с появлением ЭВМ и знание-ориентированных систем [1]. Информационные модели вошли в практику описания не только процессов коммуникации субъект-субъект, но и процессов в неживом и живом мире. При этом общепринятые инвариантные определения понятия «информация», «знания», пригодные к различным предметным областям (ПдО) макромира, отсутствуют [2].

Появление оптических и акустических сенсоров в устройствах ввода позволило формировать многомерные пространственно-временные (ПВ) и другие образы объектов. Отметим, что ПВ-модели формируются не только в устройствах ввода, но и в информационных системах (ИС), например, «Пространственно-временные Актуальные Модели Местности» [3]. Вместе с тем раздельное рассмотрение процессов передачи информации, как сообщений, сформированных человеком, и процессов передачи электрических или оптических сигналов, сформированных информационными машинами, организменных и генетических процессов не способствует интеграции теории. Новизна статьи в физико-информационном подходе ко всем указанным процессам.

При переходе от информации, как фундаментального свойства материи, к знаниям, как форме целенаправленного отражения действительности, необходима разработка тезауруса понятий, общего для естественного или формального языка субъектов и языка информационных машин. Важна разработка эмпирического и теоретического базиса иерархии информационных процессов и методологии теории информации. Широко известны классификации информационных моделей представления объектов и систем реального мира (РМ) и моделей представления знаний о РМ [5,6]. Но в них в должной степени не учитываются эмпирические модели и модели универсума [7]. И это затрудняет восприятие многообразных явлений мира, единства мира, в первую очередь, - единства различных состояний и свойств движущейся материи.

С целью преодоления все более глубокой специализации науки, усилия направляют, прежде всего, на унификацию языка науки, повышение эффективности обработки знаний. Последнее в значительной мере зависит от объективности принятой стратегии структурирования научных знаний [1, Палагин].

Цель исследований - уточнение ролей образов и аналоговых объектов-отражений, как связывающего звена исходного материального мира и мира отражений, места объекта-отражения в иерархии моделей реального мира. Постановка задачи:

1. Уточнить роль процесса зондирования и анализа носителей взаимодействий в формировании аналоговых отражений РМ.
2. Исходя из детерминированности процессов важнейших ПдО реального макромира выделить общие компоненты частных теорий информации, как основы общей теории информации макромира.
3. Определить роль и место эмпирических образов как видов информационных моделей и моделей представления знаний.

1. Частные теории информации предметных областей – основа синтеза общей теории информации макромира.

1.1 Особенности частных теорий информации макромира.

При разработке классификационной модели информационных наук на основе материально-, энерго- и информационных процессов (МЭИ-процессов) в [2] выделены частные теории для таких укрупненных процессов:

a. Физические/химические взаимодействия объектов реального мира - *F*.
b. Молекулярные и генетические процессы развития клеточных форм жизни - *G*.
c. Нейронные и организменные процессы жизнедеятельности организмов - *N*.
d. Процессы умственной деятельности и коммуникации человека - *S*.

e. Процессы переноса информации (состояний) в средствах информационных технологий (ИТ) - *I.*

Основополагающими понятиями приведенных процессов являются участники и процессы движения информации в соответствующей предметной области.

А. ***Физические процессы взаимодействий объектов реального мира.***

Устойчивые во времени неоднородности произвольной физической природы отличаются численной реакцией на воздействие переносчиками взаимодействий (*коммуникэтами*). Применительно к перечисленным выше процессам *информация* — это состояние объекта материального мира (объекта прототипа или объекта отражения), которое возникает при взаимодействии материальных объектов и/или в результате мыслительных процессов и действий субъекта [2].

В.М. Глушков в ряде работ характеризует информацию как меру неоднородности в распределении энергии (или вещества) в пространстве и времени. Информация существует постольку, поскольку существуют материальные тела и, следовательно, присущие им неоднородности» [8]. И объект-прототип, и объект-отражение существуют в виде МЭ-объекта, поэтому *информация* также существует в форме МЭ-объекта [2].

Рассмотрение МЭИ-процессов [2] показывает, что *информационные взаимодействия* – это абстракция физических взаимодействий. В макромире уровень *коммуникэтных* взаимодействий лежит выше уровня гравитационных, электромагнитных сильных и слабых взаимодействий; это уровень энергетических взаимодействий неоднородностей. Элемент неоднородности, характеризуемый массой М и энергией Э, несет в себе не один бит информации, как это принято в случае «есть/нет», а может нести квант *макроинформации,* характеризуемый численно. Его численное значение определяется способностью неоднородности к взаимодействию с определенным *коммуникэтом.*

Содержание процессов коммуникэтных взаимодействий – это формирование пространственно-временных, спектральных, а также структурных образов объектов РМ.

В. ***Генетические процессы развития клеточных форм жизни.***

Суть процессов – воплощение генетической информации в жизненном цикле (ген - белок-орган) и гомеостазе клетки. Генетическая информация — информация о строении (структуре) белков, закодированная генетическим кодом в последовательности нуклеотидов в генах (в особых функциональных участках молекул ДНК или РНК).

Одним из основных свойств материала наследственности является его способность к самокопированию – *репликация.* Это свойство обеспечивается особенностями химической организации молекулы ДНК, состоящей из двух комплементарных цепей. Нуклеиновые кислоты выполняют функцию хранения и реализации генетической информации, которые осуществляются в ходе процессов репликации, транскрипции, трансляции и биосинтеза белка [9].

Репликация (от лат. *replicatio* – возобновление) – процесс создания двух дочерних молекул ДНК на основе родительской молекулы ДНК (самокопирование)

Транскрипция (от лат. *transcriptio* «переписывание») – происходящий во всех живых клетках процесс синтеза РНК с использованием ДНК в качестве матрицы; перенос генетической информации с ДНК на РНК.

Трансляция (от лат. *translatio* – «перенос, перемещение») – осуществляемый рибосомой процесс синтеза белка из аминокислот на матрице информационной (матричной) РНК (иРНК, мРНК); реализация генетической информации.

Биосинтез белка — это многостадийный процесс синтеза и созревания белков, протекающий в живых организмах.

Содержание процессов: В простейшем случае формирование структур и *структурных образов.*

C. ***Отражение жизнедеятельности организмов. Биоинформационные модели нейронных структур органов и организмов.***

Клеточная теория – одно из общепризнанных биологических обобщений, утверждающих единство принципа строения и развития тканей и органов мира растений, животных и остальных живых организмов с клеточным строением, в котором клетка рассматривается в качестве единого /структурного элемента живых организмов. Клетка — единая система, она включает множество закономерно связанных между собой элементов, представляющих целостное образование.

Несмотря на свои малые размеры, клетка представляет собой сложнейшую биологическую систему, жизнедеятельность которой поддерживается благодаря разнообразным биохимическим процессам, которые происходят под строгим генетическим контролем. Генетический контроль развития и функционирования клетки осуществляют материальные носители информации – гены.

Содержание процессов: Формирование и перенос пространственно-временных и спектральных образов, например зрительным и слуховым каналами.

D. Отражение ментальной и коммуникационной деятельности человека.

Теория информации в докомпьютерную эпоху охватывала информационные взаимодействия между субъектами, описываемые такими цепочками:

- Природа→субъект→текст;
- Субъект адресант→Средства коммуникации→субъект-адресат.

Теория коммуникации представляет собой область научного знания, предметом изучения которой являются коммуникация, ее роль и место в обществе, а также коммуникационные методы, системы, процессы и закономерности их функционирования и развития [10]. Процесс коммуникации (в том числе как формы взаимодействия) понимается в качестве одной из основ жизни человека и общества. При этом речь у исследователей идет как о процессах коммуникации, так и о его семантике.

Содержание процессов: Формирование и движение зрительных, вербальных, а также структурных образов. Формирование моделей информационных взаимодействий.

E. ***Отражение движения информационных объектов в средствах ИТ.***

Информация сегодня является не только основой коммуникаций, но одним из важнейших ресурсов. Объемы и скорости обработки/передачи информации ограничиваются параметрами компьютеров и линий связи. Они определяются в процессе создания и МЭИ-моделирования средств ИТ [2].

Содержание процессов: Формирование, обработка и передача пространственно-временных, спектральных и структурных образов.

1.2 Трехслойная модель образа мира

Образ мира - результат отражения образа мира в сознании человека. Совокупность результатов познавательной деятельности человека образует определенную модель (картину мира). Образные модели интерпретируются сознанием соответственно контексту. Формируемый в сетчатке глаза образ Z в соответствии с некоторым контекстом преобразуется в сознании в *значение* V в виде некоторых форм (пространственный образ, слово). Например, предметное значение, слово-значение, операциональное значение, комплекс (обобщение на основе их объективных связей), синкретизм (на основе хаотичных связей). В психологии известны три направления моделирования образа мира (структура, функция, генез): 1) описание образа мира как существующей системы образов, репрезенетованных в значения форм сознания человека (содержательная, продуктивная модель); 2) описание функций образа мира (процессуальная,

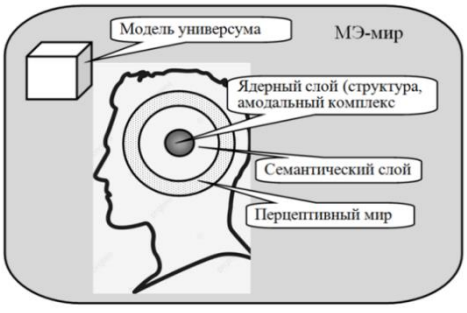


Рис. 1 Трехслойная модель образа мира

продуктивная, целевая модель); 3) описание генеза образа мира (модель развития, модель консервации) [11]. К функциональным моделям образа мира относят трехслойную модель образа мира (Артемьева, Стрелков, Серкин, 1983, 1991; Артемьева, 1999). В нашем случае образ мира представлен как на рис. 1. Объекты материально-энергетического мира характеризуются численно: в соответствии с эталонами мер измерений, созданных человечеством. Поэтому МЭ-объекты могут рассматриваться как основа определения сущности информационного объекта (ИО) и информации.

Перцептивные процессы - процессы, которые обеспечивают связь внутреннего и внешнего мира через работу органов чувств. Результатами сенсорных преобразований в живом мире и средствах ИТ являются пространственно-временные образы и спектры. Важнейшее понятие перцептивного мира «отражение» может быть обобщено как: *Отражение* (отпечаток, ИО) - результат воздействия одной материальной системы на другую. Концепция *отражения* восходит к понятию рефлексии у Гегеля и французскому материализму XVIII века.

Важнейшим понятием перцептивного и семантического слоев является понятие «информация». Семантическая информация – это сформированные человеком и выраженные знаками отражения РМ. Знания семантические - совокупность сведений о состоянии объектов предметной области и отношений между ними хранящихся в базе знаний. [12]. Слова и смыслы – результат творения (творческой деятельности) человека. Основной чертой семантической технологии (Semantic Technology) является хранение и поддержание целостности семантики (знаний, смыслов) отдельно от содержания файлов данных и от кодов программ [13].

Ядерный слой - образы структур мира. Представление фрагмента может быть амодально. Амодальный смысл — интеллектуально переживаемый (фиксируемый наблюдателем) смысл, удерживаемый в сознании без помощи образов традиционных модальностей восприятия: визуальной, аудиальной, кинестетической, вербальной. Человек, мыслящий амодальными смыслами, не использует в качестве инструментов удержания смысла ни образы, ни ощущения, ни слова.

Модель предметной области – это некоторая система, имитирующая структуру или функционирование исследуемой предметной области и отвечающая основному требованию – быть адекватной этой области. Главный критерий адекватности структурной и онтологической моделей *предметной области* – это функциональная полнота разрабатываемой ИС.

Структура – это совокупность МЭА-объектов и коммуникэтных связей (в отличие от ассоциативных) между ними, ориентированных на совместное многократное использование различными пользователями в своих приложениях.

Онтология – это набор определений, понятий и отношений между ними для фрагмента лексико-семантических знаний, ориентированных на их совместное многократное использование различными пользователями в своих приложениях [15, Звіт].

Бытие и познаваемое сущее, принято называть Универсумом [16, Вечтомов]. Универсум содержит всю наличную действительность: физическую реальность (природа); человеческое общество (социум); человеческое сознание, включая идеальный мир знания и веру. Универсум – это мир, живущий и изменяющийся (развивающийся или деградирующий) по непреложным законам, которые должна открывать наука.

Развитие науки характеризуется категоризацией, аксиоматизацией и универсализацией знаний, приведших к разработке нескольких классов универсальных моделей [14]. Факт формирования в сознании субъекта картины мира, показанной на рис.1, не означает что понятия «информация» и «знания» должны привязываться к слабо познанному сознанию человека. Интуитивно ясно, что предпочтительнее привязываться к достаточно освоенному физическому миру. Такой тренд интерпретации информации также

соответствует известному тезису Бартини [4] «Пространство-время» - основа мер измерения движения материи.

1.3 Особенности *коммуникэтной*, антропной и общей теории информации

1.3.1. О коммуникэтной теории информации.

В основе *коммуникэтной* теории информации лежат процессы *коммуникэтных* взаимодействий материальных объектов. Характерные примеры таких взаимодействий - формирование спектра, преобразование объекта-прототипа в объект-отражение камерой обскурой [17]. Структурная схема формирования изображения торца стержня в камере-обскуре, как пример формирования образа объекта в неживом мире, приведен на рис.2.

Рис. 2. Абстрактная схема формирования образа объекта-прототипа.

Блок ввода - ограничивающая посторонние потоки диафрагма; *оперант* - блок преобразований (оптическая призма, отверстие оптически непрозрачной диафрагмы); *исполнительный блок* - блок действий (рассеивающий экран, фоточувствительная среда).

Коммуникэт - переносчик взаимодействий между объектами макромира - составляющая вещественного, энергетического или полевого потоков, способная воздействовать на реципиента.

Содержание естественного коммуникэтного процесса: Формирование пространственно-временных образов либо спектра прототипа.

Комплекс оптических компонент на рис. 2 может рассматриваться как информационная машина, формирующая образ объекта-прототипа. *Образ*, в данном случае, – результат процесса отображения объекта в информационной машине. Участники процесса взаимодействий - объекты-прототипы, операнты, объекты-отображения, объекты-воплощения - именованы как *коммуниканты*. Как было показано в [18] *коммуниканты*, как и *коммуникэты,* могут рассматриваться, как М либо И-объекты и могут быть положены в основу точной формализации информационных процессов. Предметом *коммуникэтной* теории информации, очевидно, есть *коммуникэтные* взаимодействия, как между материальными, так и информационными объектами:

М→М - материальные взаимодействия.

М→И - отражение в средствах ИТ.

И→М - воплощение И-объектов средствами ИТ.

И→И - информационные взаимодействия.

Парадигма *преобразования* образов МЭИ-объектами с помощью *коммуникэт* может быть названа *коммуникэтной.* Характеризуемая этой парадигмой частная теория в МЭИ-процессов также может быть охарактеризована, как *коммуникэтная* теория информации. В приведенном подходе и объект-прототип, и объект-отражение - МЭИ-объекты; *информация* - в общем случае тоже МЭИ-объект, независимо от того, как он интерпретируется окружающим миром. Вывод*: Коммуниканты* и *коммуникэты* - важнейшие участники информационного процесса физико-информационного уровня [19].

1.3.2. Об антропной теории информации.

Коммуникэтный подход удобен для анализа информационных процессов в компьютерах и других средствах ИТ, а также удобен для описаний механизмов генетических и биологических преобразований внутри живых организмов. Однако, в случае субъекта-человека S, ввиду его суперсложности, подход недостаточен для представления процессов SS-коммуникаций и смыслов умственной деятельности. В то же время

разработка технических средств коммуникации не требует учета смысла и содержания информации; решения принимаются на основе моделей математической теории связи. Теория информационных взаимодействий «субъект-субъект» естественно определить как «*антропоцентрическую*» теорию информации [2], а теорию отношений субъект-организм, как «*антропную*».

Состав информационных процессов: формирование, передача и использование человеком пространственно-временных, вербальных и текстовых образов.

В *антропную* теорию информации естественно включить не только процесс наблюдения субъектом объекта, а и характеристики важности его окружения с точки зрения субъекта. Применительно к *антропной* теории информации, *информация* – содержание, присваиваемое ИО, посредством распространяющихся на него соглашений.

1.3.3. К общей теории информации.

Вслед за внедрением компьютеров появились интеллектуальные системы. Широко стали использоваться понятия знания, базы знаний. Развитие сенсорных устройств расширило эмпирическую познаваемость объектов РМ; развитие аппаратных и программных средств и технологий потребовало введения таких понятий как «уровни и виды представления информации и знаний», «универсум» и др. Сформировалось представление о паре - *коммуникант* и *коммуникэт* [7].

Общую теорию информации макромира (ОТИМ) определим как результат синтеза коммуникэтной, антропной, остальных частных теорий информации, включая общую теорию связи. Очевидно, что ОТИМ должна учитывать многоуровневые информационные SS-взаимодействия, состав и содержание процессов, методы создания знаний и управления ими. Поэтому синтез общей теории информации должен начинаться с выявления состава процессов, создания некоторого метаязыка, определения основных понятий процесса (тезауруса).

Состав информационных процессов ОТИМ (в первом приближении) - формирование, обработка и движение пространственно-временных, спектральных, а также структурных *образов* объектов РМ, разработка метазнаний о ПдО, алгоритмов технологических процессов разработки и изготовления сложных изделий.

Объектная область ОТИМ может быть иллюстрирована составом и *коммуникэтными* связями средств ИТ верхнего уровня на примере создания относительно сложных технологий [20,21]. Имеется в виду производств изделий, удовлетворяющим повышенным техническим требованиям, возможно изделий на новых физических принципах, и ориентирована, при этом, на использование реального либо проектируемого оборудования, обеспечение патентной чистоты и др. Решение этих задач требует применения интеллектуальных систем, включающих базы данных и знаний.

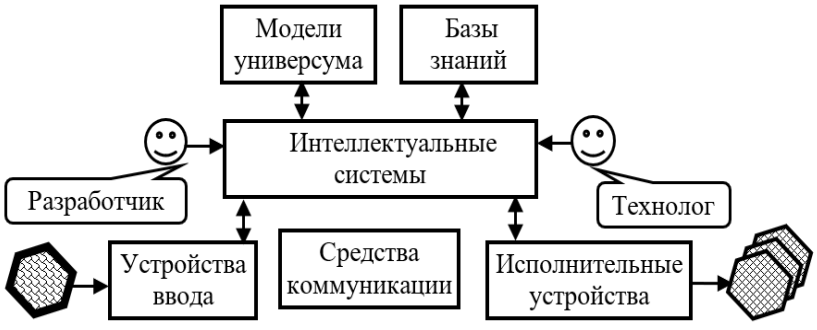


Рис. 3. Средства преобразования объекта-прототипа в объект-воплощение

На рис. 3 приведен пример состава системы, ориентированной на создание 3D-технологии изготовления изделия по прототипу, структура которой изложена в [17, рис. 5]. В пределе, например, при разработке научных теорий технологии изготовления интегральных схем, могут потребоваться и такие эмпирические и теоретические продукты

деятельности человека как универсальные модели универсума, предложенные в [14], и символьно-образные, предложенные в [7].

Таким образом, ОТИМ кроме принципов работы аппаратных средств ИТ-технологий (устройств ввода/вывода, коммуникации и обработки информации), охватывает принципы построения программ баз данных и знаний, моделей универсума.

Важнейшим понятием ОТИМ, наряду с упомянутыми средствами ИТ, является Информационный *объект.* В этом контексте он может рассматриваться: А) как вещественно-полевая неоднородность или МЭ-объект; и Б) как результат процесса отражения материальных объектов-прототипов и/или как результат деятельности человека в виде совокупности состояний ее носителя. Откуда следует определение:

Общая теория информации макромира – наука о МЭИ-объектах, изучающая формирование, движение и использование *отражений* в неживом и живом мире.

Коммуникэтная, атрибутная и антропная теории информации - составляющие ОТИМ. Эта наука включает такие, согласующиеся с утверждениями [2] определения:

Информационный объект – это:

- Объект-прототип;
- Отражение объекта-прототипа;
- Отражение некоторого процесса, в частности, деятельности субъекта, в виде состояния неоднородности МО (объекта-носителя).

Информация – совокупность информационных объектов, которые организованы в некоторую структуру. Т.е. *Информация* - совокупность *вещественно-полевых (ВП)*-объектов, поэтому в общем случае *Информация – это ВП-объект. Информация* – более широкое понятие, чем отражение, так как относится и к состоянию объектов-прототипов.

2. Образные модели - важнейшая категория отражений МЭИ-мира

2.1. О связях объектов действительности и языковых единиц.

Связи между языковыми единицами и объектами действительности принято отражать с помощью семантических треугольников (Фреге, Огдена) или квадрата Щедровицкого. Однако, как рассматривалось в предыдущих статьях [2,22], связи материальных и информационных объектов РМ характеризуются сутью отражений «реальность-процесс-образ»». Каждый материальный объект в процессе формирования его *коммуникэтного* отражения характеризуется своим ПВ (материальным и энергетическим) и информационным состояниями. В треугольнике Фреге и квадрате Щедровицкого этот важный этап воздействия зондирующего потока *коммуникэт* и формирования аналогового объекта-отражения упускается. В [22] была предложена концепция МЭИ-квадрата, в которой взаимодействие МЭ-прототип→МЭ-отображение представлено в составе коммуникэтно-информационной модели (рис.4).

2.2 Взаимосвязи представлений объекта действительного мира

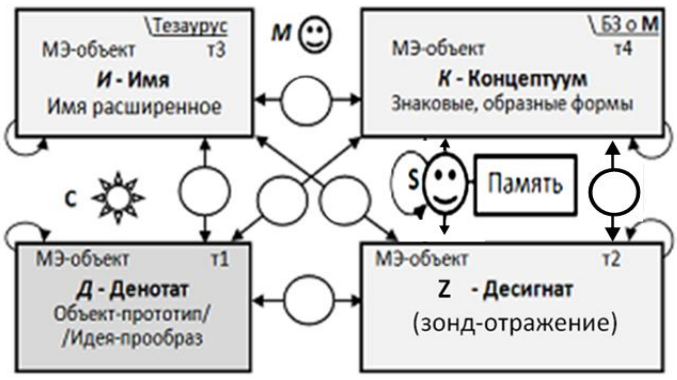


Рис. 4. Взаимосвязи представлений объекта действительного мира.

Взаимодействия между МЭ-объектами показаны кругами и обеспечиваются источником *коммуникэт* С, субъектами S и средствами ИТ. Каждый прямоугольник (вершина графа) трактуется как материально-энергетический (МЭ) объект. При сетевом подходе одна вершина Д (при семантическом D) это исходный материальный объект, вторая - зонд-отражение Z (аналоговое либо дискретное отражение), третья - имя И, четвертая К – это отражения в виде

знаковых (символьных) графических и более сложных структур (моделей в виде абстрактных и конкретных форм объектов и действий).

Зондирование объекта-прототипа *коммуникэтами* С - важнейшая операция формирования эмпирического аналогового образа Z объекта Д. Зонд-отражение Z - аналоговый/цифровой образ объекта-прототипа Д. Зонд-отражение Z может рассматриваться как: А) эмпирическая модель, формируемая в результате введения в поле восприятия любых сенсорных данных с целью дополнения сведений об окружении и улучшения восприятия информации; Б) как теоретическая модель, формируемая на основе некоторой «Идеи-прообраза» D.

Зонд-отражения, независимо от формы представления, аналоговой либо дискретной, связывают реальный мир с формируемыми информационными моделями отражений РМ. Поэтому зонд-отражение - важнейшее звено, обеспечивающее концептуальную целостность эмпирической модели РМ и знаний о нем.

Образная модель эмпирическая Z - в общем случае многомерная модель, полученная в результате сканирования (зондирования) элементов многомерного объекта, например, ПВ-модель.

Образная модель теоретическая D - результат мыслительных операций субъекта S: восприятия с помощью пяти чувств, воображения, предопределенная генетически, или информация из ноосферы, воспринятая на духовном уровне. Образные идеи-прообразы могут формироваться сознанием в виде мыслеобраза. Мыслеобраз – «это индивидуально воспринятый всеми органами чувств целостный образ предмета (явления)» [23]. Предмет ОТИМ, очевидно, должен рассматривать все коммуникэтные операции с S и Z-объектами:

S→S - информационные,

Z→S - отражение,

S→Z - материализация (воплощение),

Z→Z - физические взаимодействия, например, преобразование при проявлении скрытого оптического изображения светочувствительного слоя в видимое [21].

Таким образом, применительно к средствам ИТ, онд-отражение Z – важнейшее звено, связывающее объект РМ и относящиеся к нему отражения. Это составная часть информационных моделей РМ. Имя, образная модель, определение и концептуум - важнейшие формы отображения объекта действительного мира, которые могут быть использованы при построении частных и общей теорий информации.

2.3 Уточнение классификации информационных моделей объектов и предметных областей.

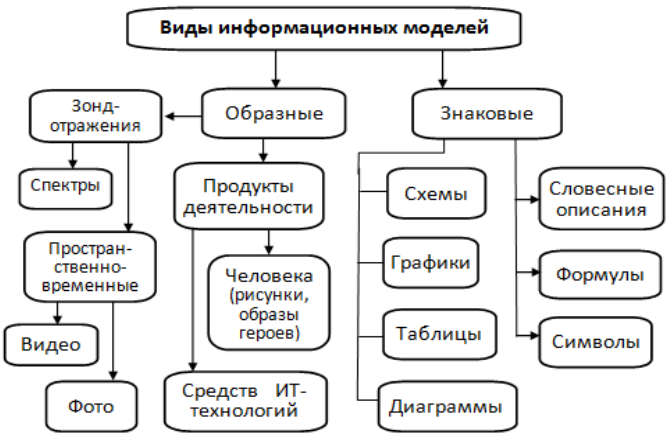


Рис. 5. Классификация информационных моделей, как «заместителей» представлений объектов или процессов реального мира

Информационная модель – совокупность информации, характеризующая свойства и состояния объекта, процесса, явления, а также взаимосвязь с внешним миром (рис. 5). Применительно к сознанию отражения **Z**→S - и важнейшие операции преобразования МЭИ-структур в значения образа мира. В технических средствах, в зависимости от способа сканирования, зонд-отражения могут представлять аналоговые ПВ-отображения либо спектры (рис. 2).

При этом *образные модели* – это обычно пространственно-временные зрительные образы объектов,

зафиксированные на каком-либо носителе информации.

Знаковые модели - информационные модели, выраженные в дискретной форме средствами формального языка [23]. *Символ* – это знак или сигнал, наполненный смыслом. Рисунок 5 иллюстрирует иерархию образных и знаковых моделей объекта или ПдО.

Вывод. Образные модели физического объекта - важнейшая базовая составляющая анализируемых информационных процессов.

3. Модели ПдО, универсума и представления знаний - важнейшие категории отражений реального мира.

3.1. Об определениях и иерархии информации, данных и знаний.

3.1.1. *Информация* — это свойство объектов РМ, проявляющееся в возможности отражения одного объекта в другом в виде состояний объекта. Информация, в соответствии с [23], – это:

- Явление (способ существования - МЭИ-объект);
- Идея (сущность вещи - состояние вещи в пространстве-времени);
- Смысл (осознание - ассоциация в сознании субъекта).

При таком подходе общее инвариантное определение информации, уточненное по отношению к [2 и 17], можно сформулировать как:

***Информация* — это наделяемое смыслом состояние объекта материального мира (объекта прототипа или объекта отражения), возникшее в результате процесса взаимодействия материальных объектов и/или результатов протекания процессов (природных, деятельности человека).**

Данные (что?) – описание результатов измерений, наблюдений инструментальных средств; протоколы экспериментов: исходные, «сырые» данные, пригодные для машинной обработки. Источники данных: субъекты, средства ИТ, М - объекты внешнего мира.

Модель есть абстрактное представление реальности в какой-либо форме (например, в математической, физической, символической, графической или дескриптивной), предназначенное для представления определённых аспектов этой реальности и позволяющее получить ответы на изучаемые вопросы[3]: [24].

Данные, модели РМ и знания - различные категории информации, отношения которых изображены на рис. 6. Основания доменов приведенных категорий информации - материально-энерго-информационные объекты 1, которые характеризуются состояниями 2. Они отличаются физическими свойствами - способностью к эмиссии коммуникэт λ, величинами коэффициентов отражения, рассеяния, поглощения и др. Их свойства отображаются как мониторами устройств ввода так и сознанием человека в виде отображаются как мониторами устройств ввода так и сознанием человека в виде символьно-образных отображений 3.

Как было отмечено в п.2.2 субъект реагирует на объекты внешнего мира, освещенные λ_1. Сознание человека также способно генерировать образы представления и воображения 4, выводимые субъектом *коммуникэтами* λ_3, формулировать новые индуктивные и дедуктивные умозаключения, накапливать их и создавать базы знаний субъекта БЗS. В случае инструментальных средств - первичные образы 5 - результат зондирования внешнего объекта коммуникэтами λ_2, приема обратного потока сенсорами и далее формирования коммуникэтного образа λ_4**.** Взаимодействующие между собою прототипы первичных образов могут образовывать системы, которые могут быть описаны субъектом языковыми средствами либо не описаны. Функционирование систем может опираться на некоторые идеи и на известные и не известные фундаментальные законы. Идеи, сотворенные субъектом, и знания - составная часть естественноязыковой картины мира 6.

На основании λ_3 и λ_4, образовательной и научной деятельности организаций формируются Естественно-языковая картина 6, базы данных и базы знаний 7 абстрактного и реального миров (АМ и РМ). ЕЯ базы знаний РМ могут включать:

– Знания об прошлом и настоящем актуального мира.
– Знания, усвоенные субъектом в процессе общего и специального образования.
– Знаня человечества, усвоенные субъектом в процессе жизни.
– Знания древних рукописей.
– Врожденные знания, определяемые генетикой организма

Формализованные данные 8 – пригодная к обработке формализованная информация**.** Отметим. что формируемый сенсорами эмпирический образ РМ (9)- важнейший компонент связи М- и И-миров. При его игнорировании нарушается концептуальная целостность эволюции отображений отдельных объектов, ПдО и универсума в целом.

Рис. 15 иллюстрирует естественность таких толкований понятия *информация*:

а) как атрибут объекта;

б) как отражение реального мира;

в) как фундаментальная категория, относящаяся к МЭ-миру и ко всем уровням отражений, данных и знаний.

Рис. 6. Уровни отражений объектов реального мира

Рисунок 6 иллюстрирует отличие информационных моделей реального мира 4, 5, 6, 7, как составляющих средств ИТ, от моделей знаний о реальном мире 9 и 10, как инструментов сознания и участников технологического процесса.

В основе кибернетических моделей 11 системы лежит фундаментальное понятие *"управление"*. *Знания* 12 *в искусственном интеллекте:* совокупность фактов, событий, а также правил, организованных субъектом для систематического применения. То-есть, знания - не просто объективная модель каких-то процессов, а результат определенных *мыслительных операций* исследователя (абстрагирования, упрощения или детализации исходной информации) применительно к интересам потребителя. Это могут быть анализ (разложение на части), синтез (объединение частей в единое целое), сравнение (сопоставление объектов для выявления у них общего или различий), обобщение (переход от единичного к общему), абстрагирование (формирование образов реальности посредством отвлечения и пополнения).

Первичные образы 5, «полученные в результате прямого опыта, прямого восприятия, без помощи накопленных ранее знаний и правил логического мышления, результаты сенсорных преобразований объекта» относят к *непосредственным знаниям*.

3.1.2. Знания. *Знания* (структура?)- организованное, интегрированное собрание фактов и обобщений [25], результат вторичной обработки данных; выявленные связи и закономерности между группами, классами данных. *Понимание* – (почему?) – объяснения выявленных закономерностей, построение теорий, дающих такое объяснение [26].

Принято считать, что знания формируются и обрабатываются только в умах людей; а данные обрабатываются вне сознания людей. Известно множество определений знаний. *Знания* - систематизированное отображение множества объектов, взаимосвязей, законов и моделей функционирования структур некоторой ПдО. В [27] приведены определения:

Знание — результат познания, который можно логически или фактически обосновать, и эмпирически или практически проверить. Знание отражает строение, структуру, функционирование и альтернативы развития объектов реального мира. Рис. 6 также иллюстрирует, что модели реального мира могут быть составляющими моделей знаний.

С развитием науки стали известны законы функционирования, статические и динамические модели реального мира. Основные виды информационных моделей РМ были приведены на рис. 5. Со становлением кибернетики были разработаны методы и модели управления реальным миром, в том числе средствами ИТ.

Знания универсума могут включать как символ в виде Универсальной/ Композиционной (символьно-образной) моделей универсума, так и результат декомпозиции некоторого уровня модели универсума [29]. Знания о ПдО могут включать частную статическую модель ПдО и целенаправленную динамическую модель ПдО. Для управления некоторой ПдО, кроме ее модели, необходимо знать законы ее функционирования, поэтому в данной работе принимаются постулаты:

К7.3. *Знания* – форма отражения структур, аконов функционирования и методов целенаправленного управления РМ.

К7.4. *Знания* - некоторая модель и законы функционирования объектной области РМ, а также способы целенаправленного управления объектной областью или моделью РМ.

С учетом [27, Юркевич] примем

К7.5. *Знания* – это информация, структурированная по важности согласно целям и желаниям пользователя.

3.2 Модели универсума - важнейшие составляющие образа мира

3.2.1 Универсальная модель мира. Согласно новой концепции Универсальной Модели [14], мир имеет конструкцию Реального Мира (РМ), над которым имеется непосредственно невидимая, но объективно существующая абстрактная надстройка в виде иерархии последовательно развивающихся Абстрактных Миров (АМ), образующих Всемирную Абстрактную Пирамиду (ВАП), начинающуюся с исходного абстракта «Ничто» и заканчивающуюся РМ (рис. 7).

Рис. 7 Абстрактная схема Вселенной

Компоненты АМ называются абстрактами и являются полноценными сущими, последовательно конкретизируемыми (наращиваемыми) в производных АМ вплоть до РМ.

Таким образом, абстракты последовательно встраиваются в абстракты низших уровней и в пределе в реальные сущие (явления) как их части, но не выделяемые в чистом виде, чем обуславливается их невидимость на всех низших уровнях. При этом, чем выше уровень абстрактов, тем труднее их выделить снизу как единое целое, но тем обще они действуют, и это действие строго закономерно. Так абстрактная часть Мира осуществляет управление РМ и при этом остается невидимой в нем.

Верхняя часть ВАП конечна по числу компонентов, непротиворечива, гармонична, симметрична и обратима, а все абстракты виртуально существуют в исходном сущем «Ничто» (Светлая часть ВАП – внутренние связи абсолютно прозрачные). Наличие универсальной модели позволит определять истинность моделей новых явлений не эмпирически, сверкой с моделью РМ, а сверкой с универсальной моделью.

Универсальная модель - модель, отображающая всю Вселенную как единое целое.

3.2.2 Композиционная модель универсума.

Основной концепцией, обеспечивающей концептуальное единство структуры модели мира и ее категориального аппарата, является представление информационных взаимодействий между объектами с помощью физических носителей взаимодействий – *коммуникэтов.* Единый поход к отображению статики и динамики ПдО позволили синтезировать идеализированный объект – *композиционную модель универсума*.

В [30] предложена абстрактная модель РМ, в виде композиции *символов* и ячеек в форме куба. Принцип построения модели включает:

A. Выделение для каждого объекта u_i универсума U ячейки объекта $я_i$ из множества $Я$;
B. Формирование в ячейке объекта $я_i$ отображения сущности объекта или ссылки на внешнюю память;
C. Объединение *символов* и ячеек, упорядоченных по категориям и ролевым признакам отображаемых объектов, в структурные элементы. Например, модули, в форме параллелепипедов;
D. Формирование отображения универсума объектов в виде композиции символов и модулей $Я_\alpha$. *Символ* - знак, наполненный (ассоциативно связанный со) смыслом. Это абстрагированная модель РМ, пригодная для расширения и дополнения содержанием конкретных абстрактных и реальных миров. Описание и пример символьно-графической модели приведено в [7].

Композиционная модель мира - некоторая композиция *локов* и соответствующих им информационных единиц (символов и образов), отражающих статику и динамику взаимодействующих между собой базовых сущностей природы (человек, объект, среда).

3.3 Уточнение классификации эмпирических и теоретических моделей представления знаний.

Знание в широком смысле — субъективный образ реальности в форме понятий, представлений и зависимостей. Знание в узком смысле — обладание проверенной информацией (ответами на вопросы), позволяющей решать поставленную задачу. Источником знаний является природа и субъект. Знание (knowleadge) — это не только представление субъекта о явлениях и закономерностях внешнего мира на естественном языке, но и соответствующее представление на машинном языке. Оперирование знаниями упрощается в случае хорошо структурированных знаний.

Рис. 8. Классификация информационных моделей представления знаний о РМ

Модель есть форма существования знаний [25]. Характерные эмпирические и теоретические модели знаний приведены на рис. 8. Модели знаний отличаются от моделей РМ прежде всего организацией знаний с определенной целью [1].

Эмпирические модели – единицы структур знаний - могут быть представлены образными и знаковыми моделями. Как отмечалось,

недостатком приведенных в [6, 32-34] представлений схем эмпирических и теоретических моделей знаний является отсутствие:

a. Принципиально важных эмпирических аналоговых образов, формируемых в технических средствах и в сетчатке глаза человека;
b. Теоретико-экспериментальных символьно-образной [7] и универсальной [14] моделей универсума.

ПВ и спектральные зонд-отражения, формируемые с помощью *коммуникэт* и сенсоров, естественно отнести к эмпирическим образным моделям. С целью единства представлений объектов РМ состав образных моделей должны быть дополнен ПВ и спектральными моделям (рис. 8). ПВ и спектральные модели-прототипы знаковых моделей – важнейшие виды моделей, связывающие материальный и информационные миры. Знаковые модели также могут представлены:

- Тройками «объект, атрибут, значение».
- Предикатами $Y_{1\text{-}n} = F\{x_1\text{-}x_m\}$ - процесс в цепочке «прототип, оперант, отображение», где Y - значение выходного коммуниканта, X - значения входного коммуниканта, F- функция преобразования.

Особенности других известных эмпирических и теоретических моделей декларативных и процедурных знаний достаточно подробно изложены в [6, 32-34]. В [6] отмечается развитие метаязыковых формализмов, а в качестве универсальной формы представления разнородных знаний – структура научной теории.

Некоторые считают, что знания – высшая форма отражения действительности. Однако, когда денотат –универсум, высшей формой отражения действительности является, очевидно, полная копия универсума.

В реальности некоторому субъекту для создания более комфортных условий существования иногда достаточно знаний, касающихся относительно небольшой части универсума, например, знания о простейших свойствах объектов. При этом знания – целенаправленная форма отражения. Таким образом,

3.4 Обсуждение результатов.

В интернете бытует мнение, что «у искусственного интеллекта (ИИ) нет единого определения, и его не стоит искать. К таким выводам пришли в компании SAS» [35]. Известный специалист в области ИИ С.Л. Крывый отмечает, что успехи в области ИИ могли привести к существенному прогрессу в теории программирования, умственного творческого труда, в социальной и гуманитарной сферах. Эти ожидания и надежды не оправдались. Одной из причин такого положения дел ногие исследователи видят в терминологическом хаосе в самом определении понятия ИИ. Отмечается, что в определениях не просматривается ядра методов, которые уникальны в этой области [36].

Рис. 9. Применение интеллектуальной информационной машины для решения сложных задач ПдО

Исходя из определенных выше отношений объектов реального мира и форм отражений в МЭИ-процессах (рис. 6), может быть предложена такая структура интеллектуальной машины (И-машины) инвариантная задачам и произвольным ПдО (рис. 9).

Структура включает следующие функциональные блоки — традиционную ИИ-машину с интеллектуальным интерфейсом, модель ПдО, решатель задач, необходимые базы знаний и интерфейс связей с окружением, включающем интеллектуальные сенсоры (агенты) и

исполнительные устройства. Причем база знаний ПдО также должна включать целенаправленные способы управления ПдО или ее моделью.

Так как программа управления ПдО формально может входить в состав базы знаний ПдО, то обобщенная структура интеллектуальной машины для некоторой ПдО может иметь вид, как на рис. 10. Тогда определение ИИ, как структуры, будет:

***Искусственный интеллект* — информационная машина с решателем задач, интерфейсами пользователя и окружения, снабженная моделью и базой знаний ПдО.**

Очевидно, что в большинстве случаев существенным является выбор методики решения задач решателем ИИ-машины и реализации интерфейса окружения. Естественно предположить, что минимум терминологических несогласований различных авторов будет достигнут при привязке терминов к РМ, а не ЯКМ. Поэтому в основу разработки ядра программных методов средств ИИ и процессов целесообразно взять физико-информационный подход и основные компоненты структуры на рис.10.

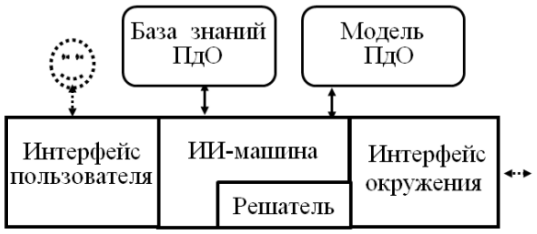


Рис. 10. Обобщенная структура

Исходя из отношений объектов реального мира и форм отражений (рис. 6), может быть предложено такое инвариантное определение функции ИИ:

***Искусственный интеллект* – объект (например, информационная машина), отличающийся состояниями и универсальным/специальным законами функционирования, содержащий модель и базу знаний ПдО.**

Эти определения, могут быть взяты в основу ядра методов средств ИИ, независимо от того «слабый» это или «сильный» ИИ.

Заключение

Приведены различия в сути определений информационных моделей, как адекватных отражений реального мира (РМ) и моделей представления знаний, как целенаправленных отражений РМ.

Исходные аналоговые отржения прототипов, формируемые сенсорами устройств ввода, - эмпирические образы РМ – целесообразно определять как компоненты информационных моделей РМ и как важнейшие компоненты моделей представления знаний. Понятие *информация* предпочтительнее определять не на основе созданной сознанием естественно-языковой картины мира, а на основе явлений материального мира.

Показано, что *коммуникэтная* и другие частные теории информации - составляющие общей теории информации, а знания – вид информации. Образные модели физического мира - важнейшие составляющие анализа информационных процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Палагин А.В., Крывый С.Л., Петренко Н.Г. Онтологические методы и средства обработки предметных знаний / Луганск 2012, с.324.
2. А.А. Мержвинский, А.А. Нерсесянц. Информация – «химера» или фундаментальная научная категория / *Труды СКФ МТУСИ – 2019.* Подготовлено по результатам Международной научно-практической конференции «ИНФОКОМ-2018» 29 – 30 апреля 2020 года, Ростов-на-Дону, с. 360-385.
3. И.Ф. Запорожцев, Д. В. Моисеев. Моделирование пространственно-временной изменчивости температуры в Таганрогском заливе с помощью модели MITgcm / Вестник МГТУ. 2017. Т. 20, № 1/2. С. 231–241.

4. Большаков Б.Е. Закон природы или как работает пространство-время. РАЕН, Межд. университет природы, общества и человека «Дубна», 2002. – 265 с.
5. Виды информационных моделей. https://www.google.com/search?q=Виды+информационных+моделей&sxsrf=ALeKk02
6. Кургаев А. Ф., Григорьев С. Н. Анализ доминирующих моделей представления и использования знаний // Управляющие системы и машины. – 2014. – № 3. – С. 64–73.
7. Мержвинский А.А. Синтез модели универсума — как теоретическая проблема кибернетики / Проблемы управления и информатики, №3, 2017, с. 160-171.
8. Глушков В.М. О кибернетике как науке / В.М. Глушков // Кибернетика, мышление, жизнь. – 1964, стр.53.
9. Нуклеиновые кислоты https://ru.wikipedia.org.wiki%D0
10. Теория коммуникации. Википедия.
11. https://studme.org/43583/psihologiya/modeli_struktury_obraza_mira.
12. Толковый словарь по инженерии знаний ./ Палагин А.В., Петренко Н.Г., Габидулин И.А. - К.: Издательство Сталь, 2014. - 292 с.
13. http://plmpedia.ru/wiki/Семантическая технология.
14. Сосницкий А.В. Универсальная модель как радикальная реформа современной науки / Математичні машини і системи, 2014, № 2, с. 161- 177.
15. Звіт. http://icybcluster.org.ua:34145/technology-documents/vk.05.36.16.pdf
16. Вечтомов, Е. М. Философия математики: монография / Е. М. Вечтомов. – Киров: Изд-во ООО «Радуга-ПРЕСС», 2013. – 316 с.
17. Мержвинский А.А. Теория информации – базовое ядро теории информатики. *Труды СКФ МТУСИ – 2019.* / Межд. научно-практическая конференции «ИНФОКОМ-2018» 19-20 апреля 2018 года, Ростов-на-Дону с. 282-295.
18. Мержвинский А.А., Будник Н.Н. Философские основы кибернетики и инфор/матики: информационный аспект / Тезисы докл. Межд. научной конф. «Современная информатика: проблемы, достижения и перспективы развития», 13-15.12.17. – Ин-т кибернетики им. В.М. Глушкова НАНУ: Киев. – с. 103-105.
19. А.А. Мержвинский, А.А. Нерсесянц. Об объектах теории информации / там же. – с. 49-62.
20. https://tehnar.net.ua/modeli-naturnyie-i-informatsionnyie/
21. Методы повышения эффективности систем электронно- лучевого экспонирования: автореф. дис... канд. техн. наук: 05.27.01 / Мержвинский Анатолий Александрович ; АН Украины, Ин-т кибернетики им. В. М. Глушкова. - К., 1992. - 17 с. http://library.lp.edu.ua/opac/page_lib.php?docid=368342&mode=DocBibRecord
22. Мержвинский А.А. Статус и соотнесение физических и информационных объектов действительного мира / *Труды СКФ МТУСИ – 2019.* Подготовлено по результатам Международной научно-практической конференции «ИНФОКОМ-2018» 29 – 30 апреля 2020 года, Ростов-на-Дону, – с. 343-359.
23. Информация как философская категория: онтологические и гносеологические аспекты. Болотова Екатерина Александровна, 2005.
24. https://ru.wikipedia.org/wiki/Модель
25. Стандарт ISO/IEC 2382-1. Термины и определения. http://www.morepc.ru/ informatisation/ iso2381-1.html
26. Знание. https://ru.wikipedia.org/wiki/https://www.google.com/Виды информационных моделей
27. Юркевич Е.В., Крюков Л.Н. / Особенности передачи образной информации/ Open education V. 21. № 5. 2017 с/ 33-431
28. ЗВІТ ЗА ПРОЕКТОМ № ВК 205.36.16 ПРОГРАМИ ІНФОРМАТИЗАЦІЇ НАН УКРАЇНИ НА 2016 РІК «СТВОРЕННЯ ПРОБЛЕМНО-ОРІЄНТОВАНИХ СИСТЕМ

ОНТОЛОГІЧНОГО АНАЛІЗУ І СИНТЕЗУ СКЛАДНИХ ОБ'ЄКТІВ НОВОЇ ТЕХНІКИ» Шифр ВК 205.36.16 (заключний) http://icybcluster.org.ua:34145/technology-documents/vk.05.36.16.pdf
29. Мержвинский А.А Патент Украины на промышленный образец № 19543 от 12.10.2009 «Комплект пристроїв для відображення універсума».
30. Мержвинский А.А. Модель универсума. Informations Models of Knowledge, XVI-th International Conference Knowledge-Dialogue-Solution, N. 15. – ITHEA, Sofia, 2009.
31. Метрология и автоматизация. http://www.energyed.ru/Auto/SysmindCh04
32. http://www.aiportal.ru/articles/knowledge-models/classification.html
33. https://ru.wikipedia.org/wiki/ Модели представления знаний.
34. М.Д. Сеченов, С.Н. Щеглов, Анализ неформальных моделей представления знаний в системах принятия решений / Известия ЮФУ. Технические науки.-2010.-№7 (108).
35. https://www.comnews.ru/content/208926/2020-09-04/2020-w36/iskusstvennyy-intellekt-ne-mozhet-nayti-opredeleniya.
36. Крывый С.Л. Проблемы анализа естественно-языковых объектов. Киевский национальный университет им. Т.Г. Шевченко. Киев, Украина. http://www.irtc.org.ua/image/Files/presentations/krivoy_2009-02-11.pdf

И.В. Головина

О ФОРМИРОВАНИИ УНИВЕРСАЛЬНЫХ КОМПЕТЕНЦИЙ В ТЕХНИЧЕСКОМ ВУЗЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: компетенции, компетентностный подход, универсальные компетенции, личностно-ориентированное образование, портфолио студента.

В статье рассматриваются проблемы, возникающие в связи с формированием универсальных компетенций у студентов, обучающихся в современном техническом вузе. Автор отмечает важность расширения списка указанных компетенций за счет включения в ФГОС 3++ группы компетенций, направленных на формирование экономической культуры и финансовой грамотности выпускников. Отмечается трудность измерения степени сформированности универсальных компетенций. В статье сформулированы предложения по совершенствованию методов контроля и оценивания результатов обучения.

I.V. Golovina

ON THE FORMATION OF UNIVERSAL COMPETENCES AT THE TECHNICAL UNIVERSITY

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

Keywords: competence, competence approach, universal competences, student-centered education, student portfolio.

The article examines the problems arising in connection with the formation of universal competencies among students studying at a modern technical university. The author notes the importance of expanding the list of these competencies by including a group of competencies aimed at the formation of economic culture and financial literacy of graduates into the Federal State Educational Standard 3 ++. The difficulty of measuring the degree of formation of universal competencies is noted. The article formulates proposals for improving the methods of monitoring and evaluating learning outcomes.

Компетентностный подход давно утвердился в высшей школе и, тем не менее, требует совершенствования, о чем свидетельствует постоянная работа над обновлением государственных образовательных стандартов третьего поколения. Последним во времени новшеством является расширение перечня универсальных компетенций за счет добавления новых групп, в частности УК-9 и УК-10, касающихся соответственно формирования экономической культуры и гражданской позиции будущих бакалавров [1].

Цель настоящей статьи заключается в выявлении возможностей достижения универсальной компетенции УК-9 средствами экономических дисциплин, предусмотренными образовательной программой и определении поддающихся измерению индикаторов освоения указанной компетенции.

Как известно, универсальные компетенции являются сквозными и едиными для всех направлений подготовки. Поэтому определение «универсальные» представляется более точным, чем ранее использовавшийся термин «общекультурные компетенции». Если универсальные компетенции осваиваются прежде всего в ходе изучения учебных дисциплин, а значит, неизбежно формируется некий профессиональный контекст, с учетом влияния которого формулируются индикаторы достижения этих компетенций, то определение «общекультурный» ориентирует на развитие кругозора как такового, что выглядит как «надстройка» над профессиональной подготовкой. Это может создать впечатление некой «необязательности», «факультативности» освоения этих компетенций, и вместе с ними и соответствующих дисциплин, в основном социальных и гуманитарных.

Осмысливая специфику реализации универсальных компетенций в реалиях технического вуза, можно выделить часть компетенций, которые формируются в первую очередь средствами конкретных учебных дисциплин и составляют цель изучения этих дисциплин, и другую часть, которая обеспечивается в ходе всего процесса обучения, рассматриваемого как единство учения и воспитания. В этой условной классификации к первой группе компетенций относятся УК-4, УК-5. УК-7, УК-8, УК-9. Вторую группу образуют компетенции УК-1, УК-2, УК-3, УК-6, УК-10. В их формировании участвуют все дисциплины, включая те, которые ориентированы по преимуществу на освоение профессиональных компетенций, а также воспитывающие мероприятия, проводимые в рамках внеучебной деятельности. Существенную роль может сыграть и правильно организованная практика студентов на предприятиях.

В связи с этим едва ли правильно, как это довольно часто делается, отдавать формирование универсальных компетенций «на откуп» дисциплинам, относящимся к обязательной части учебного плана. Освоение универсальных компетенций на протяжении всего процесса обучения будущих бакалавров обеспечивает формирование базиса, который позволит им реализоваться как в профессии, так за пределами профессиональной подготовки. Важнейшая функция универсальных компетенций заключается в том, чтобы вооружить выпускников знанием принципов принятия решений безотносительно к конкретной профессиональной области, создать предпосылки мобильности на рынке труда, а также возможность продолжать обучение на более высоких ступенях образования.

Если же говорить о задачах частного характера, то несмотря на «надпрофессиональный» характер, универсальные компетенции тесно связаны с профессиональными и даже с трудовыми функциями, прописанными в профессиональных

стандартах. Так, например, в профессиональном стандарте 06.022 «Системный аналитик» в числе прочих предусмотрены такие трудовые функции, как постановка целей создания системы, разработка концепции системы, разработка методик выполнения аналитических работ, планирование этих работ и т.п. Совершенно очевидно, что готовность выпускника к выполнению перечисленных трудовых функций во многом зависит от степени освоения им универсальных компетенций, таких, как, например, УК-1 и УК-2, т.е. от его способности определять круг задач в рамках поставленной цели, выбирать оптимальные способы их решения, применять системный поход и т.д. Конечно, такие, казалось бы, общие качества, должны целенаправленно формироваться в контексте будущей профессиональной деятельности, а, значит, в том числе, и средствами специальных дисциплин. В сущности, другими средствами для реализации компетентностного подхода, кроме как через изучение учебных дисциплин, вуз и не располагает. Поэтому представляется ошибочным суждение о том, что компетентностный подход пришел на смену знаниевому подходу, что главное – это не информированность обучающегося, а его способность осваивать приемы решения практических и профессиональных задач [2]. Здравый смысл подсказывает, что знание темы, профессиональной проблемы предшествует поиску методов и приемов ее решений. Формат образовательного процесса в вузе не предполагает формирование компетенций независимо от конкретных учебных дисциплин. Понятно, что компетенция имеет когнитивный и деятельностный аспекты, причем последний, по определению, является более важным, однако реализовать его в академической среде довольно проблематично, поскольку окончательная проверка степени достижения компетенций происходит в реальной производственной среде. Работодатель в конечном итоге оценит, насколько качества выпускника соответствуют конкретным трудовым функциям [3]. Поэтому было бы ошибочно противопоставлять друг другу когнитивный и деятельностный аспекты компетенций: реальный современный вуз все же «заточен» в основном под предметный, дисциплинарный путь формирования компетенций и располагает определенными возможностями в этом плане.

Включение в состав универсальных компетенций группы компетенций, нацеливающих на формирование экономической культуры и финансовой грамотности, является важным вкладом в дело подготовки будущих профессионалов. Наконец пришло понимание того, что выпустить бакалавра, не подготовив его к принятию экономически обоснованных решений, не сформировав у него того, что называют экономическим образом мысли – это значит допустить серьезный пробел в системе образования. Ведь любой вид деятельности, имеет экономическое измерение, любое решение приводит к экономическим и финансовым последствиям. Речь при этом идет не только о профессиональных решениях; выпускникам, вступающим во «взрослую» трудовую жизнь, придется планировать личный, семейный бюджет, заботиться о сохранении или преумножении своих доходов и делать это осознанно, с пониманием складывающейся экономической ситуации. Безусловно, не факт, что, изучив основы экономики, выпускник сразу станет принимать исключительно рациональные экономические решения, да это и невозможно в условиях неопределенности хозяйственной среды. Но он должен иметь четкие ориентиры, он должен понимать, как работают экономические механизмы, чтобы не стать объектом манипуляций со стороны опытных рыночных игроков или финансовых мошенников. Тем более важно привнести рациональность в решение профессиональных проблем, где экономические, финансовые соображения при выборе тех или иных альтернатив могут оказаться решающими.

В таком случае встает вопрос о том, как развернуть экономическую теорию, чтобы она работала на достижение УК-9, т.е. на формирование у студентов способности принимать экономически обоснованные решения в разных областях жизнедеятельности. Конечно, ключевые вопросы, темы задаются индикаторами достижения компетенции, представленными в примерных образовательных программах. Однако необходимо учитывать направление подготовки, профиль и вид деятельности, к которому готовят

будущего бакалавра и правильно расставить акценты в содержании дисциплины, а также продумать методику проведения практических занятий. Вне профессионального контекста едва ли можно рассчитывать на должную результативность освоения универсальных компетенций.

На первый взгляд может показаться, что можно ограничиться исходными экономическими положениями, такими, как ресурсы, доходы, спрос, предложение, рынок, цены, конкуренция, издержки производства, прибыль, валовой внутренний продукт, занятость, инфляция, сбережения, инвестиции и т.п., привязать их в российским экономическим реалиям, и этого в принципе будет достаточно для формирования основ экономической культуры. Безусловно, студент должен знать базовые экономические понятия, уметь говорить на языке экономических категорий, что поможет будущему инженеру, бакалавру в перспективе успешно общаться с представителями бизнеса. Однако содержание курса экономической теории все же следует скорректировать и, прежде всего, отказаться от избыточного академизма, абстрактных положений. Традиционные темы должны опираться не только на примеры из российской хозяйственной жизни, но и на особенности соответствующей отрасли и сферы будущей профессиональной деятельности.

Подготовка бакалавров по направлению «Информатика и вычислительная техника» предполагает обращение к проблемам функционирования и развития отрасли инфокоммуникаций, сформировавшейся в результате конвергенции традиционной связи и информационных технологий. Новая отрасль является высококонцентрированной, на рынке действуют крупные хозяйственные субъекты, включая естественные монополии. На фоне цифровизации возникают новые формы доминирования на рынке, связанные с сетевыми эффектами, большими данными, которыми оперируют цифровые гиганты. Поэтому есть смысл направить внимание студентов на эти новые явления и новые проблемы, адресовать их к сайтам публичных акционерных обществ, действующих в сфере инфокоммуникаций, сформулировать по этим материалам соответствующие задания на практические занятия и на самостоятельную работу. Например, студентам вполне по силам рассчитать на примере рынка услуг сотовой связи известный индекс Херфиндаля-Хиршмана и тем самым оценить уровень концентрации этого рынка. Или, скажем, проанализировать факторы внешней среды, влияющие на предприятия отрасли, и продумать способы их адаптации к возможным вызовам со стороны внешнего окружения. Главная идея заключается в том, чтобы научить студентов применять знания основ экономического устройства общества к исследованию процессов, происходящих в профессионально близкой им сфере. Возможностей подобного рода достаточно, поскольку любой процесс или явление так или иначе имеет экономическое измерение.

Если бакалавров готовят к проектной деятельности, то особое внимание стоит уделить теме планирования, в частности, бизнес-планирования. Разумеется, формат учебных занятий и ограниченный бюджет времени не позволят студентам освоить какие-либо навыки в этой области. Там не менее, главные разделы бизнес-плана, его предназначение, этапы разработки, отличия от традиционного технико-экономического обоснования проекта студенты должны себе представлять и владеть необходимыми для этого категориями, такими, как инвестиции, доходы, прибыль, затраты, риски и т.п.

Проектно-ориентированная методика должна занять заметное место в преподавании экономической теории. Можно предложить студентам достаточно много тем, работа над которыми будет способствовать достижению и других универсальных компетенций помимо УК-9, например, как УК-1, УК-2 и УК-3. Так, широкое поле для формирования навыков поиска и систематизации информации, определения целей и задач проектирования открывают такие темы, как, например, «Сравнительный анализ инвестиционных программ компаний-операторов мобильной связи», или Экономические последствия введения цифрового рубля». В то же время проектно-ориентированные занятия являются наиболее

продуктивными при организации работы малыми группами, а их темы могут быть предложены и самими студентами.

Наиболее сложным представляется вопрос о процедурах оценки степени достижения универсальных компетенций, особенно тех из них, на формирование которых должны работать различные дисциплины, в том числе, специальные, профильные. Совершенно очевидно, что традиционные зачеты и экзамены не могут рассматриваться как надежное средство измерения степени сформированности компетенций. Эти и подобные им формы контроля в лучшем случае послужат для оценивания когнитивного, но никак не деятельностного аспекта компетенции. Другими словами, с их помощью можно оценить степень освоения соответствующей дисциплины, но вовсе не готовности со стороны будущих бакалавров применять полученные знания на практике. Еще более проблематичной является оценка сформированности той части универсальных компетенций, которые по сути не привязаны к какой-либо конкретной дисциплине и должны в идеале достигаться в результате освоения всей образовательной программы. Объективные критерии оценивания достижения таких компетенций отсутствуют. Самый простой выход, к которому прибегают в реальной вузовской практике – это привязка указанных компетенций к каким-либо дисциплинам гуманитарной или общенаучной направленности, что переводит оценку универсальных компетенций в сферу ответственности преподавателей, принимающих рутинные экзамены и зачеты по своим предметам.

Понимание того, что контрольные процедуры в условиях компетентностного обучения должны быть качественно иными, находит отражение в оценочных материалах, разрабатываемых преподавателями. В частности, предлагается решение ситуационных задач, проведение компетентностно-ориентированного тестирования с кейс-наполнением, комплексные творческие задания с учетом междисциплинарных связей и т.д. Однако, будучи «заточенными» под оценку предметных знаний и умений, эти и другие методические инструменты могут только косвенно свидетельствовать в пользу сформированности «надпредметных» компетенций.

Решение проблемы возможно на пути перехода к личностно-ориентированному обучению, о преимуществах которого пишут многие исследователи [4]. Повышая степень субъектности студента, как равноправного участника образовательного процесса, личностно-ориентированное обучение создает возможности для саморазвития, выстраивания индивидуальной образовательной траектории студента с учетом его интересов, способностей, личного опыта. Если удается реализовать подобную модель, то создаются условия, в которых процесс формирования таких универсальных компетенций, как, например, способность осуществлять социальное взаимодействие и работать в команде, способность управлять своим временем, способность к саморазвитию, может стать наблюдаемым и регулируемым. Важным инструментом оценки и самооценки универсальных компетенций может стать портфолио студента, в котором фиксируются и подтверждаются документально все достижения студента за период его обучения. Именно портфолио может наиболее полно отобразить личностный аспект компетенций, уровень их освоения, обусловленный способностями студента, его вовлеченностью в учебную и внеучебную деятельность, его активностью в разных областях. Практику разработки портфолио необходимо совершенствовать с учетом необходимости более полной реализации универсальных компетенций. Это означает, что портфолио не должно быть простым собранием учебных работ студентов и полученных ими грамот и дипломов. В нем должна находить отражение и собственная рефлексия студентов по поводу образовательного процесса, отзывы кураторов, преподавателей, руководителей практики, фиксирующие значимые этапы обретения ими требуемых компетенций.

Таким образом, приходится констатировать, что существующий формат организации учебного процесса в высшей школе не обеспечивает достаточно полного и

объективного измерения степени сформированности универсальных компетенций. В конечном итоге компетентность выпускника получит оценку в ходе его профессиональной деятельности, реализуется в его карьере и личностном росте.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт высшего образования — бакалавриат по направлению подготовки 09.03.01 «Информатика и вычислительная техника». Редакция с изменениями № 1456 от 26.11.2020 (электронный ресурс) // Режим доступа: http://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Bak/090301_B_3_15062021.pdf
2. Тарханова И.Ю. Формирование универсальных компетенций студентов вуза средствами учебной и производственной практики. // Социально-политические исследования. — 2019, № 1, с. 110 – 118.
3. Головина И.В. Компетентностная модель образования: трудности реализации. // Труды СКФ МТУСИ, часть 2. — Ростов-на-Дону, 2019, с. 26-31. // Режим доступа: http://umo.skf-mtusi.ru/sbornik/sb2019_2.pdf
4. Докучаев С.А., Костецкая Г.С., Светличная Н.О. Особенности реализации компетентностного подхода в преподавании общенаучных дисциплин в условиях перехода к новым образовательным стандартам. // Труды СКФ МТУСИ. — Ростов-на-Дону, 2020, с. 162-166. // Режим доступа: http://umo.skf-mtusi.ru/sbornik/sb2020.pdf

А.М. Коршун, Е.А. Гендриксон

КИБЕРДИПЛОМ КАК ИНСТРУМЕНТ ДЛЯ ПОДГОТОВКИ ДОКУМЕНТОВ ОБ ОБРАЗОВАНИИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: диплом, приложение к диплому, программный продукт КиберДИПЛОМ, оптимизация, автоматизация, защищенность, быстродействие, FastReport, техническая поддержка.

В работе рассмотрена программа КиберДИПЛОМ для подготовки документов об образовании государственного образца. Выделены её основные достоинства, которые включают высокий уровень защищенности, быстродействие, возможность технической поддержки, наличие универсального редактора FastReport. Проанализированы основные инструменты и функции программы. Обоснована популярность данного программного продукта, а вместе с тем, предложены варианты усовершенствования и модернизации программы для более комфортной работы при подготовке документов об образовании.

A.M. Korshun, E.A. Gendrikson

CYBERDIPLOM AS A TOOL FOR THE PREPARATION OF A DOCUMENTs ON EDUCATION

North-Caucasian branch of the Moscow technical university of communication and informatics, Rostov-on-Don, Russia

Keywords: diploma, diploma supplement, CyberDIPLOM software product, optimization, automation, security, performance, FastReport, technical support.

This article presents CyberDIPLOM software for preparation of the state standard documents on education. Its main advantages which include a high level of security, performance, the possibility of technical support, presence of a universal FastReport editor are highlighted. The main tools and functions of the program are analyzed. Wide use of this software is justified, at the same time, options for improving and modernizing the program for more comfortable work during the preparation of educational documents.

Тема информационных технологий в образовательном процессе особенно актуальна в двадцать первом веке. На данный момент человечество стремится к оптимизации и автоматизации практически всех процессов. Рассмотрим одну из сторон образовательного процесса – получение документа об образовании и о квалификации. Диплом – официальный документ об окончании начального профессионального (специального), среднего профессионального или высшего учебного заведения и присвоении соответствующей квалификации. Получение документа об образовании государственного образца (диплома) – это финальный и один из самых важных этапов обучения студента.

Для заполнения бланков дипломов и приложений к ним в каждом учебном заведении имеется сотрудник с навыками работы в соответствующей программе [1]. Существует множество различных программных продуктов для формирования этих документов. Среди них можно выделить следующие программы: «Мастер Диплом», «Дипломы СПО 5.5», «Диплом и приложения к нему», «Приложения к диплому 2.4», «КиберДИПЛОМ» и др. - все они способны справиться со своей основной задачей.

«КиберДИПЛОМ» - один из самых популярных в России программных продуктов для подготовки документов об образовании государственного образца. Эту программу, которая разработана с учётом требований действующих инструкций по заполнению бланков дипломов и приложений к ним и зарегистрирована в Реестре программ для ЭВМ Федеральной службой по интеллектуальной собственности, патентам и товарным знакам, используют около трех тысяч российских учебных заведений в своей деятельности. Системные требования для работы с данным программным обеспечением базовые. КиберДИПЛОМ-ВПО разработан с учетом требований приказов Министерства образования и науки России №1100 от 01.10.2013г. [2] и №112 от 13.02.2014г. [3].

Программа КиберДИПЛОМ удобна в использовании. Она имеет понятный интерфейс и множество различных функций, которые упрощают и ускоряют работу специалиста с различными бланками титулов и приложений к дипломам, начиная от бакалавров и заканчивая адъюнктурой.

Обратимся к достоинствам данного программного обеспечения.

КиберДИПЛОМ обладает высоким уровнем защиты. Программа использует лицензированные Федеральной Службой Безопасности (ФСБ) и Федеральной службой по техническому и экспортному контролю (ФСТК) России программно-аппаратные средства защиты информации от несанкционированного доступа, средства идентификации и аутентификации пользователей производства ЗАО «Актив-софт». Программа привязана к

определенному компьютеру и может быть запущена только при наличии USB-ключа, существующего в единственном экземпляре.

КиберДИПЛОМ имеет функции импорта и экспорта данных. Нельзя не отметить высокую скорость ввода данных и их обновление. Так, например, есть возможность создания шаблонов для студентов разных групп, но одного профиля (диплом бакалавра). Данные о часах, дисциплинах и учебном заведении можно использовать из года в год, тем самым сохраняя приличное количество времени. Также значительно упрощена функция внесения оценок: ввод осуществляется с помощью цифр, а программа сама изменяет их на слова.

Еще одним достоинством обеспечения является наличие универсального редактора FastReport, который позволяет отредактировать внешний вид документа. В системе можно настроить интервалы, расположения блоков и таблиц на бланке. С помощью объекта «Текст» пользователь самостоятельно выбирает шрифт, его размер, цвет и стиль. Такой объект как «Бэнд» позволяет логически сгруппировать данные в необходимой области листа. Так, например, поместив объекты на бэндах типа «Заголовок страницы» или «Подвал страницы», пользователь сообщает системе FastReport, что информация должна помещаться на каждой странице готового отчета вверху или внизу соответственно. Все настройки можно сделать визуально с помощью панелей инструментов, а также выполнить их предварительный просмотр. После создания необходимого дизайна у пользователя имеется возможность создать его шаблон и использовать для последующих документов. Однако стоит отметить, что на официальном сайте программы «КиберДИПЛОМ» www.cybertronix.ru уже имеются шаблоны отчетов для различных типографий страны, которые достаточно просто загрузить в программу и начать использование.

В случае возникновения проблем или вопросов во время заполнения бланков документов об образовании на помощь пользователю приходит техническая поддержка. Она осуществляется по электронной почте и телефону в режиме онлайн. На любой сложный вопрос пользователю приходит грамотный совет, решающий основную проблему.

КиберДИПЛОМ является довольно популярной программой, причем не без оснований. Данную программу используют в крупнейших университетах России. Среди них юридические институты, учебные заведения культуры и здравоохранения, а также множество негосударственных образовательных учреждений.

КиберДИПЛОМ-ВПО, безусловно, оптимизирует работу сотрудника с бланками титулов и приложений к дипломам, однако существуют некоторые особенности, усовершенствовав которые программа станет более привлекательной.

Несомненным достоинством данного программного продукта является наличие на сайте разработчика в разделе Инструкции «Руководства пользователя КиберДИПЛОМ-ВПО» отдельно для всей программы и для редактора отчетов FastReport. Однако у начинающего пользователя могут возникнуть проблемы с рядом тонкостей в работе, которые не раскрыты в вышеуказанных документах.

Так, например, в «Руководстве пользователя КиберДИПЛОМ-ВПО» целесообразно обозначить следующий момент:

- в окне программы «Настройка» на вкладке «Параметры» указываются полное официальное наименование образовательной организации, наименование населенного пункта, в котором находится образовательная организация, а также фамилия, имя и отчество руководителя (полностью, без сокращений). Пользователь, конечно, имеет возможность отредактировать информацию во вкладке «Параметры». Однако необходимо помнить, что нововведенные данные автоматически будут применяться ко всем, даже ранее, созданным отчетам, которые сотрудник будет открывать на данном компьютере в программной среде «КиберДИПЛОМ».

Ежегодно в образовательную организацию поступают заявления на выдачу дубликата документа об образовании. Данная процедура не занимает много времени, однако иногда возникают проблемы, требующие быстрого решения.

Приведём пример: последняя версия программы разработана с учётом требований действующих инструкций по заполнению бланков дипломов и приложений к ним образца 2014 года. Нам приходится заполнять дубликаты документов, которые были выданы ранее. Формат приложения к диплому поменялся (А4 на А3) и изменилась структура заполнения приложения к диплому в целом.

Решением этой проблемы могла бы стать функция перевода приложения к диплому из формата А4 в формат А3 автоматически. Все требования по заполнению дубликатов описаны в приказе Министерства образования и науки РФ от 13 февраля 2014 г. № 112. Таким образом, требования являются едиными, а, следовательно, можно было бы оптимизировать создание дубликатов документов, разработав для них отдельный шаблон с необходимыми настройками в программной среде «КиберДИПЛОМ». На данный момент оперативно и качественно решать возникающие у пользователя вопросы по этой и другим проблемам помогает техническая поддержка.

Согласно главе 2 пункта 13 приказа Министерства образования и науки РФ от 13 февраля 2014 г. № 112 "Об утверждении Порядка заполнения, учета и выдачи документов о высшем образовании и о квалификации и их дубликатов" диплом и приложение к нему могут быть подписаны исполняющим обязанности руководителя организации или должностным лицом, уполномоченным руководителем организации на основании соответствующего приказа. При этом перед надписью на бланке «Руководитель» указывается символ «/» (косая черта). Данную манипуляцию можно было бы автоматизировать.

И так, существует множество различных программных продуктов для заполнения бланков дипломов и приложений к ним. Программа «КиберДИПЛОМ» имеет понятный интерфейс, предлагает своим пользователям широчайший набор функций, таких как, высокая скорость ввода данных и их обновление, функции импорта и экспорта данных, создание и использование различных шаблонов, наличие универсального редактора FastReport. Однако работу с программой «КиберДИПЛОМ» можно усовершенствовать посредством модернизации программного обеспечения и переработки «Руководства пользователя КиберДИПЛОМ-ВПО». В результате, работа над документами выпускников может стать более привлекательной, а также появится возможность максимально исключить некоторые ошибки пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Коршун А.М., Дерещук Д.О., Родякин П.А. Информационные технологии в образовательном процессе. //«ИНФОКОМ-2015»/ Материалы международной молодежной научно-практической конференции СКФ МТУСИ, Труды СКФ МТУСИ. Часть II - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, - с. 208-210.
2. Приказ Министерства образования и науки РФ от 01 октября 2013 г. № 1100 "Об утверждении образцов и описаний документов о высшем образовании и о квалификации и приложений к ним".
3. Приказ Министерства образования и науки РФ от 13 февраля 2014 г. №112 "Об утверждении Порядка заполнения, учета и выдачи документов о высшем образовании и о квалификации и их дубликатов".

Д.А. Жуковский, А.Г. Жуковский, А.А. Бородина

РОЛЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ ЭКОНОМИКИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: организация, технологии, информация.

Аннотация. В статье рассмотрена сущность и виды мобильных приложений на современном этапе развития экономики. Выявлены основные критерии оценки приложений. Рассмотрены основные аспекты инфокоммуникационных технологий в экономике. Рассмотрены основные отличия приложений. Приведены примеры современных мобильных приложений.

D. A. Zhukovsky, A.G. Zhukovskii, A.A. Borodina

ROLE OF MOBILE APPLICATIONS IN THE MODERN STAGE OF ECONOMIC DEVELOPMENT

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

Key words: organization, technologies, information.

Annotation. The article examines the essence and types of mobile applications at the present stage of economic development. The main criteria for evaluating applications are identified. The main aspects of infocommunication technologies in the economy are considered. The main differences between the applications are considered. Examples of modern mobile applications are given.

Современное представление о способе передачи информации с помощью мобильных сетей связи изменяется с каждым новым днем. На рынке мобильных приложений с небывалой скоростью увеличивается количество программных средств, с помощью которых выполнение обычных функций становится более удобным, а также появляется все больше приложений, которые способны агрегировать ряд функций в единое целое и создавать готовый и главное качественный продукт. Так, рынок современных программных средств дает пользователям возможность выбора большого количества приложений, которые в одних аспектах могут помочь пользователю, а в других выполнить целые действия за него, тем самым упрощая его жизнь.

Информационные технологии заставили полностью переосмыслить принципы построения взаимодействий организации с клиентом, тем самым уменьшая необходимость в посредниках, физическом воплощении продукта, личном присутствии клиента для выбора товара или оказания услуги, а также необходимости подписания документов. В эпоху цифровой экономики решение о характеристиках производимого продукта или услуги принимает не ее изготовитель, а потребитель. Именно клиент на сегодняшний день диктует рыночные правила и задает тренды, а компании стараются создать максимально широкий спектр связанных товаров и услуг. Исходя из этого, можно сказать о том, что необходимость одноразовой продажи некого товара перестает иметь ценность для организации. Компании заинтересованы в предоставлении не одной услуги, а целого комплекса, не унифицированного товара, а одной из составляющих группы товаров, с

целью вовлечения в собственную экосистему. Данный подход уже успешно реализуют компании «Samsung», «Amazon», «Apple», «Huawei» и другие. Главным инструментом построения такого рода взаимоотношений является информация о клиенте, посредством которой производитель и формирует свои предложения. Происходит это благодаря информационным технологиям, а именно, сетям интернет, которые хранят себе данные о каждом пользователе, хотя бы единожды побывавшем на том или ином сайте, заполнившем некоторую форму и т.д. Каждое движение пользователя в сети интернет несет за собой информацию, которая говорит о нем, как о потребителе того или иного товара или услуги. Исходя из этого, конкурентное преимущество и, соответственно, успех в бизнесе будет у той организации, которая имеет доступ к информации и механизмы ее быстрого анализа для принятия управленческого решения. Наиболее яркими представителями такого принципа ведения бизнеса выступает «Alibaba group», успех деятельности которой обусловлен сбором всей поступающей информации извне и ее обработкой на полезность с помощью искусственного интеллекта. Примерами организаций, эффективно использующей преимущества цифровой эпохи в России, служат такие компании как «Сбербанк», «Тинькофф Банк», «Яндекс», «Mail.ru Group», «Avito» цифровая экономика является основным источником роста. Это будет стимулировать конкуренцию, инвестиции и инновации, что приведет к улучшению качества услуг, расширению выбора для потребителей, созданию новых рабочих мест [3].

Рассматривая рынок приложений, стоит отметить тот факт, что большая часть из них – это уже не крупные компании разработчики, а все чаще небольшие компании или даже индивидуальные разработчики. Что в целом накладывает дополнительные аспекты в плане выбора того или иного приложения для пользователя. Не всегда пользователь готов самостоятельно выбрать нужное ему приложение из большого списка доступных, даже с учетом ряда рейтингов и оценок, которые дают современные информационные площадки.

От качества мобильных приложений зависит удобство его использования для пользователей и популярность среди целевой аудитории приложения, рейтинг, количество установок, отзывы и т.д.

Перед созданием мобильного приложения разработчик исходит из двух основных аспектов:

- Целевая аудитория приложения (пол, возраст, сфера деятельности);
- Цель создания мобильного приложения.

Мобильное приложение должно быть удобным целевой аудитории и выполнять ту цель, которая была поставлена при создании. Помимо этих основных аспектов мобильное приложение должно быть качественно сделано и быть не хуже приложений конкурентов, а возможно даже лучше. Оценку качества лучше выполнять по чётко сформулированным критериям.

Требования к дизайну мобильных приложений постоянно растут. На сегодняшний день существуют популярные направления в дизайне и при разработке это надо учитывать, но при этом восприятие пользователем приложения не должно ухудшаться. Дизайн должен соответствовать целевой аудитории приложения.

Искажения в графическом дизайне могут возникнуть при использовании мобильного приложения на определенных моделях смартфонов (особенно на устаревших моделях).

Очень важной особенностью любого мобильного приложения, является его фактическая функциональность, а именно готовность эффективно выполнять именно те задачи, которые перед ним ставит пользователь. Очень часто большое количество приложений используют в своих рекламных лозунгах желание удовлетворить всех потенциальных пользователей, что не всегда удается на практике. Чаще всего функционал приложения ограничен его техническими параметрами, либо искусственно самим разработчиком для того, чтобы в дальнейшем этот дополнительный функционал продать

как платную функцию. Данная практика все больше набирает популярность, и уже большая часть всех приложений реализует дополнительные функции на платной основе.

Использование организациями корпоративных приложений позволяет отслеживать деятельность каждого сотрудника, так как в приложении у всех работников есть личный кабинет для входа в систему, что в итоге помогает быстрее реагировать на неполадки и неверные действия. Таким образом сокращается время на корректировку бизнес-процессов предприятия. [1].

Организации используют возможности мобильных приложений, чтобы сделать свою деятельность удобной, эффективной и прибыльной. Используя мобильные приложения, компании расширяют свои функции, исследуя новые возможности и трансформируя всё, что связано с тем, как работает бизнес. Многие компании-разработчики мобильных приложений постоянно просвещают массы о стратегической важности мобильных приложений, и рано или поздно как потребители, так и корпоративные пользователи начнут использовать мобильные приложения для достижения более высоких целей. Мобильный маркетинг предоставляет компаниям потенциал для взаимодействия с клиентами в режиме реального времени через местоположение и полную информацию об их профиле. Контроль, мониторинг и использование данной информации смогут превратить этих потенциальных клиентов в реальных с помощью маркетинга мобильных приложений [2].

Современные тенденции развития отраслевых рынков предопределили необходимость перехода от привычной бизнес-модели к цифровой. Использование мобильных приложений, CRM, SRM, TMS, ERP определяет уровень цифровой трансформации организации, которая, в свою очередь, выступает важным фактором в обеспечении конкурентоспособности организации [4].

Для людей, которые перешли на удаленную работу, Slack и Zoom стали незаменимыми и жизненно необходимыми инструментами. Неотъемлемой частью продвижение услуг компаний стало продвижение в социальных сетях, таких как Facebook, Instagram, вКонтакте. Таким образом, цифровизация открывает новые возможности создания добавленной стоимости и повышения конкурентоспособности организации [5].

Подводя итоги, можно отметить, что мобильные приложения значительно сокращают время на поиск той или иной информации, а также предоставляют огромный спектр возможностей в выстраивании коммуникаций с партнерами и коллегами и реализации бизнес-процессов. На современном этапе можно говорить не только о пользе приложений в обычной жизни, для упрощения бытовых задач, но теперь приложения являются неотъемлемой частью решения рабочих задач, что в целом очень часто позволяет упростить сложные рабочие задачи.

СПИСОК ЛИТЕРАТУРЫ

1. *Ремаренко, С. А.* Анализ возможностей использования технологий мобильных приложений в деятельности предприятия / С. А. Ремаренко, Д. А. Фролов. — Текст : непосредственный // Молодой ученый. — 2015. — № 22.5 (102.5). — С. 32-34.
2. Мобильный маркетинг. [Электрон. ресурс]. – Режим доступа: https://spravochnick.ru/marketing/mobilnyy_marketing/ (дата обращения: 7.10.2021).
3. Цифровая экономика. [Электрон. ресурс]. – Режим доступа: https://ec.europa.eu/jrc/en/research-topic/digital-economy (дата обращения: 12.10.2021).
4. Современные аспекты формирования инновационной экономики и менеджмента: моногр. / *К.А. Бармута, И.О. Богданова, Ю.К. Верченко* и др.; под общ. ред. *К.А. Бармуты*; Донской гос. техн. ун-т. – Ростов-на-Дону: ДГТУ, 2020. – 159 с.
5. Цифровая трансформация экономики и промышленности: проблемы и перспективы: моногр. / *А. А. Алетдинова, И. А. Аренков, Р. Р. Афанасьева* и др.; под общ. ред. *А.*

В. Бабкина; Санкт-Петербургский политехнический университет Петра Великого. – Спб, 2017. – 216 с

Б.Б. Конкин

ОБЩИЕ НАПРАВЛЕНИЯ НАУЧНОЙ РАБОТЫ КАФЕДРЫ ОНП, НАУЧНЫЙ ПОТЕНЦИАЛ И ВОЗМОЖНОСТИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: социальная культура, безопасность, экологичность, пироэлектрический и пьезоэлектрический эффекты, экономическое мышление, анизотропная среда, ударное взаимодействие, информационная безопасность, фазовый переход, гидролого-гидрохимические параметры, интегральные операторы, исследования аббревиатур, природа сознания, методология педагогики, образовательная парадигма, компьютерная программа, инновационные технологии, цифровизация образования.

В статье представлены основные направления научно-исследовательской работы кафедры общенаучной подготовки в целом и спектр научных интересов и достижения ее сотрудников.

B.B. Konkin

GENERAL DIRECTIONS OF SCIENTIFIC WORK OF THE ONP DEPAMENT, SCIENTIFIC POTENTIAL AND OPPORTUNITIES

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

Keywords: social culture, safety, environmental friendliness, pyroelectric and piezoelectric effects, economic thinking, anisotropic environment, shock interaction, information security, phase transition, hydrological and hydrochemical parameters, integral operators, studies of abbreviations, nature of consciousness, methodology of pedagogy, educational paradigm, computer program, innovative technologies, digitalization of education.

The article presents the main directions of the research work of the Department of General Scientific Training in general and the range of scientific interests and achievements of its employees.

Основными направлениями научно-исследовательской работы кафедры общенаучной подготовки являются:

1. Математическое моделирование систем и процессов.
2. Проблемы педагогики высшей школы.
3. Информационные технологии в образовательном процессе.
4. Повышение безопасности и экологичности предприятий ЮФО.

В целом кафедра ОНП осуществляет изыскания по довольно широкому спектру научных направлений, поскольку объединяет преподавателей различных областей знаний.

Профессор Барабанова Виктория Борисовна проводит исследования в области Физической культуры и спорта через призму социально-философского осмысления, направленного на достижение наивысшего результата. В частности, показано, что физическая культура и спорт являются элементами социальной культуры. А философский научный анализ способствует открытию дополнительных возможностей преодоления ограниченности и односторонности явлений физической культуры и спорта. Помогает раскрывать многогранность различных видов жизнедеятельности человека и не только в спорте.

Исследования профессора Бинеева Энвера Абдулхаковича направлены на повышение безопасности и экологичности различных предприятий и производств ЮФО. Его научные разработки позволяют раскрывать новые представления о роли и состоянии газов в угольных пластах, которые, в свою очередь, являются теоретической базой для решения газостатических и газодинамических задач при освоении угольных формирований. Результаты научных исследований Э.А. Бинеева публикуются в журнале «Химия твердого топлива», в материалах различных международных научно-практических конференций, а также используются на предприятиях водохозяйственного и агропромышленного комплексов нашего региона.

Доцент Бородин Алексей Викторович занимается исследованием электрофизических свойств сегнетоэлектрических материалов. При этом большое внимание уделяется пироэлектрическому и пьезоэлектрическому эффектам и их применению в электронике. Рассматриваются новые перспективные материалы с целью создания на их основе пироэлектрических приемников излучения, пьезоэлектрических трансформаторов и датчиков, обладающих заранее заданными электрофизическими и пироэлектрическими характеристиками. Результаты исследований А.В. Бородина публикуются в журналах «Фундаментальные проблемы радиоэлектронного приборостроения», «Известия Российской академии наук», «Неорганические материалы».

Старший преподаватель Гаевская Любовь Александровна проводит исследования, направленные на развитие методов, повышающих уровень функционального состояния организма посредством физической культуры и спорта, которые представляются теоретической базой для практического решения задач физического воспитания.

Сфера научных интересов доцента Головиной Ирины Витальевны лежит в области экономических исследований. Ирина Витальевна обосновала идею о необходимости формирования у студентов основ экономического мышления и финансовой грамотности, поскольку в перспективе каждому придется принимать экономические решения, как в профессиональной деятельности, так и при планировании личного, или семейного бюджета. Следовательно, необходимо разбираться в работе механизмов экономики, уметь анализировать текущую ситуацию, прогнозировать ее развитие. Главной целью исследований является поиск оптимальных методических приемов, позволяющих обеспечить умение принимать верные обоснованные экономические решения в разных областях жизнедеятельности. Результаты исследований И.В. Головиной публикуются в журналах ведущих Московских университетов.

Одно из направлений научных исследований Докучаева Сергея Аркадьевича связано с решением нестационарных задач, в частности изучается механизм ударного взаимодействия твердых тел с анизотропными материалами. Разработанные математические модели анизотропной среды позволяют наглядно представить ее динамические характеристики в виде аналитических зависимостей, которые являются решением системы интегральных уравнений. Для решения краевых нестационарных задач используются различные модификации методов конечных и граничных элементов. Результаты исследований С.А. Докучаева опубликованы и продолжают публиковаться в ведущих научных изданиях, таких как: «Механика твердого тела. Известия Российской академии наук», «Прикладная математика и механика» и др.

Научные интересы доцента Ефимова Сергея Викторовича связаны с теорией линейных операторов и затрагивают вопросы нётеровости и индекса бисингулярных интегральных операторов со сдвигами. Кроме этого, Сергей Викторович курирует одно из научных направлений кафедры ОНП по теме: Математическое моделирование систем и процессов. Результаты исследований С.В. Ефимова опубликованы в журналах «Известия вузов. Математика», «Siberian Mathematical Journal».

Доцент Жуковский Денис Александрович проводит исследования, направленные на поиск новых представлений о современных цифровых технологиях в экономике и бизнесе, а также на решение проблем информационной безопасности предприятий и защите экономической информации. Результаты исследований Д.А. Жуковского опубликованы в ряде научных журналов Scopus и Web of since, а также в виде монографий.

Доцент Константинова Яна Борисовна продолжает исследования сегнетоэлектрических пьезоматериалов, находящихся в области размытого фазового перехода. Изучаются эффекты упорядочения в сегнетоэлектрических твердых растворах и влияние условий приготовления таких материалов на их свойства. Актуальность исследований Яны Борисовны подтверждается разработкой и созданием новых пьезоактивных материалов, применяемых сегодня в эхолокации и медицине. Так, в медицине эти материалы используются, например, при проведении УЗИ и лечении новообразований. Результаты исследований опубликованы в центральных журналах, в частности, «Неорганические материалы», «Известия Академии наук, серия Физика», «Журнал технической физики».

Доцент Коршун Анна Михайловна проводит исследования взаимодействия природы и общества, которые помогают спрогнозировать последствия трансформации среды и биоты под влиянием антропогенных воздействий и изменений климата. Выполнена оценка изменчивости гидролого-гидрохимических параметров ключевых водоемов Юга России - Цимлянского водохранилища и Нижнего Дона. Апробированы информационные технологии в оценке развития фитопланктонных сообществ Цимлянского водохранилища. Исследовано пространственное распространение загрязнения морского побережья Азовского моря пенополиуретаном. Результаты научных исследований А.М. Коршун направлены на улучшение экологической обстановки нашего региона и опубликованы в ведущих журналах: «Наука - проблемы и достижения», «Наука Юга России», «Экология. Экономика. Информатика».

Доцент Костецкая Галина Сергеевна исследует возможность применения интегральных операторов типа потенциала и гиперсингулярных интегралов. Показано, что использование гиперсингулярных интегралов особенно эффективно в случае работы со многими переменными и существенно упрощает решение ряда задач теории функций и интегральных уравнений. Исследования Галины Сергеевны нашли свое применение в различных областях естествознания, например, при решении задач математической физики и теории электромагнитных колебаний.

Сфера научной деятельности доцента Светличной Наталии Олеговны включает в себя область филологии, связанную с теорией языка и закономерностями его развития. Особый интерес представляют исследования аббревиатур, являющихся значительной частью словарного состава русского языка, и ярко демонстрирующих способность слов к лексико-семантическим изменениям под влиянием исторических и социокультурных преобразований в обществе.

Научный интерес доцента Устименко Дмитрия Леонидовича сосредоточен вокруг проблем истории философии. В рамках феноменологической методологии им осуществляется анализ проблем познания, природы сознания, бытия человека и истории. Результаты исследований Д.Л. Устименко представлены монографией и опубликованы в ряде научных журналов Scopus и Web of since.

Следует отметить, что ППС кафедры ОНП проводит и совместные научные изыскания. Так в области методологии педагогики под руководством Докучаева Сергея Аркадьевича выявлены особенности проблемного обучения бакалавров при изучении общенаучных дисциплин в контексте личностно-ориентированной образовательной парадигмы. Изучены различные подходы к проблеме обучения бакалавров в свете требований, предъявляемых современным рынком труда с целью организации эффективного учебно-воспитательного процесса в рамках профессиональной подготовки.

Заведующий кафедрой ОНП Конкин Борис Борисович возглавляет научное направление, связанное с внедрением инновационных технологий [1] в образовательный процесс. К настоящему времени разработана, создана, внедрена и успешно используется в процессе обучения компьютерная программа, представляющая собой контрольно-обучающий комплекс, содержащий более сотни разнообразных продуктов, направленных на освоение курса общей физики. Преимущество рассматриваемого комплекса заключается в полноте охвата материала, многоуровневом характере его использования, в свободе выбора заданий и их сложности, в возможности постоянного мониторинга успешности и адаптации к любому учебному заведению и уровню предварительной подготовки обучаемого контингента.

В представленном обзоре обозначены лишь реперные позиции научно-исследовательской работы кафедры ОНП, результаты которой ежегодно публикуются в ведущих журналах РФ, ближнего и дальнего зарубежья.

Не остаются в стороне от научно-исследовательской работы и студенты нашего вуза. Так, под руководством ППС кафедры ОНП работают на постоянной основе три студенческие научные секции. Кроме этого, преподаватели работают со студентами и персонально. Результаты своих исследований студенты представляют на различных научных площадках СКФ МТУСИ, например, выступают с докладами и публикуют статьи [2].

СПИСОК ЛИТЕРАТУРЫ

1. *Конкин Б.Б., Овчаров П.Н*. Применение компьютерных программ в образовании // Актуальные аспекты развития воздушного транспорта (Авиатранс-2019). Материалы международной научно-практической конференции 21-23 июня 2019 г. Ростов-на-Дону: Изд-во Фонд науки и образования, 2019 , с. 194-199.
2. Конкин Б.Б., Гладыщук С.В., Сопранцова Ю.С. TESTING IN THE EDUCATION PROCESS //Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 2. С. 202-204.

Н.А. Чальян, Н.С. Браун

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ЭФФЕКТИВНОСТИ ИННОВАЦИОННО-ИНВЕСТИЦИОННЫХ ПРОЕКТОВ В СОВРЕМЕННЫХ УСЛОВИЯХ УПРАВЛЕНИЯ ФИНАНСАМИ КОМПАНИИ В ОТРАСЛИ СВЯЗИ И ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Донской государственный технический университет, Ростов-на-Дону, Россия

Ключевые слова: инновации, инвестиционно-инновационный проект, оценка эффективности, прибыль, рентабельность инвестиционного капитала, эффект, эффективность, окупаемость, неопределённость, риск, инфокоммуникационные технологии.

Статья посвящена проблеме анализа методов оценки эффективности инновационно-инвестиционных проектов. В статье проанализированы существующие методы оценки эффективности инвестиционных проектов, выявлены их достоинства и недостатки. Определена спецификация инновационных проектов. При выборе того или иного метода оценки следует учитывать особенности оцениваемого проекта, его специфику и отрасль, в которой он реализуется. Наиболее точную оценку эффективности дает применение комплексного подхода, включающего в себя методы, относящиеся к разным группам (традиционные и специальные).

N.A. Chalyan, N.S. Braun

ANALYSIS OF METHODS FOR EVALUATING THE EFFECTIVENESS OF INNOVATION AND INVESTMENT PROJECTS IN MODERN CONDITIONS OF FINANCIAL MANAGEMENT OF THE COMPANY IN THE FIELD OF COMMUNICATIONS AND INFOCOMMUNICATION TECHNOLOGIES

Don state technical university, Rostov-on-Don, Russia

Keywords: innovation, investment and innovation project, performance evaluation, profit, return on investment capital, effect, efficiency, return on investment, uncertainty, risk, infocommunication technologies.

The article is devoted to the problem of analyzing methods for evaluating the effectiveness of innovation and investment projects. The article analyzes the existing methods of evaluating the effectiveness of investment projects, identifies their advantages and disadvantages. The specification of innovative projects is defined. When choosing a particular evaluation method, you should take into account the characteristics of the project being evaluated, its specifics, and the industry in which it is implemented. The most accurate assessment of effectiveness is provided by the use of an integrated approach that includes methods that belong to different groups (traditional and special).

На сегодняшний день методики оценки эффективности инновационно-инвестиционных проектов не в полном объеме учитывают специфические особенности проектов в отрасли связи и инфокоммуникационных технологий, для этого необходимо их адаптации и/или доработка.

Это и определяет актуальность исследования данной проблемы.

Инновационно-инвестиционный проект является объектом исследования в данной статье.

Совокупность методов оценки эффективности инновационно-инвестиционных проектов является предметом исследования в данной статье.

Для поддержания конкурентоспособности бизнеса на современном этапе развития экономики в отрасли связи предприятиям необходимо обновление и совершенствование производимого продукта на постоянной основе. Вложения в инновационно-инвестиционные проекты обусловливают уровень дальнейшего развития и соответственно благополучия предприятия. Именно для этих целей предприятия и используют инвестиции, как инструмент обновления производства. В этой связи и возникают вопросы оценки эффективности реализации инновационно-инвестиционных проектов. В имеющихся методиках приводятся только характеристики и описание, без точных алгоритмов выбора способа оценки экономической эффективности инновационно-инвестиционных проектов.

Верзилин Д.Н. и Кулакова А.О. в своей работе «Оценка эффективности инновационного проекта по развитию трехмерной геоинформационной системы» утверждают, что «необходимостью для любого предпринимателя выступает оценка целесообразности вложения средств в тот или иной проект. Это необходимо, прежде всего, для обоснования выбора одного из нескольких альтернативных проектов при ограниченных инвестиционных возможностях». [5]

При рассмотрении различной экономической литературы по методике оценки инвестиционных проектов, можно сделать вывод о стандартизации расчетов, без учета специфики проекта и его условий, а также адаптацией положений с учетом происходящих изменений в экономике и инфокоммуникационных технологий.

В соответствии с Федеральным законом «О науке и государственной научно-технической политике» (от 23.08.1996 N 127-ФЗ в ред. от 23.05.2016 с изм. и доп., вступ. в силу с 01.01.2017) [2] инновационный проект представляет собой «комплекс направленных на достижение экономического эффекта мероприятий по осуществлению инноваций, в том числе по коммерциализации научных и (или) научно-технических результатов».

Исходя из вышесказанного, мы можем сделать вывод о том, что для любого предпринимателя важен эффект - некий результат деятельности, который может быть, как положительным, так и отрицательным.

На сегодняшний день предпринимателям необходимо уметь отличать понятия эффект и эффективность при реализации инвестиционных и инновационных проектов. Эффект – это абсолютный показатель, а эффективность наоборот – относительный, а именно отношение результата к затратам, следовательно, можно сделать вывод, что эффективность отражает соответствие проекта целям и интересам участников.

В данной статье представлено следующее определение эффективности: эффективность представляет собой относительный или абсолютный показатель, отражающий целесообразность реализации проекта и позволяющий сделать выводы о выгоде (эффекте), получаемой от участия в нем.

Для анализа возьмем за основу данные, приведенные Верзилиным Д.Н. и Кулаковой А.О. в работе «Оценка эффективности инновационного проекта по развитию трехмерной геоинформационной системы» [5], и составим таблицы 1 и 2 для наглядного рассмотрения методов с описанием достоинств и недостатков.

Таблица 1. Сравнительный анализ методов оценки эффективности проектов

Название	Методика расчетов	Достоинства	Недостатки
Прибыль	Разница между суммарными доходами и затратами на реализацию проекта за определенный период / или весь период реализации	- однозначность трактовки - простота расчетов	- не принимается во внимание фактор времени - исключается возможность сравнения проектов, отличающихся по срокам реализации
Рентабельность инвестиционного капитала	Отношение прибыли до получения процентов и налогов к сумме инвестиций, т.е. показывает, сколько единиц полученной прибыли пришлось на одну единицу вложенных инвестиций	- с помощью этого расчета можно оценить в относительном выражении превышение получаемой выгоды над первоначальными сложениями - простота расчетов	- не анализируются риски - без учета фактора времени - при неравномерных денежных потоках от реализации проекта, затруднительно выбрать исходные значения прибыли и инвестиционных затрат
Срок окупаемости	Время, в течение которого доходы, полученные от реализации проекта, полностью покроют инвестиции, вложенные в начале реализации проекта.	- прозрачность и наглядность - можно сравнить альтернативные проекты	- не принимаются во внимание результаты деятельности за пределами установленного срока реализации проекта
Чистый приведенный доход	Стоимость, полученная путем дисконтирования всех потоков, накапливающихся за весь период реализации объекта инвестирования по ставке дисконтирования.	- определяет в какой мере будущие поступления оправдывают текущие затраты на проект	- не принимаются риски на разных этапах проекта
Дисконтированный срок окупаемости проекта	Период, в течение которого дисконтированные денежные потоки покрывают первоначальные инвестиции.	- уравновешивают недостаток простого срока окупаемости	- не принимаются в расчет доходы за пределами наступления срока окупаемости; - не оценивает эффективность вложенных инвестиций

Каждый из приведенных методов имеет как преимущества, так и недостатки и для любого организатора собственного дела необходимо на разных этапах сочетать различные методы оценки проектов.

Для дальнейшего анализа методов оценки эффективности инвестиционных и инновационных проектов в отрасли связи и инфокоммуникационных технологий систематизируем в таблицу отличительные особенности этих проектов.

Таблица 2. Отличительные особенности инвестиционных и инновационных проектов

Сравниваемый параметр	Инвестиционный проект	Инновационный проект
Начало проекта	Перед началом проекта необходимо с помощью различных методов оценки рассчитать все предполагаемые риски	При внедрении инновационного проекта высока степень неопределенности различных параметров оценки, требует вовлечения уникальных ресурсов (трудовых, финансовых и других)
Принятие проекта	Проект рекомендуется к реализации при условии экономической, финансовой и социальной эффективности.	Если при оценке эффективности проекта финансовые, и нефинансовые параметры проекта предполагают прибыль, то необходимо приступить к реализации проекта
Неопределенность и риск	Проект, как правило, не связан с высоким уровнем риска.	Проект, как правило, подвержен высокому уровню риска.
Оценка эффективности	Используются только количественные критерии при оценке эффективности	При оценке необходимо использовать количественные и качественные критерии
Влияние на стоимость компании	Незначительно влияют на стоимость компании	Значительно повышают стоимость компании

На основе проведенного сравнительного анализа можно выделить следующие факторы, которые необходимо адаптировать:

- ставка дисконтирования должна дифференцировать источники финансирования в зависимости от стадии реализации проекта;
- риски инновационного проекта подвергаются различного рода изменениям в зависимости от стадии жизненного цикла проекта.

Исходя из этого мы можем сделать вывод о том, что ставка дисконтирования обязательно должна быть ориентирована на риск и быть адаптирована к той отрасли, в пределах которой реализуется проект, его специфики и продолжительности реализации.

В силу того, что инновационно-инвестиционные проекты, имеют длительный срок реализации (это не сиюминутная прибыль), может представиться, что эти проекты неэффективны. В этом случае может понадобиться применение иной методики, нежели дисконтирование.

При реализации таких проектов эффекты от их внедрения носят качественный характер, и потому их сложно оценить в стоимостном выражении, однако очевидна их полезность ввиду повышения эффективности работы персонала организации и всего предприятия в целом.

В заключение хотелось бы сказать, что не существует унифицированного метода или подхода, дающего сто процентную гарантию на объективно-справедливую оценку любого инновационно-инвестиционного проекта. Каждый инновационный проект обладает набором специфических характеристик, делающих его уникальным. В этой связи при выборе метода оценки эффективности проекта в каждом отдельно взятом случае требует индивидуальный подход.

Для получения максимально верной оценки и построения правильных выводов необходимо использовать комплексный подход к оценке эффективности, которая предполагает применение классических (статических и динамических) и специальных (финансовых, качественных и вероятностных) методов оценки. И самое главное, при выборе метода оценки необходимо учитывать специфические особенности проекта, такие как:

- цель проведения оценки эффективности проекта;
- отрасль, в которой подлежит реализации проект;

– длительность реализации проекта;
– стадия жизненного цикла проекта и характерные риски.

СПИСОК ЛИТЕРАТУРЫ

1. *Манина Т.С.* Оценка эффективности инновационных проектов // Молодой ученый – 2019 - № 21.
2. «О науке и государственной научно-технической политике» (от 23.08.1996 в ред. от 23.05.2016 с изменения и дополнения, вступают в силу с 01.01.2017) №127-ФЗ http://www.consultant.ru/document/cons_doc_LAW_11507 (дата обращения 15.05.2020)
3. *Малинина С.Е.* Проблемы оценки экономической эффективности инновационных проектов // Креативная Экономика – 2019 - №4.
4. *Петров А.М., Антонова О.В.* Дисконтирование денежных потоков как прием финансового анализа // Kant – 2019 - № 3 - 93–97 с.
5. *Верзилин Д.Н., Кулакова А.О.* Оценка эффективности инновационного проекта по развитию трехмерной геоинформационной системы // Научный журнал НИУ ИТМО - 2019 - №1 – 10-25 с.

Э.А. Бинеев

УРОВЕНЬ ПРИЕМЛЕМОГО РИСКА В РАЗЛИЧНЫХ СФЕРАХ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: приемлемый риск, профессиональная деятельность, риск смерти.

Приведен анализ уровней среднего риска смерти в различных сферах деятельности человека. Выделены различные категории безопасности в профессиональной деятельности с учетом приемлемых уровней риска.

E.A. Bineev

LEVEL OF ACCEPTABLE RISK IN DIFFERENT AREAS OF HUMAN ACTIVITY

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

Key words: acceptable risk, professional activity, risk of death.

The analysis of levels of average risk of death in various spheres of human activity is presented. Various categories of safety in professional activity are highlighted, taking into account the acceptable levels of risk.

Традиционная цель обеспечить полную безопасность, не допустить никаких аварий, несчастных случаев (НС) и других нежелательных последствий практически недостижима.

Современный мир отверг концепцию абсолютной безопасности и принял концепцию приемлемого (допустимого) риска.

Концепция приемлемого риска сочетает технические, экономические, социальные и политические аспекты и представляет собой некоторый компромисс между уровнем безопасности и возможностями ее достижения. Для определения уровня приемлемого риска рассмотрим масштабы риска в различных сферах деятельности современного человека в промышленно развитых странах, ограничившись риском смертельных исходов. В работах [1,2] приведена классификация источников риска смерти для человека, указаны причины, средние значения риска и примеры индивидуального риска, принят средний риск R смерти в расчете на одного человека за год.

Риск смерти зависит от рассматриваемой возрастной группы. Например, риск смерти от болезней мужчин в возрасте 45–50 лет примерно в 10 раз выше, чем в группе 25–30 лет. Риск смерти от болезней во всех возрастных группах на 3 порядка превышает риск смерти в естественной среде обитания. В возрастной группе 20–25 лет риск смерти от несчастных случаев для мужчин в 2,7 раза больше смертности от болезней. Объясняется это тем, что в этой возрастной группе лицам свойственна тенденция попадать в ситуации с неоправданно высоким уровнем риска нежелательных последствий. С накоплением жизненного опыта действие этих причин, уменьшается.

Для профессиональной деятельности выделено четыре категории безопасности в зависимости от риска смерти R на одного человека в год: 1 – безопасная ($R < 10^{-4}$); 2 – относительно безопасная ($R = 10^{-4}$–10^{-3}); 3 – опасная ($R = 10^{-3}$–10^{-2}); 4 – особо опасная ($R > 10^{-2}$). При этом риск смерти для особо опасных профессий в 100 раз превышает такой риск для профессий, традиционно называемых безопасными. Средний уровень риска смерти от болезней для мужчин всех возрастов сравним лишь с риском в опасных профессиональных условиях.

Только в первом приближении можно принять независимость воздействия на человека разных источников риска. Для уточнения риска необходимо учесть корреляцию риска для разных источников. Заметим, что примеры рисков непрофессиональной деятельности в [1,2] даны для общего времени, уделенного спорту 150–200 часов в год.

Очевидно, что проблема определения приемлемого риска в различных сферах деятельности современного человека имеет социальные, экономические, психологические и другие аспекты. Социальный эффект может проявляться, например, в том, что преимущества от применения новой, более совершенной технологии концентрируются у одних членов общества, а риск неблагоприятных последствий, связанных с ее недостатками, распространяется на других членов или на все общество в целом.

Анализ приведенных в [1,2] данных позволяет заключить, что приемлемый уровень профессионального риска смерти для современного человека в промышленно развитых странах находится в интервале $(1–5)\cdot10^{-4}$ на человека в 1 год. Это значение равняется риску смерти от болезней для возрастной группы 25–30 лет, или избыточному риску смерти от несчастных случаев для мужчин в возрастной группе 20–25 лет по сравнению с группой 30–50 лет.

СПИСОК ЛИТЕРАТУРЫ

1. Бинеев Э.А. Уровни риска смерти человека в промышленно развитых странах. Безопасность и экология технологических процессов и производств: Мат-лы всероссийской научно-практ. конф.,п. Персиановский, ДонГАУ, 2004, с.11-13.
2. Бинеев Э.А.,Бородин А.В.,Попова В.П. Безопасность жизнедеятельности.Курс лекций. Уч. пособие для вузов.- Ростов н/Д: СКФ МТУСИ,2018.- 268с.

Л.А. Гаевская, Е.Р. Сабинина

ФИЗИЧЕСКАЯ АКТИВНОСТЬ КАК СРЕДСТВО УКРЕПЛЕНИЯ ЗДОРОВЬЯ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: физическая культура, двигательная активность, упражнения, функциональные возможности организма, здоровый образ жизни.

В статье описывается важная роль образовательного учреждения в пропаганде физической активности и её реализации на уроках по физической культуре и общей физической подготовки. Рассмотрены оздоровительный эффект физической активности, её роль в формирования личностных и профессиональных качеств обучающихся. Подчеркивается особое значение рациональной организации физических упражнений и тренировки.

L.A. Gayevskaia, E.R. Sabinina

PHYSICAL ACTIVITY AS A MEANS OF HEALTH PROMOTION

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

Keywords: physical culture, physical activity, exercise, body functional capabilities, healthy lifestyle.

The article describes the important role of an educational institution in the promotion of physical activity and its implementation in physical culture and general physical training lessons. The health-improving effect of physical activity, its role in the formation of personal and professional qualities of students are considered. The special importance of the rational organization of physical exercises and training is emphasized.

Физическая активность — это одно из главных условий здоровой жизни и полноценного существования человека. Она стимулирует все важнейшие процессы роста, развития и формирования организма. Вообще физическая активность зависит от многих факторов: индивидуальных возможностей человека, его возраста, пола и состояния здоровья.

Мы можем и должны преодолевать лень и пассивную бездеятельность, вести здоровый образ жизни (ЗОЖ), который включает в себя активный отдых на природе, занятия физической культурой, спортом, туризмом. Все это приводит к стабилизации и укреплению нашего здоровья. От регулярной физической активности происходит улучшение деятельности организма, это положительно сказывается на общем состоянии, работоспособности и самочувствии человека, способности противостоять утомлению и стрессам, что дает большой экономический и социальный эффект.

Таким образом, оздоровительное значение физической активности — это общая биологическая закономерность, но действует она лишь при условии полного соответствия используемой физической нагрузки функциональным возможностям организма, рациональной тренировки и здорового образа жизни. В противном случае не только трудно добиться оздоровительного эффекта, но и возможно возникновение негативных патологических состояний, развивающихся вследствие физического перенапряжения.

Важнейшими средствами обеспечения комплексного оздоровительного эффекта в занятиях физкультурой и спортом являются правильный выбор упражнений, рациональная нагрузка, максимально возможное устранение из системы подготовки факторов риска, увеличивающих вероятность физического перенапряжения, а также комплексное использование средств первичной профилактики и восстановления.

Физические упражнения положительно влияют на все жизненно важные системы человеческого организма: опорно-двигательный аппарат, сердечно — сосудистую, нервную и другие системы, улучшают процессы обмена веществ.

А при недостаточной физической активности могут нарушаться нервно - рефлекторные связи, заложенные природой и генетически закрепленные в процессе физического труда, что приводит к расстройству важнейших вегетативных систем организма, и развитию различных болезней.

Современный человек, живущий в условиях гиподинамии (малоподвижного образа жизни), не только не испытывает радостных эмоций от движений своего тела, но становится зависимым от интерорецепции (импульсов, поступающих от рецепторов внутренних органов). При отсутствии или дефиците проприорецепции (импульсов, поступающих от рецепторов мышц) преобладающими (доминирующими) становятся импульсы от рецепторов внутренних органов, что вызывает различные патологические ощущения - в сердце “колет”, в желудке “изжога”, в боку “ноющая боль” и т.д. Причем, все эти болезненные ощущения во внутренних органах проходят при повышении физической активности.

Очень важно, что выполнение физической работы способствует повышению адаптационных и защитных свойств организма, положительно влияет на все его системы.

Это проявляется в следующих эффектах:

- повышается устойчивость работы ЦНС (центральной нервной системы);
- повышаются функциональные способности и устойчивость эндокринных систем (железы внутренней секреции);
- нормализуется и улучшается обмен веществ;
- происходит обогащение кислородом мышц и тканей;
- улучшается эмоциональное состояние;
- повышаются энергетические резервы организма.

Для нашего времени очень актуальна потребность в физической активности, как средстве укрепления здоровья и повышения уровня физической подготовки человека, так как здоровье - важнейшее достояние человека, основа его жизнедеятельности, работоспособности, это путь к достижению творческих успехов, активной плодотворной деятельности и долголетию.

В нашем вузе СКФ МТУСИ уделяется большое внимание пропаганде и реализации физической активности во время лекционных и практических занятий по физкультуре и общей физической подготовке. Физическая подготовленность студентов развивает в них такие основные качества, как сила, выносливость, ловкость, гибкость, быстрота и координация. Уровень их развития, особенно в период обучения в вузе, способствует созданию здоровой основы для развития полноценной личности, помогает успешному овладению профессиональными знаниями.

СПИСОК ЛИТЕРАТУРЫ

1. Готовцев П.И., Дубровский В.И. Самоконтроль при занятиях физической культурой и спортом. М.: Физкультура и спорт, 2018.
2. Дикуль В.И., Зиновьева А.А. Как стать сильным. М.: Физкультура и спорт, 2017.

3. Ильинич В.И. Студенческий спорт и жизнь: Учеб. пособие для студентов высших учебных заведений. М.: АО "Аспект Пресс", 2008.
4. Половников П.В. Организация занятий студентов по дисциплине "Физическая культура": Учеб. пособие / СПбГТУ. СПб, 2009.
5. Практические занятия по врачебному контролю / Под общ. ред. А.Г. Дембо. М.: Физкультура и спорт, 2016.
6. Физическое воспитание: учебник / Под ред. В.А. Головина и др. М.: Высш. школа, 2016.

С.А. Докучаев, С.В. Ефимов, Г.С. Костецкая

О ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЯХ В ОБРАЗОВАТЕЛЬНОЙ ЭКОСИСТЕМЕ ТЕХНИЧЕСКОГО ВУЗА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: экосистема, цифровая образовательная среда, система управления обучением

Рассматривается использование экосистемного подхода в процессе создания цифровой образовательной среды современного технического вуза. Подчеркнута ключевая роль современных систем управления обучением (LMS) для организации непрерывного, в том числе и удаленного, взаимодействия между всеми участниками образовательного процесса. Перечислены основные преимущества LMS Moodle и MasterStudy.

S.A. Dokuchaev, S.V. Efimov, G.S. Kostetskaya

DIGITAL EDUCATIONAL TECHNOLOGIES IN THE EDUCATIONAL ECOSYSTEM OF A TECHNICAL UNIVERSITY

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

Keywords: ecosystem, digital educational environment, learning management system.

The work focuses on the use of the ecosystem approach in the process of creating a digital educational environment of a modern technical university. The key role of modern learning management systems (LMS) for the organization of continuous, including remote, interaction between all participants in the educational process is emphasized. The authors offer a list of main advantages of LMS Moodle and MasterStudy.

В настоящее время тренд на экосистемный подход распространяется на все сферы жизни современного общества. Не остается в стороне и образовательная среда. Очевидно, что в последние годы наметился явный кризис в традиционной модели обучения, которая не позволяет современным выпускникам получить практические навыки по выбранной специальности и найти свое место на рынке труда. Решение данной проблемы многие современные исследователи [1] видят в развитии экосистемного подхода к образованию,

что неизбежно должно привести к созданию образовательных экосистем на базе технических вузов.

В традиционном образовании ученики получали «багаж» знаний и мудрости, в новом образовании необходимо научиться эту мудрость создавать. Предметы должны смениться проектами, которые позволят ученикам приобретать опыт, применять знания из разных областей и принимать решения. Иерархия должна уступить место сотрудничеству, необходимо признать педагогов и учащихся как сотворцов образовательного процесса.

В традиционном образовании всех учили одинаково, в новом будут учить дифференцированно. Образование прошлого было стандартизованным: ученики проходили одну и ту же программу, их результаты оценивали в одно и то же время в соответствии с принятыми нормами. Образования будущего станет персонализированным: способности, интересы и таланты учащихся будут определять процессы обучения. Такая образовательная система будет походить не на промышленный конвейерный завод, а на живую экосистему знаний, где каждый имеет свою экологическую нишу и право на выбор.

Полноценное функционирование современной образовательной экосистемы невозможно без создания цифровой образовательной среды, обеспечивающей непрерывное, в том числе и удаленное, взаимодействие между всеми участниками образовательного процесса. Цифровая образовательная среда современного вуза строится на базе систем управления обучением (Learning Management System, LMS), наиболее распространенной из которых является LMS Moodle. Основные преимущества площадки – индивидуальность подхода к обучению, широкий спектр функциональных возможностей, мобильность, расширяемость, бесплатность, интерактивность, разнообразие заданий [2].

Moodle обеспечивает педагогические условия для эффективного дистанционного обучения студентов и их оперативного взаимодействия с преподавателем посредством чата, анкетирования, тестирования, форумов, опросов, рабочих тетрадей, семинаров. Площадка поддерживает различные структуры курсов: «календарный», «форум», «тематический», имеет простой, интуитивно понятный интерфейс. Также Moodle содержит модуль «Видеоконференция BigBlueButton», который позволяет создавать веб-конференции с открытым исходным кодом для онлайн-обучения, может быть использован и для проведения брифингов, презентаций и вебинаров. BigBlueButton поддерживает в режиме реального времени совместное использование аудио- и видеофайлов, слайдов, чата, экрана, многопользовательской доски, онлайн-опросов, комнат обсуждений, запись сеансов и их воспроизведение для последующего просмотра. Пользователям Moodle доступен полный отчет по взаимодействию с системой – время входа, количество прочтений сообщений, записи в тетрадях и прочие детали. Moodle хранит портфолио каждого обучающегося: оценки, работы, комментарии преподавателя, сообщения на форуме, посещаемость, активность, время учебной деятельности в сети. Опираясь на данную информацию, преподаватель составляет индивидуальный план работы со студентом, формирует оптимальные образовательные траектории для каждого обучающегося, стимулирует к саморазвитию и самообучению.

Использование цифровых образовательных технологий в учебном процессе дает преподавателю не только большую свободу и гибкость в изложении учебного материала, но также требует принципиально иных подходов к его представлению. Как показывает практика, современные студенты очень плохо усваивают большой объем текстовой информации, особенно по «скучным» и абстрактным математическим дисциплинам. И здесь на помощь преподавателю приходят современные системы управления обучением. Так, например, в рамках LMS MasterStudy при построении лекционного курса преподаватель может выбирать из 4-х вариантов (видеокурс, стрим, текстовый вариант, режим презентации) или использовать их симбиоз. Система также позволяет с легкостью интегрировать в учебный процесс разнообразные игровые элементы и различные системы оценки знаний студентов [].

Вывод. Переход к созданию образовательных экосистем – это веление времени, обусловленное стремительно вторгающимися в нашу жизнь IT-технологиями. И для того, чтобы качество высшего образования повышалось, необходимо разумное сочетание традиционного и онлайн обучения с применением различных форм, методов и инструментов.

СПИСОК ЛИТЕРАТУРЫ

1. Джессика Спенсер-Кейс, Павел Лукша, Джошуа Кубиста. Образовательные экосистемы: возникающая практика для будущего образования [Электронный ресурс] - http://www.imc-eduekb.ru/downloads/Ресурсные%20центры/obrazovatel_nye_jekosistemy.pdf (Дата обращения 20.10.2021).
2. Игнатьев В.П., Борисов Е.А. Обзор и анализ использования дистанционных образовательных технологий в российских вузах // Современные проблемы науки и образования. – 2021. – № 3.; URL: http://www.science-education.ru/ru/article/view?id=30691 (дата обращения: 20.10.2021).
3. С.А. Докучаев, Г.С. Костецкая «О новых подходах к преподаванию математических дисциплин в образовательной экосистеме технического вуза». Материалы XXVII Международной конференции. Математика. Экономика. Образование. 2021. с.91

С.А. Докучаев, Г.С. Костецкая, Н.О. Светличная, Л.М. Колдынская

СОВРЕМЕННЫЕ СРЕДСТВА ВИЗУАЛИЗАЦИИ УЧЕБНОГО КОНТЕНТА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: визуализация информации, инфографика, цифровой учебный материал.

Подчеркнута важная роль цифрового контента и визуализации информации в процессе формирования профессиональных знаний, навыков и умений бакалавров. Особое внимание уделено графическому представлению учебного материала в виде инфографики. Рассмотрены современные приложения для эффективного цифрового взаимодействия преподавателя и обучающихся.

S.A. Dokuchaev, G.S Kostetskaya, N.O. Svetlichnaya, L.M. Koldinskaya

MODERN TOOLS FOR VISUALIZATION OF LEARNING CONTENT

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

Keywords: information visualization, infographics, digital educational material.

The work underlines an important role of digital content and information visualization in the formation of professional knowledge, skills and abilities of bachelors. Particular attention is

paid to the graphical presentation of educational material in the form of infographics. Some modern applications for effective digital interaction between a teacher and students are considered.

В настоящее время визуализация занимает центральное место в образовательном процессе. Наглядность в обучении способствует восприятию предметов и изучаемых процессов, формирует представления об объективной действительности, и вместе с тем предлагает анализировать и обобщать воспринимаемые явления в связи с учебными задачами.

Визуализация учебной информации позволяет решить целый ряд педагогических задач, среди которых наиболее актуальными являются обеспечение интенсификации обучения, активизация учебной и познавательной деятельности, формирование и развитие критического и визуального мышления.

Использование средств визуализации для управления познавательной деятельностью в процессе обучения способствует:

- созданию образовательной среды, способной в различных учебных ситуациях демонстрировать наглядные образы изучаемых процессов и явлений, а также оперированию ими;
- развитию интеллектуального мышления;
- изменению иллюстративных свойств, средств наглядности на познавательные, которые становятся основой всего процесса обучения.

Визуализация как процесс — это формирование зрительного наглядного или мысленного образа. В этом процессе интерактивные презентации играют значительную роль, поскольку позволяет преподавателю многопланово оперировать учебным материалом: управлять процессом предоставления информационного потока; применять нелинейную анимацию, визуальные эффекты, гиперссылки; создавать линейный и иерархический тип создания навигации; перетаскивать элементы, скрывать некоторые предметы и текстовый контент до необходимого момента; использовать функции графики и видео с озвучиванием; создавать коллекции, посвящённые одной тематики [2].

Создание визуальных обучающих приложений существенно сложнее использования простых визуальных образов, однако, это компенсируется повышением качества современного образования и становится вопросом успешного конкурирования в динамичной информационно-образовательной среде. Широкое распространение глобальной сети Интернет и органичное функционирование в ней людей практически всех поколений задает тренды трансляции образовательного контента обучающимся. В этой связи содержательное, ясное, интерактивное, эстетически привлекательное визуальное представление сложной учебной информации становится требованием времени. Эти требования отражены и в современных государственных стандартах образования. Они выражены в формировании метапредметных знаний и способностей к формализации и структурированию информации, умения выбирать способы представления данных в соответствии с поставленной задачей (таблицы, схемы, графики, диаграммы и др.) с использованием соответствующих программных средств обработки данных.

Современные средства визуализации представляют собой инновационные приемы передачи учебного материала с помощью символов и образов в видео и графической обработке. В частности, одним из таких способов визуализации образовательного контента является инфографика, которую можно активно использоваться на учебных занятиях.

Инфографика — это графический способ подачи информации, данных и знаний, целью которого является быстро и чётко преподносить сложную информацию. Инфографика используется с целью представить информацию максимально наглядно, доступно и просто. Задачи инфографики, как образовательной технологии, заключаются в том, чтобы акцентировать внимание и улучшить качество восприятия передаваемого сообщения; повысить продуктивность обучения; сэкономить время для осознания и

осмысления. Контингентом, на который нацелена данная технология, могут выступать учащиеся всех возрастов: школьники, студенты, сотрудники различных компаний.

Техника графического отображения информации, доступная для использования в учебном процессе, - многообразна: онлайн-доски, сервисы для создания презентаций, интерактивные карты и ленты времени, сервисы для создания интерактивных упражнений.

На сегодняшний день существует ряд приложений, которые способствуют более наглядному и активному представлению учебного материала. Среди них выделяют:

- MindMeister – приложение для коллективной работы по созданию интеллект-карт. Данное приложение разрешает обмениваться интеллект-картами с неограниченным числом пользователей, а также позволяет организовать взаимодействие в режиме реального времени, визуализировать идеи в презентацию.
- Timetoast – инструмент для совместной работы над созданием онлайн-шкал, который дает возможность делиться графиками с группами или отдельными пользователями.
- Mentimeter.com – онлайн –сервис для проведения опросов и голосования в режиме реального времени в формате презентации.
- Padlet – виртуальная интерактивная доска для командного взаимодействия и размещения различного контента с возможностью его последующего комментирования. Интересна функция размещения вопросов аудитории в режиме реального времени.
- Scrumlr – виртуальная доска со стикерами, которая может служить инструментом для совместной работы с возможностью внесения изменений каждым участником в режиме реального времени.

Эффективны и очень востребованы, особенно в условиях дистанционного обучения, цифровые инструменты и сервисы, используемые для рисования, монтажа видео и мультимедиа. К таким инструментам относятся: WeVideo – онлайн видео редактор, BookCreator – инструмент для создания цифровых книг, Infinite Painter – инструмент для рисования на планшетах, Explain everything – инструмент для проектирования, создания скриншотов и интерактивной доски, который позволяет комментировать, анимировать любые файлы.

Таким образом, визуализация приобретает огромное значение в современном образовательном процессе.

СПИСОК ЛИТЕРАТУРЫ

1. Визуализация образовательного контента – требование времени. Дубровина И.Г. Международный педагогический портал https://solncesvet.ru/opublikovannyie-materialyi/vizualizaciya-obrazovatelnogo-kontenta--.9366472/
2. Докучаев С.А., Костецкая Г.С., Светличная Н.О. Использование интерактивных презентаций в преподавании общенаучных дисциплин для бакалавров в области инфокоммуникаций. Труды СКФ МТУСИ. Международная научно-практическая конференция СКФ МТУСИ, Ростов-на-Дону. 2020, с.162-166.
3. Гузеев В.В. Методы и организационные формы обучения. - М.: Народное образование, 2001. - 128 с.

С.А. Евдокимова

ИССЛЕДОВАНИЕ СВОЙСТВ ИМИТАЦИОННОЙ МОДЕЛИ ПРОЦЕССА РАССМОТРЕНИЯ ЗАЯВЛЕНИЙ ГРАЖДАН

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», Воронеж, Россия

Ключевые слова: имитационное моделирование, Business Studio, диаграмма eEPC, функциональная модель, инфокоммуникационные технологии.

Для оценки эффективности применения информационных и коммуникационных технологий в процессах приема заявлений граждан разработаны функциональные модели в нотации ARIS eEPC. В работе описаны параметры наступления стартовых событий, время выполнения функций, законы распределения случайных величин. В системе Business Studio проведено имитационное моделирование данных процессов, которое показало, что число обращений увеличилось на 37%. В работе особое внимание уделяется способам оценки достоверности описания имитационной модели процесса учета заявлений граждан. Использован критерий Манна-Уитни, проведена верификация модели, оценена устойчивость загрузки специалистов, выполняющих обработку заявлений граждан. Результаты исследования показали, что погрешность результатов моделирования не превышает 5%.

S.A. Evdokimova

RESEARCH OF THE PROPERTIES OF THE IMITATION MODEL OF THE PROCESS OF CONSIDERATION OF CITIZENS' APPLICATIONS

Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia

Keywords: simulation modeling, Business Studio, eEPC diagram, functional model, infocommunication technologies.

Functional models in ARIS eEPC notation have been developed to assess the effectiveness of the use of information and communication technologies in the processes of accepting citizens' applications. The paper describes the parameters of the onset of starting events, the execution time of functions, the laws of distribution of random variables. In the Business Studio system, simulation modeling of these processes was carried out, which showed that the number of requests increased by 37%. In the work, special attention is paid to the methods of assessing the reliability of the description of the simulation model of the process of accounting for citizens' applications. The Mann-Whitney criterion was used, the model was verified, and the stability of the workload of specialists processing citizens' applications was evaluated. The results of the study showed that the error of the simulation results does not exceed 5%.

Введение. В настоящее время современные информационные и коммуникационные технологии широко используются для организации электронных порталов по предоставлению различных государственных и муниципальных услуг. Удаленная форма подачи заявлений и обращений граждан в государственные организации позволяет людям, не выходя из дома получать необходимую информацию, ответы на вопросы, документы и т.д. В этом случае нет необходимости ехать, стоять в очереди, достаточно воспользоваться интернетом или электронной почтой.

Использование электронных порталов отразилось на работе сотрудников, участвующих в процессах предоставления государственных услуг [1, 2]. Для исследования эффективности применения инфокоммуникационных технологий в работе с обращениями граждан можно применять теорию систем массового обслуживания, методы имитационного моделирования, информационные системы моделирования [3-7]. Для описания процессов используются различные графические нотации [8-]. Важным этапом данного исследования является оценка достоверности результатов моделирования.

Цель работы. Целью работы является исследование свойств и проверка адекватности разработанных имитационных моделей процессов рассмотрения и учета заявлений граждан, позволяющих оценить эффективность использования средств информационных и коммуникационных технологий специалистами, занимающихся обработкой и учетом рассмотрения заявлений граждан.

Постановка задачи. Рассмотрим функциональные модели процессов обработки заявлений граждан, поступивших путем личного обращения и с помощью удаленных сервисов, приведенных в [1, 4]. Для этого использовались принципы построения диаграммы eEPC методологии ARIS, которая позволяет детально представить процесс в виде последовательности событий и функций [11].

Стартовыми событиями анализируемого процесса являются личные обращения граждан, письма, отправленные по почте России и электронной почте, а также обращения, поступающие через систему электронного документооборота (СЭД) «Мотив». В случае, когда удаленная подача жалоб не использовалась, существовали два вида обращений граждан: лично и по почте России.

События в модели описываются параметрами [1]:

- интервал времени, в течение которого оно возникает;
- тип случайной величины (момент времени или шаг запуска);
- закон распределения случайной величины;
- количество событий, которые должны возникнуть в течение заданного интервала.

Параметры наступления стартовых событий для разработанных моделей представлены в таблицах 1 и 2.

Организационными единицами (они же временные ресурсы функций) в модели процесса рассмотрения жалоб граждан являются:

- специалист-делопроизводитель, который выполняет функции «Прием обращения граждан», «Регистрация документа», «Снятие документа с контроля», «Отправка уведомления-напоминания исполнителю» и другие;
- исполнитель заявки, реализующий «Подготовку ответа на обращение граждан».

График работы временных ресурсов – 5 дней в неделю с 9:00 до 18:00, перерыв с 13:00 до 14:00.

Таблица 1. Параметры наступления стартовых событий модели без использования информационных технологий

№	Наименование события	Интервал появления события	Количество экземпляров события	Закон распределения времени наступления события
1	Поступило обращение гражданина	Каждый рабочий день	От 1 до 5	Экспоненциальный Математическое ожидание – 10:00
2	Поступило обращение по почте России	Пн, ср, пт	От 5 до 15	Экспоненциальный Математическое ожидание – 14:00

Таблица 2. Параметры наступления стартовых событий в модели с использованием средств информационных технологий

№	Наименование события	Интервал появления события	Количество экземпляров события	Закон распределения времени наступления события
1	Поступило обращение гражданина	Каждый рабочий день	От 0 до 3	Экспоненциальный Математическое ожидание – 10:00
2	Поступило обращение по почте России	Пн, ср, пт	От 0 до 5	Экспоненциальный Математическое ожидание – 14:00
3	Поступило обращение по электронной почте	Каждый день	От 0 до 5	Экспоненциальный Математическое ожидание – 20:00
4	Поступило электронное обращение в СЭД «Мотив»	Каждый рабочий день	От 3 до 6	Экспоненциальный Математическое ожидание – 14:00
5	Поступило обращение в СЭД «Мотив»	Каждый рабочий день	От 2 до 6	Экспоненциальный Математическое ожидание – 14:00

Длительность каждой операции рассматриваемого процесса определена, но может варьироваться в пределах некоторого интервала. Так, на выполнение функции «Подготовка ответа на обращение гражданина» отводится нормативных 28 дней, но возможно как более быстрое ее завершение, так и нарушение срока. Поэтому длительность шага, в общем случае, является случайной величиной, и по завершении данной функции может возникнуть одно из двух событий:

- «Получен документ об исполнении» – вероятность 0,93;
- «Срок исполнения заявки закончился, документ не получен» – вероятность 0,07.

Затраты времени на реализацию всех функций, составляющих процесс регистрации заявки и ее рассмотрение без использования информационных технологий и с ними приведены в таблице 3.

Таблица 3. Среднее время выполнения функций процесса рассмотрения заявлений граждан

Наименование функции	Приоритет	Время выполнения (или закон распределения)	
		без использования ИТ	с использованием ИТ
1	2	3	4
Прием обращения гражданина	9	Нормальный закон распределения Нижняя граница – 15 мин Верхняя граница – 1 ч Математическое ожидание – 20 мин Стандартное отклонение – 5 мин	
Регистрация обращения, поступившего по почте России	8	Нормальный закон распределения	
		Нижняя граница – 5 мин Верхняя граница – 15 мин Математическое ожидание – 10 мин Стандартное отклонение – 5 мин	Нижняя граница – 0 мин Верхняя граница – 10 мин Математическое ожидание – 5 мин Стандартное отклонение – 5 мин
Регистрация обращения, поступившего по электронной почте	8	-	Нижняя граница – 0 мин Верхняя граница – 10 мин Математическое ожидание – 5 мин Стандартное отклонение – 5 мин
Регистрация электронного обращения, поступившего в СЭД «Мотив»	8	-	Нормальный закон распределения Нижняя граница – 0 мин Верхняя граница – 10 мин Математическое ожидание – 5 мин Стандартное отклонение – 5 мин
Регистрация обращения, поступившего в СЭД «Мотив»	8	-	0 мин
Регистрация документа и его направление на рассмотрение	8	10 мин	
Подготовка ответа на обращение гражданина	9	Нормальный закон распределения Нижняя граница – 10 дней Верхняя граница – 28 дней Математическое ожидание – 21 день Стандартное отклонение – 3 дня	
Регистрация ответа и снятие документа с контроля	7	20 мин	10 мин
Отправка ответа заявителю по почте России	7	5 мин	
Отправка ответа заявителю по электронной почте	7	0 мин	
Списание дела в архив	6	5 мин	
Отправка уведомления-напоминания исполнителю	9	10 мин	0 мин

Время выполнения операции регистрации обращений граждан, поступивших по почте России или электронной почте, включает в себя прочтение полученного текста и заполнение специалистом-делопроизводителем карточек учета обращений. В случае использования электронного журнала учета обращений граждан время выполнения некоторых операций сокращается (например, время регистрации ответа от исполнителя

заявки, отправление ему напоминаний об окончании нормативного срока рассмотрения заявки), так как автоматизирован процесс подготовки соответствующих документов.

Время выполнения некоторых операций процесса учета обращений граждан, которые поданы через электронную почту или интернет, отличается от времени учета обращений, поданных лично или по почте России. Для их различия электронным жалобам присваивается соответствующий признак, который учитывается при выполнении операций процесса обслуживания заявок.

Разработанные модели процессов регистрации и учета прохождения заявлений вручную и с использованием инфокоммуникационных технологий приведены на рисунках 1 и 2.

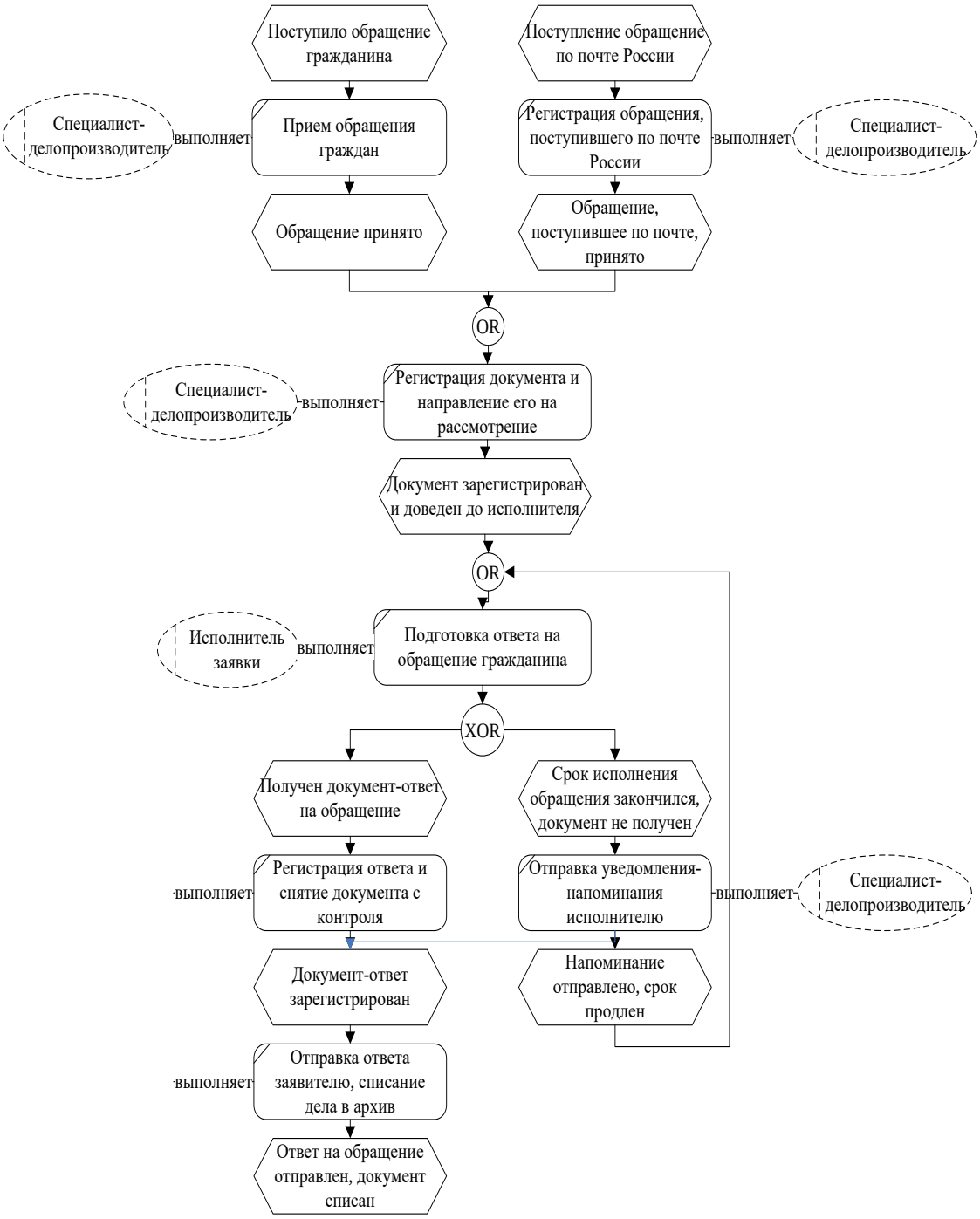


Рисунок 1. Функциональная модель процесса учета заявлений граждан, поданных лично

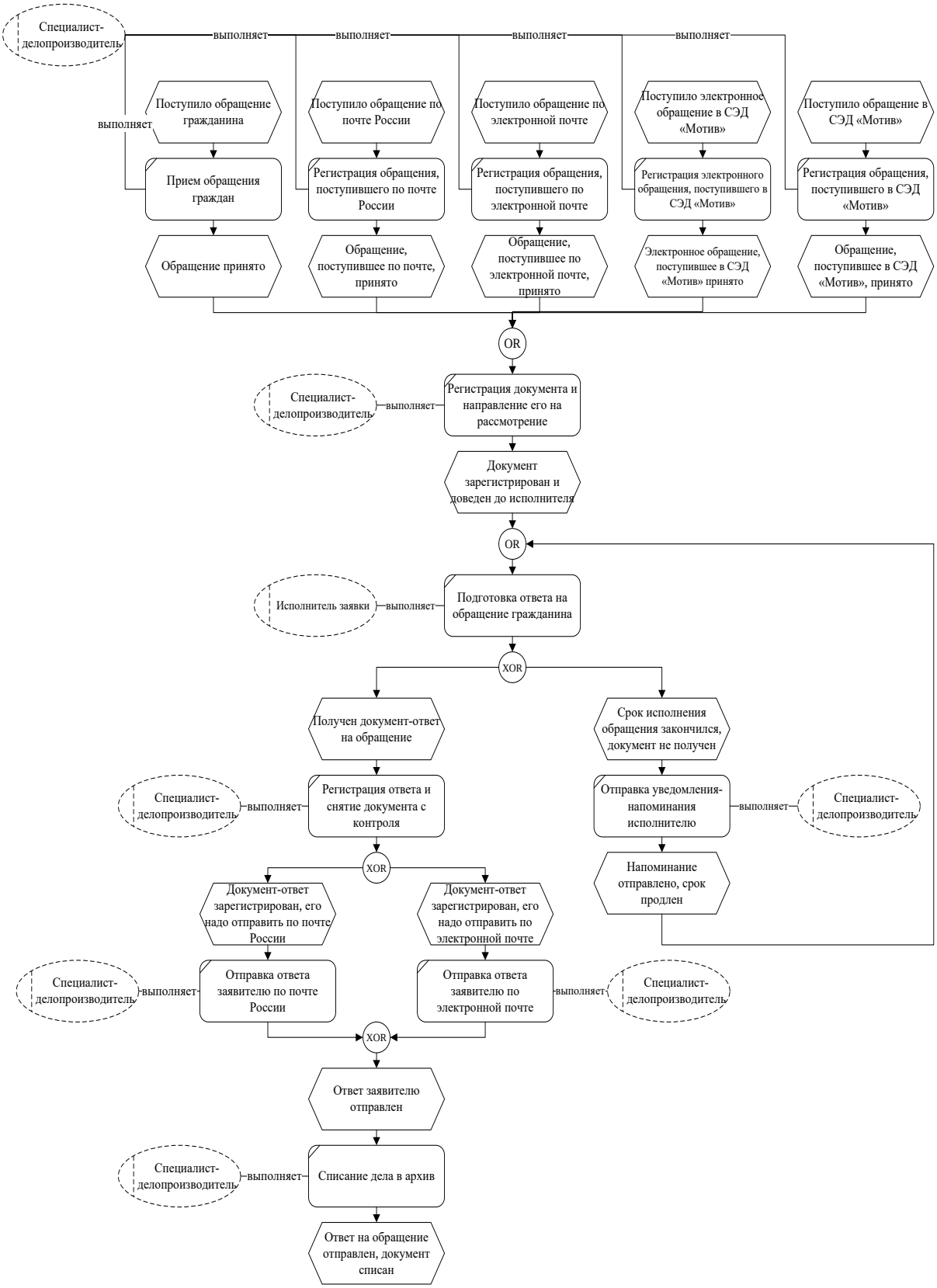


Рисунок 2. Функциональная модель процесса учета заявлений граждан, поданных с использованием инфокоммуникационных технологий

Таким образом, разработанные модели в нотации ARIS eEPC, описывающие процессы рассмотрения обращений граждан с использованием информационных

технологий и без них, позволят провести имитационное моделирование и определить достоверность результатов.

Методы исследования. Для выполнения имитационного моделирования использовалась система бизнес-моделирования Business Studio, которая поддерживает нотацию ARIS и выполняет учет временных, материальных и стоимостных ресурсов [12]. В результате проведения имитационного моделирования в Business Studio рассчитаны статистические характеристики процесса и показатели использования временных ресурсов: загруженность канала, средняя длина очереди, средняя продолжительность пребывания заявок в системе и очереди и т.д. Полные результаты моделирования приведены в [13].

Для проверки адекватности исходных данных модели воспользуемся критерием Манна-Уитни, который подходит для сравнения малых выборок [3]. Метод основан на определении того, достаточно ли мала зона перекрещивающихся значений между двумя вариационными рядами В каждой из выборок должно быть не мене 3-х значений признака.

Условием для применения U-критерия Манна-Уитни является отсутствие в сравниваемых группах совпадающих значений признака (все числа – разные) или очень малое число таких совпадений.

Результаты и обсуждение. Проведем оценку данных по U-критерию Манна-Уитни. Для расчета критерия количества поданных обращений за 12 месяцев с использованием информационных технологий составим таблицу выборок (таблица 4). Определили, что n_1 – количество случаев в первой выборке, а n_2 соответственно количество случаев во второй. Тогда получаем, что объем выборок n_1 =12, n_2 = 12. Всего случаев: N = 12+12= 24.

Таблица 4. Выборки критерия для процесса с использованием ИТ

1	Архив	285	286	268	278	236	273	302	312	311	315	352	282
2	Модель	311	304	300	312	306	288	297	292	292	294	300	304

Используя предложенный принцип ранжирования, получим таблицу рангов (таблица 5).

Сумма рангов первой выборки: R1 = 131. Сумма рангов второй выборки: R2 = 169.

Таблица 5. Ранжированный ряд выборок для процесса с ИТ

Выборка	Ранг	Выборка	Ранг
236	1	300	13,5
268	2	300	13,5
273	3	302	15
278	4	304	16,5
282	5	304	16,5
285	6	306	18
286	7	311	19,5
288	8	311	19,5
292	9,5	312	21,5
292	9,5	312	21,5
294	11	315	23
297	12	352	24

Обозначим наибольшую из этих сумм через T_x (T_x=169). Среди объёмов n_1 и n_2 выборок наибольший обозначим n_x, n_x=12. Тогда U=53, $U_{0.01}$ = 31, $U_{0.05}$ = 42, т.е. статистически значимых различий между результатами 1 и 2 групп выборки нет.

Аналогичные шаги проводим и для расчета критерия без использования ИТ (таблица 6). Определяем количество элементов n_1 и n_2, равными 12.

Соответственно строим ранжированный ряд, и также как и в первом, случаем, получаем таблицу рангов (таблица 7).

Таблица 6. Выборки критерия для процесса без использования ИТ

1	Архив	163	176	184	184	185	186	188	201	203	207	208	279
2	Модель	178	184	181	184	181	208	198	210	209	185	185	221

Таблица 7. Ранжированный ряд выборок для процесса без использования ИТ

Выборка	Ранг	Выборка	Ранг
163	1	186	13
176	2	188	14
178	3	198	15
181	4,5	201	16
181	4,5	203	17
184	6,5	207	18
184	6,5	208	19,5
184	8,5	208	19,5
184	8,5	209	21
185	10	210	22
185	11,5	221	23
185	11,5	279	24

Получаем, большая сумма из двух рангов T_x=152,5. Теперь также находим эмпирическое значение критерия U=69.5, $U_{0.01}$ = 31, $U_{0.05}$ = 42. Также получаем, что статистически значимых различий между результатами нет.

Так как $U1>Uкр$; $U2>Uкр$ – следовательно, различия между выборками статистически не значимы.

Выполним верификацию имитационной модели процесса, т.е. проверим соответствие алгоритма ее функционирования цели моделирования и назначению. При этом установим верность логической структуры модели процесса [14].

Для этого сравним время наступления событий в модели с реальным процессом и проведем оценку фактически полученных в результате моделирования распределений случайных величин и оценок их параметров с заданными значениями.

Средства системы Business Studio при выполнении имитационного моделирования представляют пользователю статистику по каждой операции исследуемого процесса и позволяют сравнить время выполнения подпроцессов модели с реальной системой. В таблицах 8 и 9 отображены сравниваемые значения, анализ которых позволяет сделать вывод, что они совпадают.

Таблица 8. Сравнение времени наступления событий в модели с реальным процессом без использования ИТ

Подпроцесс	Параметры модели	Реальные параметры подпроцесса
	Время выполнения, с	
А1. Прием обращения граждан	от 15 мин до 1 часа, среднее время – 20 мин	0:29:33
А2. Регистрация обращения, поступившего по почте России	от 5 до 15 мин, среднее время – 10 мин	00:12:30
А6. Регистрация документа и направление его на рассмотрение	10 мин	00:10:00
А7. Подготовка ответа на обращение гражданина	от 10 до 28 дней, среднее время – 21 день	20 дней12:51:43
А8. Регистрация ответа и снятие документа с контроля	20 мин	00:20:00
А9. Отправка уведомления-напоминания исполнителю	10 мин	00:10:00
А10. Отправка ответа заявителю по почте России	5 мин	00:05:00
А12. Списание дела в архив	5 мин	00:05:00

Таблица 9. Сравнение времени наступления событий в модели с реальным процессом с использования ИТ

Подпроцесс	Параметры модели	Реальные параметры подпроцесса
	Время выполнения, с	
А1. Прием обращения граждан	от 15 мин до 1 часа, среднее время – 20 мин	00:25:39
А2. Регистрация обращения, поступившего по почте России	от 0 до 10 мин среднее время – 5 мин	00:05:13
А3. Регистрация обращения, поступившего по электронной почте	от 0 до 10 мин среднее время – 5 мин	00:04:52
А4. Регистрация обращения, поступившего в СЭД "Мотив"	от 0 до 10 мин среднее время – 5 мин	00:05:04
А5. Регистрация электронного обращения, поступившего в СЭД "Мотив"	0 мин	00:00:00
А6. Регистрация документа и направление его на рассмотрение	10 мин	00:10:00
А7. Подготовка ответа на обращение гражданина	от 10 до 28 дней, среднее время – 21 день	22 дня 03:09:20
А8. Регистрация ответа и снятие документа с контроля	10 мин	00:10:00
А9. Отправка уведомления-напоминания исполнителю	5 мин	00:05:00
А10. Отправка ответа заявителю по почте России	5 мин	00:05:00
А11. Отправка ответа заявителю по электронной почте	0 мин	00:00:00
А12. Списание дела в архив	5 мин	00:05:00

Таким образом, верификация разработанных моделей подтверждает соответствие алгоритмов их функционирования цели моделирования и назначению.

Валидация данных имитационной модели предполагает исследование свойств имитационной модели, когда оцениваются такие свойства модели, как устойчивость, точность и другие свойства модели.

Устойчивость результатов моделирования – это сходимость контролируемого параметра моделирования к определенной величине при увеличении времени моделирования варианта сложной системы.

Для оценки устойчивости загрузки сотрудников использовалась следующая методика: пусть модельное время t=360 дней, с шагом Δt=30 дней будем снимать значения параметра ρ (процент загруженности специалиста-делопроизводителя), а затем рассчитаем амплитуду изменения данной характеристики (таблица 10).

На основе данных таблицы 10 и графиков процента загрузки специалиста-делопроизводителя (рисунок 3) можно сказать, что исследуемый процесс имеет устойчивый характер имитаций. При этом процент загрузки специалиста-делопроизводителя при использовании информационных технологий возрастает на 15%.

Таблица 10. Амплитуда изменения процента загруженности специалиста-делопроизводителя

Количество дней	Модель без использования ИТ		Модель с использованием ИТ	
	Процент загрузки	Амплитуда изменения	Процент загрузки	Амплитуда изменения
30	52,3	-	64,95	-
60	58,4	6,10	81,71	16,76
90	65,8	7,40	85,50	3,79
120	78,6	12,80	92,46	6,96
150	79,4	0,80	93,69	1,23
180	80,39	0,99	94,26	0,57
210	80,12	0,27	94,35	0,09
240	80,43	0,31	94,22	0,13
270	80,06	0,37	94,31	0,09
300	80,15	0,09	94,38	0,07
330	80,08	0,07	94,27	0,11
360	80,11	0,03	94,32	0,05

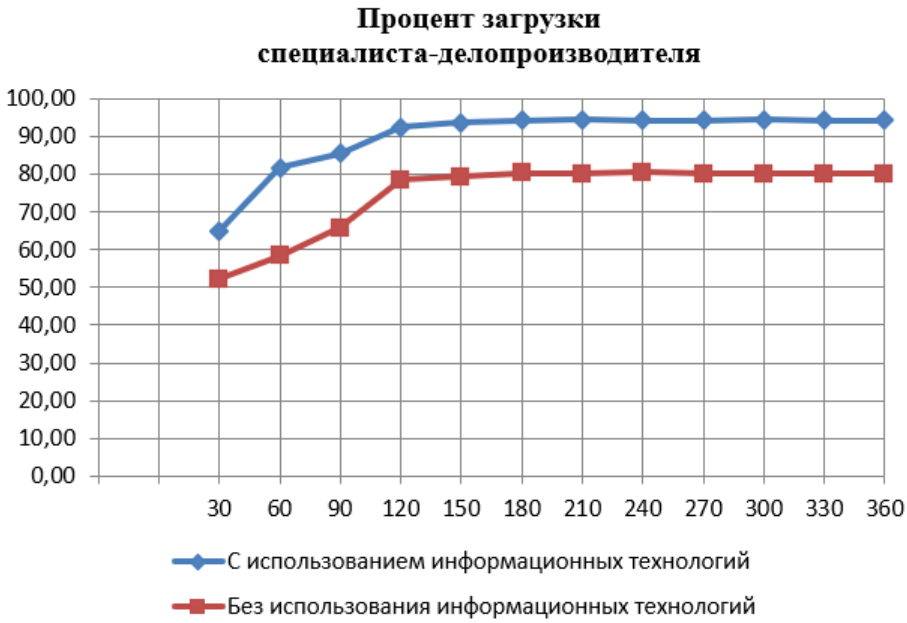


Рисунок 3. Графики процентов загрузки специалиста-делопроизводителя

Заключение. Разработанные функциональные модели процессов учета заявлений граждан в нотации ARIS eEPC позволили оценить производительность сотрудников и увидеть, что использование средств информационных и коммуникационных технологий

для подачи и учета обращений граждан обеспечивает не только удобство подачи заявлений, но и уменьшает время работы с заявлениями.

Исходные данные моделей проверены на адекватность по критерию Манны-Уитни, а также проведена оценка устойчивость результатов моделирования. Погрешность результатов моделирования не превышает 5%.

СПИСОК ЛИТЕРАТУРЫ

1. *Евдокимова С.А., Драгина Д.Н.* Функциональная модель управления входными документами организации в нотации ARIS // Моделирование систем и процессов. - 2017. - Т. 10, № 1. - С. 14-20. - DOI: 10.12737/article_5926f7b172b318.01917519
2. *Новикова Т.П., Новиков А.И., Дорохин С.В.* Математическая модель распределения трудовых ресурсов при технической эксплуатации и ремонте автотранспортных средств // Актуальные вопросы инновационного развития транспортного комплекса. Материалы 5-ей Международной научно-практической интернет-конференции. – Воронеж: ВГЛТУ, 2016. - С. 133-139.
3. *Лычкина Н.Н.* Имитационное моделирование экономических процессов. – М.: Академия АйТи, 2005. – 164 с.
4. *Евдокимова С.А., Драгина Д.Н.* Имитационное моделирование процесса рассмотрения обращений граждан // Моделирование систем и процессов. - 2018. - Т. 11, № 3. - С. 15-24. - DOI: 10.12737/article_5c4f196b54f076.49037955
5. *Novikova T.P., Novikov A.I.* Economic evaluation of mathematical methods application in the management systems of electronic component base development for forest machines // IOP Conference Series: Earth and Environmental Science. International scientific and practical conference "Forest ecosystems as global resource of the biosphere: calls, threats, solutions" (Forestry-2019). - 2019. - С. 012035. - DOI: 10.1088/1755-1315/392/1/012035
6. *Novikov A.I., Novikova T.P.* Non-destructive quality control of forest seeds in globalization: problems and prospects of output innovative products // GLOBALIZATION AND ITS SOCIO-ECONOMIC CONSEQUENCES. Proceedings. Edited by prof. Ing. Tomas Kliestik. - 2018. - С. 1260-1267.
7. *Novikova T.P., Novikov A.I.* Production of complex knowledgebased systems: optimal distribution of labor resources management in the globalization context // GLOBALIZATION AND ITS SOCIO-ECONOMIC CONSEQUENCES. Proceedings. Edited by prof. Ing. Tomas Kliestik. - 2018. - С. 2275-2281.
8. *Новикова Т.П., Бодин А.А., Евдокимова С.А.* Разработка алгоритма и модели функционирования информационной системы для платного отделения стоматологической поликлиники // Моделирование систем и процессов. - 2021. - Т. 14, № 1. - С. 51-58. - DOI: 10.12737/2219-0767-2021-14-1-51-58
9. *Зарипова Р.Х., Рассказова М.Н., Стариков В.И.* Использование EPC-диаграмм в моделировании бизнес-процессов производственно-сбытовой деятельности малых предприятий швейной отрасли // Омский научный вестник. – 2016. – № 5 (149). – С. 155-159.
10. *Новикова Т.Б.* Опыт моделирования диаграммы EPC в социальных и экономических системах // Международный журнал экспериментального образования. – 2016. – №12. – С. 400-403.
11. *Евдокимова С.А.* Выбор методологии моделирования предметной области при проектировании информационной системы // Моделирование систем и процессов. - 2015. - Т. 8, № 3. - С. 18-22. - DOI: 10.12737/17161
12. Business Studio: управление бизнесом, бизнес-моделирование, описание, регламентация и оптимизация бизнес-процессов. – URL: https://www.businessstudio.ru/ (дата обращения: 20.10.2021).

13. *Евдокимова С.А., Драгина Д.Н.* Анализ результатов имитационного моделирования процесса учета обращений граждан / Информатика: проблемы, методология, технологии. Материалы XIX международной научно-методической конференции. – Воронеж: ВГУ, 2019. - С. 1113-1117.
14. *Клейнен Дж.* Статистические методы в имитационном моделировании. – М. : Статистика, 2008. – 224 с.

И.А. Енгибарян[1], С.С. Тимашов[2], Л.В. Черкесова[2], О.А. Сафарьян[2]

СИСТЕМА МОНИТОРИНГА ПОВЕДЕНИЯ ОБУЧАЮЩИХСЯ ПРИ ПРОВЕДЕНИИ АТТЕСТАЦИОННЫХ МЕРОПРИЯТИЙ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия [1]
ФГБОУ ВПО «Донской государственный технический университет» (ДГТУ),
г. Ростов-на-Дону, Россия[2]

Ключевые слова: система прокторинга, онлайн-прокторинг, онлайн-образование, машинное обучение, формы контроля, Covid-19.

Рассматривается особенности систем онлайн-прокторинга и их применения как инструмента образовательной деятельности в дистанционном формате обучения. Принимая во внимание отличительные черты данных систем, предложена разработка схемы функционирования данной системы.

I.A. Engibaryan[1], S.S. Timashov[2], L.V.Cherckesova[2], O.A. Safaryan[2]

THE SYSTEM OF MONITORING THE BEHAVIOR OF STUDENTS DURING CERTIFICATION ACTIVITIES

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Don State Technical University (DSTU), Rostov-on-Don, Russia[2]

Keywords: proctoring system, online-proctoring, online-education, machine learning, forms of control, Covid-19.

The features of online proctoring systems and their application as a tool for educational activities in a distance learning format are considered. Taking into account the distinctive features of these systems, it is proposed to develop a scheme for the functioning of the system.

В 2020 году в связи с распространением коронавирусной инфекции большинство учебных заведений были вынуждены перейти на дистанционный формат обучения[1-3], что в свою очередь привело к некоторым проблемам во время проведения различного рода аттестационных работ в формате онлайн. Давно известно, что человеческий организм далёк от совершенства, и уследить за группой обучающихся в 20 или более человек в данном формате физически невозможно. Многие учащиеся во время проведения самостоятельных и контрольных работ пользовались различными хитростями и посторонними ресурсами, что категорически нарушает правила сдачи аттестационной работы и ведёт к обнулению её

результатов. Для того чтобы решить проблемы в лице распространения короновирусной инфекции между учащимися и сотрудниками, а также поддержания контроля и качества проведения аттестационных работ в дистанционном формате некоторыми учебными заведениями было принято решение использовать системы онлайн-прокторинга[4] предназначенные для сопровождения и контроля во время сдачи проверочных работ.

Целью данной работы является аналитический разбор систем онлайн-прокторинга и построение схемы разрабатываемой системы.

Первая система онлайн-прокторинга была разработана в Америке в 2008 году компанией ProctorU. В то время система представляла собой всего лишь дистанционное наблюдение за студентами через веб-камеру и фиксацию проктором всех нарушений в ручном режиме. Однако с того времени технологии шагнули далеко вперёд и данные системы автоматизировали и усовершенствовали. В большинстве из них стали применять методы и алгоритмы из различных областей искусственного интеллекта. Ведущими областями данного направления являются машинное обучений и компьютерное зрение, благодаря которым и проходит самообучение данных систем и сам процесс распознавания нечестного поведения [5-8].

В настоящее время существует несколько видов контроля в зависимости, от которого меняется функционал систем [9]:

1) Автоматический прокторинг – проверочная работа проводится в любое удобное для студента время. Программное обеспечение в автоматическом режиме сопровождает обучающихся от начала и до конца аттестационной работы. С помощью методов машинного обучения и компьютерного зрения система проводит идентификацию личности студента посредством сравнения фото с веб-камеры обучающегося и сравнения его с фотографией находящейся в профиле. Далее после начала сеанса начинается запись из трёх источников (аудио, видео с веб-камеры, рабочий стол) после чего система помечает все подозрительные действия в поведении обучающегося и формирует отчёты с результатами и в конечном итоге формирует оценочную базу, выставляя общий балл за прошедшую проверочную работу. Однако данный вид систем имеет довольно значительные минусы:

- слепая зона веб-камеры;
- необъективность программного обеспечения;

Первый минус решается посредством применения дополнительных веб-камер или камер с мобильного телефона. Второй минус под собой подразумевает неточность в оценке поведения участника тестирования. Программа способно принимать некоторые обычные действия участника за мошенничество в связи, с чем довольно сильно может меняться конечная оценка. Решение в данном случае приходится на использование человеческих ресурсов, что под собой предполагает асинхронный прокторинг.

2) Асинхронный прокторинг – комбинированный вид контроля. Система также в автоматическом режиме сопровождает обучающихся от начала и до конца сеанса сдачи проверочной работы и в тоже время делается запись трансляций с временными метками обнаруженных нарушений. Далее после окончания записи происходит её проверка проктором и выставление результатов. Минусом данного подхода является задержка во времени в моментах между окончанием записи и ручной перепроверкой, в особенности достаточной нагрузки на проктора.

3) Синхронный прокторинг – также является комбинированным видом контроля. Однако помимо программного сопровождения в режиме реального времени за обучающимися наблюдает сам проктор, который в своё очередь избавляет от главных недостатков прошлых видов систем. В любой момент специалист может попросить обучающегося повернуть камеру и показать как рабочую поверхность, так и то, что происходит вне поля зрения камеры в обычном положении. Программное обеспечение оповещает о замеченных нарушениях в поведении участника тестирования, а специалист, отреагировав на данное нарушение, делает выводы о присутствии или отсутствии такового.

Также у последних двух видов онлайн-прокторинга имеется общий минус – стоимость часа работы проктора и развёртывания или интеграции системы в целом.

В результате этого для решения проблем в лице возможного присутствия нечестного поведения во время проведения аттестационных работ и цены за обеспечение деятельности системы онлайн-прокторинга вместе со специалистом, планируется разработать собственный комплекс, состоящий из нескольких модулей, реализующих функции системы онлайн-прокторинга.

В ходе анализа информации предоставленной в открытом доступе сети интернет о существующих системах онлайн-прокторинга, было принято решение разработать схему функционирования комплекса системы онлайн-прокторинга, реализующую работоспособность между различными компонентами посредством приложения. На рисунке 1 представлена схема.

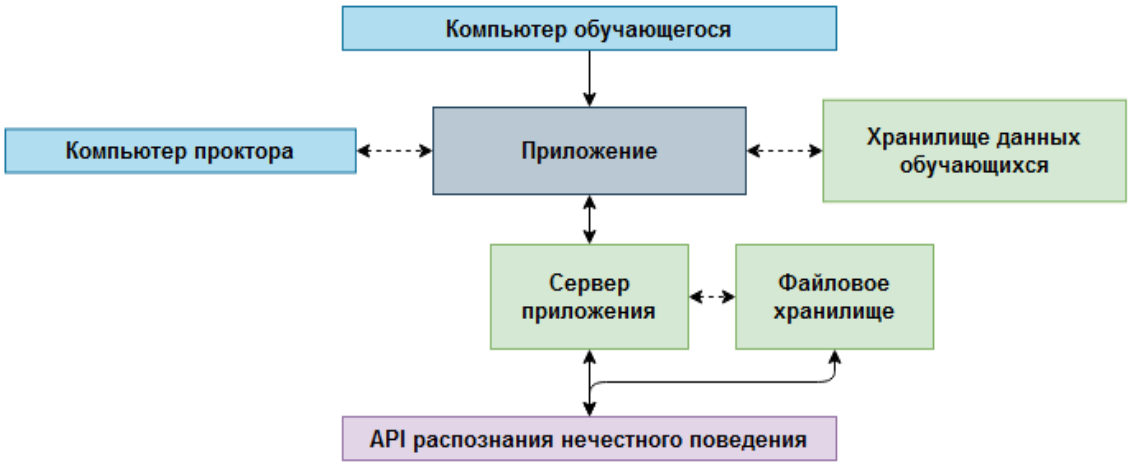


Рисунок 1. Схема системы

Данная система будет состоять из нескольких компонентов, отвечающих за различные источники получения информации. После авторизации обучающегося и присоединения к сессии для прохождения тестирования приложение будет отсылать все информационные потоки на сервер с API для распознания поведения.

Заключение

В данной статье были рассмотрены общие вопросы, касающиеся существующих систем онлайн-прокторинга, затронуты их особенности функционирования и минусы каждой из них. Была предложена схема разрабатываемой системы онлайн-прокторинга и поставлена задача в реализации компонента отвечающего за отслеживание поведения.

СПИСОК ЛИТЕРАТУРЫ

1. Дистанционная форма обучения: что это такое. URL: http://www.sano.ru/articles/distanczionnaya-forma-obucheniya-chto-eto-takoe.html (дата обращения 07.10.2021).
2. Moore M.G., Kearsley G. Distance education: a systems view of online learning // Wadsworth Cengage Learning. – Belmont, Calif.: 2012. – 384. – ISBN: 978-1-111-52099-1.
3. Ключевская И. С. Проблемы развития высшего образования в условиях пандемии Covid -19 // Трансформация вузовского образования: от локальных кейсов

к тенденциям развития. – Москва: «Московский экономический институт», 2020, с 141-147. – ISBN: 978-5-6044533-4-6.
4. Система прокторинга ProctorEdu. URL: https://proctoredu.ru/ (дата обращения: 07.10.2021).
5. Сохина С.А., Немченко С.А., Машинное обучение. Методы машинного обучения // Современная наука в условиях модернизационных процессов: проблемы, реалии, перспективы. – Уфа: ООО НИЦ «Вестник ума», 2021, с 165-168.
6. Загребин А.Н., Николева И.В. Алгоритмы компьютерного зрения: обнаружение лиц // Информационное общество: современное состояние и перспективы развития. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2019, с 151-153.
7. Галимов Р.Г. Основы алгоритмов машинного обучения - обучение без учителя // Аллея науки. – Томск: «Quantum», 2017, с 807-809.
8. Галимов Р.Г. Основы алгоритмов машинного обучения - обучение с учителем // Аллея науки. – Томск: «Quantum», 2017, с 810-817.
9. Что такое прокторинг и чем он полезен на экзаменах, тестировании и в обучении. URL: https://finacademy.net/materials/article/proktoring (дата обращения 08.10.2021)

О.В. Аликина, Д.Л. Устименко

ПРИМЕНЕНИЕ ИГРОВЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: игровые технологии, информационная безопасность, обучение.

В статье рассмотрена проблема адаптации процесса образования под стремительно развивающиеся информационные технологии, предоставлены основные методы внедрения игрового процесса в обучение специалистов по информационной безопасности, описано влияние игр на развитие профессиональных навыков.

O.V. Alikina, D.L. Ustimenko

THE USE OF GAMING TECHNOLOGIES IN THE TRAINING OF INFORMATION SECURITY SPECIALISTS

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

Keywords: gaming technologies, information security, training.

The article deals with the problem of adapting the educational process to rapidly developing information technologies, provides the main methods of introducing the game process into the training of information security specialists, describes the impact of games on the development of professional skills.

Введение

В настоящее время происходит переход от индустриального общества к информационному. Поэтому современный человек, а тем более специалист в сфере информатики должен свободно ориентироваться в постоянно растущем и изменяющимся потоке информации. Стремительное совершенствование технологий, развитие мощных компьютерных систем хранения и обработки информации повысили уровни ее защиты. С развитием сложной архитектуры хранения данных, необходим и рост их эффективной защиты.

Получается, специалисты по информационной безопасности должны уметь угнаться за быстрорастущим прогрессом. И тут возникает вопрос: как можно обучиться тому, что будет необходимо через несколько лет?

Игровые технологии – вот один из ответов. Добыча необходимой информации для решения поставленных задач, да еще и подогрев игрового интереса для ее решения – все это осуществимо благодаря игровому механизму. В процессе игры человек примеряет на себя несвойственные ему роли и добивается успехов. Например, мультиплеерные игры дают возможность контактировать, коммуницировать и соревноваться с другими людьми.

Игровые технологии в образовании

Изобретение компьютерных технологий позволило создать принципиально новый класс систем. С совершенствованием компьютеров, увеличением их производительности удалось уйти от абстрактных игр, таких как Тетрис, Luxor и пр., к играм, имитирующим окружающую реальность, что позволило создать системы с принципиально новыми возможностями, которые можно применять в обучении.

Существует множество определений игры. Как отмечает А. Л. Каткова, игра – это один и видов образовательной деятельности учащихся, мотивом которой является сам процесс или действия с воображаемыми объектами в виртуальной или реальной ситуации, «направленный на познание, освоение и преобразование действительности и используемый в педагогическом процессе в качестве средства воспитания и обучения» [3]. Технология обучения – это набор методов, приемов и путей передачи социального опыта, и также техническое оснащение этого процесса. Можно прийти к выводу, что игровая технология – это способ получения знаний, который построен на игровых принципах и специфических процессах – игровых механиках, позволяющих приобретать необходимый навык.

Игры психологически готовят человека к напряженным эмоциональным ситуациям, позволяют проявить способность действовать в кризисных моментах. В процессе игры мы получаем различный опыт: позитивный и негативный. Отталкиваясь от биологии человека, можно сказать, что позитивный опыт способствует приливу эндорфинов – гормонов удовольствия. Так же эндорфины, за счет своего воздействия на процесс запоминания, «укладывают» информацию в долгосрочную память. А роль негативного опыта заключается в том, что после неудачи в правильном учебном процессе начинается анализ неверных действий, который подталкивает нас на получение положительного результата в дальнейшем [1].

Не мало важным аспектом является игровой сленг, без которого не обойтись в этом виртуальном мире. В широком смысле под игровым сленгом понимают любые слова, используемые только в той или иной игре. В чем же его польза? - В его особенности. Ведь у игроков нет нужды специального изучения слов. Значения слов игрового сленга запоминаются сами по себе, как бы «приклеиваются» к игроку в процессе раскрытия контекста игры. Такой же метод можно применять в процессе изучения профессиональной терминологии, что будет весьма эффективно.

В последние годы (с 2008 г.) в игровом мире становится популярным среде жанр интерактивного кино. Такая игра предполагает выбор игроком одной из нескольких сюжетных линий, которые ведут к той или иной концовке. Каждое действие, порой даже не самое важное, может привести к различным финалам. Интерактивные игры положительно

влияют на психологические особенности игрока. Так возможность выбора, помогает игроку осознано принимать и решения и в дальнейшем осознавать его результат.

Игровые процессы и инструменты в обучении специалистов по информационной безопасности

Нынешние компьютерные игры переполняет огромнейшее количество игровых процессов и инструментов, с помощью которых разработчики игр подогревают интерес к своему продукту и не теряют целевую аудитории.

Главным и основным игровым процессом, возможным для применения в образовании специалистов по информационной безопасности, является моделирование. Большинству очень интересно почувствовать себя летчиком, гонщиком, предводителем и т.д. Этот процесс особенен тем, что в смоделированной деятельности игрок сначала выполняет ее интуитивно, а потом уже с опорой на свои знания и опыт, тем самым увеличивая игровые показатели. Практически любой процесс из деятельности специалистов по защите информации возможно смоделировать, например, поиск уязвимостей или проектирование хранилища – не на пустых информационных ресурсах, а на приближенных к реальным.

Неотъемлемой частью игрового процесса является – погружение. В игровых стратегиях и симуляторах погружение побуждает пользователя выполнять многочисленные связанные между собой действия, влияющие на исход игры. В информационной безопасности возможно погружать обучающихся в отдельные много процессные виды деятельности - такие, как разработка и внедрение мероприятий по предотвращению рисков. Обучающиеся не только тренируют и развивают определенные профессиональные навыки, но и учатся последовательно мыслить, продумывать действия заранее.

Большая часть игр построена на командных взаимодействиях игроков. В реальной действительности успех выполнения проекта в установленные сроки зависит от набора знаний, навыков и действий сотрудников, выполняющих проект. Если моделирование строить для команды, то у обучающихся начнет вырабатываться навык взаимодействия в команде - не только социального, но и профессионального характера. При моделировании виртуальной ситуации из жизни специалистов по информационной безопасности, основанных на командном взаимодействии, у обучающихся будут развиваться навыки оперативной оценки ситуации и принятия решений.

Игры, помимо самих игровых процессов, имеют и такое преимущество как, игровые инструменты: система достижений, шкала успеха и награды.

Шкала успеха удобна тем, что она служит графическим представлением обширных задач, что всегда легче воспринимается, также имеет способность поддерживать интерес обучающегося на протяжении всего погружения или моделирования, и конечно дает наглядное представление освоенности курса в целом. Данный инструмент является частью всех сюжетных игр, симуляторов жизни и т.д.

Комплексное применение игровых процессов

Рассмотренные в предыдущем разделе игровые процессы и инструменты применимы не только в высшем профессиональном образовании, но и в дополнительном.

Стоит заметить, что для дополнительного профессионального образования возможно использовать игровые технологии также на курсах повышения знаний и навыков в сфере информационной безопасности для сотрудников, которые не связаны непосредственно с защитой информации. Например, моделирование ситуации кражи данных.

Использование игровых технологий для повышения квалификации специалиста в сфере информационной безопасности на основе моделирования эксплуатации новых уязвимостей и их устранения, также служит отличным примером применения инструментов игрового процесса.

Педагогу лишь остается организовать образовательный процесс, предоставив подготовленные игровые площадки и базовые учебные материалы. Потом активируется процесс приобретение обучающимися "мягких" навыков, которые нацелены на приспособление своих действий, подбор необходимой информации и инструментария, а также «жестких" профессиональных навыков и опыта их применения в рабочем контексте.

Итоги

Подводя итоги, можно сказать, что при правильно организованном процессе использования компьютерных игр, можно добиться успехов в обучение специалистов по информационной безопасности. Ведь особенности игры идеально подходят для этих целей. Так как игра – это тоже часть быстро развивающегося технологического прогресса, именно она позволяет обучаться навыкам, которые будут необходимы сейчас и в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Сумцова О. В. Влияние английского языка на формирование компьютерного сленга в русском языке // Молодой ученый. 2011. №4. С. 241.
2. Лорич И.В., Тюгаев И.М., Применение игровых технологий в обучении специалистов по информационной безопасности // Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2019. № 4. С. 59-63.
3. Каткова А. Л. Развитие ИКТ-компетентности преподавателей педагогического вуза // Вестник вятского государственного гуманитарного университета, 2015 г. № 5 стр. 132-135.

С.А. Швидченко, Л.М. Колдынская, А.М. Коршун, Х.Р. Хуссейн

РЕШЕНИЕ ЗАДАЧИ ПРОДВИЖЕНИЯ И ПРЕДСТАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ВУЗА В МОБИЛЬНОЙ СРЕДЕ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, приложения, учебные заведения, студенты, мобильное приложение, университетская среда, кроссплатформенное приложение, пользовательский сценарий.

В статье проведен анализ проблемы текущего веб-клиента СКФ МТУСИ, основными из которых являются отсутствие адаптивности при взаимодействии с мобильных устройств и неудобная навигация. Выполнен обзор систем графического дизайна интерфейсов и разработаны пользовательские сценарии для визуализации навигации в программе и представления функциональных возможностей.

S.A. Shvidchenko, L.M. Koldynskaya, A.M. Korshun, H.R. Hussein

SOLVING THE PROBLEM OF PROMOTING AND PRESENTING THE UNIVERSITY'S ACTIVITIES IN A MOBILE ENVIRONMENT

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

Keywords: information technologies, applications, educational institutions, students, mobile application, university environment, cross-platform application, user scenario.

The article analyzes the problems of the current SCF MTUCI web client, the main of which are the lack of adaptability when interacting with mobile devices and inconvenient navigation. An overview of the graphic design systems of interfaces has been performed and user scenarios have been developed for visualizing navigation in the program and presenting functionality.

Введение

Двадцать первый век по праву считается веком информационных технологий. Без них невозможно обойтись во многих сферах жизни. Сфера образования не является исключением. На сегодняшний день стремительно растет численность пользователей мобильных устройств. Благодаря росту популярности мобильных устройств, крупные высшие учебные заведения России, такие как «РАНХиГС», «НИУ ВШЭ», «РУДН» и др., не говоря уже о крупных коммерческих компаниях, предпочитают осуществлять поддержку мобильных клиентов наряду с веб-сайтами. Основными преимуществами мобильных приложений по сравнению с веб-сайтами является то, что они адаптивны для устройств выбранной операционной системы, что предполагает более высокую производительность и нативный интерфейс, в отличие от сайтов, просматриваемых через веб-браузер, могут иметь доступ к нативному функционалу, систему уведомлений, возможность функционирования в автономном режиме и др [1].

Каковы главные потребности пользователей приложений для учебных заведений. Учитывая, что наибольший контингент – студенты, то, в первую очередь, они заинтересованы в постоянном доступе к расписанию, своевременных уведомлениях, просмотре новостей, сведений об успеваемости и все это не открывая сайт в поисках нужного раздела. Преподаватели наряду со студентами хотели бы иметь мгновенный доступ к своему расписанию занятий и новостям.

Вследствие вышеперечисленного, нельзя преуменьшать важность мобильного клиента – это важный элемент экосистемы, предоставляющий востребованный инструментарий для людей, задействованных в образовательном процессе.

Объектом исследования работы является процесс продвижения и представление деятельности ВУЗа в мобильной среде. Предметом разработки является мобильное приложение для СКФ МТУСИ.

Обзор предметной области

Университетская среда – это место, где регулярно происходит обмен огромными потоками информации. Студенты и преподаватели должны быть в курсе расписания, они обмениваются информацией о домашних заданиях, консультациях, событиях и т.д.

Проанализировав информационную инфраструктуру университета, был определен ряд проблем, с которыми ежедневно сталкиваются студенты, преподаватели и сотрудники. Основной список проблем, следующий [5,6]:

- неудобство доступа к расписанию для студентов на веб-сайте: приходится постоянно находить нужный раздел, выбирать группу из списка, поскольку верстка сайта не адаптивна, с мобильного устройства это сделать очень сложно;

- неудобство доступа к расписанию для преподавателей: аналогичная проблема, что и для студентов, к тому же, для преподавателей выбор из списка отсутствует, и приходится вбивать ФИО в соответствующее поле, которое чувствительно к регистру, и не имеет отображения результатов поиска в реальном времени;
- нет возможности гибкой настройки отображения расписания по категориям: группа, преподаватель, аудитория;
- отсутствие уведомлений об изменениях в расписании;
- неудобства при просмотре ленты новостей с мобильного устройства;
- отсутствие автоматизации при запросе справок и документов для студентов;
- неудобный доступ к сведениям об успеваемости: приходится находить нужный раздел на веб-сайте загружать таблицу в формате Excel для просмотра, с мобильного устройства это неудобно и др.

Кроссплатформенные приложения – программы, которые имеют возможность работать на нескольких платформах. Преимуществами разработки кроссплатформенного приложения являются [2]:

- использование одного кода для каждой операционной системы;
- низкая стоимость и высокая скорость разработки по сравнению с созданием нативных приложений.

К недостаткам относятся:

- возможная необходимость создания части нативного кода;
- в некоторых случаях, производительность может быть ниже по сравнению с нативными приложениями;
- в некоторых случаях, размер занимаемого пространства на локальном хранилище устройства может быть больше, по сравнению с нативными приложениями.

Таким образом, выбор подхода к разработке производится в зависимости от необходимых технических требований, предъявляемых к мобильному приложению.

Инструменты для создания мобильного приложения

Разработку нативных приложений для устройств под управлением Android можно осуществлять на компьютерах под управлением операционной системы Windows, так и macOS и Linux. Традиционно создание программ под Android происходит в интегрированной среде разработки Android Studio с использованием языка программирования Java. Создание нативных приложений под iOS происходит с использованием интегрированной среды разработки Xcode, наряду с такими IDE, как Android Studio и Visual Studio Code и языка программирования Swift. Существенным недостатком разработки приложений является необходимость устройства под управлением операционной системы macOS [4,5].

Для разработки кроссплатформенных приложений используются различные фреймворки, такие как Xamarin, React Native, Flutter, Ionic и др. Также, как и при создании нативного приложения, чтобы скомпилировать кроссплатформенное на iOS необходим компьютер под управлением операционной системы macOS. Проанализировав инструментарий для создания мобильных приложений, было решено использовать Flutter SDK, в основе которого лежит объектно-ориентированный язык программирования dart. Данный комплект средств разработки позволит создать кроссплатформенное приложение с нативной производительностью и минимальными затратами времени на правки для каждой платформы. Разработка будет выполнена в интегрированной среде разработки Android Studio 4.1.3.

Постановка задачи

Целью данной работы является обеспечение удобства для пользователей, взаимодействующих с информационной системой СКФ МТУСИ и представление деятельности ВУЗа в мобильной среде, путем создания мобильного кроссплатформенного клиента университета. Разрабатываемое программное средство будет предоставлять следующие функции [6,7]:

- просмотр ленты новостей университета;
- поиск и просмотр расписания для категорий: группы, преподаватели, аудитории;
- получение push-уведомлений о новостях, изменениях в расписании;
- личный кабинет студента с возможностью просмотра сведений об успеваемости и зачетной книжки;
- личный кабинет администратора с возможностью публикации/удаления новости и др.;
- раздел с информацией о преподавательском составе с персонализированной страницей для каждого преподавателя;
- раздел телефонной книги с функцией поиска по ФИО сотрудника университета, должности и отделению;
- раздел оформления справок с возможностью выбора справки с последующей отправкой по эл. почте;

Обзор аналогов показал, что подобный перечень функций реализован далеко не во всех приложениях, и разработка данного программного продукта является достаточно актуальной на сегодняшний день. В результате выполнения поставленных задач, будет создано кроссплатформенное приложение для мобильных платформ Android и iOS, выполняющее вышеописанные функции.

Проектирование интерфейса приложения

Основная задача мобильного приложения состоит в том, чтобы помочь решить проблему пользователя как можно быстрее [8]. Здесь речь идет о секундах, а иногда и о долях секунд. Когда речь заходит о дизайне мобильного приложения, первая проблема, которую необходимо решить разработчику – обеспечение наиболее удобного и знакомого пользователю данной платформы дизайна интерфейса и навигации [4,5,7]. Для ускорения процесса решения проблем пользователя в приложении были разработаны гайдлайны. На данный момент существуют два гайдлайна под две крупные платформы: Android и iOS.

При проектировании дизайна пользовательского интерфейса необходимо выделить этапы, в результате прохождения которых будет создан прототип интерфейса. Основные этапы, следующие [2,3]:

- проектирование пользовательского сценария (user-flow);
- создание структурных схем экранов (wireframes).

Перед проектированием экранов приложения необходимо визуализировать последовательность действий пользователя - на какие экраны будет возможен переход и с какой из текущих вкладок этот переход будет осуществлен. Для этих целей служит user-flow - пользовательский сценарий перемещения по вкладкам, представлен в соответствии с рисунком 1.

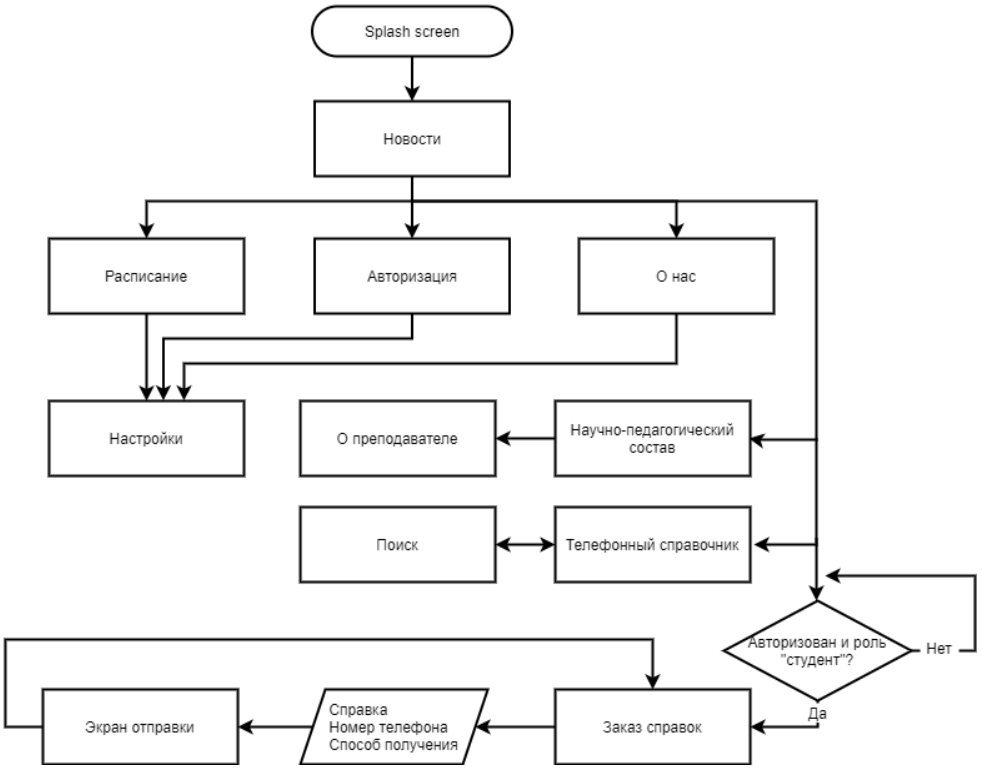


Рисунок 1. Пользовательский сценарий перемещения по вкладкам приложения

Исходя из поставленной задачи к функционалу программы, необходимо реализовать экраны «Научно-педагогический состав», «Телефонный справочник» и «Заказ справок» для студентов. Поскольку каждый из данных экранов равнозначен для пользователя, и к ним всегда необходим доступ, было принято решение разместить их в навигационном меню. Также необходимо учесть экран «Настройки», к которому необходим доступ со всех вкладок приложения, поскольку в любой момент при навигации пользователю может понадобиться изменить визуальную составляющую интерфейса программы, узнать информацию о программе или же осуществить связь с разработчиками.

Затем выполняется детализация схемы вкладок «Расписание» и «Аккаунт» для иллюстрации всех возможных сценариев действий пользователя. При выборе функции поиска будет осуществлен вызов экрана, на котором будет доступен поиск по ключевому слову. После успешного поиска, на вкладке «Расписание» будет отображено текущее расписание. При этом пользователь всегда может осуществить вызов экрана поиска с данной вкладки. Детализация пользовательского сценария вкладки «Расписание» представлена в соответствии с рисунком 2.

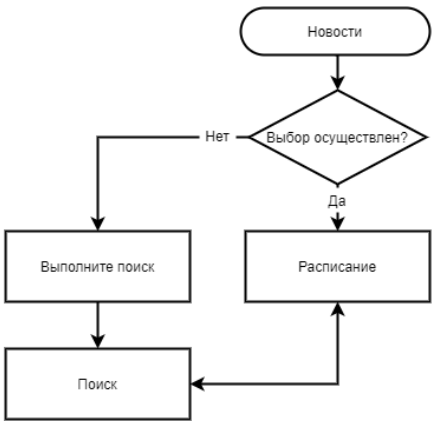


Рисунок 2. Детализация пользовательского сценария экрана «Расписание»

Вкладка «Авторизация» должна быть заменена на «Личный кабинет» в случае, если пользователь успешно прошел авторизацию. При этом, содержимое данной вкладки должно зависеть от роли пользователя. На момент написания данной работы личный кабинет будет предоставлять функционал для двух ролей: студент и администратор.

Студенту будет предоставлен доступ к вкладкам успеваемости в текущем семестре и сведений зачетной книжки. Администратор будет иметь доступ к экрану «Создание новости». Детализация пользовательского сценария вкладки «Авторизация» представлена в соответствии с рисунком 3.

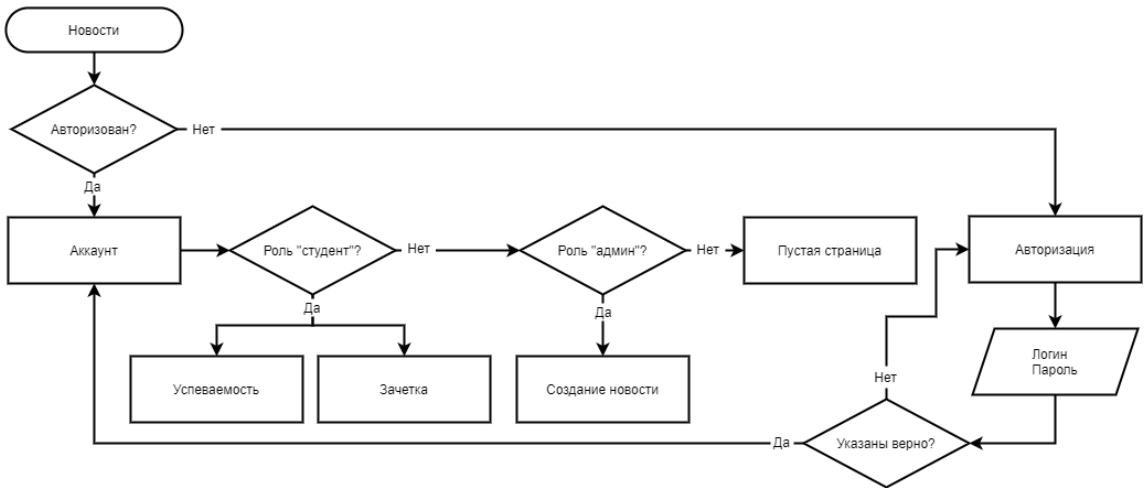


Рисунок 3. Детализация пользовательского сценария экрана «Авторизация»

Таким образом, построение пользовательских сценариев выполнено в полном объеме. Следующим шагом следует объединить все построенные пользовательские сценарии в общую схему.

Выводы

Обзор предметной области обосновал актуальность данной работы, в результате были обозначены проблемы текущего веб-клиента, основными из которых являются отсутствие адаптивности при взаимодействии с мобильных устройств и неудобная навигация [6]. В рамках данной статьи был проведен обзор систем графического дизайна интерфейсов, в результате которого были выделены системы построения пользовательских интерфейсов от создателей мобильных платформ, каждая из которых определяет набор рекомендаций, правил и принципов, следуя которым можно спроектировать единообразный интерфейс для каждой из целевых платформ.

Разработанные пользовательские сценарии позволили визуализировать навигацию в программе и представить функциональные возможности.

На основе пользовательских сценариев проведено прототипирование экранов приложения, необходимых для создания программного средства с требуемой функциональностью. В результате имеется полный прототип интерфейса, визуализирующий функционал проектируемого программного продукта и достаточный для того, чтобы можно было приступить к алгоритмизации и программной реализации.

СПИСОК ЛИТЕРАТУРЫ

1. *Унгер Р.,* Чендлер К. UX-дизайн. Практическое руководство по проектированию опыта взаимодействия. – СПб.: Символ-Плюс, 2011. – 336 с.
2. Native vs Cross platform app development. URL: https://uptech.team/blog/native-vs-cross-platform-app-development (дата обращения 03.10.21).

3. Apple Human Interface Guidelines. URL: https://developer.apple.com/design/human-interface-guidelines/ios/ (дата обращения 08.06.2021).
4. *Березовский В.В.,* Швидченко С.А., Коршун А.М., Абделмаксуд М.А.А. Анализ оборудования для организации связей между ядром сети и устройствами распространения сети провайдера. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 1. С. 123-125.
5. *Швидченко С.А.* Анализ обеспечения безопасности информации в АСУ. - В сборнике: Актуальные аспекты развития воздушного транспорта (Авиатранс-2018). Материалы международной научно-практической конференции. 2018. С. 257-262.
6. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство опроса и сбора программно-аппаратных характеристик персональных компьютеров. Свидетельство о регистрации программы для ЭВМ RU 2020613849, 23.03.2020. Заявка № 2020612910 от 16.03.2020.
7. *Bezuglov D.A.,* Bezuglov Y.D., Shvidchenko S.A. Method of discrete wavelet analysis of edges on the random background. В сборнике: 22nd International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision, WSCG 2014, Poster Papers Proceedings - in co-operation with EUROGRAPHICS Association. 22. 2014. С. 15-19.
8. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.

С.А. Швидченко, Л.М. Колдынская, А.М. Коршун, В.В. Гаврилов

ПРОЕКТИРОВАНИЕ СТУДЕНЧЕСКОГО ЧАТ-БОТА ДЛЯ РЕШЕНИЯ ЗАДАЧИ ПРЕДСТАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ВУЗА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, чат-бот, учебные заведения, студенты, мессенджеры, телеграмм-канал, мобильные устройства.

В статье проведен анализ проблемы взаимодействия студенческого общества с вузом СКФ МТУСИ и предложено решение на основе разработки студенческого чат-бота с широким списком функциональных возможностей.

S.A. Shvidchenko, L.M. Koldynskaya, A.M. Korshun, V.V. Gavrilov

DESIGNING A STUDENT CHATBOT TO SOLVE THE PROBLEM OF PRESENTING THE UNIVERSITY'S ACTIVITIES

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

Keywords: information technology, chatbot, educational institutions, students, messengers, mobile devices.

The article analyzes the problem of interaction of the student society with the university of the NCF MTUCI and offers a solution based on the development of a student chatbot with a wide list of functionality.

Введение

В современном мире технологии развиваются с высокой скоростью и мессенджеры постоянно предлагают пользователям новые возможности. Одна из таких возможностей — это создание чат-бота, программы, позволяющей общаться с пользователем в автоматическом режиме, круглосуточно, без привлечения реального человека. В настоящее время практически все современные мессенджеры предоставляют возможность создания чат-ботов. Область применения чат-ботов очень широкая: от поиска музыкальных композиций до рекламных промо-акций, от кулинарного помощника до помощника, подбирающего одежду в соответствии с погодой в указанной местности, от напоминаний о приеме лекарств до робота, отправляющего изображение в соответствии с заданным описанием [1].

Обзор предметной области

Под ботом обычно подразумевается некоторая программа, которая выполняет определенные действия через интерфейс, предназначенный для человека. Как правило, они используются для выполнения однотипных действий для увеличения скорости выполнения. Также боты могут использоваться для обеспечения более быстрой реакции на определенные события. Различных ботов объединяет то, что они имитируют поведение человека. Одной из разновидностей ботов является чат-бот. Чат-бот — это программа, имитирующая собеседника в чате. Она в автоматическом режиме позволяет удовлетворить потребности пользователя. В большинстве случаев, чат-бот ведет диалог от лица некоторой организации для оперативного предоставления актуальной информации.

Перечислим одни из самых перспективных направлений применения чат-ботов: 1) 1) Промо-кампании. Учитывая мобильное потребление и популярность мессенджеров, чат-бот является хорошим решением, которое позволяет упростить путь пользователя для участия в промо. 2) Здравоохранение. В англоязычных странах набирают популярность приложения и боты с персональными медицинскими помощниками, которые анализируют показатели здоровья человека и выдают персональные рекомендации. 3) Чат-бот как элемент креатива [2].

Из преимуществ чат-ботов над мобильными приложениями и сайтами можно выделить следующее пункты: персональное внимание к каждому клиенту; текстовый интерфейс потребляет мало трафика; низкая стоимость разработки; гибкость и скорость ответа; защита от конкурентов; не требует установки и авторизации.

Этапы и задачи разработки проекта

Данный проект разрабатывается как онлайн-помощник студентам и преподавателям, автоматизирующий различные рутинные задачи [3,6]. Изначально задуманный как чат-бот для расписания, он обзавелся другими, более сложными и полезными функциями. Основным отличием от традиционного мобильного приложения или веб-сайта является удобство и скорость получения необходимой информации. Основанный на обмене текстовой информацией, он позволяет в краткой и лаконичной форме удовлетворить самые частые запросы студентов.

В зависимости от типа и содержимого сообщения чат-ботом вызывается соответствующая модель. Если более подробно, то сообщения могут быть разных типов — это либо простое текстовое сообщение, либо мультимедиа, либо inline-запрос, либо callback-запрос. Разработанный чат-бот понимает разные типы запросов. Очевидно, что и содержимое этих запросов может разниться. Различные запросы позволяют использовать различные функции данного чат-бота [4,5]. Перечислим основные из них, которые реализованы в нем на данный момент:

1. Узнать пары в текущий момент времени с точностью до секунды. Этот функционал создавался для возможного использования совместно с автоматизированными системами подачи звонков и интерактивными табло, показывающими текущий статус занятий: либо сейчас пара, либо перемена, либо занятия закончились.
2. Узнать пары сегодня, завтра. В любое время за одно нажатие можно узнать какие будут пары у выбранной пользователем группы.
3. Узнать расписание звонков. В связи с пандемией во избежание лишних контактов студентов друг с другом университетом было введено отдельное расписание звонков для каждой группы. Это ввело определенную путаницу. Чат-бот решил эту задачу и в автоматическом режиме позволяет студенту получить расписание звонков именно его группы.
4. Узнать расписание занятий. За счет автоматических запросов к официальному сайту расписание занятий всегда поддерживается в актуальном состоянии. Расписание, доступное на сайте, всегда доступно и чат-боте. Причем оно доступно во многих форматах: все расписание одним списком, разбитое по неделям, по дням. Благодаря удобным функциям больше не нужно искать нужный день в длинном списке пар, достаточно указать его в чат-боте и он выведет соответствующие пары.
5. Загрузка PDF-файлов с различными расписаниями. Чат-бот может автоматически генерировать расписание не только в текстовом формате, но и в формате PDF. Файл может быть разбит таким образом, что один лист содержит расписание одной недели и одного дня. Это сделано для удобства печати сгенерированного PDF-файла. Также внизу каждой страницы отображается дата генерации документа во избежание путаницы с устаревшими документами.
6. Возможность изменить свою группу. Пользователь может изменить свою группу для того, чтобы узнать расписание другой группы либо в случае перевода. Это возможность всегда присутствует и ничто не ограничивает пользователя в пару кликов менять ее.
7. Основная информация о преподавателях. Фамилия, имя, отчество, фотография, ученая степень и прочая информация о преподавателе доступна в удобной форме прямо внутри мессенджера. Это виртуальный аналог стенда с фотографиями преподавателей, которые пользуется большой популярностью у студентов.
8. Возможность использования бота в inline-режиме. Можно узнать информацию о преподавателе в другом чате или диалоге введя в строку сообщения название бота. Таким образом студенты в чате могут отвечать другим студентам не ссылкой на сайт, а сразу результатом работы чат-бота.
9. Некоторые служебные и отладочные функции. Целый рад функций, направленный для тестирования работоспособности бота и устранения неполадок.
10. Справочная информация. Многим абитуриентам и их родителям часто бывает нужно справочная информация об университете — адрес, телефон, часы работы и тому подобное. Все это доступно в одно нажатие, изложено в подробной форме с интегрированными картами и геолокацией.

Взаимосвязь проекта с платформой

Разработанный проект можно разделить на несколько частей, которые тем или иным образом взаимодействуют друг с другом [7]. Необходимо рассмотреть различные подходы к процессу получения обновлений с серверов мессенджера. Также необходимо смоделировать как проект связан с самим мессенджером и конечным пользователем.

Описанные выше задачи помогут разобрать все этапы, которые проходят данные на пути от пользователя до приложения и обратно. Для наглядности все взаимосвязи изображены на рисунке 1.

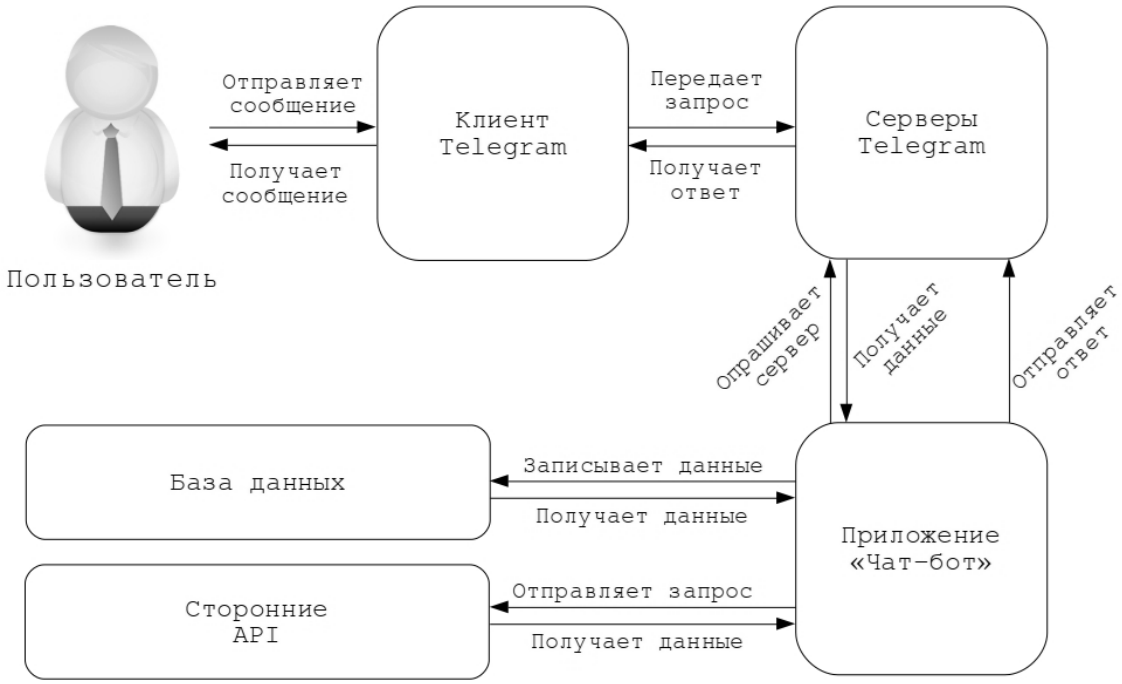


Рисунок 1. Взаимосвязь компонентов проекта

В общем случае пользователь использует клиент одного мессенджеров — в нашем случае это клиент мессенджера Telegram. Не играет роли какой тип клиента установлен: мобильный, десктоп или web-версия. Существование различных клиентов для разных типов операционных систем это зона ответственности разработчиков Telegram. Также по внутренним протоколам осуществляется обмен информацией между клиентом и серверами Telegram.

Далее пользователь путем использования клиента отправляет сообщение, которое направляется серверам Telegram. Сервер Telegram принимает это сообщение и должен отправить его в приложение чат-бота для дальнейшей обработки.

В зависимости от того, какой тип получение обновлений используется — Long Polling или WebHook — приложение получает отправленное пользователем сообщение. Как было отмечено ранее, данный проект использует Long Polling, поэтому, как только сервер Telegram получит данные, они сразу же отправятся в ответ на один из периодических запросов приложения.

Далее, в зависимости от типа и содержимого сообщения, контроллер вызовет одну из моделей, которая в свою очередь совершит некоторые действия, например, считает какие-либо данные из базы данных или обратится к сторонним API.

Согласно шаблону MVC, данные из модели направляются прямиком в представление, которым в данном проекте является клиент Telegram. Таким образом, приложение отправляет ответ на серверы Telegram, где он, за счет внутренних механизмов мессенджера, отображается в клиентском приложении пользователя

Выводы

В результате работы разобраны различные инструменты и методологии, используемые для дальнейшей разработки проекта: отдельное внимание уделено языку JavaScript, стандарту ECMAScript, серверной платформе Node.js и ее пакетному менеджеру [7]. Изучен фреймворк node-telegram-bot-api — основа данного проекта, принято решение за основу взять шаблон проектирования MVC при работе с информационными технологиями [5,6].

СПИСОК ЛИТЕРАТУРЫ

1. *Пауэрс Ш.* Изучаем Node. Переходим на сторону сервера. 2-е изд., доп. и перераб. — СПб.: Питер, 2017. — 304 с.: ил.
2. Официальная документация Telegram Bot API [Электронный ресурс]. URL: https://core.telegram.org/bots/api#inline-mode (Дата обращения: 07.06.2021)
3. *Березовский В.В.,* Швидченко С.А., Коршун А.М., Абделмаксуд М.А.А. Анализ оборудования для организации связей между ядром сети и устройствами распространения сети провайдера. - Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 1. С. 123-125.
4. *Швидченко С.А.,* Рыбалко И.П., Жуковский А.Г. Программа исследования корреляционных свойств псевдослучайных последовательностей. Свидетельство о регистрации программы для ЭВМ RU 2020614058, 26.03.2020. Заявка № 2020612871 от 16.03.2020.
5. *Bezuglov D.A.,* Bezuglov Y.D., Shvidchenko S.A. Method of discrete wavelet analysis of edges on the random background. В сборнике: 22nd International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision, WSCG 2014, Poster Papers Proceedings - in co-operation with EUROGRAPHICS Association. 22. 2014. С. 15-19.
6. *Безуглов Д.А.,* Швидченко С.А. Информационная технология вейвлет-дифференцирования результатов измерений на фоне шума. Вестник компьютерных и информационных технологий. 2011. № 6 (84). С. 40-45.
7. *Безуглов Д.А.,* Швидченко С.А. Синтез общей модели обеспечения безопасности для неоднородной системы обработки данных. В сборнике: Системный анализ, управление и обработка информации. труды X Международной научной конференции. 2020. С. 109-114.

Е.А. Щерба, С.А. Швидченко

АНАЛИЗ ЗАДАЧИ ИССЛЕДОВАНИЯ ПРОЦЕССОВ ЕСТЕСТВЕННОГО МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ОТБОРА

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия

Ключевые слова: информационные технологии, искусственный интеллект, машинное обучение.

В статье проведен анализ проблемы использования машинного обучения и искусственного отбора на основе алгоритмов обучения, требующих большого количества данных. Рассматривается возможность быстро и автоматически создавать модели и алгоритмы, которые могут анализировать крупные и сложные данные, обеспечивающие более быстрые и точные результаты в больших масштабах.

E.A. Shcherba, S.A. Shvidchenko

ANALYSIS OF THE PROBLEM OF STUDYING THE PROCESSES OF NATURAL MACHINE LEARNING AND ARTIFICIAL SELECTION

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

Keywords: information technology, artificial intelligence, machine learning.

The article analyzes the problem of using machine learning and artificial selection based on learning algorithms that require a large amount of data. The possibility of quickly and automatically creating models and algorithms that can analyze large and complex data, providing faster and more accurate results on a large scale, is being considered.

Введение

Практически любая автоматизация интеллектуальной человеческой деятельности относится к области искусственного интеллекта. Искусственный интеллект принято делить на три категории – слабый (распознавание образы, речи, генерация текста, голосовые помощники), средний и сильный (глобальный самостоятельный искусственный интеллект человеческого масштаба).

Машинное обучение

Машинное обучение – одно из направлений такого понятия, как искусственный интеллект, когда на основе введенных данных машина сама может сделать какие-то выводы. Машинное обучение сейчас применяется для решения широкого круга задач. Распознаванием лиц в наши дни давно уже никого не удивишь, почти в каждом смартфоне встроена такая функция, равно как и генерация рукописного текста, машинный перевод текста на иностранные языки, причем со временем исчезли нелепости перевода. «В последние годы большое количество исследований искусственного интеллекта, интуиции связано с нейронными сетями» [5].

Сегодня поиски нейрокибернетиков максимально ориентированы на моделирование программных устройств, структура которых максимально сходна со структурой мозга. Однако, пока ни один суперкомпьютер не может сравниться с мощностью головного мозга. Поэтому одним из направлений, над которым работают ученые и инженеры - создание электронных аналогов человеческого интеллекта [6,7,8].

«Машинное обучение концентрируется на разработке таких компьютерных программ и алгоритмов, которые сами учатся расти и адаптироваться при подаче новых данных. Этот процесс не похож на процесс интеллектуального анализа данных. Обе системы проходят через предоставленные им данных или собираются в поисках шаблонов. Однако в приложениях для интеллектуального анализа данных, данные извлекаются для понимания человеком, в то время как алгоритмы машинного обучения используют эти данные для поиска шаблонов в данных и соответственно изменения действий программы» [3].

«Машинное обучение также можно определить как процесс решения практической задачи путем:

1. Формирования набора данных;
2. Алгоритмического построения статистической модели на его основе. Предполагается, что эта статистическая модель будет каким-то образом использоваться для решения практической задачи.

Обучение может быть с учителем, без учителя и с подкреплением. Цель алгоритма обучения с учителем — на основе набора исходных создать модель, которая принимает вектор признаков x на входе и возвращает информацию, которая позволяет определить метку для этого вектора признаков. Например, модель, созданная с использованием набора данных собак, могла бы принимать вектор признаков, описывающих собаку, и возвращать вероятность, какой породы эта собака. В обучении без учителя набор данных представлен коллекцией неразмеченных образцов. задачи. Например, в задачах кластеризации модель возвращает идентификатор кластера для каждого вектора признаков в наборе данных.

Обучение с подкреплением — это раздел машинного обучения, где предполагается, что машина «живет» в определенном окружении и способна воспринимать состояние этого окружения как вектор характеристик. Машина может выполнять некоторые действия в каждом состоянии. Разные действия приносят разные вознаграждения, а также могут перевести машину в другое состояние окружения. Цель алгоритма обучения с подкреплением — выучить желательную линию поведения.» [2]

«Одна из наиболее серьезных проблем, возникающих в обучении с подкреплением и отсутствующих в других видах обучения, — это проблема поиска компромисса между изучением и применением. Чтобы получить большее вознаграждение, агент, обучающийся с подкреплением, должен предпочитать действия, которые он уже проверил в прошлой своей деятельности и обнаружил, что они эффективны с точки зрения получения поощрения. Однако, чтобы обнаруживать их, надо пробовать выполнять такие действия, которые еще не выполнялись ранее. Агент должен применять те действия, про которые уже известно, что они позволяют получить вознаграждение, но он должен такжеи изучать новые действия, чтобы иметь возможность делать лучший выбор в будущем.[4] Например.

Мобильный робот решает, должен ли он войти в очередную комнату при сборе мусора или же ему уже пора начинать искать дорогу назад, к месту, где он сможет зарядить свои аккумуляторы. Он принимает соответствующее решение на основе данных о том, насколько быстро и просто удавалось найти зарядную станцию в прошлом. Помимо агента и среды, можно указать следующие четыре основных элемента, входящие в состав систем, реализующих обучение с подкреплением: стратегия, функция поощрения, функция ценности и, возможно, модель среды» [4].

«Следующим классом методов, являющимся ещё одним представителем восходящей парадигмы создания искусственного интеллекта, являются эволюционные алгоритмы. Этот класс методов является отдельным направлением в рамках исследований по искусственному интеллекту, в котором исследуются и моделируются процессы естественного машинного обучения и искусственного отбора. Все эволюционные алгоритмы моделируют базовые эволюционные процессы в природе – наследование, мутации и отбор. Что, если вычислительные процессы могли бы эволюционировать так же,

как это делают биологические виды в своей экологической среде? Возможно, получилось бы «выращивать» программы для оптимального решения поставленной задачи?» [1]

Заключение

В основном используется диапазон или спектр на основе метода оптимизации большого количества параметров. Для людей нецелесообразно находить такую оптимальную настройку вручную. Например, распознавание динамика из тона, тона и амплитуды [7]. Нет гарантии, что машинное обучение будет работать в каждом случае. Иногда машинное обучение терпит неудачу, требуя понимания проблемы, которая должна быть решена, чтобы применить правильный алгоритм. Очень большие требования к данным. Эти алгоритмы обучения требуют большого количества данных обучения. Было бы очень сложно работать с такими большими объемами данных или собирать такие данные. Но такие вещи, как увеличение количества и вариации доступных данных, разнообразие обработки, которое является более дешевым и мощным, и более доступное хранилище данных, в наши дни мы можем быстро и автоматически создавать модели и алгоритмы, которые могут анализировать более крупные и более сложные данные, обеспечивающие более быстрые и точные результаты в больших масштабах. Поэтому машинное обучение быстро становится очень важной и широко внедряемой частью нашей повседневной жизни [5, 6, 8].

СПИСОК ЛИТЕРАТУРЫ

1. Душкин Р. В.Исусственный интеллект. – М.: ДМК Пресс, 2019. – 280 с.
2. Машинное обучение без лишних слов. — СПб.: Питер, 2020. — 192 с.: ил. — (Серия «Библиотека программиста»).
3. *Черкасов Д.Ю.,* Иванов В.В. Машинное обучение - https://cyberleninka.ru/article/n/mashinnoe-obuchenie/viewer (дата обращения 20.10.2021)
4. Обучение с подкреплением [Электронный ресурс] /Р. С. Саттон, Э. Г. Барто ; пер. с англ. - 2-е изд. (эл.). - Электрон. текстовые дан - М. : БИНОМ. Лаборатория знаний, 2014. - 402 с.
5. *Флах П.* Машинное обучение. М.: ДМК Пресс, 2015.
6. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Программное средство проектирования однозоновой сети транкинговой связи для ее оперативного развертывания. Свидетельство о регистрации программы для ЭВМ 2021610521, 14.01.2021. Заявка № 2020665716 от 03.12.2020.
7. *Безуглов 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. - Нелинейный мир. 2012. Т. 10. № 11. С. 846-852.
8. *Швидченко С.А.,* Манин А.А., Жуковский А.Г. Автоматизированная система расчёта зон радио покрытия базовых станций системы сотовой связи. Свидетельство о регистрации программы для ЭВМ RU 2019610389, 10.01.2019. Заявка № 2018665175 от 24.12.2018.

В.А. Ландышев[1,2], О.Н. Ландышева[3]

ПРОВЕДЕНИЕ УЧЕНОГО СОВЕТА ВУЗА В РЕЖИМЕ УДАЛЕННОЙ РАБОТЫ

Северо-Кавказский филиал ордена Трудового Красного Знамени
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Ростов-на-Дону, Россия[1]
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»,
Ростов-на-Дону, Россия[2]
Институт водного транспорта имени Г.Я. Седова - филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный морской университет имени адмирала Ф.Ф. Ушакова»,
Ростов-на-дону, Россия[3]

Ключевые слова: Удаленная работа, ученый совет, удаленное голосование, работа в режиме самоизоляции.

В статье рассмотрены вопросы организации работы ученого совета ВУЗа в режиме удаленной работы с использованием облачных технологий. Рассмотрены преимущества и недостатки данного подхода.

V.A. Landyshev[1,2], O.N. Landysheva[3]

CONDUCTING THE SCIENTIFIC COUNCIL OF THE UNIVERSITY IN REMOTE WORK

North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia[1]
Federal State Budgetary Educational Institution of Higher Education "Don State Technical University", Rostov-on-Don, Russia[2]
Institute of Water Transport named after G.Ya. Sedov - a branch of the Federal State Budgetary Educational Institution of Higher Education “State Maritime University named after Admiral F.F. Ushakova », Rostov-on-Don, Russia[3]

Key words: Remote work, academic council, remote voting, work in self-isolation mode.

The article discusses the issues of organizing the work of the academic council of the university in the mode of remote work using cloud technologies. The advantages and disadvantages of this approach are considered.

В настоящее время для всех образовательных организаций в сфере образования основным фактором, влияющим на их повседневную деятельность, является пандемия COVID–19 и как следствие режим самоизоляции, которого вынуждены придерживаться студенты, преподаватели и учебно-вспомогательный персонал. В организациях Минобрнауки с 16 марта 2020 г. введены следующие меры борьбы с распространением новой коронавирусной инфекции [1]:

- контроль температуры при входе в здания;
- установка в зданиях средств дезинфекции;
- ограничение проведения очных совещаний и направления работников в служебные командировки;

– перевод работников на удаленный режим работы при необходимости.

Работа на “удаленке” требует нового подхода к решению ряда учебных и административных задач в повседневной деятельности образовательного учреждении. Все значимые управленческие решения в Донском государственном техническом университете, как и в любом российском вузе принимаются на Ученом совете в связи с чем регулярное проведение ученого совета является ключевым мероприятием в управлении Вузом. К задачам, решаемым на заеданиях ученого совета, относится проведение выборов деканов и заведующих кафедрами.

Решения Ученого совета по выборам деканов факультетов, заведующих кафедрами и представлению к ученым званиям принимаются тайным голосованием. Другие решения принимаются открытым голосованием. Решение о представлении к ученому званию считается принятым, если за него проголосовало не менее 2/3 голосовавших при участии в заседании Ученого совета не менее 2/3 от списочного состава его членов [2]

В связи с этим перед управлением информатизации была поставлена задача по проведению виртуального ученого совета в ДГТУ. Основными задачами, поставленными при выборе системы для проведения ученого совета, была определены как возможность:

- Заслушивание повестки дня и основных докладчиков участие в дискуссиях;
- Регистрации участников;
- Тайного голосования по выборам профессорско-преподавательского состава;
- Принятие решения по основным вопросам;
- Принятие решений по разным вопросам;
- Предоставление доступа к материалам.

В результате проведённого анализа решений представленных на рынке решений выбор был сделан в сторону облачного сервиса office 365 [3]. Для реализации системы виртуального Ученого совета применялись технологические элементы платформы:

- Microsoft Form – Формы голосования;
- Microsoft Teams – Заслушивание докладчиков дискуссия обсуждение вопросов повестки дня;
- Microsoft Share Point – обеспечение безопасного архивирования материалов ученого совета;
- Microsoft One Drive – хранение файлов с материалами ученого совета.

На рисунке 1 приводится отображение результатов тайного голосования членов Ученом совете

Рисунок 1 Результаты голосования

В результате проведения ученого совета было подключено порядка 180 пользователей в голосовании приняло участие 157 человек. Состоялась дискуссия и обсуждение повестки дня. Время проведения совета составила 3 ч 15 мин. В качестве клиентский устройств использовались как мобильные устройства Android и Apple. Персональные компьютеры под управлением MAC OS и Windows.

Выводы

1. Предложенная технология работы позволяет значительно повысить вовлеченность членов ученого совета в работу и обеспечить выполнение положений о кворуме голосов.
2. Повысить эффективность обмена информацией в рамках проведения ученого совета, повысить общую эффективность их работы.
3. Повысить скорость обработки результатов голосования от нескольких часов до минут.
4. Провести стратегически важно мероприятие во время режима вынужденной самоизоляции.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Министерства науки и высшего образования РФ от 14 марта 2020 г. № 398 “О деятельности организаций, находящихся в ведении Министерства науки и высшего образования Российской Федерации, в условиях предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации”
2. Положение об Ученом совете университета https://donstu.ru/structure/administrative/uchenyy-sovet/menu/dokumenty_uchsovet/
3. Справочная система Office 365 https://support.office.com/ru-RU

D.V. Lavrinenko, E.V. Evlanova, L.P. Koroleva

THE INTRODUCTION OF INFORMATION AND COMMUNICATION TECHNOLOGIES TO THE AVIATION MISSILE WEAPONS CONTROL SYSTEM

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia

The transience of modern combat operations makes it necessary to fully automate the management of troops and weapons at all levels of management, which is achieved by implementing infocommunication technologies in the management system. Management, implemented on the basis of automated and automatic systems, is a set of targeted actions of management bodies, organizing the activities of management objects, combined and organized through the use of a set of hardware and software technical means. At the same time, automated control systems differ from automatic ones in that they retain the most General, goal-setting, or non-automated functions for a person.

The development and implementation of modern and advanced information and communication technologies in military Affairs greatly accelerate and change the order of planning and conducting modern combat operations, as the increase in the effectiveness of command and control is achieved by increasing the speed of processing and transmitting information, or, in military terms, the efficiency of the control system. New approaches to modern warfare have led to the formation of the concept of network-centric warfare.

The concept of network-centric warfare [1] is based on the idea of conducting modern combat operations based on operational processing at the strategic or operational level with the help of artificial intelligence of a multidimensional array of data of all types of intelligence, the state of their troops and the enemy's troops, weapons systems, combat and logistics support using an extensive self-organizing infocommunication network that covers all links of combat orders and logistics and engineering support. Such networks are called "network-centric infocommunication networks" [2]. As a result, a single network of all types and means of intelligence, communication, data transmission and control is created, functioning in real time, interconnected with the network of control of weapons of destruction and networks of combat and other types of support. Thanks to the creation of a single digital information and communication space, information superiority on the battlefield is achieved, which allows for many times more effective and efficient implementation of the combat potential of groups of troops in the course of military operations. It becomes possible to anticipate the enemy at all stages of preparation and conduct of combat operations.

Thus, at the present time in Russia, a digital automated control system of the air force and air defense is in demand, combining its elements into a single high-speed transport network, which can become the basis of an automated control system (ACS) for air force and air defense weapons, that is, a network-centric control system for heterogeneous forces and means in the conflict region.

With the help of this automated control system, the command post of the integrated area accumulates and displays heterogeneous information coming from radars, long-range radar detection aircraft and space detection equipment, intelligence services of other types and types of troops that are connected to the system. Communication and information exchange in the system are provided by mobile wireless broadband complexes [3].

Efficiency of management, the most important of which criteria is the efficiency of the management system, provides system-wide software ACS that solves the problems of data exchange, electronic document management, collective work with documents, editing cartographic documents, video conferencing, information security, systematization of unified time, visualization and evaluation of results.

The introduction of information technologies that implement the capabilities of network-centric infocommunication networks in the control system of the air force and air defense, will solve global problems of automated collection, generalization, distribution and timely communication of data on the situation in headquarters and control points; automated development of documents and information interaction between management bodies at various levels; automated exchange of information in operational and tactical management links.

This approach implements fundamentally new approaches to the management of aviation weapons. Aviation weapons it is a set of complexes, systems, aggregates and means intended for combat impact on the enemy or providing such impact, placed on aircraft (LA).

The aircraft armament includes [4]:

- means of destruction;
- installations of weapons of destruction;
- artillery weapons;
- aircraft weapons control systems;
- aircraft defense systems;
- aircraft targeting systems;
- aviation support facilities.

Aviation weapons control systems include:

- guidance and targeting systems;
- system of fire control, start-up, reset;
- command devices;
- power supply systems;
- computer programming devices;
- targeting systems

The sighting systems include various sights and sights, thermal direction finders, target illumination stations (primarily laser), rangefinders, and on-Board computers for controlling the electronic component of the above-described equipment. The most important means of destruction are aircraft missiles.

Aircraft aiming systems of missiles implement the following basic principles of guidance [5]:

- command guidance;
- homing;
- autonomous guidance.

With command guidance, the missile's control system changes its trajectory based on information transmitted from an external source. There are systems that transmit both continuous and discrete information.

The following guidance systems operate based on the command guidance principle:

- radio command;
- TV command;
- radio beam guidance;
- laser beam guidance.

Modern radio command guidance systems are able to independently control the location of the missile using an optical sensor that tracks the missile tracer, or radar and calculate the trajectory of the missile to hit the target; the guidance operator can only hold the aiming marker on the target.

Control of the rocket is carried out directly by the operator of the AIRCRAFT carrier, which changes the deviation of the control handle of the rudder of the rocket itself, thereby controlling its flight path. The advantage of the radio guidance system is its independence from weather conditions and time of day, as well as high noise immunity of the communication channel and relatively high secrecy. Disadvantages include limited maneuverability of the carrier after launch and the need to detect and recognize the target before launch. The use of network-centric infocommunication networks makes it possible to eliminate these shortcomings by transmitting more detailed processed information and conducting automatic start - up from the management level of any level.

The television command guidance system is generally similar to the radio command guidance system. The main difference is the television camera installed on Board the rocket, which is used by the guidance operator to control the flight of the rocket. The guidance operator receives a real-time image of the terrain over which the missile is flying, and controls the flight by focusing on visible landmarks. After detecting the target, the operator orients the missile in its direction.

Similarly, the effectiveness of the TV command guidance system can be increased by including it in the structure of network-centric infocommunication networks. In this case the TV camera of the missile will interact automatically with the reconnaissance UAVs via broadband channels, and the guidance and launch will be carried out automatically.

The structure of the network-centric control can be turned on and the guidance system on the radio beam and by laser beam. This requires mainly the development of appropriate software, as telecommunications high-speed receiving and transmitting equipment is developed and widely used in wireless cellular networks (for example, LTE 4G).

Thus, it can be assumed that the introduction of nfocommunication technologies in the aviation weapons management system will significantly improve the quality of their combat use.

LIST OF REFERENCES

1. Kalistratov A. To the question about setentries actions in the armed struggle of the future.// Military Thought 2008 №12 p p. 22-70
2. The hierarchical network model is a promising system
3. control the defense of the state. https://ic.pics.livejournal.
4. com/general_skokov/65350025/64592/64592_900.jpg
5. p://arsenal-otechestva.ru/analytic/223-sistema-upravlenia-aviatsiej-i-pvo
6. https://wiki.wargaming.net/ru/Navy: Aircraft armament.
7. https://lektsii.org/3-22917.html

V.V. Ptitsyn, E.V. Evlanova, L.P. Koroleva

ENSURING CYBERSECURITY OF ONBOARD ELECTRONIC EQUIPMENT OF UNMANNED AERIAL VEHICLES

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia

Keywords: unmanned aerial vehicles (UAVs), onboard electronic equipment (OEE), cyber-attacks, cybersecurity, substitution of control information, violation of system integrity, the conditions of electronic suppression, introduction of software, vulnerabilities in software.

The most important of Unmanned aerial vehicles (UAVs) is the complex of onboard electronic equipment. OEE systems allow you to solve many tasks using an interconnected set of the systems and subsystems. Further development of tasks solved by military UAVs implies the need to consider advanced OEE as a set of interconnected automated systems. At the same time, the task of ensuring the safety of complexes becomes particularly urgent. Cyber attacks using software-defined radio technologies are considered the most promising.

Unmanned aerial vehicles (UAVs) for military purposes are aircraft platforms equipped with complex multi-component complexes. The most important of them is the complex of onboard electronic equipment (OEE).

OEE UAV systems allow you to solve the following tasks:

- preparing for departure;
- navigation;
- UAV management at all stages of the flight;
- provision of radio communication and information data transmission;
- providing group actions of UAVs and interaction, if necessary, with manned aircraft;
- target load management;
- ensuring the intended use;
- monitoring and diagnostics of on-Board equipment.

To solve these tasks avionics OEE UAVs for military purposes are an interconnected set of the following systems and subsystems:

1. Information and control system:
   1.1. On-Board computer network;
   1.2. Automatic control subsystem;
   1.3. Interface equipment with General facility equipment;
   1.4. On-Board equipment monitoring and diagnostics subsystem;
   1.5. Equipment for switching and converting information.
2. Navigation system:
   2.1. Inertial-satellite navigation subsystem;
   2.2. Air signal subsystem;
   2.3. Radio altimeter;
   2.4. Autonomous navigation subsystem for Earth’s physical fields;
   2.5. Low-altitude sensor subsystem.
3. Radio communication and data transmission subsystem:
   3.1. Radio control line equipment;
   3.2. High-speed data transmission equipment;
   3.3. Satellite communication equipment.
4. Target load systems:
   4.1. Optical-electronic subsystem;
   4.2. Radar subsystem;
   4.3. The subsystem of technical vision;
   4.4. Laser radar.
5. Radar identification system.

Further development of tasks solved by military UAVs implies the need to consider advanced OEE as a set of interconnected automated systems that solve the above and new functional tasks. At the same time, the task of ensuring the safety of OEE UAV in the conditions of electronic suppression and, first of all, preventing cyber-attacks against OEE UAV becomes particularly urgent. This is due to the fact that in parallel with the development of UAVs, the potential enemy is developing methods and means for purposefully disrupting the normal

functioning of OEE UAV, since modern technical means allow not only to detect and target radio channels for controlling and transmitting UAV data, but also to interfere with the operation of avionics and ground-based automated workstations (APMS) The main risk factors for cyber-attacks of OEE UAVs include:

- destructive radio-electronic effects on the information and control system;
- unauthorized access to the main nodes of the onboard computer network at the software level and, as a result, violation of technological cycles;
- blocking management due to the destructive impact of embedded software viruses;
- human factor (free access to OEE elements, programmer errors, etc.);
- using standard operating systems and hardware with existing undeclared capabilities.

Cyber-attacks can provide basic technical capabilities for an intruder:

- influence on the electrical parameters of the signal in the data bus;
- creating overloads;
- sending destructive packets (data in the wrong format, which can lead to failure of computer devices in OEE);
- unauthorized use of undocumented device capabilities, prohibited commands (falsification of sender device addresses);
- the substitution of the navigation data;
- substitution of control information;
- violation of system integrity.

All this determines the need to develop effective measures to ensure cybersecurity in relation to the OEE UAVs information management system, considered as a digital specialized UAV management system.

In this context, the concept of cybersecurity for OEE UAV is considered as a set of conditions under which all components of the information management system and the processes that occur in it are protected from the maximum possible number of threats and impacts with undesirable consequences.

UAVs are controlled remotely via satellite or other wireless communication and data channels. Their operators can be thousands of kilometers away in the NPU.

In this regard, the following types of cyber-hacking of the UAV computer network can be used most often.

1. Interference and introduction of malicious software into the UAV computer network by intercepting radio communication channels and transmitting data.
2. Traffic interception, which consists in intercepting data sent from the control point to the UAV, and going in the opposite direction both on radio channels and on satellite channels.
3. Simulating and spoofing GPS signals by sending false signals to disrupt the UAV's navigation system in order to guide the UAV along a path where it will crash, or be intercepted and planted in a given area.

Currently, cyber attacks using software-defined radio technologies are considered the most promising. These attacks have a special place, because the development of software-defined radio technologies makes it possible to obtain tools available to a wide range of people that allow the following deliberate actions to be carried out.

1. Read and transmit signals at any frequency from 100 MHz to 1 GHz, thanks to the availability of universal radio transmitters. We are talking about the vulnerability of almost all frequency bands that are used for data transmission (4G, Wi-Fi, FM, GPS). Such radio transmitters can be tuned to any frequency, instantly record and reproduce the signal. By connecting this transmitter to a computer, it is theoretically possible to programmatically emulate a modem of any standard.

2. Using a universal transmitter to intercept and decrypt radio signals, including for "traffic injection". Any unsecured radio Protocol can be compromised. Theoretically, this way you can intercept the management of UAVs.
3. Extraction of secret encryption keys for hardware and software when conducting an economical electromagnetic attack with the measurement of side electromagnetic radiation within a few seconds. Such attacks can be carried out using available hardware: a consumer radio receiver or a USB module with a software-defined radio system (Software-defined radio).

The main directions of countering cyber threats OEE UAVs can be formulated as follows:

- analysis and testing of information managers components of OEE to identify vulnerabilities and their subsequent classification by the degree of possible threats;
- development of a secure info communication system infrastructure for specialized management systems;
- development of methods for finding vulnerabilities in software providing information management OEE systems and nodes;
- creating a certification system and standard stands special functional and load testing software;
- improving the regulatory framework for ensuring information security in information management systems;
- development of individual tools for each UAV model, using blocking templates to protect against attacks via the data communication bus and installation hardware hidden bookmarks on the bus, or reprogramming the regular unit management.

These and other measures will reduce the risk of cyber threats, increase the level of UAV flight safety and efficiency of performing their tasks.

LIST OF REFERENCES

1. http://militaryreview.ru/aktualnye-voprosy-obespecheniya-kiberbezopasnosti-bespilotnyx-letatelnyx-apparatov.html
2. https://cyberleninka.ru/article/n/kiberneticheskaya-bezopasnost-bespilotnogo-transporta
3. https://topwar.ru/99011-tehnologii-borby-s-bespilotnikami-chast-1.html
4. https://topwar.ru/99011-tehnologii-borby-s-bespilotnikami-chast-1

D.D. Schirokov, N.I. Nepluev, A.V. Lavruhina

TASKS OF CREATING A UNIFIED INFORMATION SPACE OF THE ARMED FORCES

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia

Keywords: Unified Information Space, cloud system, JEDI, PaaS platform, cloud provider, network-centric systems, big data, military cloud.

Research on the development and implementation of technologies that ensure the transition from the formation of disparate information resources to the creation and development of unified information spaces aimed at solving various tasks in the interests of defense and security is carried out in all states with developed Armed Forces.Accordingly, it is necessary to create a single

information space in the Armed Forces of the Russian Federation, which will ensure the interaction of all levels of management of combat units and units of the Armed Forces.

Currently, one of the decisive factors that has a significant impact on the defense capability of any country is the level of development and application of information technologies, including those related to the formation and development of information spaces. In the leading countries of the world, work is being carried out on the development and implementation of technologies that ensure the transition from the formation of disparate information resources to the creation and development of unified information spaces aimed at solving various tasks.

The Unified Information Space (UIP) is a distributed data warehouse, implemented on modern computer technologies and covering both information sources and possible consumers of information, created in the interests of state power and military administration.

UIP s in the interests of defense and security are created in all States that have developed Armed Forces (AF). The base of the UIP of the Armed Forces should be cloud computing platforms using artificial intelligence (a single cloud system, “military cloud”) that provide access to the information contained in them to authorized users from anywhere in the world using gigabit data transfer speeds with guaranteed security.

Currently, the United States is developing such a cloud computing platform, called the "Joint Enterprise Defense Infrastructure (JEDI)" [1]. JEDI will provide innovations for the digital battlefield, including secure data storage, fast processing, and high – speed access to information of various levels of secrecy. This approach, using the latest technologies, will allow you to get SaaS software, IaaS infrastructure and PaaS platform through the cloud, that is, they will combine three categories of services: SaaS-Software as a Service-applications running in the cloud, accessed by end users via the Internet, including through email and office applications used by the client, and the basic application settings are managed by the provider.

IaaS – Infrastructure as a Service – computing infrastructure in the form of a service, including servers, data storage, networks, and operating systems, which is provided to customers to deploy and run their own software solutions, and resources are purchased from third-party providers. IaaS involves receiving services using a public or private cloud, as well as a hybrid cloud.

PaaS – Platform as a Service – a set of tools and services that facilitate the development and deployment of cloud applications. PaaS is a model for providing cloud computing, in which the consumer gets access to the use of information technology platforms: operating systems, database management systems, linking software, development and testing tools hosted by a cloud provider. PaaS, like IaaS, includes infrastructure servers, storage, and networks, but also middleware, development tools, analytical tools, database management systems, and other capabilities. PaaS is designed to support the full lifecycle of web applications, with the applications managed by the client and the operating system managed by the provider.

The positive characteristics of the introduction and development of information and telecommunications technologies in the Armed Forces of the Russian Federation, in general, and cloud technologies, in particular, were presented in the report of the Minister of Defense of the Russian Federation, General of the Army S. K. Shoigu, which does not lose relevance over time in its information and policy content, at an expanded meeting of the Board of the Ministry of Defense of the Russian Federation in December 2016.

As follows from the report, to solve the tasks set, it is necessary to create a single information space in the Armed Forces of the Russian Federation (UIP of the AF), which will ensure the interaction of all levels of management of combat units and divisions of the AF, parts of logistics, research institutions and industrial enterprises of the military-industrial complex in any situation conditions based on the concepts of big data and network-centric management.

Network-centric management of armed forces facilities is characterized by the principles of openness, self-organization, a weak hierarchy in the decision-making circuit and the ability to

generate goals within itself [2] and is based on the principle of building weapons systems, based on comprehensive computerization of forces and means of armed struggle at all levels: tactical, operational, and strategic.

The technical support of network-centric management involves the creation of highly effective network-centric systems (NCS) that guarantee high-speed and covert exchange of information in all conditions of the situation and the mastery of the skills of using NCS in real-time warfare by officials of all levels of combat management.

The implementation of network-centric technologies requires processing large amounts of data based on the big data technology package. In the professional PG community, the term "big data" is similar to the popular metaphors "big earth", "big oil", etc. and is considered as the second most important direction in the information technology infrastructure (after energy saving and monitoring).

Paragraph 20 of the Strategy for Scientific and Technological Development of the Russian Federation, approved by Presidential Decree No. 642 of December 1, 2016, states, in particular (subparagraph a), that in the next 10 to 15 years, the priorities of scientific and technological development of the Russian Federation should be those areas that will ensure the creation of systems for processing large amounts of data.

The application capabilities of the Big Data technology package will be provided to the highest degree by the creation and development of the "military information cloud" of the Armed Forces of the Russian Federation (RF AF).

This leads to the conclusion that the effective functioning of the EIP of the Armed Forces requires the formation of a perfect military information cloud. To form a military information cloud, first of all, it is necessary to solve the following tasks:

- development of special cloud services and technologies;
- creation and development of data centers;
- development of high-performance computing;
- creation of a special telecommunications infrastructure;
- development of artificial intelligence;
- creation of network-centric networks and technologies;
- ensuring the protection of information in information and communication networks.

In addition, it is necessary to develop a training system for the operation of the UIP of the Armed Forces.

To this end, it is necessary to create completely Russian clouds and a closed military cloud storage for official and secret information – "ultra-secure iCloud". The military Internet, which is not connected to the usual one, is connected to a network of geographically distributed disaster-resistant information processing centers, and the military cloud functions only in a closed data transmission segment. Servers for data storage are located in Russia and do not depend on foreign technologies. Access to the information in the digital storage is possible only through personal computers that are certified by the state secret protection services.

Thus, the creation of a single information space of the Armed Forces will improve the quality of information support for management processes in various areas of military construction by providing timely, up-to-date and reliable information.

LIST OF REFERENCES

1. Principles and directions of the development of a single information space in the interests of military construction. Armament and Economy No. 1 (5) / 2009 Military-technical policy. http://militera.lib.ru/periodic/0/v/vooruzhenie-i-ekonomika/vooruzhenie-i-ekonomika_2009-01.pdf

2. Opportunities of cloud technologies in the military sphere. https://russiandrone.ru/publications/vozmozhnosti-oblachnykh-tekhnologiy-v-voennoy-sfere/
3. Unified cloud for military information. https://nvo.ng.ru/realty/2019-10-31/1_1068_information.html
4. Cloud Computing http://ru.wikipedia.org

A.D. Kalmychin, A.S. Meleshin, L.P. Koroleva

RADIO COMMUNICATION SYSTEMS WITH PROGRAMMABLE PARAMETERS IN AVIONICS

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia

Keywords: software-defined radio systems, programmable logic integrated circuits, field-programmable gate array, transport layer protocol, software communication architecture, unified tactical radio system. unified Tactical Radio System

The development of digital broadband data transmission systems and computer technologies has led to the emergence of a new class of radio systems — software-defined radio systems. From the point of view of avionics, the most promising is the technical implementation of software-defined radio systems based on programmable logic integrated circuits. Radio communication systems with programmable parameters are considered for their use in avionics

A software-defined radio system (software-defined radio, SDR [1] includes a central processor that controls the radio transmitting and receiving units. The radio transmitting and receiving units use a technology that allows the software to set or change the operating radio frequency parameters, including, in particular, the operating frequency range, the type of modulation, the output power, with the exception of changing the operating parameters used in the normal pre-defined work with the pre-settings of a particular specification or system.

In software-defined radio systems, the radio transmitting unit has a switching processor, the main task of which is to pack the bits of transmitted data into modulation symbols and generate a modulating signal based on them. Then the modulating signal is transmitted to the digital-to-analog converter (DAC), and in the digital code it is further transmitted to the radio interface [2].

The radio receiving unit contains an analog-to-digital converter (ADC), a switching processor that demodulates the signal and converts the demodulated signals into data bits.

From the point of view of avionics [2,3], the most promising is the technical implementation of software-defined radio systems based on programmable logic integrated circuits (in the English version - field-programmable gate array (FPGA), which allows you to create on-board radio channel equipment in a single-crystal design with minimal weight characteristics.

Radio interfaces, ADCs and DACs are implemented as independent integrated devices.

FPGA technology allows you to create a large number of different programmable processing units on a single chip, which ultimately leads to the possibility of simultaneous operation of aircraft avionics on many radio channels. The use of FPGAs provides high flexibility of data transmission over radio channels, since they can be reprogrammed in whole or in part at any time.

The organization of data transmission using software-defined radio systems is based on data exchange protocols between the nodes of the system, capable of transmitting digital signals in real time and with the transparency of network traffic. An important requirement for such protocols is their high flexibility, which should allow processing radio data without loading communication processors and other system elements with unnecessary calculations. Exchange protocols should also provide for the transmission of packets of signal information about the parameters of the radio signal, such as the channel number, transmission or reception time, communication frequency, geodetic coordinates of objects.

The use of transport layer protocols is determined by the architecture of the system and the type of tasks to be solved. The conversion of protocols from internal to external and vice versa should be performed using tables, such as ARP tables in Ethernet networks and programmable internal and external address mapping tables. ARP (Address Resolution Protocol) — a protocol for determining the correspondence between the logical address of the network layer (IP) and the physical address of the device (MAC). The communication between the two devices in the network itself takes place at the channel level (where the mac addresses belong). The ARP protocol has a buffer where the IP-address — MAC-address pair is stored. This information is entered in the so-called ARP table. It serves to ensure that devices do not spend extra traffic on the next identification — this reduces precious milliseconds during data transmission.

An important task for software-defined radio systems is the unification of interfaces and the development of portable and extensible software. To unify the interfaces of software components of software-defined radio systems, a specification called “Software Communication Architecture” (SCA) has been developed, which defines the architectural framework of distributed switching elements of SDR systems. The SCA architecture defines not only how to broadcast a radio signal through a switching network and remotely configure SDR systems, but also how to manage hardware and software.

The first SDR systems can be called Internet telephony networks (Voice over IP, VoIP), which are considered as a prototype of software-defined radio systems.

In the United States, in the interests of the Department of Defense, a unified Tactical Radio System (JTRS) is being created based on the principles and technologies of software-defined radio systems.

JTRS is built on the basis of the open SCA architecture, which defines the structure of applications and communication protocols (waveforms). The compatibility of various radio means is ensured due to the fact that the software components of communication protocols are easily transferred to any radio means that support the SCA architecture. This approach assumes the existence of a network interface and software interface at each terminal of the system, whether it is radio or data transmission systems tactical and higher levels of command and control, avionics modern aircraft, modems, unmanned aerial vehicles, etc.

Thus, the creation of domestic software-defined radio will allow you to proceed to the formation of efficient and secure radio on-air network control, communications, and data transmission.

LIST OF REFERENCES

1. Distributed software-defined radio systems. Sorokhtin E. M., Mineev S. A. Vestnik Nizhegorodskogo universiteta im. n.I. Lobachevsky, 2010, no. 5 (2) p / 383-388 eugene@nifti.unn.ru
2. Basics of software-configurable radio. Galkin V. A.-M.: Hotline-Telecom, 2013. - 372 p. - ISBN 978-5-9912-0305-0.
3. Aviation systems and radio communication complexes. A textbook for students and cadets of Air Force universities. Ed. by V. I. Tikhonov-M. Ed.VVIA im. prof. N. E., Zhukovsky, 2007 - 784 p.

4. Kuticov P.A., Meleshin A.S., Koroleva L.P. Directions of development of avionics radiocommunication in the interests of improving the quality air traffic control. Proceedings of the North Caucasus branch of the Moscow technical University of communications and Informatics. Rostovon-Don.: SCF MTUCI University. – 2018-pp 270-272 .

A.L. Papyan, N.I. Nepluev, A.V. Lavruhina

RADIOPHOTONICS AS THE MAIN DIRECTION OF AVIONICS DEVELOPMENT

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia

Keywords: radio electronics, radiophotonic technologies, quantum mechanics, photon, extended bandwidth, electromagnetic compatibility, phase stability, radar systems, nanophotonic, nanophoton structures, radio-optical phased array.

In recent decades, a new direction in radio electronics has been formed in the field of ultra-wideband transmission systems - radiophotonic technologies, in which the process of replacing "electronic" systems with "photonic" ones takes place.

The advantages of radiophotonics are based on the fundamental properties of quantum mechanics, which consist in the fact that the photon, the information carrier, is a massless elementary particle that can exist only moving at the speed of light and having an electric charge equal to zero and the properties of the propagation medium (quartz optical fiber). The basic direction of the development of radiophotonics is nanophotonics. The advantages of radiophotonics based on the use of nanophoton structures are realized when creating an active radio-optical phased array antenna.

In recent decades, a new direction in radio electronics has been formed in the field of ultra-wideband transmission systems - radiophotonic technologies, in which the process of replacing "electronic" systems with "photonic" ones takes place [1].

The advantages of radiophotonics are based on the fundamental properties of quantum mechanics, which consist in the fact that the photon, the information carrier, is a massless elementary particle that can exist only moving at the speed of light and having an electric charge equal to zero and the properties of the propagation medium (quartz optical fiber).

This provides [2]:

- increased performance (up to tens of femtoseconds);
- extended bandwidth (up to the terahertz range);
- low transmission losses (<0.2 dB / km) and their independence from the frequency of modulation in the radio frequency range;
- much better weight and size characteristics (fiber cable: weight 1.7 kg/km, diameter 250 microns; coaxial cable: weight 560 kg/km, diameter 10 mm);
- insensitivity to electromagnetic interference (dielectric): improving electromagnetic compatibility within the system; increasing the imitability of the equipment;
- significantly better phase-temperature characteristics: phase stability and the possibility of coherent signal reception and processing.

Radiophotonics, based on the interaction of optical and microwave signals and using the conversion of a signal from the microwave radiation range to the optical range, allows you to create electronic devices with parameters that are unattainable by traditional means [3]. The optical range is quite wide – it includes all types of radiation, including laser, terahertz range. This is a very high frequency, the width of which can reach several hundred gigahertz when modulated. This bandwidth is incomparably greater than what can be achieved on existing systems today.

Radiophotonics emerged from the merger of radio electronics, integrated and wave optics, microwave optoelectronics and a number of other branches of science and industrial production and allows us to create fundamentally new components for avionics, such as:

- ultra-high-frequency optoelectronics;
- ultra-wideband radio communication;
- ultra-wideband radar;
- sources of coherent optical radiation (lasers);
- radiophoton ADC and DAC;
- ultra-wideband analog processors microwave frequency range;
- optoelectronic ultra-high frequency generators;
- electro-optical modulators based on thin films of molecular crystals;
- integrated electro-optical modulators;
- AFAR radar systems;
- multifunctional receiving tracts;
- fiber-optic delay lines;
- planar and fiber optic waveguides;
- passive component base.

As a result, radiophotonic systems, in comparison with electronic ones, have a much greater range and transmission speed, a signal bandwidth, and, which is especially necessary for military avionics, are not subject to external electromagnetic influences.

The main advantages of radio frequency devices [4]:

- ultra-low optical fiber loss and dispersion (less than 0.2 dB / km at 1550 nm, optical carrier ~200 THz);
- ultra-wideband (available optical fiber frequency band ~50 Hz, the frequency band of modern photodiodes and modulators up to 100 GHz and higher);
- low level of phase noise (the process of direct optical detection using a photodiode is not susceptible to the phase of optical radiation and phase noise of the optical carrier);
- high phase stability of the optical fiber;
- immunity to electromagnetic interference;
- no mutual interference;
- galvanic isolation of photonic circuits;
- low weight and size of the optical fiber;
- mechanical flexibility of the optical fiber, which facilitates the design.

The basic direction of the development of radiophotonics is nanophotonics.

Nanophotonics studies the interaction of optical waves with matter, which takes place on scales of the order of the wavelength or smaller, where the physical, chemical, and whether the structural properties of artificial or natural matter nanostructures directionally control optical radiation cannot propagate. Photonic crystal modulators and photocrystalline fiber are currently being developed and used on the basis of photonic crystals. Nanophotonic devices are not only significantly superior to their electronic counterparts, but also allow us to successfully solve problems related to heat generation and power supply, which is essential for avionics.

The main components of nanophotonics are dielectrics-optical or semiconductor nanoscale structures with periodically alternating regions with different material properties. Such materials are called photonic crystals or materials with " photonic bandgap (PBG)". In them, due to in-phase layer-by-layer reflection (Bragg reflection), "forbidden zones " arise, i.e., frequency ranges of electromagnetic, in particular optical radiation, cannot propagate. Photonic crystal modulators and photocrystalline fiber are currently being developed and used on the basis of photonic crystals [5].

Nanophotonic structures are the basis of modern quantum devices - semiconductor lasers and photodetectors. At present, new nanophotonic structures – monatomic graphite films (graphenes), which have many very valuable physical properties and allow solving the problems of miniaturization of many radio-electronic systems, have been obtained and studied.

The advantages of radiophotonics based on the use of nanophoton structures are realized when creating an active radio-optical phased array (ROFAR) [6]. The performance characteristics of the AFAR radar will significantly exceed the capabilities of modern electronic radars. Radar stations operating on the principles of radio-optical phased array antennas will provide output not typical for the current radar image in the form of dots on the screen, but a video image familiar to human vision, as if we could see an object at a distance of hundreds of kilometers, zoom in, view it from all sides, or even look inside. In this case, everything happens in real time, since the speed of the photon is equal to the speed of light.

Unlike the headlights of traditional radars, it will not be possible to drown out the ROFAR with traditional EW means physically. The dynamic range of a photonic crystal is approximately 200 dB. A modern radio-electronic receiver, for comparison, has a range of 40-60 dB, and we use modern electronic warfare systems to provide a signal to the input of the radio receiver-70-80 dB relative to its threshold sensitivity. Thus, the device that should receive the signal is brought out of the operational state. Even after removing the interference, there are still processes inside it that do not allow it to work. But there is simply no power source on Earth to supply a signal with a power exceeding 200 dB, so this logic simply does not work in the case of ROFAR.

Thus, radiophotonics will become one of the main directions of the development of avionics of the new, sixth generation of military aviation, so it is very important for our country today to focus on the implementation of projects in this area and the appropriate training of technical specialists.

LIST OF REFERENCES

1. We are on the threshold of a new technological order. The magazine "Wings of the Motherland" in social networks. https://aftershock.news/
2. Why do we need to go into radiophotonics? http://radiofotonika.ru/
3. Introduction to Radiophotonics. http://radiofotonika.ru/books/
4. Photonic radars, radiophotonics, and stealth technologies.https://naukatehnika. com/fotonnye-radary-fotonika-stels-texnologii.html naukatehnika.com.
5. Goals and materials/nanophotonics devices. Promising areas of development.https://intellect.icu/nanofotonika-792.
6. Systems and devices based on radiophotonics in relation to radar. Journal of radio electronics, issn 1684-1719, n6, 2017.

D.I. Zacepilon, A.S. Meleshin, N.O. Svetlichnaya

ANALYSIS OF THE CHARACTERISTICS OF UAV CONTROL SYSTEMS IN THE INTERESTS OF IMPROVING ELECTRONIC WARFARE

Federal state military professional educational institution "183 training center" Ministry of Defense of the Russian Federation, Rostov-on-Don, Russia
North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

Keywords: unmanned aerial vehicle (UAV), kamikaze drones, control channel, electronic warfare, ground control point, radio-electronic environment, pseudo-random radio frequency hopping.

One of the main applications of UAVs is military operations. UAVs are currently considered as promising weapons for reconnaissance, bombing, and air combat. The creation of this type of combat aircraft requires the appropriate development of methods of countering and combating it. Discussions of methods of countering equipment, an alternative to destruction is very often proposed – the suppression of UAV radio-electronic system. The generalized parameters and characteristics typical for the products of the majority of foreign UAV manufacturers are analyzed

Currently, unmanned aerial vehicles (UAVs) are becoming increasingly common. This type of aircraft has proven itself as a reliable and effective means of conducting reconnaissance, striking enemy targets and performing a number of other tasks. At the same time, one of the most important priorities in this regard was the comprehensive improvement of such a class of weapons as barrage ammunition, also commonly known as kamikaze drones [1].

According to some estimates, only in the United States over the past 15 years, more than 30 thousand UAVs of various classes and types have been produced, most of which are used by the Ministry of Defense and special services. UAVs have been actively used in all the notable armed conflicts of recent times. The successful detection and destruction of targets, repeatedly performed by UAVs in Iraq, Afghanistan and Nagorno-Karabakh, clearly demonstrates the capabilities of such aircraft.

The creation of this type of combat aircraft requires the appropriate development of methods of countering and combating it.

The first logical way to get rid of an enemy UAV is to fire it. Any flying equipment can be shot down by conducting a successful attack on it by means of air defense.

The destruction of UAVs is associated with a number of difficulties in detecting and hitting the target. Therefore, in discussions of methods of countering such equipment, an alternative to destruction is very often proposed – the suppression of UAV radio-electronic systems (RES) [2].

Some modern UAVs have the ability to perform certain tasks independently, but almost all such equipment is controlled by the operator, and commands are transmitted via radio channels. Thus, the suppression of the control channel of electronic warfare (EW) can, at least, interfere with the task, and at most take control of the UAV itself, followed by the landing of the UAV in a given area. This method of dealing with UAVs in the present and future time in pre-war conditions and military conflicts is the most promising.

Solving the problems of electronic counteraction requires knowledge of the specifics, structure and features of the standard protocols (modes) used in the UAV control channels [3,4]. This is the basis for the development of solutions and counteraction technologies.

Currently, in UAVs produced by foreign manufacturers, the most commonly used noise-resistant modes of pseudo-random radio frequency hopping (PRFH) in the channels of ground control points (GCP) with UAVs.

Despite the considerable variety of types, models, and manufacturers of UAVs (using PRFH in control channels), the analysis of open sources allows us to identify generalized parameters and characteristics typical of the products of most foreign manufacturers:

- the maximum "legal" power of the emitted electromagnetic signal (in the control channel) – 100 MW;
- typical (priority) radio frequency ranges – 2.4 and 5.8 GHz;
- speed range of PRFH modes - 350-500 jumps /sec (max. 2 900 jumps /sec);
- types of digital modulation –FSK2 (less commonly-PSK2 (A/V) and OFDM);
- transmission pulse duration) - 500 ms – 2.5 ms;
- frequency bandwidth of the elementary pulse - 300 kHz – 2 MHz;
- the transmission rate of elementary pulses –1 000 – 2 000 kbod;
- Bandwidth of the " PRFH grid"» –about 80 MHz;
- number of channels of the " PRFH grid» – up to 40.

The specifics and features of the control channels of modern UAVs (the PRFH mode) dictate the main requirements for counteraction systems that implement passive (radio-radio engineering) methods for detecting signals of the GCP (control channel).

The main problems associated with the quality of the tasks of bearing and identification are related to two key parameters of the UAV control channel signals – the low power of the electromagnetic signal of the control channel (up to 100 MW) and the use of the fast PPRF mode (from 300 jumps /sec).

At the same time, it should be taken into account that critical violations of the UAV control function occur only in the case of suppression of almost 100% of the channels of the "PPRF grid". In the case of not suppressing even 1-2 channels, the UAV operator still has the ability to carry out stable control of the aircraft.

The presented data allow us to formulate the main requirements for counteraction systems that perform the functions of detecting signals of UAV control channels with PRFH:

- the operating frequency range used (at least 2.4 and 5.8 GHz, taking into account the possible use of VHF-MICROWAVE radio channels in the UAV equipment);
- the ability to detect signals of extremely low power RES (level 100 MW) –
- increased requirements for the "sensitivity" parameter of the detection system;
- the ability to detect signals in difficult conditions of the radio-electronic environment in the presence of a large number of interference signals – increased requirements for the "selectivity" parameter of the detection system;
- the ability to detect short-term, pulsed signals of "fast PRFH " - increased requirements for the "speed" parameter of the detection system;
- the ability to detect short-term, pulsed "fast PRFH " signals distributed in a wide (at least 80 MHz) frequency band;
- increased requirements for the "simultaneous analysis band" parameter of the detection system.

At the same time, it is necessary to take into account the additional difficulties associated with solving the problems of detection and identification in real conditions of the radio-electronic environment.

The task of detecting the signals of the UAV control channel with PRFH is the first, necessary step in the algorithm for using electronic systems to counter UAVs. For radio receiving, radio monitoring and radio measuring equipment of the primary or middle class, the detection (bearing) of the very fact of the operation of the "fast PRFH " RES and its identification is an extremely difficult task.

The identification task is significantly complicated in the conditions of a complex radio-electronic environment and the presence of a large number of signals of extraneous RES. Without solving the problem of high-quality identification, the system can almost continuously respond to

numerous signals of extraneous RES (constant false positives), which will significantly reduce the possibility of its practical application in real-world conditions. Lowering the trigger threshold (in order to minimize false alarms) is fraught with the risk of missing the signals of a dangerous object (not detecting the fact of potentially dangerous use of UAVs).

Thus, we can conclude that unmanned aerial vehicles of various classes and types are not a unique means of solving the tasks set, which cannot be countered. The enemy UAV can be destroyed, you can prevent it from completing its task, or even make it your trophy. Of course, all methods of counteraction require specialized electronic warfare equipment to combat UAVs.

LIST OF REFERENCES

1. The surge of a new military revolution. Kamikaze drones will ensure a quick victory over the enemy. https://nvo.ng.ru/armament/2021-03-11/1_1132_drones.html
2. How to counteract a drone? https://topwar.ru/69167-kak-protivodeystvovat-bespilotniku.ht
3. F.V. Madinsky, A.S. Meleshin, N.O. Svetlichnaya Structure of aviation radio communication and direction of its improvement. Proceedings of the North Caucasus branch of the Moscow technical University of communications and Informatics. Rostovon-Don.: SCF MTUCI University. – 2019. – v 2 – pp. 224-228
4. Organization of aviation radio communication of a group of unmanned aerial vehicles based on networkcentric self-organizing networks Proceedings of the North Caucasus branch of the Moscow technical University of communications and Informatics. Rostovon-Don.: SCF MTUCI University. – 2020. – pp. 528-530.

N.O. Svetlichnaya, B.B. Konkin,
Ya.B. Konstantinova, L.V. Koldynskaya, L.A. Gayevskaia

FEATURES OF THE IMPLEMENTATION OF DISTANCE LEARNING IN THE UNIVERSITY

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

Keywords: e-learning, effectiveness of the educational process, psychological problems, technical skills.

The article considers relevance of distance learning, as well as its advantages and problems that arise for students and teachers in the implementation of the educational process in this form. Some ways of solving the described problems are given.

Distance learning is the process of acquiring knowledge remotely over the Internet through video calls, online courses or mobile applications, when the teacher and student are physically located in different places.

The e-learning market is growing as online learning is cost-effective, convenient and beneficial to people. One of main advantages of distance learning is its affordability to everyone. Remote study is an ideal solution for those students who, for various reasons, cannot visit the university, as well as employees who want to improve their qualifications. The opportunity to gain knowledge without leaving home makes the learning process comfortable, flexible and less tiring,

for example, because one does not need to spend time getting to a university or overcoming traffic jams. Besides, distance learning provides an opportunity to master new skills.

In today's world, online learning is becoming not just a convenience, but a necessity. Due to the COVID-19 pandemic, distance learning is becoming more relevant than ever and is being introduced in all educational institutions.

However, in practice, both students and teachers face serious difficulties that hinder successful learning. The following problems are highlighted:

– difficulty in adapting to the online format;

Moving from traditional classroom learning to online learning makes the learning process completely different. Virtual classes encourage students to discuss, work with a personal account and materials in various multimedia formats. It can be difficult for students to adapt to these changes. Teachers also have to spend more time to prepare for classes in an online format, as well as to check the student papers.

– insufficient computer literacy;

The low level of computer literacy is a serious problem for both students and teachers. Both participants in the educational process may face a lack of understanding of distance learning tools, such as educational online platforms, video conferencing systems, various applications related to communication and viewing of educational materials.

– technical difficulties;

Technical problems such as compatibility of educational platforms with operating systems, browsers or smartphones, low speed of the Internet connection can lead to missing online classes or difficulties in downloading lessons in video format. All this reduces the involvement of students in the learning process.

– ignorance of the basics of time management;

Distance education places higher demands on discipline and self-organization. Mismanagement of time can lead to serious backlog of the curriculum and cause severe stress.

– weak self-motivation;

Lack of motivation is a common problem for all types of learners. The online format requires a lot of discipline and dedication to complete assignments on your own, stay motivated, and make progress.

– lack of social interaction;

The transition to distance learning deprives students of the opportunity to communicate with groupmates. Lack of personal contact with friends and the teacher makes the student feel isolated, which is a strong psychological factor that negatively affects motivation and academic performance.

Thus, it becomes obvious that distance learning is very different from the traditional one and generates certain problems. To overcome them, both students and teachers need to stop resisting new things, change their attitude towards the online format and acquire additional technical skills. The experience of the teachers of NCB MTUCI proves the necessity and effectiveness of the following solutions, applicable to the listed problems. Students are required to strengthen discipline and self-organization skills through rational planning of the working day and adherence to the plan. Teachers are encouraged to maintain enthusiasm, maintain interest in the subject by arranging emotional and engaging lectures, discussions, linking the material of the classes with real life. At the same time, teachers are supposed to set concrete and achievable goals for students. For example, to maintain a reporting form of lectures and practical classes, as a result of which students form a micro-summary of the lesson and can demonstrate it to the teacher on demand. Educators use praise and rewards as motivation: positive responses are individually emailed using fun videos, GIFs, and images. A group chat or blog to talk and discuss specific topics can help students overcome feelings of isolation.

Obviously, distance learning makes it possible to acquire new skills, become flexible, master new standards, and, with certain efforts of all participants in educational activities, maintain the proper level of effectiveness of the educational process.

LIST OF REFERENCES

1. Студенты назвали основные проблемы онлайн-обучения. Им не хватает общения с преподавателем и подводит техника. https://www.rbc.ru/society/19/08/2020/5f3bbdae9a7947d167de1a41
2. Проблемы, возникающие при переходе ВУЗов на дистанционное обучение. Смолянкин Н.Н. Быков А.А. Киселева О.М.Современные проблемы науки и образования. – 2021. – № 5. https://science-education.ru/ru/article/view?id=31099

A.A. Borodina, Ya.B. Konstantinova, N.O. Svetlichnaya

BASIC METHODS OF PHOTOPOLYMER PRINTING

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

Keywords: photopolymer printing, 3-D printer, stereolithography, composite materials.

The work focuses on the physical foundations of photopolymer printing and photopolymer resins. A qualitative comparison of modern 3-D printing technologies is provided. The paper considers some prospects for the application of 3-D-printing technology in various branches of science and technology.

3D printers can be classified not only by the printing technologies, but also by the used consumables. Consider devices that use photopolymer resins to build models.

Photopolymer resins are liquid polymers that harden when exposed to light. Typically, such materials are sensitive to the ultraviolet range, which determines the design of photopolymer printers. One of the most common structural elements is a transparent colored cover or a housing made of a material that filters ultraviolet radiation. This is done both to protect the user's eyes and to protect the consumable inside the printer from sunlight and background lighting.

The physical properties of resins after polymerization vary widely. Both solid and flexible options are available, transparent and matte. A wide variety of colors are also available. Resin consistency and exposure times also vary, so the range of compatible materials should also be considered when choosing a printer. The last aspect to consider when choosing a material is its toxicity. There are both fairly toxic options and biologically safe ones.

The cost of consumables for photopolymer printing is quite high. The plants themselves are already available at a reasonable price, but inexpensive photopolymer resins are very rare. We hope that the proliferation of inexpensive photopolymer printers will lead to increased production of consumables and lower prices.

The firstborn of photopolymer printing and modern 3D printing in general is laser stereolithography (SLA). The technology was developed in 1984 by Charles Hall, who later founded 3D Systems. SLA printers use laser emitters to cure photopolymer consumable material. A typical SLA printer consists of a drawer with consumables seated under a build platform, driven vertically by a lift and lower mechanism. Above the cuvette is a laser emitter and a mirror system for deflecting the laser beam. During the printing process, the platform is immersed in the

consumable material to the thickness of one layer of the digital model. Since photopolymer resins can be quite thick, a leveling mechanism is often used to speed up the process.

After alignment, the process of material exposure begins. Illumination is produced by laser irradiation. Most photopolymer resins are designed to polymerize when exposed to ultraviolet light, which determines the choice of the frequency of laser radiation. The movement of the beam along the X and Y axes is determined by the operation of the deflecting mirrors. After finishing drawing a layer, the platform is immersed in the material to the thickness of one more layer, and the process is repeated with drawing the next layer of the digital model.

SLA printing takes quite a long time, and printers using this method tend to have relatively small build areas.

This is due to the high cost of laser emitters: printing large objects with one laser will take too long, and the installation of additional emitters and mirrors will complicate the design, increase the size of the installation and significantly raise the price.

Despite the success of this technology, projection stereolithography (DLP) is considered a more promising, albeit very similar method. A close relative of laser stereolithography, this technique uses digital LED projectors instead of mirror-deflection lasers. The method became popular thanks to the development of technology for the production of low-cost, high-resolution digital projectors by Texas Instruments. Illumination of layers is performed using a digital projector, which illuminates the templates of a whole layer, which distinguishes this method from SLA, where the "picture" is progressively drawn with the help of an ultraviolet laser. Simultaneous illumination of an entire layer using projectors can significantly speed up the printing process, even in comparison with SLA printers with a high beam travel speed. In addition, such printers are less sensitive to harsh physical impact due to the lack of delicate mirror systems. The absence of mechanical mirror systems allows for increased accuracy. Finally, the cost of projectors sets them apart from laser systems. The projection size can be quite significant.

An interesting feature of DLP printers is the ability to "reverse" or "reverse print". In this case, the projector is installed under a transparent (the choice of material is important for transparency in relation to ultraviolet light) cuvette, and the platform does not sink into the material, but gradually rises, pulling out the layers of the exposed polymer. This approach eliminates the alignment mechanism and achieves even higher Z-resolution than SLA printers.

In addition, the size of the models in height is not limited by the depth of the cuvette, which favorably affects the dimensions of the printer and the possibility of increasing the build area.

Another modern 3D printing technology is multi-jet printing. The very principle of multi-jet polymer printing was developed by the Israelite company Objet, which eventually became one of the divisions of Stratasys. The construction of models is carried out by spraying a photopolymer using linear arrays consisting of many nozzles. The applied layer is immediately illuminated with ultraviolet lamps - as a rule, two processes occur simultaneously. By the time the array reaches the end of the working chamber, the previously applied material is hard enough to print a new layer.

This approach allows you to achieve a very high print speed, but it is characterized by a high design complexity, which negatively affects the cost of such installations and limits their distribution to professional use.

One of the advantages of the technology is the ability to create composite structures from photopolymer resins with different physical characteristics.

Thus, it is possible to create models with easily removable supports, the use of multiple colors and the parallel use of flexible and solid materials within the same model.

Recently, there has been a fashion for hand-held printing devices called 3D pens. At the moment, there are two main options for such devices: drip-jet pens, called BioPen which are used in the development of new methods of treating damaged tissues, and developments in 3D painting with photopolymer resins.

In recent years, 3D printing has become available to the mass consumer: the prices of printers have dropped significantly, and their use has become more convenient. Photopolymer 3D

printers print detailed models with high precision and resolution. The number of users is growing. This is facilitated by the availability of ready-made files for 3D printing and the availability of software for creating models.

3D printing is already becoming a standard solution in such industries as medicine, jewelry, orthopedics, construction, mechanical engineering, and aerospace. This technology has a great importance for electronics and radio electronics, as it is an increasingly popular method of creating printed circuit boards, by applying conductive and dielectric tracks on the surface of various materials.

LIST OF REFERENCES

1. 3D-печать в радиоэлектронике
   https://habr.com/en/company/top3dshop/blog/399179/
2. Обзор применения 3D-печати в электронике https://3d_print.jofo.me/1791842.html
3. Самые распространенные проблемы фотополимерной печати по версии HARZ Labs. 26.10.2020, 3Dtoday.ru https://3dtoday.ru/blogs/harz-labs/samye-rasprostranennye-problemy-fotopolimernoi-pecati-po-versii-harz-labs
4. Stereolithography / 3D Printing / Additive Fabrication/ Additive Manufacturing
5. https://photopolymer.com/3d-printing
   Formlabs Announces Acquisition of Spectra and Investment in ISO 13485 Biocompatible Material Manufacturing. Nov. 12, 2019 https://formlabs.com/company/press/formlabs-aquisition-spectra-biocompatible-manufacturing/