Научно-технический журнал

Информационные системы и технологии

№ 3 (95) май-июнь 2016

Издается с 2002 года. Выходит 6 раз в год

Учредитель – федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс» (Госуниверситет – УНПК)

Сдано в набор 15.04.2016 г.
Подписано в печать 26.04.2016 г.
Дата выхода в свет 16.05.2016 г.
Формат 60x88 1/8.
Усл. печ. л. 7,5. Тираж 300 экз.
Цена свободная. Заказ № 81/16п2
Отпечатано с готового оригинал-макета на полиграфической базе ФГБОУ ВПО «Госуниверситет - УНПК» 302030, г. Орел, ул. Московская, 65

Подписной индекс 15998 по объединенному каталогу

«Пресса России»

Журнал входит в **Перечень ведущих рецензируемых научных журналов и изданий**, определенных ВАК для публикации трудов на соискание ученых степеней кандидатов и докторов наук.

Рубрики номера

Редакция

О.И. Константинова
А.А. Митин

Адрес учредителя журнала

302020, г. Орел, Наугорское шоссе, 29
(4862) 42-00-24; www.gu-unpk.ru;
E-mail: unpk@ostu.ru

Адрес редакции

302020, г. Орел, Наугорское шоссе, 40
(4862) 43-40-39; www.gu-unpk.ru;
E-mail: konstaoksana@yandex.ru; isit@ostu.ru

Зарег. в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Св-во о регистрации средства массовой информации ПИ № ФС77-47350 от 03.11.2011 г.

Scientific and technical journal

Information Systems and Technologies

№ 3 (95) May-June 2016

The journal is published since 2002, leaves six times a year

The founder – State University – Education-Science-Production Complex

It is sent to the printer's on 15.02.2016,
26.02.2016 is put to bed
Format 60x88 1/8.
Convent. printer's sheets 7,5. Circulation 300 copies
The order №
It is printed from a ready dummy layout
on polygraphic base of State University – ESPC
302030, Orel, Moskovskaya street, 65

Index on the catalogue
***«Pressa Rossii»** 15998*

Journal is included into the list of the Higher Attestation Commission for publishing the results of theses for competition the academic degrees.

In this number

The editors

Konstantinova O.I.
Mitin A.A.

The address of the founder of journal

302020, Orel, Highway Naugorskoe, 29
(4862) 42-00-24; www. gu-unpk.ru;
E-mail: unpk@ostu.ru

The address of the editorial office

302020, Orel, Highway Naugorskoe, 40
(4862) 43-40-39; www.gu-unpk.ru;
E-mail: konstaoksana@yandex.ru; isit@ostu.ru

Journal is registered in Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications.
The certificate of registration
ПИ № ФС77-47350 from 03.11.2011.

СОДЕРЖАНИЕ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМАХ

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СЕТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

CONTENT

MATHEMATICAL AND COMPUTER SIMULATION

INFORMATION TECHNOLOGIES IN SOCIAL AND ECONOMIC AND ORGANIZATIONAL-TECHNICAL SYSTEMS

AUTOMATION AND CONTROL OF TECHNOLOGICAL PROCESSES AND MANUFACTURES

SOFTWARE OF THE COMPUTER FACILITIES AND THE AUTOMATED SYSTEMS

TELECOMMUNICATION SYSTEMS AND COMPUTER NETWORKS

INFORMATION AND DATA SECURITY

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

УДК 621.39

Е.Г. ЖИЛЯКОВ, С.П. БЕЛОВ,
А.А. АЛЕКСАНДРОВА, А.В. БОЛДЫШЕВ

ИССЛЕДОВАНИЕ МЕТОДА СЕЛЕКЦИИ ПАУЗ В РЕЧЕВЫХ СООБЩЕНИЯХ

В статье представлен метод селекции пауз в речевых сообщениях на основе применения субполосного анализа. Использование предложенного подхода позволяет определять участки отсутствия звуков речи с меньшей вероятностью ошибочного принятия решения в сравнении с другими методами обнаружения пауз.

Ключевые слова: *речевой сигнал; селекция пауз; субполосный анализ; обнаружение пауз; сегментация речи.*

В настоящее время огромное внимание уделяется развитию речевых технологий, связанных с анализом и преобразованием речевых данных. Одним из важных этапов при анализе речевых сообщений является определение участков отсутствия речи. Точное определение границ между речью и паузой позволяет повысить эффективность последующих преобразований. Так, в системах распознавания речи верное определение участков пауз позволяет уменьшить вероятность ошибок. В свою очередь, в системах сжатия речи точное определение границ пауз позволяет либо повысить степень сжатия, либо улучшить качество восстановления речевого сообщения.

В существующих системах для обнаружения пауз используются так называемые алгоритмы Voice Activity Detector (VAD). В алгоритмах VAD широко используются коэффициенты автокорреляции для определения энергетического уровня сигнала и его стационарности. Решение о наличии речевого сигнала принимается в том случае, если энергия сигнала превышает пороговое значение и сигнал является нестационарным.

Простейшие алгоритмы VAD основаны на сравнении энергии отрезка сигнала с пороговым: решение о наличии паузы принимается в случае, если энергия анализируемого отрезка не превышает пороговое значение. Однако данный подход имеет значительно высокие значения вероятностей ошибочного принятия решения. Поэтому для принятия решения о наличии паузы также учитывается наличие стационарности отрезка сигнала. Для определения уровня сигнала и его стационарности широко используются коэффициенты автокорреляции. Решение о наличии речевого сигнала принимается в том случае, если энергия сигнала превышает пороговое значение и сигнал является нестационарным. Шумы в паузах имеют различную природу, что может приводить к увеличению вероятности ошибочного принятия решения.

Исследования тонкой структуры энергетического спектра речевого сигнала в частотной области позволили установить, что энергия звуков речи распределена неравномерно и сосредоточена в достаточно узких частотных интервалах, в то время как энергия отрезка сигнала, принадлежащего паузе, распределена равномерно во всем анализируемом частотном диапазоне.

На рисунках 1-12 представлены фрагменты сигналов, порожденных различными звуками русской речи и шумами в паузах, а также их спектры при длительности отрезка анализа 128 отсчетов (частота дискретизации Fd=8кГц, разрядность кода 16 бит).

Использование различий в частотном распределении энергий РС, порожденных различными звуками русской речи и шумами в паузах, позволяет построить решающие процедуры селекции пауз. При этом необходимо отметить, что использования только одной из характеристик отрезка не достаточно.

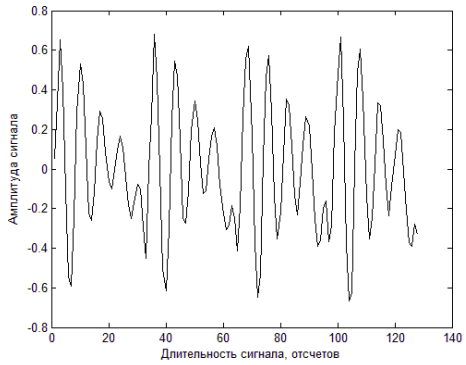

Рисунок 1 – Фрагмент сигнала, порожденного звуком «а»

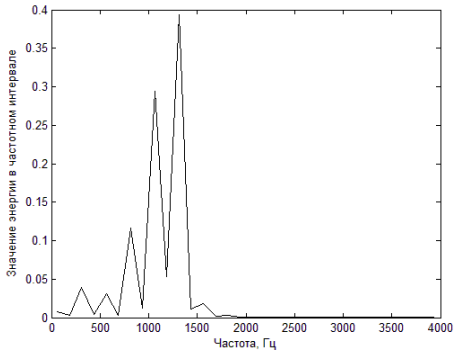

Рисунок 2 – Спектр сигнала, порожденного звуком «а»

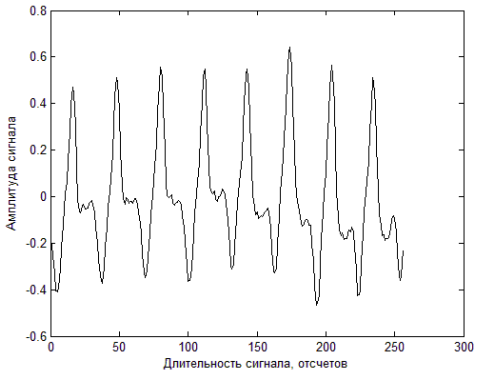

Рисунок 3 – Фрагмент сигнала, порожденного звуком «л»

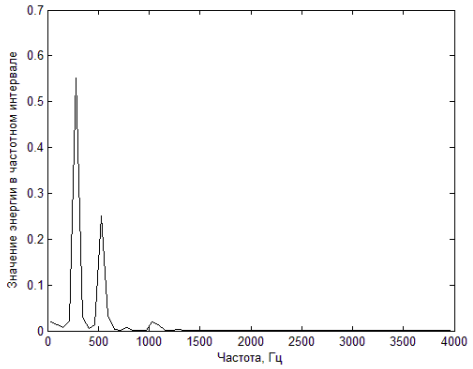

Рисунок 4 – Спектр сигнала, порожденного звуком «л»

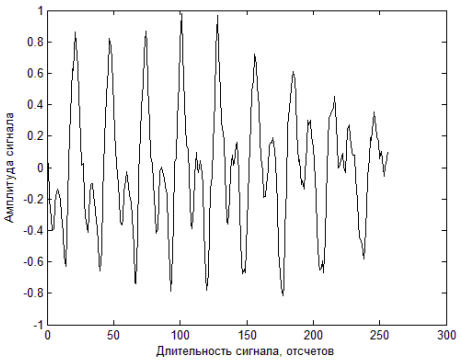

Рисунок 5 – Фрагмент сигнала, порожденного звуком «б»

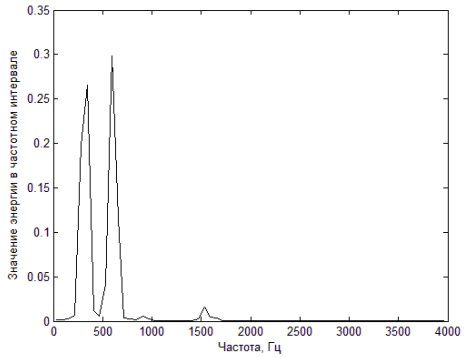

Рисунок 6 – Спектр сигнала, порожденного звуком «б»

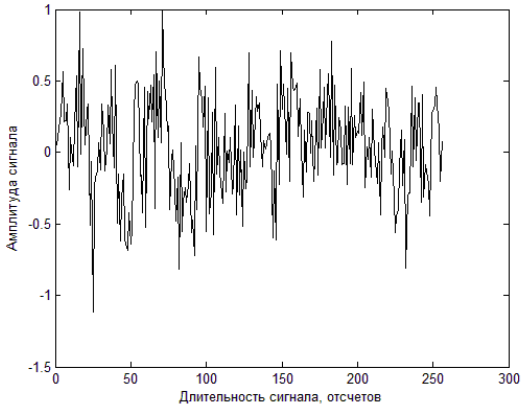

Рисунок 7 – Фрагмент сигнала, порожденного звуком «ч»

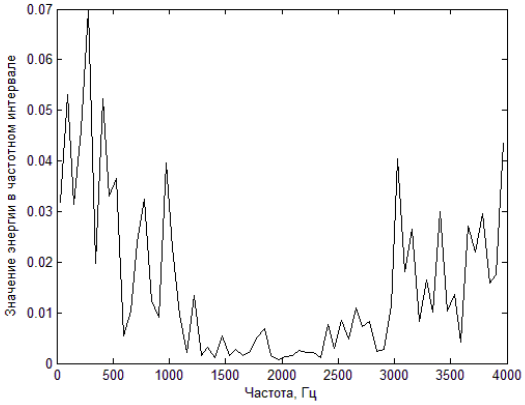

Рисунок 8 – Спектр сигнала, порожденного звуком «ч»

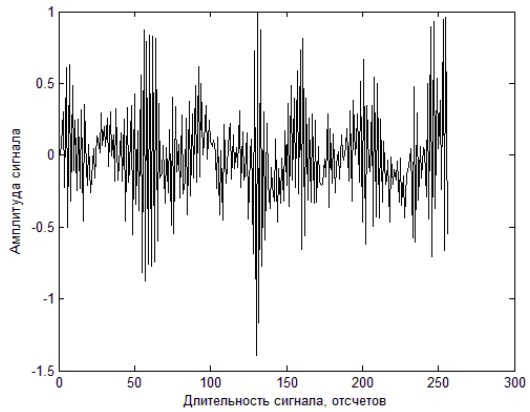

Рисунок 9 – Фрагмент сигнала, порожденного звуком «ш»

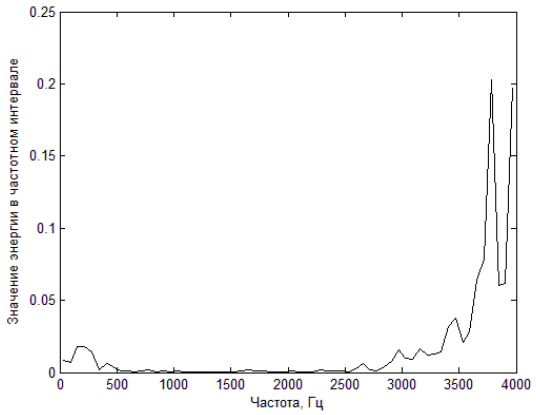

Рисунок 10 – Спектр сигнала, порожденного звуком «ш»

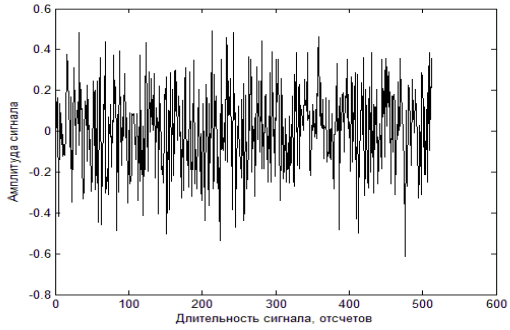

Рисунок 11 – Фрагмент сигнала, порожденного шумом в паузе

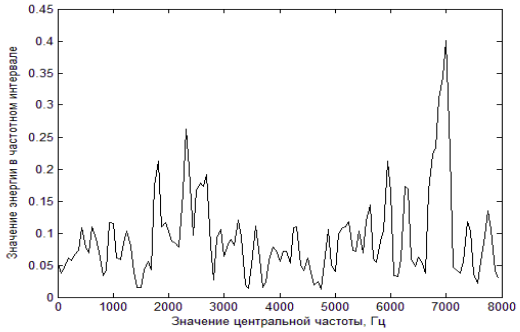

Рисунок 12 – Спектр сигнала, порожденного шумом в паузе

Основная проверяемая гипотеза формулируется следующим образом.

H_0 – анализируемый отрезок РС $\vec{x} = (x_1,..,x_N)^T$ порожден шумами в паузе речи

$$\vec{x} = \vec{u} = (u_1,..,u_N)^T. \quad (1)$$

Альтернатива H_1 заключается в том, что хотя бы часть компонент рассматриваемого вектора зафиксирована в присутствии звуков речи

$$\vec{x} = \vec{u} + \vec{s},\ \vec{s} = (s_1,..,s_N)^T. \quad (2)$$

Здесь и в дальнейшем, где это не вызывает затруднений, индекс у векторов опущен.

Ввиду неодинаковости и изменчивости во времени воздействий, оказываемыми различными звуками речи, по-видимому, единственной возможностью является использование в качестве признаков энергетических характеристик: энергия (квадрат евклидовой нормы) анализируемого вектора $\| \vec{x} \|^2$ и распределение ее по частотным интервалам в виде наборов соответствующих долей

$$Pd_n(\vec{x}) = P_n(\vec{x}) / \sum_{k=0}^{N/2-1} P_k(\vec{x}), n = 0,..,N/2-1. \quad (3)$$

Непосредственно из этого определения следует равенство

$$\sum_{n=0}^{N/2-1} Pd_n(\vec{x}) = 1. \quad (4)$$

Тогда в качестве одной из мер различий между векторами можно использовать аналог расстояния Питмена [1]

$$\gamma(x,y) = (\sum_{n=0}^{N/2-1}((Pd_n(\vec{x}))^{1/2} - (Pd_n(\vec{y}))^{1/2})^2)^{1/2}, \quad (5)$$

которую естественно называть субполосным расстоянием.

Отметим, что использование квадратных корней позволяет выровнять вклады разностей долей энергий из различных частотных интервалов.

С учетом свойства (4) соотношение (5) преобразуется к следующему виду

$$\gamma(x,y) = (2(1 - \sum_{n=0}^{N/2-1}(Pd_n(\vec{x}) \cdot Pd_n(\vec{y}))^{1/2}))^{1/2}. \quad (6)$$

Пусть теперь D_n^2, G_u – математические ожидания долей энергий отрезков шумов в паузах

$$D_n^2 = M[Pd_n(\vec{u})], \quad n = 0,..,N/2-1 \quad (7)$$

и их квадратов евклидовых норм

$$G_u = M[|\vec{u}|^2]. \quad (8)$$

Легко показать, что в виду (4) будет иметь место равенство

$$\sum_{n=0}^{N/2-1} D_n^2 = M[\sum_{n=0}^{N/2-1} Pd_n(\vec{u})] = 1. \quad (9)$$

В качестве решающей функции (РФ) при селекции пауз предлагается использовать статистику [2]

$$F_u = W_u(x) \cdot \gamma_u(x), \quad (10)$$

где

$$\gamma_u(x) = (\sum_{n=0}^{N/2-1}((Pd_n(\vec{x}))^{1/2} - D_n)^2)^{1/2} = (2(1 - \sum_{n=0}^{N/2-1} D_n(Pd_n(\vec{x}))^{1/2}))^{1/2}; \quad (11)$$

$$W_u(x) = \| \vec{x} \|^2 / G_u. \quad (12)$$

На рисунках 13-15 представлены фрагмент РС, порожденного словом «черепаха», и результат оценки характеристик (11) и (12). При этом определение математических ожиданий D_n^2 и G_u определялось на основе анализа фрагмента шума в паузе длительностью 0,19 сек.

Функция $W_u(x)$ реагирует на изменение энергии по сравнению со средней, тогда как $\gamma_u(x)$ реагирует на изменение ее распределения по частотным интервалам.

Гипотеза H_0 отвергается при выполнении неравенства

$$F_u > h_\alpha, \quad (13)$$

где $h_\alpha > 0$ – порог, удовлетворяющий условию

$$PR(F_u > h_\alpha / H_0) \le \alpha. \quad (14)$$

Здесь PR – символ вероятности, а α – желаемый уровень вероятности ошибок первого рода.

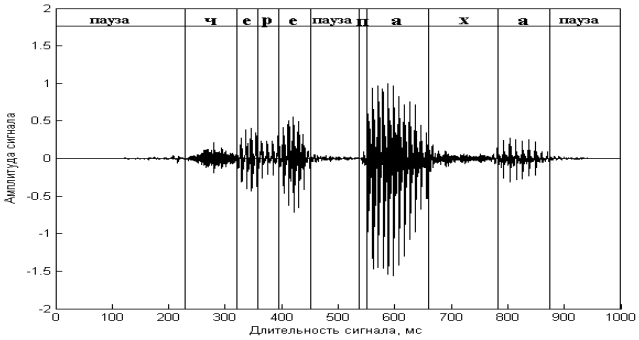

Рисунок 13 – Фрагмент РС, порожденного словом «черепаха» (f_d=16кГц)

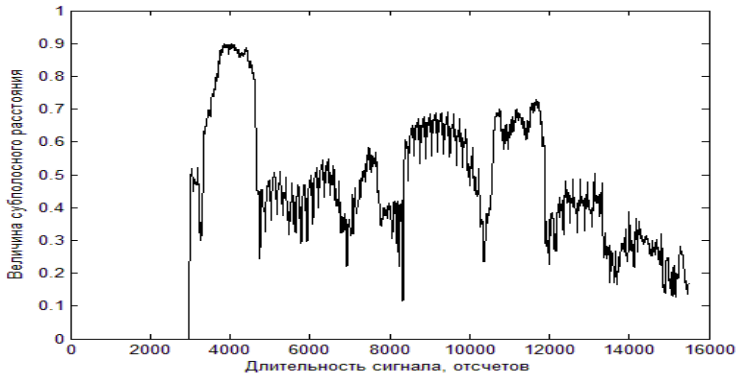

Рисунок 14 – Результат оценки субполосного расстояния $\gamma_u(x)$ фрагмента РС, порожденного словом «черепаха» (f_d=16кГц, N=256)

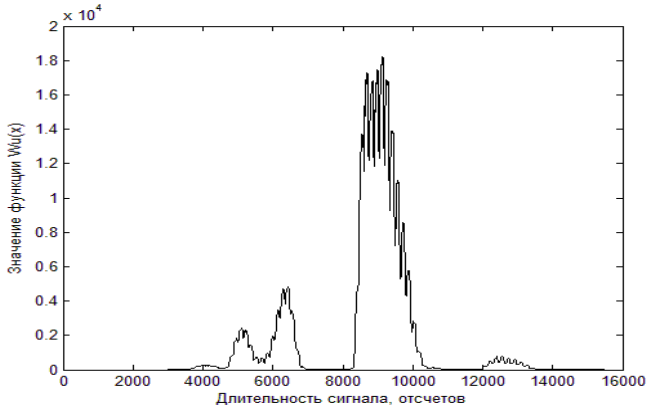

Рисунок 15 – Результат оценки функции $W_u(x)$ фрагмента РС, порожденного словом «черепаха» (f_d=16кГц, N=256)

Оценивание математических ожиданий (7) и (8), а также порогов для правила (13) осуществляется в режиме обучения по совокупности реализаций шумов в паузах речи.

Для оценки эффективности разработанного алгоритма были использованы оценки вероятностей ошибок первого и второго рода. Оценка вероятности ошибки первого рода определена на основе анализа сигнала, соответствующего участку шума в паузах (185000 отсчетов). Величина вероятности определялась как:

$$P_{1ош} = N_{ошиб.речь} / N_{пауз}, \qquad (15)$$

где $N_{ошиб.речь}$ – количество отрезков, ошибочно отнесенных к РС в присутствии звуков речи; $N_{пауз}$ – количество отрезков РС, порожденных шумами, использованных для анализа (185000 отрезков).

Для оценки вероятности ошибки второго рода был использован речевой материал с предварительно удаленными участками пауз (230000 отрезков). Вероятность ошибки определялась с использованием отношения вида:

$$P_{2ош} = N_{ошиб.пауз} / N_{речи}, \quad (16)$$

где $N_{ошиб.пауз}$ – количество отрезков, ошибочно отнесенных к шуму в паузе; $N_{речи}$ – количество отрезков РС в присутствии звуков речи, использованных для анализа (230000 отрезков).

В таблицах 1-2 представлены результаты сравнений метода селекции пауз на основе разработанной РФ с методом селекции пауз на основе РФ с максимальной чувствительностью [3] и методом селекции пауз на основе различий корреляционных свойств шумов в паузах и РС, порожденных звуками речи (VAD) при различных отношениях шум/сигнал *k*. В таблице представлены результаты оценки вероятностей ошибок первого и второго рода для алгоритма VAD при порядке модели p=30. Выбор такого значения порядка модели позволяет обеспечивать наименьшие вероятности ошибок первого и второго рода.

Таблица 1 – Значения вероятностей ошибок первого и второго рода при различных параметрах (f_d=16кГц, N=128)

	Субполосная РФ		**РФ максимальной чувствительности**		**VAD на основе корреляционного анализа**	
	$P_{1ош}$	$P_{2ош}$	$P_{1ош}$	$P_{2ош}$	$P_{1ош}$	$P_{2ош}$
без шума	0,0332	$<10^{-4}$	0,0459	$<10^{-4}$	0,0957	0,0001
***k*=0,1**	0,0374	0,0002	0,0517	0,0001	0,1656	0,0003
***k*=0,2**	0,0410	0,0015	0,0583	0,0011	0,1580	0,0038
***k*=0,3**	0,0462	0,0027	0,0590	0,0011	0,1535	0,0123
***k*=0,4**	0,0507	0,0092	0,0586	0,0049	0,1524	0,0323
***k*=0,5**	0,0537	0,0184	0,0560	0,0093	0,1494	0,0610
***k*=0,6**	0,0559	0,0298	0,0514	0,0143	0,1453	0,1007
***k*=0,7**	0,0573	0,0465	0,0462	0,0194	0,1433	0,1467
***k*=0,8**	0,0582	0,0621	0,0422	0,0293	0,1428	0,2035
***k*=0,9**	0,0584	0,0904	0,0395	0,0421	0,1437	0,2981
***k*=1**	0,0583	0,1161	0,0362	0,0577	0,1445	0,3524

Таблица 2 – Значения вероятностей ошибок первого и второго рода при различных параметрах (f_d=16кГц, N=256)

	Субполосная РФ		**РФ максимальной чувствительности**		**VAD на основе корреляционного анализа**	
	$P_{1ош}$	$P_{2ош}$	$P_{1ош}$	$P_{2ош}$	$P_{1ош}$	$P_{2ош}$
без шума	0,0791	$<10^{-4}$	0,0984	$<10^{-4}$	0,2143	0,0001
k=0,1	0,0861	$<10^{-4}$	0,1074	$<10^{-4}$	0,2894	0,0001
k=0,2	0,0902	$<10^{-4}$	0,1173	$<10^{-4}$	0,3105	0,0007
k=0,3	0,0963	0,0002	0,1221	$<10^{-4}$	0,3359	0,0035
k=0,4	0,1027	0,0006	0,1233	0,0007	0,3503	0,0065
k=0,5	0,1081	0,0029	0,1243	0,0010	0,3612	0,0125
k=0,6	0,1127	0,0057	0,1241	0,0023	0,3693	0,0192
k=0,7	0,1164	0,0075	0,1221	0,0043	0,3747	0,0301
k=0,8	0,1201	0,0109	0,1189	0,0051	0,3836	0,0482
k=0,9	0,1235	0,0187	0,1152	0,0097	0,3927	0,0627
k=1	0,1265	0,0256	0,1112	0,0108	0,3961	0,0830

Метод, основанный на использовании РФ максимальной чувствительности, более чувствителен к увеличению энергии отрезка шума.

Полученные результаты показывают, что предлагаемый метод позволяет выделять участки пауз с меньшей вероятностью ошибочного принятия решений.

Работа выполнена при поддержке гранта РФФИ № 15-07-01463 «Разработка методов и алгоритмов автоматического распознавания устной речи с использованием субполосного анализа речевых сигналов».

СПИСОК ЛИТЕРАТУРЫ

1. Питмен Э. Основы теории статистических выводов; пер. с англ. – М.: Мир, 1986. – 104 с.
2. Жиляков Е.Г. и др. Об одном алгоритме кодирования пауз в речевых данных / Е.Г. Жиляков, Е.И. Прохоренко, А.А. Фирсова, А.В. Болдышев // Журнал «Вопросы радиоэлектроники». Серия «Электронная вычислительная техника» (ЭВТ), 2013. – Выпуск 1. – С. 17-25.
3. Белов С.П., Фирсова А.А. Исследование решающей функции максимальной чувствительности к изменению частей энергии в частотных интервалах // Научные ведомости Белгородского государственного университета. Серия «Информатика», 2012. – № 13(132). – Выпуск 23/1. – С. 227-231.

Жиляков Евгений Георгиевич
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Доктор технических наук, профессор, заведующий кафедрой информационно-телекоммуникационных систем и технологий
Тел.: 8 (4722) 30-13-92
E-mail: Zhilyakov@bsu.edu.ru

Белов Сергей Павлович
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Доктор технических наук, профессор кафедры информационно-телекоммуникационных систем и технологий
Тел.: 8 (4722) 30-13-00 (доб. 2174)
E-mail: Belov@bsu.edu.ru

Медведева Александра Александровна
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Кандидат технических наук, старший преподаватель кафедры информационно-телекоммуникационных систем и технологий
Тел.: 8 (74722) 30-13-00 (доб. 2174)
E-mail: Medvedeva_aa@bsu.edu.ru

Болдышев Алексей Владимирович
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Кандидат технических наук, старший преподаватель кафедры информационно-телекоммуникационных систем и технологий
Тел.: 8 (4722)30-13-00 (доб. 2174)
E-mail: Boldyshev@bsu.edu.ru

E.G. ZhILYaKOV *(Doctor of Engineering Sciences, Professor,*
Head of the Department of Information and Telecommunication Systems and Technologies)

S.P. BELOV *(Doctor of Engineering Sciences,*
Professor of the Department of Information and Telecommunication Systems and Technologies)

A.A. MEDVEDEVA *(Candidate of Engineering Sciences,*

Senior Teacher of the Department of Information and Telecommunication Systems and Technologies)

A.V. BOLDY'ShEV *(Candidate of Engineering Sciences,*
Senior Teacher of the Department of Information and Telecommunication Systems and Technologies)
Belgorod National Research University, Belgorod

RESEARCH OF A METHOD OF SELECTION OF PAUSES IN SPEECH MESSAGES

In article the method of selection of pauses is presented in speech messages on the basis of application of the subband analysis. Use of the offered approach allows to define sites of lack of sounds of the speech with smaller probability of wrong decision-making in comparison with other methods of detection of pauses.

Keywords: *speech signal; selection of pauses; subband analysis; detection of pauses; segmentation of the speech.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Pitmen E'. Osnovy' teorii statisticheskix vy'vodov; per. s angl. – M.: Mir, 1986. – 104 s.
2. Zhilyakov E.G. i dr. Ob odnom algoritme kodirovaniya pauz v rechevy'x danny'x / E.G. Zhilyakov, E.I. Proxorenko, A.A. Firsova, A.V. Boldy'shev // Zhurnal «Voprosy' radioe'lektroniki». Seriya «E'lektronnaya vy'chislitel'naya texnika» (E'VT), 2013. – Vy'pusk 1. – S. 17-25.
3. Belov S.P., Firsova A.A. Issledovanie reshayushhej funkcii maksimal'noj chuvstvitel'nosti k izmeneniyu chastej e'nergii v chastotny'x intervalax // Nauchny'e vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya «Informatika», 2012. – № 13(132). – Vy'pusk 23/1. – S. 227-231.

УДК 004.75

В.Г. ГРИШАКОВ, И.В. ЛОГИНОВ

УПРАВЛЕНИЕ ДИНАМИЧЕСКОЙ РЕКОНФИГУРАЦИЕЙ ИТ-ИНФРАСТРУКТУРЫ В МЕНЯЮЩИХСЯ УСЛОВИЯХ

В статье рассмотрены основные задачи управления, состав и структура типовых систем управления динамической реконфигурацией ИТ-инфраструктуры крупной организации. Сформулирована проблема и поставлена задача исследования, заключающаяся в разработке метода адаптации виртуальных систем управления ИТ, которые бы позволяли обеспечивать динамическую реконфигурацию архитектуры систем управления в соответствии с изменениями условий внешней среды и потребностей организации в качественном информационно-телекоммуникационном обеспечении своего функционирования. Построена модель динамической реконфигурации ИТ и предложны общие подходы к решению проблемы структурно-функциональной реконфигурации путем реализации детерминированной стратегии управления развитием ИТ-системы. Цель управления развития ИТ-системы достигается минимизацией средних потерь в единицу времени на множестве допустимых стратегий управления. Рассмотрены вопросы минимизации затрат при информационном обеспечении процессов управления в рамках организации единой модели управляемого объекта, построенной на основе методологии CALS/ИПИ.

Ключевые слова: *ИТ-инфраструктура; управление; реконфигурация; развитие; модель.*

ВВЕДЕНИЕ

Информационно-телекоммуникационная (ИТ) инфраструктура является сложной динамической системой, которая должна развиваться в соответствии с динамикой организации. Целью развития ИТ-инфраструктуры является перевод ее в новое состояние, которое больше отвечает требованиям предприятия по информационному обеспечению управленческих и технологических процессов. Задача управления развитием ИТ характеризуется неопределенностью области допустимых состояний. Управление системной динамикой в процессе развития ИТ-инфраструктуры реализует система административного управления [1, 2]. Процесс управления реализуется как реконфигурация ИТ-инфраструктур в соответствии с изменением внешних условий и внутренних факторов. Базой процесса управления являются данные мониторинга внешней среды и компонентов ИТ, а также результаты их последующего анализа. Значительная доля собираемой информации является неполной и нечеткой.

Значительное влияние эффективности ИТ-инфраструктуры на результативность функционирования организации, особенно для высокотехнологичной сферы, обосновывает необходимость формирования методического базиса по реконфигурации сложных ИТ-систем. Высокие риски неэффективного использования ресурсов на модернизацию и низкая результативность функционирования ИТ-инфраструктур определяет необходимость разработки методов ее динамической реконфигурации в условиях изменении внутренних и внешних факторов. Эта задача принимает особую актуальность в условиях наблюдаемого существенного уменьшения продолжительности жизненного цикла технических решений и ускорении скорости внедрения новых технологий в ИТ-сфере.

ПРОБЛЕМА УПРАВЛЕНИЯ РАЗВИТИЕМ ИТ-ИНФРАСТРУКТУРЫ КРУПНОЙ ОРГАНИЗАЦИИ

Развитие базовой организации и изменение технологий информатизации обосновывает необходимость непрерывного повышения уровня автоматизации, информатизации и компьютеризации. Для управления процессом развития ИТ-инфраструктуры в литературе [3-5] предлагается развертывать соответствующую систему управления (например, организовывать процесс непрерывного улучшения по ИСО 20000). Функционирование таких систем управления осуществляется в условиях оперативного

реагирования на изменение условий функционирования и потребностей в информатизации со стороны управляющей организации. Реакцией на внешние воздействия является реконфигурация ИТ-инфраструктуры вместе с ее системой управления.

В статье рассматриваются системы управления (СУ) ИТ-инфраструктурами, осуществляющие управление развитием предоставляемых ИТ-услуг через структурно-функциональное изменение объекта управления. По своей сути такие системы управления являются корпоративными операторами связи и телематических услуг. Общее количество выделенных ИТ-подсистем корпоративного уровня достигает нескольких десятков, для каждой из которых развертывается собственная система управления.

Результаты системного анализа проблем управления процессами развития ИТ-инфраструктур показывают, что реконфигурация ИТ-инфраструктуры организации (S) является производной от изменения ее системы управления (MS). В свою очередь, система управления ИТ изменяется в рамках процесса непрерывного улучшения под изменение потребностей (Z) в ИТ-услугах (рис. 1).

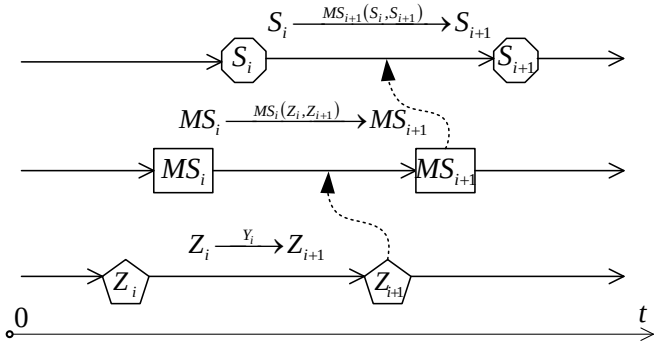

Рисунок 1 – Схема развития ИТ-инфраструктуры организации

В результате изменения потребностей ($Z_i \xrightarrow{Y_i} Z_{i+1}$) под воздействием внешних по отношению к организации факторов (Y) системой модернизации (SM) реконфигурируется система управления ИТ ($MS_i \xrightarrow{SM(Z_i,Z_{i+1})} MS_{i+1}$). В общем случае система модернизации (SM) может рассматриваться как часть общей системы управления ИТ, тогда $MS_i \xrightarrow{MS_i(Z_i,Z_{i+1})} MS_{i+1}$. Перевод системы управления в новое состояние с изменением иерархии управляющих компонентов приводит к изменению ИТ-инфраструктуры: $S_i \xrightarrow{MS_{i+1}(S_i,S_{i+1})} S_{i+1}$. При этом система предоставляемых ИТ-услуг ($\{s\}_{i+1} = f(S_{i+1})$) должна соответствовать потребностям в услугах $\{s\}_{i+1}^{\text{тр}} = f(Z_{i+1})$: $\Delta\{s\} = \left|\{s\}_{i+1}^{\text{тр}} - \{s\}_{i+1}\right| \to \min$. Такое управление ИТ-системой под воздействием внешних эволюционных изменений является эволюционным.

В общем случае задача исследования заключается в решении задачи создания аппарата адаптации СУ ИТ, которые бы позволяли обеспечивать динамическую реконфигурацию архитектуры систем управления ($\exists MS_i, R_i, Z_{i+1}$, надо найти MS_{i+1} : $S_{i+1} = MS_{i+1}(S_i, R_{i+1})$ $\Delta\{s\}_{i+1} = \left|\{s\}_{i+1}^{\text{тр}} - \{s\}_{i+1}\right| \to \min$) в соответствии с изменениями условий внешней среды и потребностей организации в качественном информационно-телекоммуникационном обеспечении ($Z_i \xrightarrow{Y_i} Z_{i+1}$).

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ УПРАВЛЕНИЯ ТРАНСФОРМАЦИЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

Для крупного высокотехнологичного предприятия характерно наличие такой ИТ-инфраструктуры, для которой управление развитием является ресурсоемкой задачей и

которая требует привлечения значительного количества квалифицированных специалистов. Формируемая для решения задачи система управления трансформируется в форму виртуального предприятия [6], интегрирующего несколько внутренних подразделений и осуществляющего предоставление набора информационных и телекоммуникационных сервисов [7]. Управление трансформацией сложных ИТ-систем является актуальной задачей, широко рассматриваемой в литературе [8-12].

Основными технологическими проблемами управления, характерными для ИТ-сферы в соответствии с [10], являются проблемы совершенствования базовых свойств адаптивных ИТ-систем: самоконфигурирования, самообслуживания, самооптимизации, отказоустойчивости (самозащиты). Также в [10] выделяется проблема обоснования состава, структуры, количественных и качественных характеристик информации, необходимой для эффективного управления как самими бизнес-приложениями, так и информационными системами, обеспечивающими их успешную реализацию.

Теоретические аспекты управления трансформацией ИТ-систем сосредоточены на совершенствовании методологий обоснования стратегий развития и разработке методов реконфигурации для конкретных условий. Для долгосрочного планирования (проектирования) ИТ-инфраструктуры используются базовые методологические подходы, в рамках которых увязываются задачи предприятия, развитие ИТ-сферы и архитектура ИТ-инфраструктуры. В литературе [4, 5, 12] выделяются модель Захмана, методологии Gartner и TOGAF, модель федеративной архитектуры FEA. Известные подходы широко используются в рамках целеполагания при модернизации ИТ-инфраструктуры [11]. Отмечается важность осуществления экономического анализа вариантов развития [13].

В [14] рассмотрен подход к формированию методологии управления развитием информационных систем для предприятий, опирающийся на сочетание разделяемой точки зрения на роль ИТ в организации и шаблонов стратегического поведения (паттернов), среди которых выделяются методы принятия решений о реализации инициатив в области ИТ, оценивания эффекта от реализованных инициатив и поддержания адаптивности ИТ-систем. Для управления ИТ-компонентами на всех этапах жизненного цикла применяется CALS/ИПИ-подход, заключающийся в управлении объектом на основе интегрированных информационных моделей [2, 15]. Использование информационной модели в управлении позволяет объединить все данные в рамках одной модели и повысить эффективность разработки, внедрения и сопровождения ИТ-сервисов.

Решение проблемы оптимальной реконфигурации сложных систем сопряжено с разработкой методов структурно-функциональной адаптации объектов управления под изменяющиеся внешние условия. В [16] рассмотрены задача и основные методологические основы решения проблемы планирования структурно-функциональной реконфигурации сложных объектов с целью повышения надежности и живучести сложных систем в динамически изменяющихся условиях. В [17] рассмотрены вопросы проактивного управления сложными объектами, реализуемого за счет обеспечения модельно-алгоритмического описания процессов смысловой интерпретацией всех возможных штатных и нештатных состояний и формирования объектов контроля с интегральными оценками состояний. В [18] рассмотрены вопросы сценарного анализа при управлении сложными организационно-техническими системами, что достигается решением задачи об оптимуме номинала при непрерывной функции полезности для выбора наилучшего импульсного процесса управления. В [19] предложено управлять состоянием и качеством функционирования сложной технической системы на основе нахождения рабочей точки в области работоспособности. В [20] предложны механизмы оптимизации иерархических систем на основе определения субоптимальных иерархий управления, что может быть использовано при реконфигурации систем управления под изменения требований внешней среды.

Проведенный анализ известных подходов и методов управления реконфигурацией ИТ-систем показал их ориентированность на определение целей развития либо на достижение четко определенных целей, что при управлении в области ИТ в большинстве случаев не наблюдается. Это определяет актуальность решения задачи разработки подхода к динамической реконфигурации ИТ-систем в изменяющихся условиях.

МОДЕЛЬ СЕРВИС-ОРИЕНТИРОВАННОГО УПРАВЛЕНИЯ ИТ-СИСТЕМОЙ

В статье рассматривается сервис-ориентированная модель ИТ-инфраструктуры, в рамках которой она может быть представлена в виде множества услуг:

$$S = \left\{ s_{id_i}^{\overline{M},m'_i} \right\}, i = 1..n,$$

где $s_{id_i}^{\overline{M},m'_i}$ – модель ИТ-услуги на всем жизненном цикле; n – количество поддерживаемых ИТ-услуг; $\overline{M}$ – модель жизненного цикла ИТ-услуги связи; m' – текущий этап жизненного цикла услуги; id – уникальный идентификатор ИТ-услуги в рамках каталога ИТ-услуг организации.

В рамках такой модели предполагается равнозначность ИТ-услуги и ИТ-системы ее предоставляющей, поскольку целью управления является достижение требуемых параметров качества услуги, а не способ ее предоставления.

Каждая i-я ИТ-услуга может находиться в одном из нескольких состояний (обозначим j-е состояние как ИТ-услугу s_i). Состояние ИТ-услуги является векторным показателем, отражающим качественные показатели предоставления услуги абонентам (sv – параметры ИТ-услуги), состояние систем, предоставляющей ИТ-услуги и обеспечивающей ее функционирование.

Требования к качеству предоставляемых услуг могут быть определены для каждого показателя (k) по отдельности в виде функции: $sv_k^{\text{тр}}(t)$, имеющей несколько участков с некоторым уровнем обслуживания $QoS_{k,i}$:

$$sv_k^{\text{тр}}(t) = \begin{cases} \dots \\ QoS_{k,j}, t \in [t_{j1}; t_{j2}) \\ QoS_{k,j} + \dfrac{\Delta QoS_{k,j+1}}{t_{(j+1)1} - t_{j2}}(t - t_{j2}), t \in [t_{j2}; t_{(j+1)1}) \\ QoS_{k,j+1}, t \in [t_{(j+1)1}; t_{(j+1)2}) \\ \dots \end{cases} \quad (1)$$

Сервис-ориентированная модель управления ИТ-услугой (ИТ-системой) предполагает два контура управления в составе единой системы управления ($MS = U \cup OTS$): управление развитием ИТ-услуги (U – система управления, обеспечивающая развитие ИТ-услуги) и управление качеством предоставления услуги (OTS – организационно-техническая система, осуществляющая поддержку предоставления ИТ-услуг). ИТ-система (sm) представляет услуги связи с заданными параметрами (sv) на основе ресурсов ($r_{(sm)}$), необходимых на ее функционирование.

Задачи компонентов ИТ-услуги (рис. 2):

– техническая составляющая ИТ-системы (sm) должна представлять услуги связи с заданными параметрами качества;

– система, осуществляющая поддержку предоставления ИТ-услуг (OTS), должна минимизировать отклонения реальных показателей качества от установленных на некоторый промежуток времени;

– система управления, обеспечивающая развитие ИТ-услуги (U), должна обеспечивать адаптацию качества предоставляемых услуг к изменению требований.

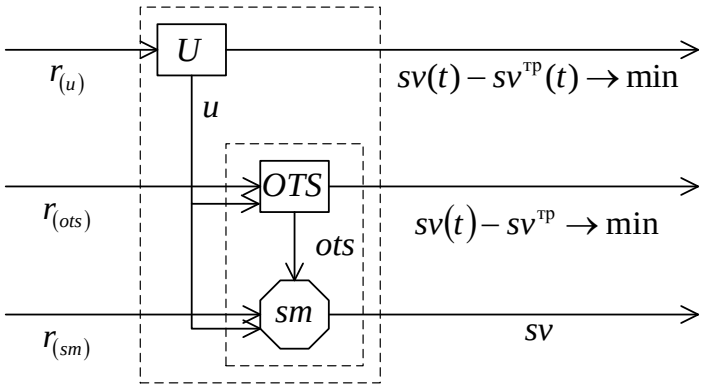

Рисунок 2 – Модель сервис-ориентированного управления ИТ-системой

ДЕТЕРМИНИРОВАННАЯ СТРАТЕГИЯ УПРАВЛЕНИЯ РАЗВИТИЕМ ИТ-СИСТЕМЫ

Для поддержания заданной технической эффективности ИТ-системы (соглашений о качестве обслуживания применительно к пользователю и затрат ресурсов с точки зрения ИТ-подразделения) осуществляется его оперативное управление сервисом (ots) со стороны системы, реализующей сопровождение (OTS). В данном конкуре управления обеспечивается поддержание уровня услуг и тем самым реализуется доступность услуги:

$$ots(y) = \underset{b \in B(y)}{arg\ min} \left[sv(t, y, ots(r_{(ots)})) - sv^{тр} \right], y \in Y \tag{2}$$

Объединение технической системы, предоставляющей услуги и ОТС, обеспечивающей ее функционирование, позволяет предоставлять услуги заданного (требуемого качества) $sv(t) - sv^{тр} \to min$. Вторым аспектом управления сервисом является обеспечение его развития с точки зрения внутренних и внешних факторов, изменений потребностей пользователя, внешней среды и состояния организации:

$$u(y) = \underset{b \in B(y)}{arg\ min} \left[sv(t, y, u(r_{(u)})) - sv^{тр}(t) \right], y \in Y \tag{3}$$

Управление совершенствованием ИТ-систем рассматривается с точки зрения изменения их структуры и состава как с помощью внутренних ресурсов, так и путем привлечения внешних организаций. Управляющие воздействия трансформируют как технический, так и организационно-технический аспекта ИТ-системы $u = u_{ots} \cup u_{sm}$. Суммарные ресурсы на предоставление ИТ-услуги равны $r = r_{(sm)} + r_{(ots)} + r_{(u)}$. Такое управление позволяет обеспечить учет изменения требований к качеству предоставляемых услуг: $sv(t) - sv^{тр}(t) \to min$.

Учет изменения потребностей к ИТ-услугам и преобразования их в требования к ИТ-системе осуществляется с некоторой задержкой (τ). Эта задержка зависит от возможностей по идентификации изменений требований и вида функции изменения требований к качеству услуг ($sv^{тр}(t)$). По итогам реализации ИТ-системы осуществляется потребление ИТ-услуг $sv^{пт}(t) = min\left(sv^{тр}(t), sv(t)\right)$. Мгновенные ожидаемые потери ($C_k(t)$) на предоставление ИТ-услуг (рис. 3) включают затраты ресурсов на функционирование системы ($C_{k,r}(t) = \psi(r(t))$)

и от потерь неполного удовлетворения потребностей в уровне обслуживания ($C_{k,QoS}(t)=\varphi(sv_k^{\text{тр}}(t)-sv_k^{\text{пт}}(t))$): $C_k(t)=C_{k,r}(t)+C_{k,QoS}(t)$.

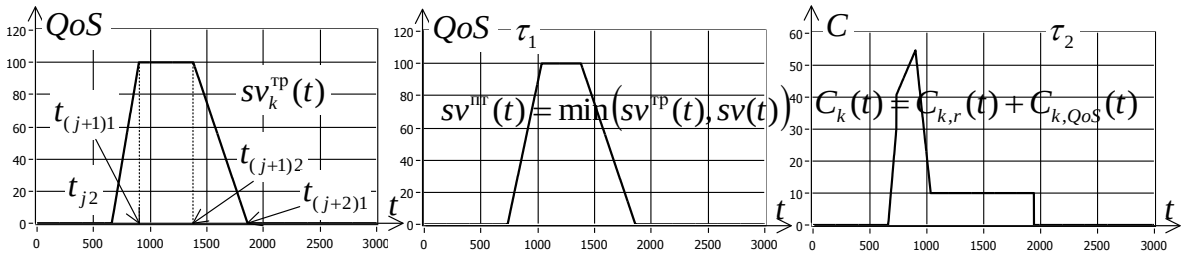

Рисунок 3 – Диаграмма функции потерь при управлении развитием ИТ-системы под изменение требований

Детерминированная стратегия управления развитием ИТ-системы задается функцией $g:\{MS\}\to U$, определяющей независимое от прошлых состояний системы управление $g(y)\in U(y)\subseteq U$, когда внешние воздействия на ИТ-систему находятся в состоянии $y\in Y$.

Целью управления развитием ИТ-системы будет минимизация средних потерь в единицу времени на множестве допустимых стратегий управления:

$$u^g=\lim_{t\to\infty}\frac{1}{t}C_k(y,t)=\lim_{t\to\infty}\frac{1}{t}\sum_{y\in Y}c_k(y,g(y),t)\to\min. \qquad (4)$$

При управлении развитием ИТ-инфраструктуры система управления (MS) должна рассматривать множество альтернатив, позволяющих реализовать новые требования внешней среды (Y) и потребности организации в инфокоммуникационных услугах соответствующего качества (Z). Анализ альтернатив осуществляется на прогнозных и оценочных моделях в соответствии со схемой «агент-менеджер» (рис. 4).

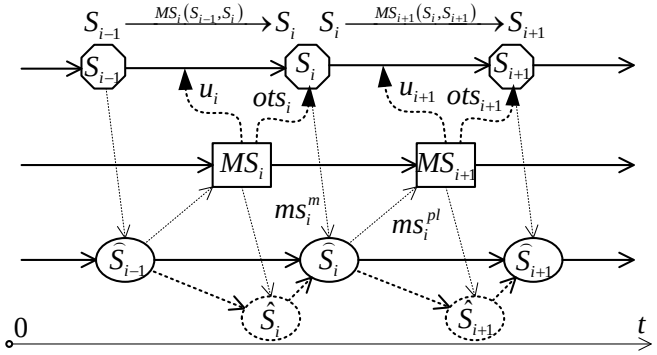

Рисунок 4 – Управление развитием ИТ-инфраструктурой на основе модели

Система управления ИТ с использованием входящей в ее состав системы мониторинга оценивает состояние объекта управления $S_i \xrightarrow{MS_i^m} \hat{S}_i$. При необходимости реагирования на изменение требований в услугах создается множество прогнозных моделей ИТ-системы: $\hat{S}_i=MS_i^{pl}\left(\hat{S}_i,\hat{S}_i^{\text{тр}}\right): \hat{S}_i\in\{S_i\}^{\text{доп}}$. Из сформированного множества альтернатив выбирается та, при реализации которой достигается минимизация средних потерь (4) в условии реализации управлений (2) и (3).

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА УПРАВЛЕНИЯ РЕКОНФИГУРАЦИЕЙ

Использование моделирования в процессе управления реконфигурацией показывает необходимость оптимальной интеграции разнородных моделей, описывающих ИТ-системы на разных стадиях жизненного цикла.

Состояние ИТ-системы (S) как сложной стохастической системы может быть описано в виде многомерной случайной величины $X=(X_1,X_1,\ldots,X_m)^{\mathrm{T}}$. Модель ($\hat{S}^k$) ИТ-системы ($S$) может быть представлена как частная оценка $X=(X_1,X_2,\ldots,X_m)^{\mathrm{T}}$ с использованием отдельной процедуры k $X^k=MS^k(X_1,X_2,\ldots,X_m)^{\mathrm{T}}=\left(ms_1^k(X_1),ms_2^k(X_2),\ldots,ms_m^k(X_m)\right)^{\mathrm{T}}$, где MS^k – стохастический процесс. Следовательно, $X^k=\left(X_1+ms_1^k,X_1+ms_2^k,\ldots,X_m+ms_m^k\right)^{\mathrm{T}}$, где ms^k – случайная величина, определяющая ошибку оценивания.

Отличие между двумя моделями может быть определено через условную энтропию $H\left(X^{k=1}\mid X^{k=2}\right)=-\int\limits_{X^{k=1}}\int\limits_{X^{k=2}}p\left(X^{k=1},X^{k=2}\right)log\ p\left(X^{k=1}\mid X^{k=2}\right)dX^{k=1}dX^{k=2}$, где $X=(X_1,X_2,\ldots,X_m)^{\mathrm{T}}$, $p_X=(x_1+ms_1,x_2+ms_2,\ldots,x_m+ms_m)$ – совместная плотность распределения суммы случайных величин. Ошибка при использовании двух моделей объекта управления зависит от величины ошибки описания объекта: $\xi\left(u(ms^1=ms^2)-u(ms^1\neq ms^2)\right)=\zeta\left(H\left(X^1\mid X^2\right),|u|\right).$

Эффективное управление требует минимизации ошибки, что обосновывает интеграцию моделей ИТ-системы разных стадий жизненного цикла. Реализацию минимизации ошибки предлагается осуществлять с опорой на принципы методологии CALS/ИПИ при проектировании системы управления. Они определяют необходимость использовать в качестве объединяющего компонента систему моделирования, поддерживающую единую модель ИТ-инфраструктуры. СУ ИТ новой организации при этом может быть представлена в виде инварианта системы управления CALS/ИПИ-типа, компоненты которой идентифицированы элементами системы управления ИТ-инфраструктурой (табл. 1).

Таблица 1 – Отображение инвариантных понятий CALS для СУ ИТ CALS-типа

Базовое понятие	**Область методологии CALS/ИПИ**	**Область концепции виртуальных СУ ИТ**
Субъект управления	Система управления предприятием	Система управления ИТ CALS-типа
Объект управления	Сложное наукоемкое изделие на всем жизненном цикле	ИТ-инфраструктура крупной организации на всем жизненном цикле
Интегрированная информационная среда (ИИС)	АСУ предприятия	Виртуальная система гибридного моделирования
Методы управления	Базовые технологии управления	Информационно-имитационные технологии управления жизненным циклом
Методы информационного обеспечения	Базовые технологии управления данными	Технологии управления процессами распределенного гибридного моделирования
Информационное обеспечение	Общая база данных об изделии	База моделей – порождаемая гибкая гибридная модель ИТ-инфраструктуры

Применение концепции CALS/ИПИ для управления ИТ-инфраструктурой позволяет обосновать возможность управления ИТ-инфраструктурой на основе информационного сопровождения всего ее жизненного цикла путем создания и поддержки интегрированной информационной модели ($\hat{S}$).

ЗАКЛЮЧЕНИЕ

В работе рассмотрены основные задачи управления, состав и структура типовой системы управления динамической реконфигурацией ИТ-инфраструктуры. Сформулирована проблема исследования, заключающаяся в разработке метода адаптации виртуальных СУ ИТ, которые бы позволяли обеспечивать структурно-функциональную реконфигурацию ИТ-инфраструктур в соответствии с изменениями условий внешней среды и потребностей организации в качественном информационно-телекоммуникационном обеспечении. Проведен комплексный анализ известных подходов к управлению реконфигурации ИТ, который показал, что в рамках существующих концепций управления разрабатываются методы решения отдельных задач управления структурно-функциональной динамикой, однако для нечетко сформулированных целей оптимизации задача не решена. Построена модель динамической реконфигурации ИТ и предложны общие подходы к решению проблемы путем реализации детерминированной стратегии управления развитием ИТ-системы. Цель управления развитием ИТ-системы достигается минимизацией средних потерь в единицу времени на множестве допустимых стратегий управления. Рассмотрены вопросы минимизации затрат на управление путем единого информационного обеспечения процессов управления.

СПИСОК ЛИТЕРАТУРЫ

1. Соломенцев Ю.М., Павлов В.В. Моделирование иерархии целей функционирования производительных систем в CALS-технологиях // Вестник МГТУ Станкин, 2009. – № 1. – С. 98-101.
2. Губанов Н.Г. Анализ методов информационной поддержки принятия решений управления жизненным циклом сложных технических объектов // Вестник Самарского ГТУ: технические науки, 2006. – № 41. – С. 12-18.
3. ISO 20000-1:2005. Information technology – service management. Part 1. Specification.
4. Alison Cartlidge and other. The IT Infrastructure // Alison Cartlidge, Ashley Hanna, Colin Rudd, Ivor Macfarlane, John Windebank, Stuart Rance // An Introductory Overview of ITIL v3, 2007. – itSMF. UK. – 58 p. – ISBN 0-9551245-8-1.
5. William E. Hefley, Ethel A. Loesche. The eSCM-CL v1.1: Model Overview. The esourcing capability model for client organization. Carnegie Mellon University. Institute for software research international. Technical report № CMU-ITSOC-06-002, 27.09.2006, Pittsburg, Pennsylvania, USA. – 114 p.
6. Гришаков В.Г., Логинов И.В. Представление систем административного управления АСУП в виде виртуальных предприятий // Информатика и системы управления, 2011. – № 3(29). – С. 125-132.
7. Курц А.Л. и др. Принципы построения средств управления ИТ-инфраструктурой на примере модели ITSM компании HP / А.Л. Курц, А.Л. Фридман, Б.Н. Андерс, Н.А. Фандюшина, Л.Я. Чумаков // Системы и средства информатики, 2008. – Т. 18. – № 2. – С. 69-85.
8. Розенберг И.Н., Гончаренко Г.И., Богомаз М.Ю. Интеллектуализация проектирования эволюционирующих систем корпоративного управления на основе CALS-технологий // Известия Южного федерального университета. Технические науки, 2000. – Т. 16. – № 2. – С. 55-57.
9. Сизов А. Трансформация архитектуры предприятия: причины, действующие лица и пути реализации // Директор информационной службы, 2010. – № 8. – С. 30-32.
10. Соколов Б.В., Цивирко Е.Г., Юсупов Р.М. Анализ влияния информатики и информационных технологий на развитие теории и систем управления сложными объектами // Труды СПИИРАН, 2009. – № 11. – С. 10-51.
11. Сидорова Н.П. Методы и средства моделирования ИТ-инфраструктуры предприятия // Вопросы региональной экономики, 2010. – Т. 3. – № 3. – С. 81-90.
12. CobIT v4.1 Excerpt. Executive summary framework // USA. IT Governance Institute. – 31 p.
13. Хвецкович О.Э. Экономический анализ вариантов модернизации ИТ-инфраструктуры организации // Наука о человеке: гуманитарные исследования, 2009. – № 4. – С. 70-78.

14. Зеленков Ю.А., Логиновский О.В. Методология управления развитием информационных систем промышленных предприятий // Известия высших учебных заведений. Уральский регион, 2013. – № 3. – С. 57-66.
15. Буров Д.А., Остроух А.В., Попов Д.И. Проблемы и перспективы внедрения компонентов CALS-технологий на промышленных предприятиях // Научный вестник Московского государственного технического университета гражданской авиации, 2008. – № 130. – С. 138-146.
16. Павлов А.Н. Методологические основы решения проблемы планирования структурно-функциональной реконфигурации сложных объектов // Известия ВУЗов. Приборостроение, 2012. – Том 55 (11). – С. 7-12
17. Охтилев М.Ю. и др. Концепция проактивного управления сложными объектами: теоретические и технологические основы / М.Ю. Охтилев, Н.Г. Мустафин, В.Е. Миллер, Б.В. Соколов // Известия ВУЗов. Приборостроение, 2014. – Т. 57. – № 11. – С. 7-15.
18. Верба В.А. Выбор сценариев устойчивого развития сложных систем // Вызовы глобального мира. Вестник ИМТП, 2014. – № 1. – С. 27-32.
19. Сиротин Н.Н. Управление состоянием и качеством функционирования сложной технической системы (объекта) // Научный вестник ГосНИИ ГА, 2014. – № 4(315). – С. 55-61.
20. Губко М.В. Алгоритмы построения субоптимальных организационных иерархий / Автоматика и телемеханика, 2009. – № 1. – С. 162-179.

Гришаков Вадим Геннадьевич
Академия ФСО России, г. Орел
Кандидат технических наук
E-mail: gvg2003@gmail.com

Логинов Илья Валентинович
Академия ФСО России, г. Орел
Кандидат технических наук
E-mail: loginov_iv@bk.ru

V.G. GRIShAKOV *(Candidate of Engineering Sciences)*

I.V. LOGINOV *(Candidate of Engineering Sciences)*
The Academy of Federal Security Guard Service of the Russian Federation, Orel

THE MANAGEMENT OF IT-INFRASTRUCTURE DYNAMIC RECONFIGURATION IN THE CHANGED CONDITIONS

The main management task, consist and structure of base management system of corporate IT-infrastructure dynamic reconfiguration are viewed in the article. The problem and task of research are formulated as to design adaptation method for virtual management system of IT, that could be provide dynamic reconfiguration of management system architecture coordinated with transformation of external environment and corporation requirements in the quality information and telecommunication maintenance. The model of IT dynamic reconfiguration and the main method for structure functional reconfiguration problem decision as realization of determine strategy of IT-system development management are offered in the article. The goal of IT development management is achieved by minimization of average loss by time on a set of admissible management strategies. The algorithms of loss minimization in the information maintenance of management process based on common managed object model realized on CALS methodology are offered in the article.

Keywords: *IT-infrastructure; management; reconfiguration; development; model.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Solomencev Yu.M., Pavlov V.V. Modelirovanie ierarxii celej funkcionirovaniya proizvoditel'ny'x sistem v CALS-texnologiyax // Vestnik MGTU Stankin, 2009. – № 1. – S. 98-101.

2. Gubanov N.G. Analiz metodov informacionnoj podderzhki prinyatiya reshenij upravleniya zhiznenny'm ciklom slozhny'x texnicheskix ob''ektov // Vestnik Samarskogo GTU: texnicheskie nauki, 2006. – № 41. – S. 12-18.
3. ISO 20000-1:2005. Information technology – service management. Part 1. Specification.
4. Alison Cartlidge and other. The IT Infrastructure // Alison Cartlidge, Ashley Hanna, Colin Rudd, Ivor Macfarlane, John Windebank, Stuart Rance // An Introductory Overview of ITIL v3, 2007. – itSMF. UK. – 58 p. – ISBN 0-9551245-8-1.
5. William E. Hefley, Ethel A. Loesche. The eSCM-CL v1.1: Model Overview. The esourcing capability model for client organization. Carnegie Mellon University. Institute for software research international. Technical report № CMU-ITSOC-06-002, 27.09.2006, Pittsburg, Pennsylvania, USA. – 114 p.
6. Grishakov V.G., Loginov I.V. Predstavlenie sistem administrativnogo upravleniya ASUP v vide virtual'ny'x predpriyatij // Informatika i sistemy' upravleniya, 2011. – № 3(29). – S. 125-132.
7. Kurc A.L. i dr. Principy' postroeniya sredstv upravleniya IT-infrastrukturoj na primere modeli ITSM kompanii HP / A.L. Kurc, A.L. Fridman, B.N. Anders, H.A. Fandyushina, L.Ya. Chumakov // Sistemy' i sredstva informatiki, 2008. – T. 18. – № 2. – S. 69-85.
8. Rozenberg I.N., Goncharenko G.I., Bogomaz M.Yu. Intellektualizaciya proektirovaniya e'volyucioniruyushhix sistem korporativnogo upravleniya na osnove CALS-texnologij // Izvestiya Yuzhnogo federal'nogo universiteta. Texnicheskie nauki, 2000. – T. 16. – № 2. – S. 55-57.
9. Sizov A. Transformaciya arxitektury' predpriyatiya: prichiny', dejstvuyushhie lica i puti realizacii // Direktor informacionnoj sluzhby', 2010. – № 8. – S. 30-32.
10. Sokolov B.V., Civirko E.G., Yusupov R.M. Analiz vliyaniya informatiki i informacionny'x texnologij na razvitie teorii i sistem upravleniya slozhny'mi ob''ektami // Trudy' SPIIRAN, 2009. – № 11. – S. 10-51.
11. Sidorova N.P. Metody' i sredstva modelirovaniya IT-infrastruktury' predpriyatiya // Voprosy' regional'noj e'konomiki, 2010. – T. 3. – № 3. – S. 81-90.
12. CobIT v4.1 Excerpt. Executive summary framework // USA. IT Governance Institute. – 31 p.
13. Xveckovich O.E'. E'konomicheskij analiz variantov modernizacii IT-infrastruktury' organizacii // Nauka o cheloveke: gumanitarny'e issledovaniya, 2009. – № 4. – S. 70-78.
14. Zelenkov Yu.A., Loginovskij O.V. Metodologiya upravleniya razvitiem informacionny'x sistem promyshlenny'x predpriyatij // Izvestiya vy'sshix uchebny'x zavedenij. Ural'skij region, 2013. – № 3. – S. 57-66.
15. Burov D.A., Ostroux A.V., Popov D.I. Problemy' i perspektivy' vnedreniya komponentov CALS-texnologij na promy'shlenny'x predpriyatiyax // Nauchny'j vestnik Moskovskogo gosudarstvennogo texnicheskogo universiteta grazhdanskoj aviacii, 2008. – № 130. – S. 138-146.
16. Pavlov A.N. Metodologicheskie osnovy' resheniya problemy' planirovaniya strukturno-funkcional'noj rekonfiguracii slozhny'x ob''ektov // Izvestiya VUZov. Priborostroenie, 2012. – Tom 55 (11). – S. 7-12
17. Oxtilev M.Yu. i dr. Koncepciya proaktivnogo upravleniya slozhny'mi ob''ektami: teoreticheskie i texnologicheskie osnovy' / M.Yu. Oxtilev, N.G. Mustafin, V.E. Miller, B.V. Sokolov // Izvestiya VUZov. Priborostroenie, 2014. – T. 57. – № 11. – C. 7-15.
18. Verba V.A. Vy'bor scenariev ustojchivogo razvitiya slozhny'x sistem // Vyzovy' global'nogo mira. Vestnik IMTP, 2014. – № 1. – S. 27-32.
19. Sirotin N.N. Upravlenie sostoyaniem i kachestvom funkcionirovaniya slozhnoj texnicheskoj sistemy' (ob''ekta) // Nauchny'j vestnik GosNII GA, 2014. – № 4(315). – S. 55-61.
20. Gubko M.V. Algoritmy' postroeniya suboptimal'ny'x organizacionny'x ierarxij / Avtomatika i telemexanika, 2009. – № 1. – S. 162-179.

УДК 004.942+343.591

Ю.Б. САВВА

РАЗРАБОТКА ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ АНАЛИЗА АКТИВНОСТИ УЧАСТНИКОВ ВИРТУАЛЬНОЙ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ», ВЕДУЩИХ ПРОТИВОПРАВНУЮ И ДЕСТРУКТИВНУЮ ДЕЯТЕЛЬНОСТЬ

С позиций объектно-ориентированного подхода рассмотрены требования к информационной системе анализа активности участников виртуальной социальной сети. Описаны модели взаимодействия пользователей с системой, структура базы данных. Разработан алгоритм обеспечения безопасности системы и данных.

Ключевые слова: *виртуальные социальные сети; информационная система; объектно-ориентированная модель; база данных; безопасность данных.*

ВВЕДЕНИЕ

Достижения в области информационно-коммуникационных технологий привели к глобальной информатизации общества и возникновению нового цифрового мира, в котором развитие каждого человека, сообществ людей, государств, политики и экономики существенно зависят от использования телекоммуникаций. В то же время глобальная информатизация позволяет использовать новые информационно-коммуникационные технологии в целях дестабилизации социальной обстановки в различных странах государственными структурами, а также вести противоправную и деструктивную деятельность политическими, криминальными и террористическими организациями.

В условиях усиления нестабильности ситуации в международных отношениях и мировой экономики появились новые вызовы и угрозы национальной безопасности и устойчивому развитию России, в том числе в виртуальной среде. В связи с этим особую актуальность приобрела проблема обеспечения кибербезопасности российских граждан в процессах их взаимодействия в виртуальных социальных сетях, через которые проводятся масштабные воздействия в целях изменения их сознания и поведения.

Одной из самых популярных виртуальных социальных сетей в России является сеть «ВКонтакте». Особенно популярна эта сеть среди молодых людей, чье сознание еще только формируется, что и обусловило выбор сети «ВКонтакте» для анализа активности ее участников, ведущих противоправную и деструктивную деятельность посредством специализированной информационной системы.

ПОСТАНОВКА ЗАДАЧИ

Целью создания информационной системы анализа активности участников сети «ВКонтакте» является обеспечение контроля за активностью как отдельных участников, так и их групп путем формирования отчетов о дате и времени.

Функциональные требования к информационной системе включают:

− необходимость авторизации пользователя в системе по выданным ему логину и паролю для работы в системе;

− обеспечение возможности добавления участников социальной сети для контроля системой, достаточным условием работы которой является ввод пользователем идентификатора страницы добавляемого участника социальной сети;

− обеспечение возможности добавления сообществ участников социальной сети для контроля системой, условиями работы которой является ввод пользователем идентификатора сообщества «ВКонтакте», а также заданного набора фильтров: по городу, по полу, по возрасту, по наличию фотографии профиля, по наличию номера телефона на странице;

− наличие удобного пользовательского интерфейса, позволяющего пользователю выбрать конкретного участника социальной сети из списка добавленных ранее и уже контролируемых системой участников, для просмотра его активности;

− обеспечение возможности, позволяющей пользователю выбрать сообщество социальной сети из списка добавленных ранее и уже контролируемых системой сообществ для просмотра активности его участников;

− форматом вывода активности выбранного участника социальной сети в приложении должна быть таблица, столбцами которой являются: дата активности, время активности, статус участника социальной сети и устройство, с которого проявляется активность участника;

− наличие возможности экспорта данных из системы в формате электронных таблиц Microsoft Excel.

Эксплуатационные требования к системе:

− программное обеспечение системы должно быть выполнено в формате web-приложения;

− должна быть предусмотрена возможность фильтрации участников сообщества «ВКонтакте» при добавлении группы участников для контроля системой. Так как сообщества и группы «ВКонтакте» бывают достаточно большими по количеству участников, а участников, вызывающих интерес, значительно меньше, то их необходимо отфильтровать для дальнейшей обработки;

− для обеспечения безопасности системы необходимо предусмотреть возможность регистрации ограниченного числа ее пользователей. Логины и пароли пользователям должны быть выданы администратором базы данных;

− возможность работы с системой не должна быть ограничена конкретным местом (офисом сотрудников). Необходимо обеспечить возможность зарегистрированным пользователям входа в систему из любой точки России;

− помимо версии для стационарных компьютеров, должна быть и мобильная версия сайта (web-приложения) для удобства ее использования зарегистрированными пользователями, для предоставления им возможности оперативного внесения данных в систему не только в офисе за компьютером, но и в другом месте с мобильного устройства;

− обеспечение безопасности системы от несанкционированного входа, включая защиту от SQL-инъекции в базу данных для получения приватной информации;

− обеспечение функционирования системы в непрерывном режиме сбора данных об активности контролируемых участников сети и их сообществ. При этом пользователи не должны иметь доступа к панели включения/отключения системы;

− функциональные возможности администратора и пользователей системы должны быть отличаться друг от друга.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ОРГАНИЗАЦИИ СБОРА ИНФОРМАЦИИ ОБ АКТИВНОСТИ УЧАСТНИКОВ ВИРТУАЛЬНОЙ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»

Виртуальные социальные сети представляют собой уникальный источник данных о личной и общественной жизни их участников. Для сбора информации об истории активности сети в «ВКонтакте» могут быть использованы два подхода: проведение «парсинга» и подключение специального приложения к платформе VK Open API.

«Парсинг» персональной страницы участника виртуальной социальной сети «ВКонтакте» представляет собой реализуемый специальной программой – «парсером», – написанной с использованием скриптовых и серверных языков программирования, процесс последовательного синтаксического анализа информации, размещенной на странице этого участника, результат которого используется для дальнейшего изучения и обработки.

Согласно [1], любой парсер состоит из трех частей, отвечающих за процесс парсинга:

1) получение контента в исходном виде – скачивание кода веб-страницы, из которой необходимо извлечь данные. Одним из самых подходящих решений для получения кода требуемой страницы является библиотека с URL для скриптового языка программирования PHP;

2) извлечение и преобразование полученных данных – извлечение требуемых данных из полученного на первом этапе кода страницы. Обычно для этого используют регулярные выражения. На этом этапе также происходит преобразование извлеченных данных к нужному формату, если это необходимо;

3) генерация результата – завершающий этап. На нем происходит вывод или запись полученных на втором этапе данных в требуемый формат. Чаще всего, запись ведется в базу данных.

VK Open API – платформа, созданная владельцами сети «ВКонтакте» для разработчиков сайтов и приложений иных компаний, которая предоставляет возможность легко авторизовать пользователей на данном сайте или в приложении [1]. Кроме этого, разработчик получает доступ к информации о пользователе, его друзьях, сообществах, аудиозаписях, видеозаписях, фотокарточек и прочих данных для более глубокой интеграции в приложение. Для подключения к VK Open API необходимо создать специальное приложение, которое позволяет использовать на стороннем ресурсе или в приложении все текущие методы Client API.

После подключения пользовательского приложения, ему присваивается идентификатор, в соответствии с которым ему разрешено использование открытых методов «ВКонтакте», и специальный защищенный ключ, который необходим при авторизации приложения на сервере. Удобство использования VK Open API также связано с тем, что доступна полная статистика приложения – количество запросов в сутки, сколько из них возвращено с ошибкой и другие параметры.

Следовательно, для решения задачи сбора и обработки информации для анализа активности участников виртуальной социальной сети «ВКонтакте» наиболее эффективным средством является специальное пользовательское приложение, подключенное к VK Open API.

РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ АНАЛИЗА АКТИВНОСТИ УЧАСТНИКОВ ВИРТУАЛЬНОЙ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»

Для разработки модели информационной системы был использован объектно-ориентированный подход. В соответствии со сформулированными требованиями к системе выделены две категории ее пользователей – пользователи, решающие задачи контроля и анализа активности участников виртуальной социальной сети («Пользователь»), и пользователи с правами «Администратор».

Сценарий взаимодействия с системой пользователей, решающих задачи контроля и анализа активности участников виртуальной социальной сети («Пользователь»), включает следующую последовательность шагов:

1. Пользователь добавляет участника в систему для отслеживания его активности путем ввода идентификатора его страницы.

2. Пользователь просматривает историю активности участника, выполнив ввод идентификатора его страницы.

3. Пользователь добавляет сообщество в систему для отслеживания активности его участников.

- пользователь вводит идентификатор страницы сообщества;
- пользователь указывает требуемые фильтры.

4. Пользователь просматривает историю активности сообщества, выбрав его участников.

Модель взаимодействия «Пользователя» с системой, отражающая указанные действия, представлена на рисунке 1 в виде диаграммы прецедентов.

Рисунок 1 – Модель взаимодействия с системой пользователя с правами «Пользователь»

В соответствии со сформулированными требованиями к системе в модели взаимодействия пользователя с правами «Администратор» в сценарий его взаимодействия с системой включены два дополнительных шага, именно:

1. Остановить отслеживание активности выбранного участника сети.
2. Удалить выбранного участника сети из системы.

Модель взаимодействия пользователя с правами «Администратор» с системой, отражающая указанные действия, представлена на рисунке 2 в виде диаграммы прецедентов.

Рисунок 2 – Модель взаимодействия с системой пользователя с правами «Администратор»

РАЗРАБОТКА СТРУКТУРЫ БАЗЫ ДАННЫХ

Для хранения информации об активности участников социальной сети, их персональной информации, информации о наличии подписки на определенные группы, а также информации для авторизации пользователей в системе необходимо использовать базу данных, которая будет размещена на удаленном сервере в сети Интернет. Подключение к базе данных должно инициироваться непосредственно в коде программного обеспечения системы.

В базе данных присутствуют четыре основных сущности. К ним относится:

1) сущность «Участник», которая хранит персональную информацию об участнике социальной сети (идентификатор страницы, имя и фамилию, пол, мобильный телефон, город, возраст и фотографию профиля);

2) сущность «Сообщество», которая предназначена для хранения сообществ социальной сети (идентификатор страницы сообщества и название сообщества);

3) сущность «Пользователь», хранящая информацию о пользователях программного комплекса (логин, пароль, права доступа к функционалу программной системы);

4) сущность «Активность», предназначенная для хранения информации об активности участника социальной сети (идентификатор участника в базе данных, день активности, время активности, статус и устройство, с которого участник проявляет активность).

Помимо основных сущностей, есть вспомогательная сущность «Сообщество-Участник», отвечающая за принадлежность участника социальной сети одному или нескольким сообществам.

Для обеспечения целостности базы данных используются специальные триггеры ON DELETE {CASCADE}.

При помощи каскадных ограничений ссылочной целостности можно определить список действий, которые SQL-сервер будет принимать при попытке пользователем удалить или обновить ключ в таблице, на который указывают еще существующие внешние ключи.

Триггер ON DELETE {CASCADE} указывает, что при попытке удалить строку с ключом, на которую ссылаются внешние ключи в строках других таблиц, все строки, содержащие эти внешние ключи, также должны быть удалены.

Например, если удалить участника социальной сети из базы данных, то связанные с ним записи в таблицах «История активности» и «Сообщество-Участник» также будут удалены.

Концептуальная схема базы данных информационной системы представлена на рисунке 3.

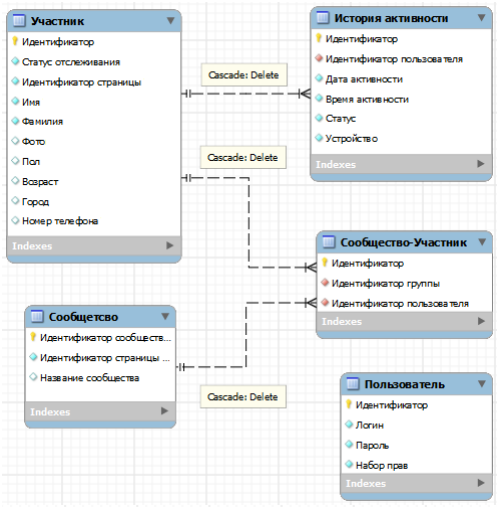

Рисунок 3 – Концептуальная схема базы данных информационной системы

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМЫ И ДАННЫХ

Для регистрации пользователя обычно используется стандартный шаблон анкеты, после ее заполнения пользователь получает свой уникальный логин и пароль. Воспользовавшись этим паролем, пользователь получает право доступа к определенным сервисам сайта.

В информационной системе выявления активности участников социальной сети исключается возможность зарегистрироваться в системе, в соответствии с требованиями к которой она может использоваться только ограниченным кругом лиц, которым право доступа будет предоставлено, согласно их полномочиям.

Для использования всех возможностей системы пользователь должен ввести выданные ему логин и пароль. Если же пользователь по какой-либо причине не знает свой пароль (забыл, утеря, кража), то ему необходимо будет обратиться к администратору системы, который внесет необходимые изменения в учетные записи в базе данных, заполнив для этого необходимые поля в таблице, и назначит пользователю права доступа.

В системе в соответствии с выделенными категориями пользователей предусматривается использование двух видов прав доступа – расширенные права для пользователя правами «Администратор» и пользователей, которым предоставлены различные наборы функций для решения задач контроля и анализа активности участников виртуальной социальной сети. Такое разграничение сделано для обеспечения безопасности использования системы.

В модели процесса авторизации пользователя в системе используется защита от SQL-инъекций, которая обеспечивает безопасность системы при попытке несанкционированного доступа или получения информации из базы данных, реализуемая посредством специальной функции экранирования. Работа процедуры защиты может быть проиллюстрирована на примере поступления следующего кода:

```
$name = $_POST['name'];
$query = "SELECT phone_number FROM users WHERE name = '$name'";
$result = mysql_query($query);
```

Приведенный в примере код является небезопасным, функция экранирования сработает следующим образом. Пусть переменная $name принимает значения в следующем порядке:

1) Alex;
2) Mr’ Alex;
3) Alex’; DROP TABLE users;--.

Что произойдет, когда данные запросы попадут в базу данных? В первом случае при занесении в базу данных переменной со значением Alex не произойдет никакой утечки информации или сбоев в работе базы данных. Запрос, составленный на основе значения этой переменной, вполне безопасен. Во втором случае при занесении в базу данных переменной со значением Mr’ Alex будет поврежден синтаксис СУБД из-за наличия апострофа. В третьем случае при занесении в базу данных переменной со значением Alex’; DROP TABLE users;-- базе данных может грозить непоправимая опасность. Может показаться, что запрос не имеет смысла, но для базы данных это далеко не так. Она «не знает», откуда поступил данный запрос – извне или же это следующая команда исполняемого приложения. Единственное, что она «видит» – это два запроса: найти номер пользователя по имени Alex, а затем удалить таблицу users. И если такая таблица в базе данных есть, она должна быть удалена, причем безо всяких подтверждений со стороны системы.

Таким образом, использование лишь одной строки кода не позволит никому получить несанкционированный доступ к базе данных или выполнить SQL-инъекцию.

Алгоритм авторизации в системе представлен на рисунке 4.

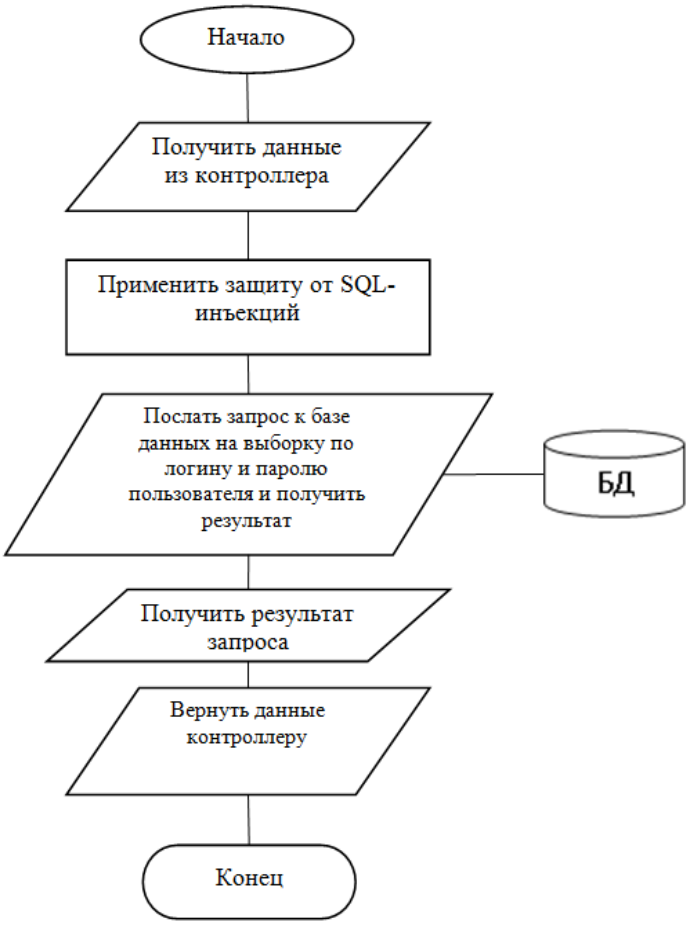

Рисунок 4 – Алгоритм авторизации пользователя в системе

ЗАКЛЮЧЕНИЕ

В соответствии с разработанными моделями была создана программа выявления активности участников виртуальных социальных сетей [2], которая при совместном использовании с программами [3, 4] позволяет выявлять тех участников сетей, которые ведут противоправную и деструктивную деятельность.

В настоящее время система проходит апробацию в ряде уполномоченных организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Парсинг данных. Начинаем разбираться [Электронный ресурс]. – URL: https://vk.com/page-58162909_47522877 (дата обращения 27.04.2015).
2. Савва Ю.Б., Савченко В.А. Программа выявления активности участников виртуальных социальных сетей: свидетельство об официальной регистрации программы для ЭВМ № 2015660186 Российская Федерация; заявитель и правообладатель ФГБОУ ВПО «Госуниверситет – УНПК» (RU). – № 2015616913; заявл. 28.07.2015; зарегистрировано в реестре программ для ЭВМ 24.09.2015. – 1 с.
3. Программа автоматизированного построения социального графа контактов участников виртуальных социальных сетей: свидетельство об официальной регистрации программы для ЭВМ № 2015660019; заявитель и правообладатель ФГБОУ ВПО «Госуниверситет – УНПК» (RU). – № 2015616927; заявл. 28.06.2015; зарегистрировано в реестре программ для ЭВМ 21.09.2015. – 1 с.
4. Савва Ю.Б. Программа кластеризации и шкалирования нечетких данных: свидетельство об официальной регистрации программы для ЭВМ № 2015612445 Российская Федерация; заявитель и правообладатель ФГБОУ ВПО «Госуниверситет – УНПК» (RU). – №

2014663471; заявл. 23.12.2014; зарегистрировано в реестре программ для ЭВМ 18.02.2015. – 1 с.

Савва Юрий Болеславович
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат технических наук, доцент кафедры «Информационные системы»
Тел.: 8 906 569 92 20
E-mail: su_fio@mail.ru

Yu.B. SAVVA *(Candidate of Engineering Sciences,*
Associate Professor of the Department «Information Systems»)
Orel State University named after I.S. Turgenev, Orel

DEVELOPMENT OF OBJECT-ORIENTED MODEL OF SYSTEM FOR ANALYSIS OF ACTIVITY OF PARTICIPANTS OF VIRTUAL SOCIAL NETWORK «VKONTAKTE» WHO LEAD ILLEGAL AND DESTRUCTIVE ACTIVITIES

From positions of object-oriented approach requirements to information system of the analysis of activity of participants of a virtual social network are considered. Models of interaction of users with system, structure of the database are described. The algorithm of safety of system and data is developed.

Keywords: *virtual social networks; information system; object-oriented model; database; data security.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Parsing danny’x. Nachinaem razbirat’sya [E’lektronny’j resurs]. – URL: https://vk.com/page-58162909_47522877 (data obrashheniya 27.04.2015).
2. Savva Yu.B., Savchenko V.A. Programma vy’yavleniya aktivnosti uchastnikov virtual’ny’x social’ny’x setej: svidetel’stvo ob oficial’noj registracii programmy’ dlya E’VM № 2015660186 Rossijskaya Federaciya; zayavitel’ i pravoobladatel’ FGBOU VPO «Gosuniversitet – UNPK» (RU). – № 2015616913; zayavl. 28.07.2015; zaregistrirovano v reestre programm dlya E’VM 24.09.2015. – 1 s.
3. Programma avtomatizirovannogo postroeniya social’nogo grafa kontaktov uchastnikov virtual’ny’x social’ny’x setej: svidetel’stvo ob oficial’noj registracii programmy’ dlya E’VM № 2015660019; zayavitel’ i pravoobladatel’ FGBOU VPO «Gosuniversitet – UNPK» (RU). – № 2015616927; zayavl. 28.06.2015; zaregistrirovano v reestre programm dlya E'VM 21.09.2015. – 1 s.
4. Savva Yu.B. Programma klasterizacii i shkalirovaniya nechetkix danny’x: svidetel’stvo ob oficial’noj registracii programmy’ dlya E’VM № 2015612445 Rossijskaya Federaciya; zayavitel’ i pravoobladatel’ FGBOU VPO «Gosuniversitet – UNPK» (RU). – № 2014663471; zayavl. 23.12.2014; zaregistrirovano v reestre programm dlya E’VM 18.02.2015. – 1 s.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМАХ

УДК 004.421

А.В. АВЕРЧЕНКОВ, Е.Э. АВЕРЧЕНКОВА

АВТОМАТИЗИРОВАННОЕ ПРИНЯТИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ОСНОВЕ МОДЕЛЕЙ И АЛГОРИТМОВ ИНФОРМАЦИОННОЙ СОВЕТУЮЩЕЙ СИСТЕМЫ

В условиях оптимизации деятельности региональной власти в РФ актуальным направлением является разработка программных средств, позволяющих повысить качество принимаемых управленческих решений на региональном уровне. Автор рассматривает регион РФ как сложную социально-экономическую систему, которая находится под воздействием различных факторов малопрогнозируемой внешней среды. В статье предлагается использовать возможности автоматизации для повышения эффективности управленческой деятельности на региональном уровне. Таким образом, была предложена модель информационной советующей системы расчетно-диагностического типа и дано описание алгоритмов ее работы. Основная цель программного комплекса – мониторинг и выявление положительных и негативных тенденций со стороны динамично меняющейся региональной социально-экономической системы, а также внешней среды. Выходными параметрами системы является повышение качество принимаемых управленческих решений на региональном уровне.

Ключевые слова: *структурно-функциональная модель; алгоритмы; информационная советующая система; управленческие решения.*

ВВЕДЕНИЕ

Автоматизация управленческой деятельности широко применяется в современном бизнесе, однако остается актуальной разработка программных средств, позволяющих повысить качество принимаемых управленческих решений на региональном уровне [8]. Для формирования информационного решения, обеспечивающего мониторинг и автоматизацию принятия управленческих решений, была разработана структурно-функциональной модель информационно-советующей системы и описаны основные алгоритмы ее работы.

Создание такой информационной советующей системы основывается на построении нечетких моделей, описывающих влияние факторов внешней среды на составляющие региональной социально-экономической системы [6]. Это позволит выявить наиболее сильные взаимосвязи и учесть их при разработке эффективных управленческих решений. С другой стороны, создание советующей системы потребует формирование нечеткой модели функционирования внешней среды региона [1, 3]. Ранее в работах [1, 2] уже описывалась нечеткая модель региона как открытой социально-экономической системы, ее математический аппарат и алгоритмы. Результатом работы разработанной информационной советующей системы является комплекс рекомендаций, позволяющих повысить качество принимаемых управленческих решений для различных уровней управленческий кадров в региональных правительствах.

НЕЧЕТКАЯ МОДЕЛЬ ВЛИЯНИЯ ФАКТОРОВ ВНЕШНЕЙ СРЕДЫ НА СОСТАВЛЯЮЩИЕ РЕГИОНАЛЬНОЙ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

Рассмотрим регион как элемент подсистемы более крупной системы национальной экономики России. В этих целях сформируем последовательность, позволяющую оценить влияние факторов малопрогнозируемой внешней среды F_{ijk} на составляющие региональной социально-экономической системы S_{mn} [3, с. 56]:

1. Формирование классификатора составляющих региональной социально-экономической системы S_{mn}.

2. Формирование классификатора факторов малопрогнозируемой внешней среды F_{ijk}.

3. Проведение экспертного опроса для определения уровня влияния факторов малопрогнозируемой внешней среды F_{ijk} на составляющие региональной социально-экономической системы S_{mn}.

4. Формализация оценок экспертов в виде лингвистических переменных.

5. Определение нечетких подмножеств влияния факторов малопрогнозируемой внешней среды F_{ijk} на составляющие региональной социально-экономической системы S_{mn}.

6. Суммирование нечетких оценок экспертов с целью поиска общей нечеткой оценки и доверительного интервала.

В соответствии с предложенной последовательностью представим регион как социально-экономическую систему, т.е. сложную систему взаимосвязанных и взаимодействующих составляющих и отношений между ними в условиях малопрогнозируемой внешней среды [3,с. 60]:

$$S = \langle \{S_{mn} : \ m,n \in N, 1 \le m \le 7\}, O \rangle, \tag{1}$$

где S – составляющие региональной социально-экономической системы; S_{mn} – n-я составляющая m-й группы региональной социально-экономической системы; N – множество натуральных чисел; O –набор взаимосвязей, определяющий взаимное влияние S_{mn} друг на друга.

Предлагается разбивка всех составляющих социально-экономической системы региона по группам 1-го порядка: S_{1n} – промышленные и производственные составляющие; S_{2n} – общегосударственные цели и политические составляющие; S_{3n} – общеэкономические составляющие региона; S_{4n} – социально-демографические составляющие; S_{5n} – составляющие инвестиционной привлекательности региона; S_{6n} – составляющие инновационного развития региона; S_{7n} – рейтинговые оценки региона. Далее производится разбивка составляющих 1-го порядка на более частные составляющие 2-го порядка S_{mn}.

В связи с изменениями в бизнес-среде особое внимание следует уделить взаимодействию региональной социально-экономической системы с внешней средой. Для определения наличия или отсутствия влияния факторов малопрогнозируемой внешней среды на региональную социально-экономическую систему предложена следующая модель [2]:

$$S_{mn} = f(\langle \{F_{ijk} : i,j,k \ \in N, 1 \le i \le 5\}, V \rangle, G^h = \left\| \left\langle g_{uy}, G^{'}, g^{'} \right\rangle \right\|_{u=1,y=1}^{67\times 65}), \tag{2}$$

$$g^{'} \Leftrightarrow \forall S_{mn} \left[S_{mn} \in S \to S_{mn} = f(F) \right] : m,n \in N, 1 \le m \le 7$$

где S_{mn} – n-ая составляющая m-ой группы региональной социально-экономической системы; F_{ijk} – k-й фактор j-й подгруппы i-ой группы факторов внешней среды; N – множество натуральных чисел; V – взаимосвязь факторов малопрогнозируемой внешней среды F_{ijk} между собой; G^h – матрица размера 67×65, элементами которой являются кортежи, определяющие оценку эксперта направленного воздействия факторов F_{ijk} малопрогнозируемой внешней среды на составляющие региональной социально-экономической системы S_{mn}; g_{uy} – элементы кортежа, описывающие наличие связи между

F_{ijk} и S_{mn}, $G^{'}$ – сила влияния F_{ijk} на S_{mn}, задаваемая лингвистической переменной; $g^{'}$ – направленность влияния F_{ijk} на S_{mn}; F – множество факторов внешней среды F_{ijk}, определяемое как $F = \{F_{ijk} : i, j, k \in N, 1 \le i \le 5\}$.

Отметим, что i-ую группу факторов внешней среды Брянской области можно представить следующим образом: F_1 – политико-правовые, F_2 – экономические, F_3 – научно-технологические, F_4 – социально-демографические, F_5 – природно-географические факторы.

Влияние составляющих социально-экономической системы региона на факторы внешней среды достаточно сложно оценить точным числовым параметром, поэтому для математического описания влияния факторов внешней среды F_{ijk} на составляющие региональной социально-экономической системы S_{mn} и операций с ними используются понятия теории нечетких множеств и нечеткой логики.

В работе предлагается следующий подход: для каждой составляющей S_{mn} влияние всех факторов F_{ijk} определяется в виде лингвистических термов: «низкое влияние», «среднее влияние», «высокое влияние». Значения термов задаются в виде интервалов. В результате обработки ответов экспертов формируется матрица, определяющая силу влияния $G^{'}$.

Термы, определяющие силу влияния $G^{'}$ факторов F_{ijk} на составляющие S_{mn}, могут быть формализованы в виде следующей лингвистической переменной $ЛП_{G^{'}}$:

$$ЛП_{G^{'}} = \left\langle \lambda_{ijk}, P_{ijk}, X_{ijk}, J_{ijk}, V_{ijk} \right\rangle, \quad (3)$$

где λ_{ijk}- название ijk-го фактора внешней малопрогнозируемой среды; P_{ijk} – множество значений $ЛП_{G^{'}}$, представляющее термы: P_{ijk}={«слабое влияние», «среднее влияние», «сильное влияние»}; X_{ijk} – область определения ijk-го фактора внешней малопрогнозируемой среды, задаваемая экспертами; J_{ijk} – синтаксическое правило; V_{ijk} – семантическое правило задания нечетких подмножеств множества X_{ijk}.

Таким образом, представленная нечеткая модель взаимодействия факторов малопрогнозируемой внешней среды на составляющие региональной социально-экономической системы формирует основу для дальнейшей работы по переводу качественных взаимосвязей в точную количественную оценку. Кроме того, сформированный математический аппарат обработки экспертных данных позволит в дальнейшем разработать информационную советующую систему, которая повысит качество принимаемых управленческих решений на разных уровнях региональной власти. Приведем модель региональной социально-экономической системы, функционирующей в условиях малопрогнозируемой внешней среды (рис. 1).

Входными параметрами модели являются изменения во внешней среде, а выходными параметрами – информационная советующая система и управленческие решения, обеспечивающие эффективное управление на разных уровнях региональной власти.

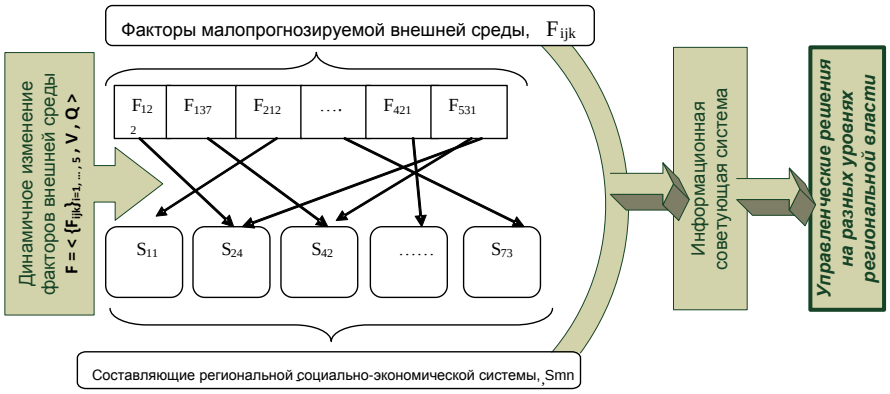

Рисунок 1 – Модель, описывающая взаимосвязь между факторами малопрогнозируемой внешней среды F_{ijk} и составляющими региональной социально-экономической системой S_{mn}

МОДЕЛЬ ИНФОРМАЦИОННОЙ СОВЕТУЮЩЕЙ СИСТЕМЫ

Создаваемую информационную советующую систему можно отнести к подклассу расчетно-диагностических советующих систем, которые называются мониторинговыми, так как основная цель их создания заключается в наблюдении за состоянием каких-либо объектов или процессов, своевременной сигнализации о появлении негативных явлений, оценке последних и выдаче рекомендаций для их ликвидации. Мониторинг изменений, происходящих во внешней среде и влияющих на региональную социально-экономическую систему, будет осуществлять предлагаемая информационная советующая система.

Структурно-функциональная модель разработанного программного комплекса представлена на рисунке 2.

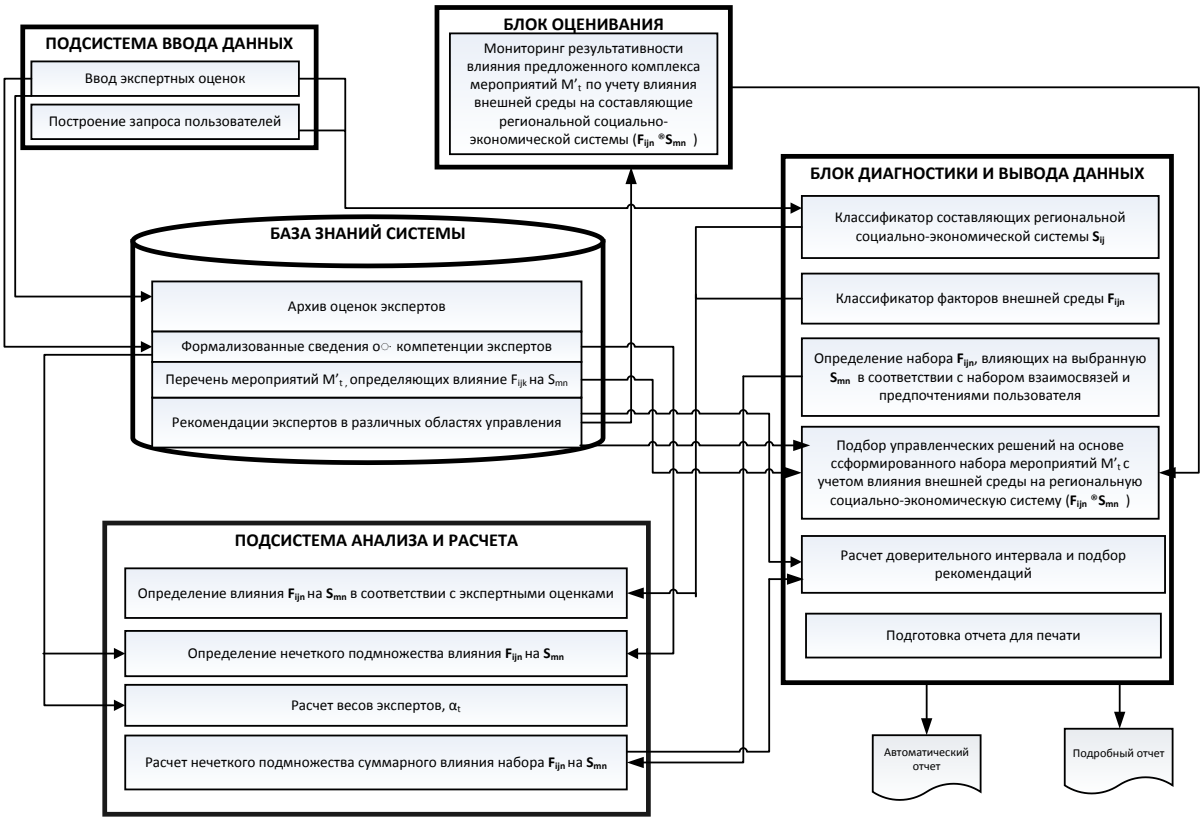

Рисунок 2 – Структурно-функциональная модель информационной советующей системы оценочно-диагностического типа

Подсистема ввода данных отвечает за корректный ввод оценок экспертов, взаимосвязей и построение запроса пользователем. В оценочном блоке представлены процедуры оценки (мониторинга) результативности влияния предложенного комплекса мероприятий ($M_t^{'}$) по учету влияния факторов внешней среды (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}). В блоке диагностики и вывода данных формируются классификаторы факторов внешней среды F_{ijk} и составляющие социально-экономической системы региона S_{mn}. Здесь же осуществляется подбор управленческих решений на основе сформированного набора мероприятий ($M_t^{'}$) с учетом влияния внешней среды на региональную систему. Также в блоке диагностического направления представлены таблицы взаимного влияния факторов внешней среды (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}). Там же формируются отчеты для печати.

Подсистема анализа и расчета программного комплекса состоит из блока процедур, оценивающих влияние F_{ijk} на S_{mn}, блока определения нечеткого подмножества влияния F_{ijk} на S_{mn}, блока процедур, обеспечивающих расчет весов экспертов α_t, а также расчета нечеткого подмножества суммарного влияния F_{ijk} на S_{mn}.

База знаний системы содержит архив оценок экспертов, формализованные сведения о компетенции экспертов, набор мероприятий ($M_t^{'}$), учитывающих влияние F_{ijk} на S_{mn}, а также набор рекомендации экспертов в различных областях знаний. Заполнение базы знаний, используемой при формировании управленческих решений в информационной советующей системе, будет происходить с помощью опытных экспертов – топ-менеджмента промышленных предприятий, представителей региональной власти разных уровней управления, привлекаемых внешних экспертов-консультантов транснациональных консалтинговых агентств. Результатом работы информационной советующей системы будет являться формирование комплекса управленческих решений, позволяющих повысить качество управления на разных уровнях региональной власти.

АЛГОРИТМЫ РАБОТЫ ПРОГРАММНОГО КОМПЛЕКСА

Общий алгоритм работы пользователя с программным комплексом представлен на блок-схеме (рис. 3). Из классификатора факторов внешней среды региона (F_{ijk}), находящегося в блоке диагностики программного комплекса, пользователь выбирает те факторы, которые следует подвергнуть анализу и исследованию. На основе таблиц, представленных в блоке диагностики программного комплекса, определяется влияние факторов внешней среды региона (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}). Далее пользователю предлагается выбрать пары взаимосвязи факторов внешней среды и региональной социально-экономической системы ($F_{ijk} \to S_{mn}$). На основе обращения ко множеству мероприятий ($M_t^{'}$), представленных в базе знаний программного комплекса, определяется возможное значение влияния факторов внешней среды на региональную социально-экономическую систему ($F_{ijk} \to S_{mn}$) как положительное, нейтральное или отрицательное. Данный этап рассмотрен подробнее ниже в виде отдельного алгоритма. Из базы знаний программного комплекса формируется набор мероприятий ($M_t^{'}$) по усилению или снижению влияния факторов внешней среды на региональную социально-экономическую систему ($F_{ijk} \to S_{mn}$).

Некоторые элементы предложенного алгоритма требуют пояснения и представлены ниже в виде отдельных алгоритмов. Так, такой элемент основного алгоритма, как

«Определение влияния факторов внешней среды региона (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn})», представлен на рисунке 4.

Пользователю предлагается выбрать конкретную составляющую региональной социально-экономической системы S_{mn} (классификатор S_{mn}, состоящий из 67 позиций, представлен в блоке диагностики и вывода данных программного комплекса). Проверяется, имеет ли влияние конкретный фактор внешней среды F_{ijk} на выбранную составляющую региональной социально-экономической системы S_{mn} на основе обращения к базе данных в блоке диагностики и вывода данных программного комплекса. Далее формируется нечеткое подмножество влияния F_{ijk} на S_{mn} и последующая сортировка результатов степени этого влияния.

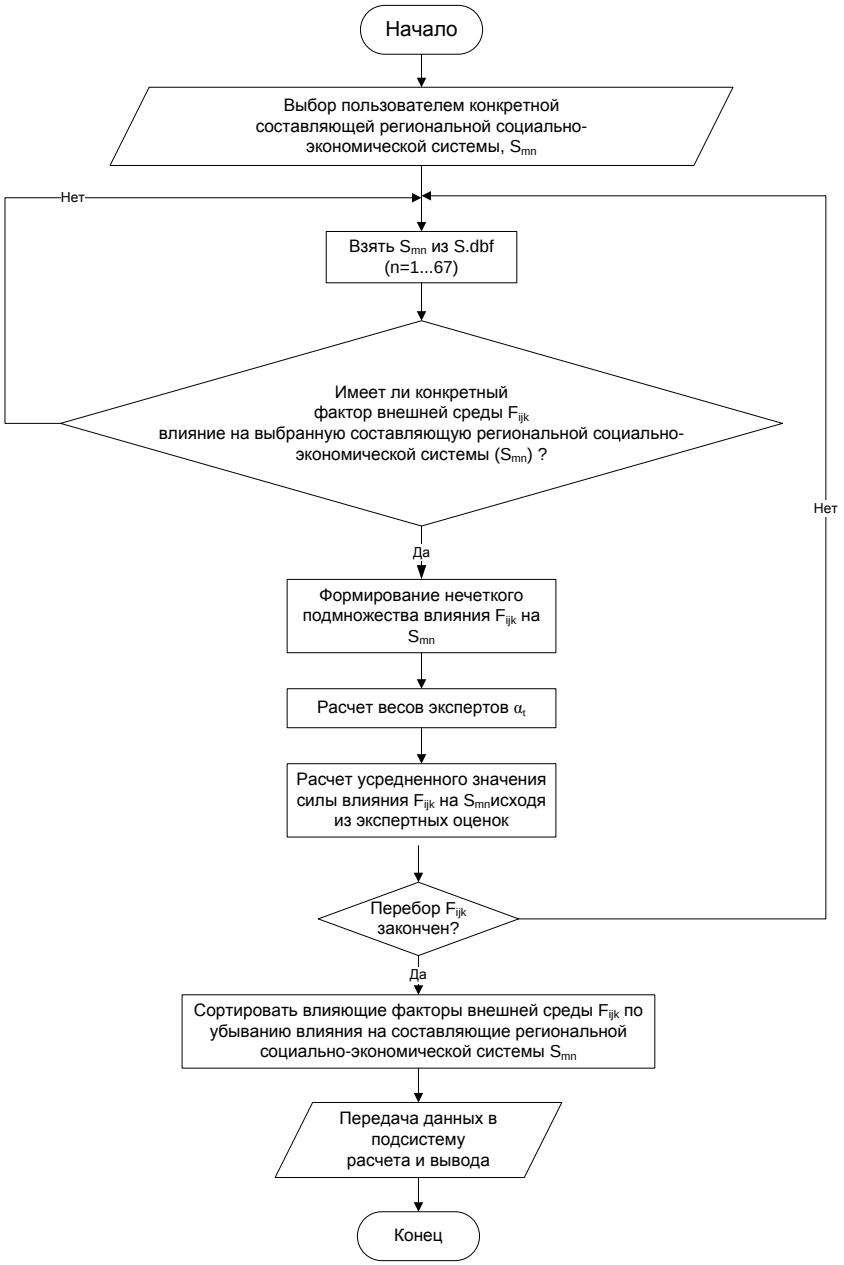

Рисунок 4 – Блок-схема алгоритма определения влияния факторов внешней среды региона (F_{ijk}) на составляющие социально-экономической системы региона (S_{mn}) в соответствии с экспертными оценками

Далее необходимо рассмотреть алгоритм определения суммарного нечеткого подмножества влияния F_{ijk} на S_{mn} (рис. 5).

Для определения суммарного нечеткого подмножества влияния F_{ijk} на S_{mn} формируется запрос значений рассчитанных ранее весов экспертов α_t из базы данных программного комплекса, на их основе производится расчет оценок экспертов A_h. Далее осуществляется расчет вершин b_1, b_2, b_3 и функции принадлежности μ_b лингвистической переменной TR-типа результирующего подмножества B.

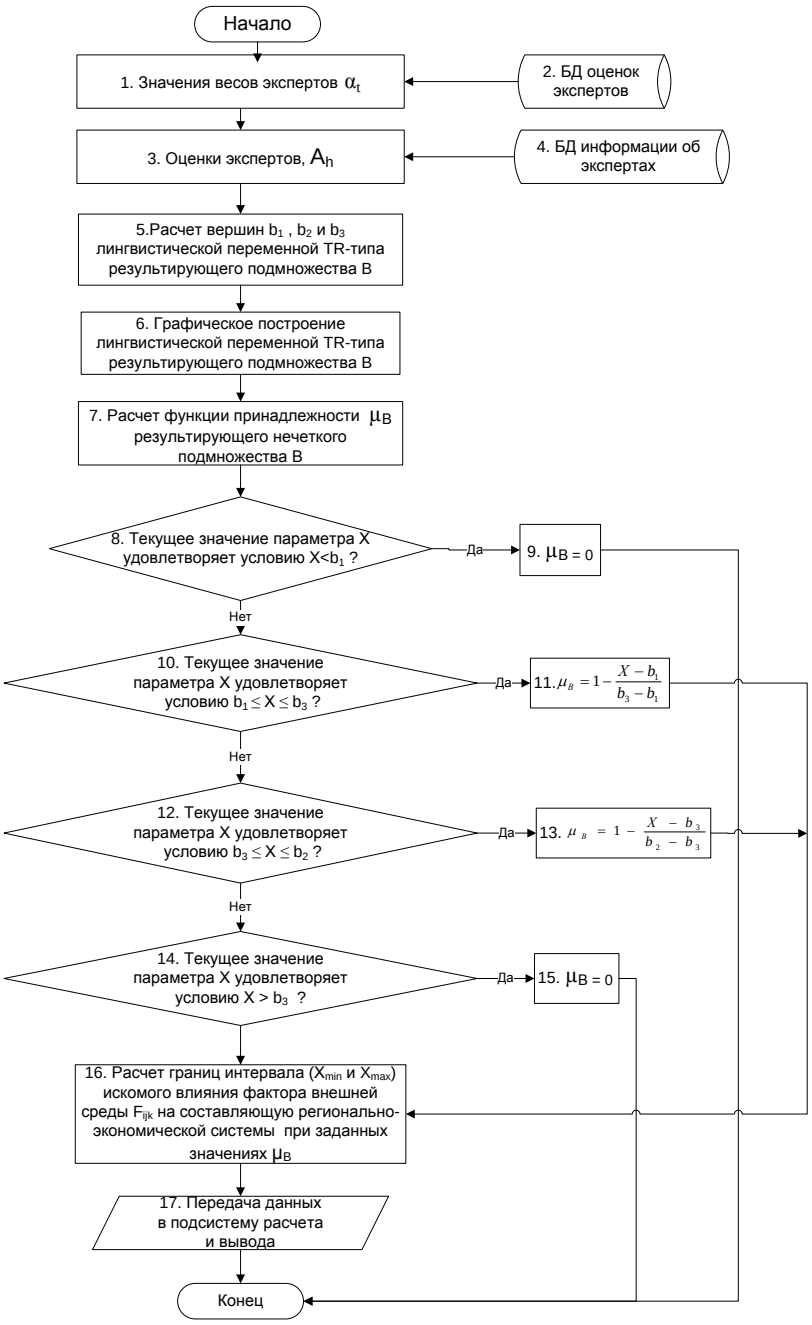

Рисунок 5 – Блок-схема алгоритма определения суммарного нечеткого подмножества влияния F_{ijk} на S_{mn}

Проверка текущего значения параметра X осуществляется на удовлетворение условию $X<b_1$, $b_1 \le X \le b_3$, $b_3 \le X \le b_2$ и $X>b_3$. Производится расчет границ интервала (X_{min} и X_{max}) искомого

влияния фактора внешней среды F_{ijk} на составляющие региональной социально-экономической системы S_{mn} при заданных значениях μ_b.

ЗАКЛЮЧЕНИЕ

Таким образом, предложенные в данной статье алгоритмы работы программного комплекса и его структурно-функциональная модель позволят полно и оперативно управлять данными и информацией, используемой в разрабатываемой информационной советующей системе. Итогом работы программного комплекса станут результаты проводимого мониторинга и выявление тенденций в региональной социально-экономической системе и ее внешней среде. На их основе будут формироваться эффективные управленческие решения, принимаемые на региональном уровне.

СПИСОК ЛИТЕРАТУРЫ

1. Аверченкова Е.Э., Аверченков А.В. Нечеткая модель внутренней среды промышленного предприятия. Экономические системы современной России: теоретические и практические проблемы развития: коллективная монография / под ред. А.Д. Шафронова, Ю.Н. Каткова. – Брянск: Издательство ООО «Новый проект», 2015. – С. 33-55.
2. Аверченкова Е.Э., Аверченков А.В. Особенности управления региональными социально-экономическими системами на основе нечеткой логики (на примере Брянской области). Экономические системы современной России: теоретические и практические проблемы развития: коллективная монография / под ред. А.Д. Шафронова, Ю.Н. Каткова. – Брянск: Издательство ООО «Новый проект», 2015. – С. 55-70.
3. Аверченкова Е.Э., Аверченков А.В. Особенности производственной деятельности малых инновационных предприятий. – Москва: Издательство Московского психолого-социального университета, 2012. – 124 с.
4. Аверченкова Е.Э., Аверченков А.В. Перспективы развития технологического предпринимательства и инноваций на базе российских университетов // Михаило-архангельские чтения: сборник статей VIII международной научно-практической конференции, 15.11.2013. – Рыбница: Издательство Преднестровского государственного университета. – С. 56-59
5. Аверченкова Е.Э. и др. Модель региональной социально-экономической системы, функционирующей в условиях малопрогнозируемой внешней среды для информационной советующей системы (на примере Брянской области) / Е.Э. Аверченкова, А.В. Аверченков, В.К. Черкасов, Д.В. Аксененко // Вестник БГТУ, 2015. – № 1(45). – С. 73-79.
6. Управление социально-экономической системой: монография / под ред. А.П. Егоршина, В.А. Кожина. – Нижний Новгород: НИМБ, 2009. – 288 с.
7. Тарасов Н.А. Стратегические приоритеты региональной экономической политики // Terra Economicus, 2014. – № 1-2. – Т. 8 [Электронный ресурс]. – URL: http://cyberleninka.ru/article/n/strategicheskie-prioritety-regionalnoy-ekonomicheskoy-politiki-1.

Аверченков Андрей Владимирович
ФГБОУ ВПО «Брянский государственный технический университет», г. Брянск
Доктор технических наук, доцент, профессор кафедры «Компьютерные технологии и системы»
Тел.: 8 903 868 58 55
E-mail: mahar@mail.ru

Аверченкова Елена Эдуардовна
ФГБОУ ВПО «Брянский государственный технический университет», г. Брянск
Кандидат технических наук, доцент кафедры «Экономика, организация производства и управление»
Тел.: 8 903 869 13 30
E-mail: lena_ki@inbox.ru

A.V. AVERChENKOV *(Doctor of Engineering Sciences, Associate Professor,*

Professor of the Department «Computer Technologies and Systems»)

E.E'. AVERChENKOVA *(Candidate of Engineering Sciences,*
Associate Professor of the Department «Economy, Organization of Production and Management»)
Bryansk State Technical University, Bryansk

AUTOMATED MANAGERIAL MAKING DECISIONS ON THE BASE OF THE MODELS AND ALGORITHMS OF INFORMATION ADVISING SYSTEM

The development of software is actual In the context of optimization of regional authorities in the Russian Federation. It improves the quality of management decisions at the regional level. The author considers the region of the Russian Federation as a complex social economic system. It is under the influence of various factors of changing environment. Using of automation will improve the efficiency of administrative activity at the regional level. Thus, it was proposed the information advising system model of counting and diagnostic type. There are the its' algorithm. The main purpose of software is the monitoring and detection of positive and negative trends in the dynamically changing regional social and economic system and in the environment. The output parameters of the software are improving the quality of managerial decisions on the regional level.

Keywords: *structural and functional model; algorithms; information and advising system; managerial decisions.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Averchenkova E.E'., Averchenkov A.V. Nechetkaya model' vnutrennej sredy' promy'shlennogo predpriyatiya. E'konomicheskie sistemy' sovremennoj Rossii: teoreticheskie i prakticheskie problemy' razvitiya: kollektivnaya monografiya / pod red. A.D. Shafronova, Yu.N. Katkova. – Bryansk: Izdatel'stvo OOO «Novy'j proekt», 2015. – S. 33-55.
2. Averchenkova E.E'., Averchenkov A.V. Osobennosti upravleniya regional'ny'mi social'no-e'konomicheskimi sistemami na osnove nechetkoj logiki (na primere Bryanskoj oblasti). E'konomicheskie sistemy' sovremennoj Rossii: teoreticheskie i prakticheskie problemy' razvitiya: kollektivnaya monografiya / pod red. A.D. Shafronova, Yu.N. Katkova. – Bryansk: Izdatel'stvo OOO «Novy'j proekt», 2015. – S. 55-70.
3. Averchenkova E.E'., Averchenkov A.V. Osobennosti proizvodstvennoj deyatel'nosti maly'x innovacionny'x predpriyatij. – Moskva: Izdatel'stvo Moskovskogo psixologo-social'nogo universiteta, 2012. – 124 s.
4. Averchenkova E.E'., Averchenkov A.V. Perspektivy' razvitiya texnologicheskogo predprinimatel'stva i innovacij na baze rossijskix universitetov // Mixailo-arxangel'skie chteniya: sbornik statej VIII mezhdunarodnoj nauchno-prakticheskoj konferencii, 15.11.2013. – Ry'bnica: Izdatel'stvo Prednestrovskogo gosudarstvennogo universiteta. – S. 56-59
5. Averchenkova E.E'. i dr. Model' regional'noj social'no-e'konomicheskoj sistemy', funkcioniruyushhej v usloviyax maloprognoziruemoj vneshnej sredy' dlya informacionnoj sovetuyushhej sistemy' (na primere Bryanskoj oblasti) / E.E'. Averchenkova, A.V. Averchenkov, V.K. Cherkasov, D.V. Aksenenko // Vestnik BGTU, 2015. – № 1(45). – S. 73-79.
6. Upravlenie social'no-e'konomicheskoj sistemoj: monografiya / pod red. A.P. Egorshina, V.A. Kozhina. – Nizhnij Novgorod: NIMB, 2009. – 288 s.
7. Tarasov N.A. Strategicheskie prioritety' regional'noj e'konomicheskoj politiki // Terra Economicus, 2014. – № 1-2. – T. 8 [E'lektronny'j resurs]. – URL: http://cyberleninka.ru/article/n/strategicheskie-prioritety-regionalnoy-ekonomicheskoy-politiki-1.

УДК 658.512.6

А.С. БЫЧКОВА, А.Б. НЕЧАЕВА, О.Н. ЛУНЁВА,
Р.А. ЛУНЁВ, А.А. СТЫЧУК, А.Е. ЯСТРЕБКОВ

АКТУАЛЬНОСТЬ РАЗРАБОТКИ СЕРВИСА АВТОМАТИЗАЦИИ СОСТАВЛЕНИЯ ПРОГРАММ ТРЕНИРОВОК С УЧЕТОМ ФИЗИОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЯ

В данной статье показывается актуальность разработки сервиса автоматизации составления программ тренировок с учетом физиологических особенностей пользователя. Описываются проблемы людей, связанные с занятием спортом, и возможные решения этих проблем. Приводятся аргументы о необходимости разработки комплексного решения описанных проблем. Рассмотрены преимущества комплексного решения. Приводится состав функций разрабатываемого сервиса. Показывается необходимость автоматизации каждой из описанных функций сервиса. Показывается необходимость создания сервиса автоматизации составления программ тренировок с учетом физиологических особенностей пользователя.

Ключевые слова: *веб-сервис; комплексное решение; автоматизация; программы тренировок.*

Развитие современного общества, повышение уровня и качества жизни рождает новые тенденции. В последние годы в России начался и идет настоящий бум на здоровый образ жизни. Поход в тренажерный зал или фитнес-клуб стал неотъемлемой частью повседневной жизни многих людей, привнеся в нее яркие краски и положительные эмоции. В нашей стране особое внимание уделяется привлечению молодежи к здоровому образу жизни. Каждый год открываются новые фитнес-центры, поэтому занятие спортом и поход в тренажерный зал становится все актуальнее с каждым днем. Количество занимающихся увеличивается. Спорт удовлетворяет многие психологические и физиологические потребности человека. «Президент России, Владимир Путин, поручил в ближайшие пять лет увеличить число россиян, занимающихся спортом. В ближайшие пять лет число занимающихся спортом россиян должно увеличиться и достигнуть как минимум 40%. Также глава государства отметил, что за последние годы число граждан, регулярно занимающихся спортом, выросло на 6 млн и составляет сейчас около 35 млн человек» – по данным ИТАР-ТАСС.

Разработка сервиса автоматизации составления программ тренировок с учетом физиологических особенностей пользователя является актуальной задачей, потому что сегодня занятия фитнесом и бодибилдингом очень популярны. По данным РОССТАТА, свыше 30 млн человек в России регулярно посещают спортивные залы [1].

Интерес к занятиям в спортивном зале растет с каждым днем. Спорт очень быстро входит в жизнь каждого, кто решает заняться своим телом и включить физические нагрузки в свое расписание. Но приходя в спортзал, новички совершенно не знают, чем им стоит заняться, а человек, занимающийся на протяжении долгого времени, может не получать желаемого результата от своих занятий, и для многих это становится проблемой. Многие желающие заниматься спортом просто боятся прийти в спортивный зал, постоянно откладывая занятия фитнесом или бодибилдингом по причине отсутствия необходимых для этого знаний и навыков. И даже в том случае, если человек все же отважился на поход в спортивный зал, важно не просто заниматься, а заниматься с пользой для здоровья, избегая ненужных травм и ошибок. Необходимо соблюдать огромное количество ограничений, которые индивидуальны для каждого человека и являются результатом особенностей физиологического строения тела занимающегося, его образа жизни, личных предпочтений.

Сегодня подавляющее большинство людей занимается в залах, не уделяя должного внимания составлению тренировочного процесса, это приводит к тому, что через какое-то время люди прекращают занятия спортом по причине отсутствия результатов и, как следствие, мотивации.

Самое распространенное решение этих проблем – это обратиться за помощью к специалисту, чтобы всякий раз, когда потребуется сформировать или изменить диету, комплекс упражнений или распорядок дня, он оказывал квалифицированную помощь. Как показывает практика, подобное решение не очень удобно по целому ряду причин. Во-первых, в условиях столь бурного развития популярности занятий фитнесом и бодибилдингом квалифицированных специалистов просто не хватает. Особенно остро недостаток специалистов ощущается в небольших населенных пунктах. Многим специалистам приходится заниматься сразу с несколькими подопечными, что с ростом числа тренирующихся приводит к снижению качества оказываемой им помощи. Практикуются также удаленные занятия с использованием современных средств коммуникации. Данные средства коммуникации не предназначены для проведения подобных консультаций и в принципе не могут позволить оказывать качественную помощь в этих вопросах. Во-вторых, это дорого. Услуги хороших персональных тренеров за постоянные консультации или сопровождение в течение определенного тренировочного периода могут стоить достаточно больших денег. В-третьих, мало кто будет так сильно заинтересован в конечном результате, как сам тренирующийся. Никто, кроме самого тренирующегося, не чувствует, как реагирует его тело на те или иные виды тренировок, изменения в рационе питания и распорядке дня. Поэтому разработка специализированного сервиса, который позволит в автоматизированном режиме сформировать программу тренировок, определив характерные для пользователя физиологические особенности, составить распорядок дня и рацион питания с учетом личных предпочтений, является актуальной задачей [2].

Сервис автоматизации составления программ тренировок позволит пользователю упростить формирование собственного тренировочного процесса и даст возможность квалифицированным специалистам, тренерам максимально качественно помогать большему количеству подопечных одновременно. Сервис позволит сформировать тренировочный процесс пользователя с учетом его физиологических особенностей и, отслеживая прогресс подопечного, вносить в него корректировки, автоматизируя функции ведения тренировочного дневника, составления программы тренировки, распорядка дня и рациона питания.

Для того, чтобы система автоматизации могла оказывать качественную помощь в занятиях спортом, необходимо реализовать приложение, способное решать вопросы составления программы тренировок, диеты и распорядка дня, с учетом физиологических особенностей пользователя в комплексе. Не секрет, что человек получает энергию и все необходимые для жизнедеятельности элементы из белков, жиров и углеводов. Для построения красивого и здорового тела соотношение БЖУ является одним из ключевых факторов. Так, например, организм склонен запасать жиры (запасник энергии) в стрессовых ситуациях, таких, как, недостаток калорий – голод, или в случае избытка калорий – переедание. В первом случае важно равномерное, с четко заданными интервалами потребление калорий и необходимых питательных веществ, иными словами – диета+распорядок дня. Во втором случае, дабы избежать избытка калорий, необходимы регулярные физические нагрузки, т.е. режим тренировок.

Таким образом, вопросы составления диеты, распорядка дня и программы тренировок необходимо решать в комплексе, только в этом случае возможно достижения успеха в деле построения красивого и здорового тела.

Система автоматизации составления программ тренировок – комплексное решение, позволяющее пользователю шаг за шагом, используя мобильное приложение:

– определить физиологические особенности пользователя или «соматотип», выяснив индивидуальные особенности строения его тела;

– составить распорядок дня с учетом времени тренировок и текущего режима дня пользователя;

– сформировать диету здорового питания, исходя из кулинарных предпочтений пользователя, его потребностей в белках, жирах и углеводах и желаемого количества приемов пищи;

– составить программу тренировок из знакомых и понятных пользователю упражнений с учетом его физиологических особенностей и предпочтений в тренировках;

– изучать опыт других спортсменов в достижении результата.

Определение соматотипа, т.е. генетических особенностей организма спортсмена, является одним из ключевых этапов для формирования и составления правильного тренировочного процесса – выбора стратегии тренировок. Стратегии, которая позволит добиться максимальных результатов в занятиях спортом, отталкиваясь от физиологических предрасположенностей собирающегося в спортивный зал человека. Под соматотипом понимается тип строения тела. Этот термин применяется в системе классификации, в соответствии с которой все люди могут быть отнесены к одному из трех основных типов телосложения. Эндоморфный тип склонен к полноте, мезоморфный обладает крепкой костно-мышечной системой и развитой мускулатурой, а для эктоморфного характерны худощавость и хрупкость. Определение своего соматотипа поможет вам понять, в какой пропорции эти черты сочетаются в вашем организме. Соматотип предполагает наличие у человека определенных качеств. Например, эктоморфы зачастую демонстрируют лучшие аэробные способности, чем эндоморфы, для которых, в свою очередь, характерны лучшие показатели силы и выносливости [3].

В теории говорится о том, что в каждом человеке присутствуют все три соматотипа одновременно – эндоморф, мезоморф и эктоморф, однако один или несколько типов могут быть выражены более ярко, чем другие. Телосложение каждого человека обозначается как кодировка из трех цифр в шкале от «1» до «7» в порядке эндо-мезо-экто. Исследования показывают, что чистых соматотипов не существует, а наиболее частыми являются «3-4-4», «4-3-3» и «3-5-2» [4]. Отсюда можно сделать вывод, что определение соматотипа является важной и достаточно сложной процедурой автоматизации, которая позволит в значительной степени облегчить жизнь желающим заняться спортом.

О пользе соблюдения режима дня написано очень много [5]. У человека, соблюдающего режим дня, организм привыкает к повторяющемуся ритму, становится послушным. Например, привычка человека обедать в одно и то же время приводит к тому, что минут за 10-15 до еды по приказу пищеварительного центра железы желудка рефлекторно выделяют сок – сигнал готовности к приему пищи. Таким же образом организм настраивается к определенному часу на зарядку, тренировку, умственную работу, сон и отдых. Очень важно заранее составить режим дня, определить время тренировок, приемов пищи, время пробуждения и отхода ко сну.

В условиях бешеного ритма жизни включить в свой график занятия спортом может быть непросто [6]. Другая задача из разряда нелегких – распланировать график приема пищи и легких перекусов. Переедание и употребление определенных продуктов может негативным образом отразиться на эффективности тренировки и вызвать расстройства пищеварения, в частности, его замедление, тошноту и рвоту. С другой стороны, если с последнего после тренировки приема пищи прошло более шести часов, то вы можете почувствовать слабость и отсутствие мотивации. Правильный выбор продуктов и времени их употребления очень важен. Плотный завтрак нежелателен перед утренней пробежкой, однако подойдет для бега трусцой в предобеденное время.

Автоматизация составления распорядка дня позволит пользователю экспериментировать со своим распорядком дня для нахождения оптимального сочетания времени приема пищи в дни тренировок и отдыха, а также позволит вести дневник питания и занятий. Также это даст возможность пользователя, записывая, что и когда он ест и как чувствует себя во время тренировок, определить продукты, повышающие его производительность во время тренировки, и продукты, которые делают его тренировки менее продуктивными.

Помимо того, что питаться нужно в одно и то же время, важно, чтобы пища была разнообразной, полноценной по составу: белки, жиры, углеводы, витамины. Одна из стремительно набирающих популярность составных частей здорового образа жизни – правильное питание. Все чаще люди предпочитают здоровую пищу и соблюдают правильный рацион питания. И чтобы добиваться результатов от занятий спортом, правильное питание просто необходимо. Поэтому сейчас активно развивается направление пищевой промышленности по разработке рецептур функционального питания [7].

Автоматизация процесса составления рациона питания позволит не только облегчить процесс подсчета необходимых калорий для достижения тренирующимся поставленной цели – набор мышечной массы, похудение и т.д., но и позволит соблюсти при составлении диеты верное соотношение белков, жиров, углеводов, исходя из физиологических особенностей пользователя – его соматотипа, пола, предпочтений в еде и пр.

На сегодняшний день существует огромное количество формул и методик расчета суточной потребности пользователя в калориях. Автоматизация расчета всех необходимых для этого показателей и параметров позволит пользователю вносить изменения в свой рацион питания по мере необходимости, не прибегая к услугам диетолога. Возможность подбора продуктов из предопределенного специалистами набора облегчит составление диеты.

Существует огромное количество информации, предназначенной для того, чтобы любой желающий мог самостоятельно составить программу тренировок. В процессе составления программы тренировок тренирующийся должен для себя ответить на большое количество вопросов и учитывать огромное количество факторов. Вот наиболее важные из них:

– пол и возраст пользователя – существуют серьезные различия для занятий в спортивном зале между мужчинами и женщинами;

– соматотип пользователя – учет особенностей физиологического строения пользователя с целью более эффективного подбора упражнений для пользователя, количество их повторения и рабочих весов;

– цель занятий пользователя в зале – в зависимости от цели занятий формируются различные тренировочные программы как с разным набором упражнений, так и с разным количеством повторений в рамках одного упражнения, различными рабочими весами, временем отдыха между упражнениями и т.д.;

– набор упражнений и порядок их следования в тренировочной программе – важно выбрать верные упражнения на нужные группы мышц, не ошибиться в порядке их следования и технике выполнения.

Помимо выше названных факторов, существует еще огромное количество различных нюансов, требующих учета при составлении программы тренировок, которые в равной мере могут быть отнесены к тому или иному фактору, требующему учета. Это:

– количество подходов и количество упражнений на отдельную группу мышц;

– выбор типов упражнений или типов нагрузки;

– скорость выполнения упражнений и порядок их выполнения;

– отдых между тренировками, оптимальное время продолжительности в зависимости от типов тренировки;

– лучшее время для тренировок, методики тренировок в фитнесе и бодибилдинге и т.д.

Важной составляющей в достижении результата при занятиях в спортивном зале является дневник тренировок, в котором отмечается вся необходимая информация, на основании которой делаются выводы о внесение корректировок в программу питания, режим дня, программу тренировок. Несомненно, автоматизация процесса составления программы

тренировок и ведения тренировочного дневника сильно облегчит жизнь желающим заниматься спортом, которые не решаются прийти в спортивный зал.

Таким образом, с учетом распространения и популяризации здорового образа жизни, разработка сервиса автоматизации составления программ тренировок с учетом физиологических особенностей пользователя является актуальной задачей. С помощью сервиса решается задача автоматизированного составления программ тренировок, формирование рациона питания, определения соматотипа пользователя, составления распорядка дня. Данный сервис поможет пользователю упростить формирование собственного тренировочного процесса, а также даст возможность специалистам оказывать квалифицированную помощь занимающимся. В разрабатываемом сервисе вопросы составления диеты, распорядка дня и программы тренировок решаются в комплексе, что позволит оказывать более качественную помощь в достижении успеха в построении красивого тела и поддержании своего здоровья. Разработка сервиса автоматизации составления программ тренировок позволит перейти на качественно новый уровень использования сервисов по автоматизированному составлению программ тренировок.

СПИСОК ЛИТЕРАТУРЫ

1. Лунев Р.А., Бычкова А.С., Тарасов А.О. Сервис автоматизации составления программ тренировок с учетом физиологических особенностей человека // Сборник докладов IV Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных в образовании, науке и производстве» (ТИМ’2015). – Екатеринбург: УрФУ, 2015. – С. 188-191.
2. Лунев Р.А. и др. Сервис автоматизации составления программ тренировок с учетом физиологических особенностей человека как электронная услуга населению / Р.А. Лунев, В.Н. Волков, А.А. Стычук, А.С. Бычкова // Научные ведомости БелГУ. Серия «Экономика. Информатика». – Белгород: НИУ «БелГУ». – Издательский дом «Белгород», 2015. – № 7(204). – Выпуск 34/1. – С. 132-136. – ISSN 2411-3808.
3. Программа тренировок для женщин в тренажерном зале [Электронный ресурс]. – URL: http://sportwiki.to/Программа_тренировок_для_женщин_в_тренажерном_зале.
4. Somatotype and constitutional psychology, source [Электронный ресурс]. – URL: http://en.wikipedia.org/wiki/Somatotype_and_constitutional_psychology.
5. Режим дня и его польза [Электронный ресурс]. – URL: http://www.zoonoz.ru/rezhim-dnya.php.
6. Health|HowStuffWorks [Электронный ресурс]. – URL: health.howstuffworks.com.
7. Лунева О.Н., Зегелева В.В. Функциональные продукты, направленные на снижение холестерина // V Международная научно-практическая конференция молодых ученых «Основные перспективы развития пищевой инженерии и гигиены питания», ОрелГИЭТ, 25-26 мая 2015 года. – С. 23-25.

Бычкова Анастасия Сергеевна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент-магистрант УНИИ ИТ
Тел.: 8 (4862) 42-36-12
E-mail: anastasiya@skb-it.ru

Нечаева Анастасия Борисовна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент-магистрант УНИИ ИТ
Тел.: 8 (4862) 42-36-12
E-mail: nechaeva@skb-it.ru

Лунёва Ольга Николаевна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат технических наук, доцент, доцент кафедры «Технология и товароведение продуктов питания»

Тел.: 8 (4862) 41-98-99
E-mail: olga_lu@list.ru

Лунёв Роман Алексеевич
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат технических наук, доцент, директор НОЦ ФиПИТ
Тел.: 8 920 287 79 85
E-mail: rolu@yandex.ru

Стычук Алексей Александрович
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат технических наук, доцент, заместитель директора ресурсного центра информатизации образования по научно-методической работе
Тел.: 8 (4862) 43-49-56
E-mail: stichuck@yandex.ru

Ястребков Артём Евгеньевич
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Аспирант УНИИ ИТ
Тел.: 8 (4862) 42-36-12
E-mail: nerlin@skb-it.ru

A.S. BY'ChKOVA (*Master Student of Educational and Research Institute of Information Technologies)*

A.B. NEChAEVA *(Master Student of Educational and Research Institute of Information Technologies)*

O.N. LUNYoVA *(Candidate of Engineering Sciences, Associate Professor,*
Associate Professor of the Department «Technology and Commodity Research of Food»)

R.A. LUNYoV *(Candidate of Engineering Sciences, Associate Professor,*
Director of Research and Education Center «Fundamental and Applied Information Technologies»)

A.A. STY'ChUK *(Candidate of Engineering Sciences, Associate Professor,*
Deputy Director of Resource Center of Informatization of Education on Scientific and Methodological Work)

A.E. YaSTREBKOV *(Post-graduate Student of Educational and Research Institute of Information Technologies)*
Orel State University named after I.S. Turgenev, Orel

THE DEVELOPMENT ACTUALITY OF AUTOMATIZED SERVICE OF TRAINING PROGRAM CREATION WITH TAKING INTO ACCOUNT USER PHYSIOLOGICAL FEATURES

This research paper shows the development actuality of automatized service of training program creation with taking into account user physiological features. It describes physical activity problems and solutions to them. The paper brings arguments for development of complex solutions to described problems, discusses advantages of complex solution. It enumerates the list of functions of service that will be developed, shows the need of automation of described service functions. In this paper showed the need of automatized service of training program creation that would take into account user physiological features.

Keywords: *web-service; complete solution; automation; training programs.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Lunev R.A., By'chkova A.S., Tarasov A.O. Servis avtomatizacii sostavleniya programm trenirovok s uchetom fiziologicheskix osobennostej cheloveka // Sbornik dokladov IV Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molody'x uchyony'x v obrazovanii, nauke i proizvodstve» (TIM'2015). – Ekaterinburg: UrFU, 2015. – S. 188-191.
2. Lunev R.A. i dr. Servis avtomatizacii sostavleniya programm trenirovok s uchetom fiziologicheskix osobennostej cheloveka kak e'lektronnaya usluga naseleniyu / R.A. Lunev, V.N. Volkov, A.A. Sty'chuk, A.S. By'chkova // Nauchny'e vedomosti BelGU. Seriya «E'konomika. Informatika». – Belgorod: NIU

«BelGU». – Izdatel'skij dom «Belgorod», 2015. – № 7(204). – Vy'pusk 34/1. – S. 132-136. – ISSN 2411-3808.
3. Programma trenirovok dlya zhenshhin v trenazhernom zale [E'lektronny'j resurs]. – URL: http://sportwiki.to/Programma_trenirovok_dlya_zhenshhin_v_trenazhernom_zale.
4. Somatotype and constitutional psychology, source [E'lektronny'j resurs]. – URL: http://en.wikipedia.org/wiki/Somatotype_and_constitutional_psychology.
5. Rezhim dnya i ego pol'za [E'lektronny'j resurs]. – URL: http://www.zoonoz.ru/rezhim-dnya.php.
6. Health|HowStuffWorks [E'lektronny'j resurs]. – URL: health.howstuffworks.com.
7. Luneva O.N., Zegeleva V.V. Funkcional'ny'e produkty', napravlenny'e na snizhenie xolesterina // V Mezhdunarodnaya nauchno-prakticheskaya konferenciya molody'x ucheny'x «Osnovny'e perspektivy' razvitiya pishhevoj inzhenerii i gigieny' pitaniya», OrelGIE'T, 25-26 maya 2015 goda. – S. 23-25.

УДК 623.618:004:369(470+470.345)

Л.И. ЕФРЕМОВА

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПЕНСИОННЫМ ФОНДОМ РФ В Г.О. САРАНСК РЕСПУБЛИКИ МОРДОВИЯ

Статья посвящена модернизации автоматизированной информационной системы УПФР в г.о. Саранск. Обоснованы причины модернизации, сформулированы принципы, на которых базируется совершенствование информационной системы. Особое внимание уделяется одной из функциональных подсистем – системе персонифицированного учета, в частности, улучшению работы ее электронного архива за счет реализации программы Cognitive Technologies.

Ключевые слова: *пенсионный фонд РФ; система персонифицированного учета; автоматизированная информационная система; программно-технический комплекс; электронный архив персонифицированного учета.*

Пенсионный фонд РФ (ПФР) – одна из немногих вертикально интегрированных структур в современной российской власти. Его органы доходят до уровня районов во всех субъектах Российской Федерации, сохраняя отношения субординации. Это дает возможность осуществлять единую стратегию управления пенсионной системой на всем социальном пространстве России и доставать до самых отдаленных ее уголков.

Современная корпоративная сеть управления пенсионным фондом РФ (УПФР) в г.о. Саранск обеспечивает функционирование электронного документооборота и хранение данных для персонифицированного учета в единой базе, что позволяет наладить эффективное взаимодействие между управлениями и отделением. Корпоративная сеть связана мощными магистральными каналами связи, но постоянно обновляемая информация, рост внешних запросов и появление новых функций требует от линий связи все большей пропускной способности. Необходимо отметить проблемы, связанные с издержками на обработку информации.

В условиях постоянного взаимодействия УПФР с различными организациями необходима дружественная гибкая информационная система (ИС), позволяющая работать по единым стандартам к безопасности и к технике. Базовыми требованиями к системе являются: применение промышленных платформ для формирования модулей системы; обеспечение независимости данных от прикладных программ; расширяемость и адаптивность; графический интерфейс пользователя; использование современных методов и средств защиты информации; проблемная ориентация и соответствие системы классу решаемых задач; соответствие уровня решаемых задач уровню руководства; модульность построения системы; системность построения, предполагающая, что отдельные модули должны быть интегрированы в общую систему [1]. Такая ИС позволит сократить расходы человеческих и финансовых ресурсов, уменьшить временные затраты на обработку различных запросов, даст возможность оперативно вносить изменения.

Сегодня АИС ПФР использует несколько десятков приложений, которые поддерживаются в централизованном режиме. Кроме того, на уровне региона в инициативном порядке разрабатывались собственные приложения, количество которых далеко перевалило за сотню. Совместно работающие приложения обмениваются сообщениями по принципу «каждый с каждым» и нередко дают сбои в силу сложности в интеграции. Одна из проблем АИС ПФР состоит в том, что составные части системы создавались в разное время. В создании системы участвовало большое количество подрядчиков, данный процесс проходил в условиях отсутствия единых технологических стандартов и регламентов, что привело к созданию системы, состоящей из разнородных,

слабо интегрированных и трудно совместимых компонентов. Такие подсистемы не отвечают требованиям гибкости и системности.

Также наблюдаются проблемы и из-за разных программно-технических средств, которые используются в работе УПФР. Эти проблемы затрагивают и системное администрирование, и обновление программного обеспечения. Избежать конфликтов возможно, если использовать однотипное и стандартное программное обеспечение внутри всей структуры УПФР.

Постоянные изменения в законодательстве РФ, экономическая нестабильность, регулярный рост и обновление информационной базы требуют укрепления материально-технической базы, модернизацию и постоянного совершенствования ИС. Существенные перемены в правовом пространстве пенсионной системы и принимаемые в ПФР решения по улучшению бизнес процессов привели к необходимости совершенствования информационной системы.

АИС ПФР претерпевает кардинальные изменения, приспосабливаясь под изменения во внешней среде страны. Экономическая, правовая, политическая, налоговая и множество других сфер имеют прямое и косвенное влияния на пенсионную систему. Следовательно, необходима такая АИС, которая позволит быстро и качественно вносить все необходимые изменения в любой компонент и в любую программу.

Для повышения эффективности выполнения задач УПФР необходимо балансировать вычислительную нагрузку. Неоптимальное использование сетевого трафика порождают простои в работе системы. Оптимизация трафика будет необходима при внедрении сторонних приложений, интеграция подобных «внесистемных» решений допустима, но не оптимальна. Подобные решения порождают ряд проблем при администрировании и мониторинге системных ресурсов.

Немаловажной проблемой УПФР считается обеспечение информационной безопасности. Сегодня активно идут процессы информатизации различных сфер государственного и муниципального управления, разрабатываются и внедряются автоматизированные ИС в области административного планирования, учета и контроля, к которым относятся многочисленные системы персонального учета (СПУ) населения. СПУ содержит строго конфиденциальную информацию – персональные сведения застрахованных лиц. Такая информация подлежит мощной защите от несанкционированного доступа. Меры безопасности персональных данных включают информационные технологии и технические средства, позволяющие обрабатывать данные с использованием средств автоматизации в безопасном режиме. Особенную актуальность проблема безопасности ИС ПФР приобретает сегодня, поскольку внедрение новых информационных технологий позволяет собирать, обобщать и разъяснять массивы данных, накапливать их и передавать без ведома граждан.

В целях защиты ИС УПФР была разработана подсистема информационной безопасности, которая обеспечивает единую структуру идентификации и аутентификации, авторизацию доступа к ресурсам системы, целостность и защиту данных от несанкционированного доступа. При обнаружении любых несанкционированных действий лицо, отвечающее за безопасность информации (оператор), должно блокировать данные, подвергшиеся атаке. Для информационной безопасности в УПФР используются программные продукты, криптографические подписи, шифровальные средства.

Модернизация существующей на базе УПФР информационной системы обоснована расширением возможности для граждан в оперативном режиме пользоваться госуслугами, следовательно, повышается эффективность функционирования госорганов в части получения дополнительных сведений о статистических показателях необходимых для принятия стратегических решений. Построение гибкой и масштабируемой технологической инфраструктуры, на базе которой будут работать функциональные подсистемы, обеспечит высокую скорость доступа к информационным ресурсам, автоматизирует предоставление госуслуг в удаленном режиме, упростит технологические и административные процессы.

На сегодняшний день тактической задачей, необходимой для создания гибкой и масштабируемой технологической инфраструктуры, на основе которой можно будет обеспечить оперативную интеграцию существующих и создание новых информационных подсистем, является создание единого информационного пространства, которое позволит оперативно получить доступ к информационным ресурсам УПФР, автоматизировать процессы выполнения госфункций и госуслуг, относящихся к компетенции УПФР, и упростить административные и технологические процедуры.

Совершенствование ИС базируется на различных принципах:

– принцип однократного ввода и многоразового использования информации. Данный принцип необходим для программно-технического комплекса (ПТК) СПУ, так как вся информация, которая содержится в БД СПУ, хранится долгое время, а при однократном вводе меньше риска допустить ошибку в данных;

– принцип централизации и консолидации вычислительных мощностей и информационных ресурсов. Централизованная система сократит затраты на обслуживание информационной инфраструктуры, способствует ее упрощению, повысит управляемость. Данный принцип целесообразно использовать при модернизации ПТК СПУ;

– принцип единства, который поддерживает методологическое, техническое, общесистемное и информационное единство в ИС ПФР. Все системы в ПФР имеют функциональную связь и при модернизации любой из них приходится вносить изменения в связанную компоненту.

Модернизация, прежде всего, должна коснуться СПУ. Следует отметить, что архитектура системы персонифицированного учета построена на трех уровнях: федеральном, региональном и районном. Каждый уровень оснащен ПТК СПУ, соответственно, комплексы различаются между уровнями, т.к. на каждом уровне информация проходит различные преобразования. Сбор информации происходит на районных уровнях, обработку и проверку сведений проводят на уровне региона, после чего все сведения отправляются на дальнейшее хранение на сервер, который находится на федеральном уровне. Анализ ПТК СПУ проводился на региональном уровне. Подсистема персонифицированного учета является одной из самых первых подсистем, разработанных в ПФР, она сформировалась в 1996 году. Информационные ресурсы данной подсистемы являются базой для формирования пенсионных накоплений работающего населения. Первоочередное совершенствование данной подсистемы должно касаться части интеграции, т.к. ПТК «Система персонифицированного учета» является одним из самых используемых за пределами ПФР. Предоставление необходимой информации налоговым службам, Росреестру, фонду медицинского страхования не обходится без данной системы. Но зачастую интеграция является «односторонней», если сделать систему более «дружественной», можно обойти многие проблемы взаимодействия. Если начать анализ ситуации с внешней стороны, то необходимо внести изменения в интерфейсную часть программы для внесения любых изменений в части интерфейса.

В плане совершенствования интерфейсной части программы наши предложения заключаются в следующем. УПФР должна располагать программами с открытым кодом, т.е. в любое время должна иметься возможность вносить изменения в программу. Данная возможность позволит не менять программный продукт целиком, а модернизировать его локально. Таким образом, при интеграции с любой сторонней программой мы открываем конфигурацию программы, вносим необходимые для взаимодействия программ изменения и успешно интегрируем приложение. При завершении работы с той или иной организацией либо при изменении условий функционирования можно в любой момент времени сделать бэкап системы. Такая возможность представляется при работе с программой с открытым кодом, в который мы можем самостоятельно вносить изменения.

Еще один вариант модернизации – присоединение дополнительного модуля к ИС. В этом случае в существующую ИС не требуется вносить никаких изменений, изменения будут

происходить при прохождении данных через дополнительный модуль. Мы предлагаем включить специализированный программный модуль, который будет запускаться лишь при обнаружении файлов формата «.jpg» и форматировать отсканированные документы в формат «.odt». Такое решение даст возможность разгрузить основную программу.

Совершенствование интеграции ПТК «Система персонифицированного учета» с электронным архивом персонифицированного учета (ЭАПУ) мы рассматриваем на основе предоставления прямого доступа к БД системы. ЭАПУ является составной частью ПТК «Система персонифицированного учета», он отделился от данной системы при поступлении в БД документов различного вида. Поступление документов предполагается в трех видах: бумажные документы, бланки и электронные документы. Современная АИС предполагает использование лишь электронного документооборота, однако для УПФР бумажные документы необходимы, и отказаться от данного вида документооборота не предоставляется возможным. ЭАПУ приводит все документы к единому виду. Но при систематических изменениях ПТК «Система персонифицированного учета» ЭАПУ остается неизменным, поэтому возникают проблемы в интеграции, возникают ошибки во взаимодействии, понижается отказоустойчивость электронного архива, наблюдается потеря данных. Решением перечисленных проблем, на наш взгляд, может являться предоставление прямого доступа к БД СПУ. Данное решение не предполагает внесения кардинальных изменений, т.к. обе системы реализованы на единой платформе IBM AS/400 с СУБД DB2/400. Обе системы физически работают на одном и том же сервере. ЭАПУ предполагает обращение к БД СПУ в режиме чтения, т.е. дублирование и несогласованность функций систем исключается. Безопасность данных в БД обеспечивается мощными программными средствами, поэтому любое изменение не останется незамеченным. Синхронизация данных будет осуществляться с минимальными затратами мощности и временными издержками.

В плане совершенствования работы электронного архива мы предлагаем внедрить программу компании Cognitive Technologies. Комбинация систем автоматизации документооборота и систем управления электронными документами обеспечивает полную автоматизацию работы с документами [2]. Данный электронный архив уже внедрен в центральном аппарате ПФР, но его нет в УПФР г.о. Саранск. Для оптимизации вычислительной мощности необходимо создание конфигураций электронного архива на уровне региона, межрайонного уровня и района. Данные решения необходимо интегрировать между собой. Внедрив решение Cognitive Technologies, в УПФР г.о. Саранск будет осуществлена комплексная автоматизация ввода информации с документов СПУ, заполненных вручную, включающая в себя:

- разработку машиночитаемых форм различных типов документов СПУ;
- реализацию потокового сканирования с использованием высокопроизводительного промышленного сканера;
- автоматизированную сортировку по типам входящих документов;
- автоматическую комплектацию многостраничных документов;
- автоматическое распознавание;
- средства коррекции результатов распознавания и визуального контроля;
- экспорт данных в базу данных ПФР, полученных в процессе распознавания;
- автоматическое формирование статистической отчетности о результатах работы системы.

Электронный архив фирмы Cognitive Technologies для ПФР включает в себя четыре основные подсистемы, связанные друг с другом: подсистема ввода, подсистема безопасности, подсистема архивации, подсистема статистики и анализа. Определенная независимость подсистем и их внутренняя архитектура дают возможность гибкого конфигурирования как используемого оборудования, так и самих подсистем.

Система электронного архива строится по принципу гибкой масштабируемости. Без изменения технологического процесса обработки информации в систему могут быть

добавлены (изъяты) технические средства в зависимости от конкретной ситуации. К системе автоматически подключается необходимое количество станций распознавания (редактирования) при увеличении нагрузок (количества обрабатываемых документов в день). В обычном режиме архив обрабатывает до нескольких тысяч документов в день.

Повышение отказоустойчивости БД УПФР будет достигнуто за счет выгрузки всей нагрузки на электронный архив, объем которого позволяет заносить до 30 млн документов в год, а мощная защита информации позволит избежать потери и изменения информации. Информационная безопасность архива обеспечивается за счет наличия в его составе средств, обеспечивающих конфиденциальность работы с информацией. Осуществляется шифрование всей конфиденциальной информации, выводимой на внешние носители. Четко сформулированы разграничения полномочий доступом к информации на основе трехмерной матрицы. Для каждого пользователя системы определяются объекты (программы, данные, устройства), к которым он имеет доступ и полномочия (открытие, сохранение, копирование, просмотр и т.д.) доступа. Подсистема управления доступом контролирует доступ субъектов к операциям шифрования и криптографическим ключам.

Программно-аппаратные средства обеспечивают целостность системы. Целостность программного продукта проверяется автоматически при инсталляции системы и выводится сообщение о результатах проверок на экран монитора. При загрузке системы обеспечивается целостность программного обеспечения, целостность средств защиты информации от несанкционированного доступа, целостность записей в базу данных. Следует отметить, что ошибочные действия пользователей и обслуживающего персонала не нарушают работу средств защиты информации. Обязательным условием формирования системы является дублирование ПТК и оперативный переход на резервные компоненты. Предусматривается также возможность дублирования средств защиты информации ведением двух копий БД и периодического обновления этих средств с контролем их работоспособности.

Такой электронный архив обязателен для новой системы ПФР, она гибкая и интегрируемая, есть широкие возможности для взаимодействия с различными государственными органами, использующими информационную базу ПФР, т.е. электронный архив будет автоматизировать работу СПУ не только внутри ПФР, но и активно взаимодействовать с внешней средой организации.

Таким образом, модернизация автоматизированной информационной системы УПФР в г.о. Саранск будет способствовать достижению конкурентных преимуществ организации, которые обеспечат его устойчивое функционирование и перспективное развитие в условиях все возрастающих объемов хранимой в БД информации в области персонифицированного учета.

СПИСОК ЛИТЕРАТУРЫ

1. Ефремова Л.И. Формирование информационно-аналитической системы в области энергосбережения // Информационное общество, 2013. – № 3. – С. 49-57.
2. Ефремова Л.И. Формирование корпоративной информационной системы энергетической компании с использованием геоинформационной системы // Информационные системы и технологии, 2014. – № 3(83). – С. 39-43.

Ефремова Лидия Ивановна
ФГБОУ ВПО «Мордовский национальный исследовательский государственный университет имени Н.П. Огарева», г. Саранск
Кандидат экономических наук, доцент, доцент кафедры статистики, эконометрики и информационных технологий в управлении
Тел.: 8 (8342) 29-06-80
E-mail: efremovali@mail.ru

L.I. EFREMOVA *(Candidate of Engineering Sciences, Associate Professor,*

Associate Professor of the Department of Statistics, Econometrics and Information Technologies in Management)
Mordovia National Research State University named after N.P. Ogarev, Saransk

MODERNIZATION OF AUTOMATED INFORMATION MANAGEMENT SYSTEM OF THE RUSSIAN PENSION FUND IN G. O. SARANSK REPUBLIC OF MORDOVIA

The article is devoted to the modernization of the automated information system UPFR in the city of Saransk. Substantiated reasons for modernization, formulated the principles that underpin the improvement of the information system. Particular attention is paid to one of the functional sub – system of personified accounting, in particular, improve the operation of its electronic archive at the expense of implementation of the program of Cognitive Technologies.

***Keywords**: pension fund of the Russian Federation; the system of personified registration; automated information system; software and hardware; electronic archive of personified registration.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Efremova L.I. Formirovanie informacionno-analiticheskoj sistemy' v oblasti e'nergosberezheniya // Informacionnoe obshhestvo, 2013. – № 3. – S. 49-57.
2. Efremova L.I. Formirovanie korporativnoj informacionnoj sistemy' e'nergeticheskoj kompanii s ispol'zovaniem geoinformacionnoj sistemy' // Informacionny'e sistemy' i texnologii, 2014. – № 3(83). – S. 39-43.

УДК 004.353, 004.5

П.В. КАЛИНИН, Ю.Ю. ВОЮЦКАЯ, М.Е. ТАРАСОВ

О ПРИМЕНЕНИИ НЕЙРОИНТЕРФЕЙСА ДЛЯ БЕСКОНТАКТНОГО УПРАВЛЕНИЯ МОБИЛЬНЫМ УСТРОЙСТВОМ

В статье рассматривается вопрос построения устройства, которое способно обрабатывать активности головного мозга и формировать сигналы управления для мобильного устройства на платформе «Андроид».

***Ключевые слова**: нейроинтерфейс; приложение для мобильного устройства.*

ВВЕДЕНИЕ

Головной мозг человека состоит из огромного числа клеток – нейронов, которые способны возбуждаться, т.е. эти клетки способны генерировать электрические импульсы. Активность одного нейрона головного мозга сложно анализировать и интерпретировать, но если такую активность проявляют миллионы клеток, то ее можно получить даже с поверхности головы человека. Такой сигнал называют «сырым», в котором выделяют пять основных диапазонов волн: дельта-волны, тэта-волны, альфа-волны, бета-волны, гамма-волны. Данная классификация позволяет опираться не только на уровень сигнала и частоту, но и на время реакции [1]. Из «сырого» сигнала можно формировать команды для внешних устройств. Устройство, принцип работы которого базируется на преобразовании активности нейронов головного мозга в некую командную систему, получил название нейроинтерфейс.

Данная технология находится в самом начале своего развития и имеет ряд ограничений быстродействия, но в недалеком будущем даст возможность людям управлять не только простейшими предметами, но и техникой и электроникой. Кроме этого, перспективными являются разработки в области коммуникации людей, где информация будет напрямую направляться в мозг собеседника.

В настоящее время темпы развития мобильной индустрии находятся на высоком уровне. Интеграция нейроинтерфейса в данную сферу обозначит новый вектор развития. Поэтому задача применения нейроинтерфейса для управления мобильным устройством является наиболее актуальной, так как открывает путь к новым возможностям человеко-машинного взаимодействия.

Существует ряд организаций, занимающихся разработками в сфере нейроинтерфейсов. Среди этого множества можно выделить американскую компанию NeuroSky. В 2011 году ими был создан продукт MindWave, который завоевал рынок нейроинтерфейсов, так как он является портативным, в отличие от конкурентов (InteractiveProductline, OCZ Technology, EmotivSystems) имеет невысокую стоимость, приятный внешний вид и высокий потенциал для применения.

ОПИСАНИЕ УСТРОЙСТВА

Изучив возможности нейроинтерфейса, было предложено использовать данную технологию для создания комплекса программно-аппаратных решений для мобильного устройства, отличительной особенностью которого будет возможность бесконтактного управления всеми функциями устройства. Это позволит использовать устройство как обычными людьми, так и людьми с ограниченной подвижностью конечностей, которых инвалидность лишила или ограничила в возможности управлять движениями рук и пальцев, которые не смогут нажать на кнопки или управлять функциями мобильного телефона иным способом.

На рисунке 1 приведена структурная схема устройства, состоящая из трех основных модулей:

1. НейроинтерфейсNeuroSky MindWave.Нейросетевой интерфейс построен на базе специализированной микросхемы (ASIC), производства компании NeuroSky, поставляемой в виде готового модуля TGAM1. Модуль имеет 3 входа EEG (электрод на лбу), REF и GND (электрод на клипсе, размещаемой на ухе). Все электроды подключены экранированным кабелем. Питание модуля 3,3 В формируется DC-DC преобразователем, размещенном на основной плате. Питание гарнитуры от одного элемента AAA напряжением 1,5 В [2];

2. Bluetooth. Являясь беспроводной персональной сетью, Bluetooth связывает в одно целое личные устройства (ноутбуки, мобильные телефоны, мышки, наушники, GPS адаптеры и т.д.). Работает в диапазоне частот 2.4 ГГц, расстояние в зависимости от класса сети может составлять от одного до ста метров[3];

3. Приложение для мобильного устройства на платформе Android. Приложение, которое позволяет бесконтактно использовать все возможности мобильного устройства, получая управляющие сигналы с нейроинтерфейса по средствам беспроводной технологии Bluetooth.

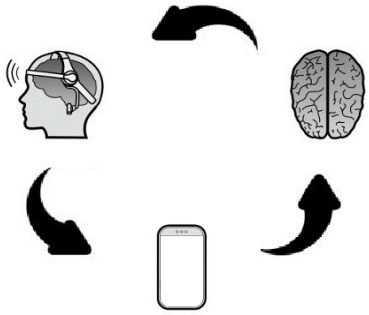

Рисунок 1 – Схема взаимодействия элементов системы

ПРИНЦИП ФУНКЦИОНИРОВАНИЯ УСТРОЙСТВА

Взаимодействие компонентов системы управления заключено в следующие этапы:

1. Получение данных с нейроинтерфейса. Нейроинтерфейс NeuroSky является одноканальным интерфейсом, базирующимся на электроэнцефалограмме головного мозга. В устройстве 2 датчика: один необходим для получения электроэнцефалограммы головного мозга, другой фиксирует отсутствия биоэлектрической активности. Принятый сигнал, разбитый по основным частотным диапазонам, передается интерфейсом на любое устройство, которое будет предусмотрено разработчиками, в зависимости от поставленных целей. Сигнал несет в себе информацию о моргании глаз человека, а также концентрации и медитации.

2. Передача сигналов от нейроинтерфейса по беспроводной технологии Bluetooth до мобильного устройства.

3. Обработка сигнала от нейроинтерфейса. Основываясь на величине сигнала, формируется управляющая команда для мобильного устройства.

Ограниченность состояний обусловлена проблемой распознавания сигнала, который поступает с нейроинтерфейса (передаются следующие данные: сырой сигнал ЭЭГ в диапазоне от 0 Гц до 70 Гц, передается сигнал о моргании глаз (чувствительность может настраиваться) и передаются параметры концентрации (внимательности) и медитации (ментальной релаксации)). У разных людей, которые могут находиться в разных психофизических состояниях в определенные моменты времени (возраст, состояние здоровья) величина сигнала, параметров напряжения и расслабления может варьироваться в определенном диапазоне. Учитывая уровень сложности обучения конечного пользования и уровень возможности точного распознавания сигналов от различных пользователей, была принята схема управления устройством (рис. 2), которая базируется на 7 состояниях:

– четыре состояния обеспечивают передвижение выбранного элемента в четырех возможных направлениях (вверх-вниз, вправо-влево);

– пятое состояние необходимо для перехода системы управления устройством в режим «блокировки» управления устройством;

– шестое состояние необходимо для перехода системы управления устройством в режим «снятия блокировки» управления устройством;

– седьмое состояние формируется в процессе двойного моргания в короткий временной интервал. Речь идет именно о двойном моргании, потому что необходимо исключить обычное (рефлекторное) моргание, которое необходимо для нормального функционирования глазного яблока.

Пользователь в каждый момент выполнения каких-либо действий должен иметь возможность убедиться в том, что все задуманные им изменения свершились. Для реализации этого предусмотрена обратная связь, которая представлена в звуковом и графическом виде. Таким образом, связь в направлении телефон-пользователь не будет значительным образом отличаться от обычного мобильного устройства.

Минусом данного программно-аппаратного комплекса, как и всех устройств, работающих с нейроинтерфейсом, являются трудности в обучении пользователя. Для грамотного использования придется уделить некоторое время для того, чтобы пользователь был способен точно управлять собой (показатель напряжения-расслабления должен соответствовать диапазону, предусмотренному разработчиком).

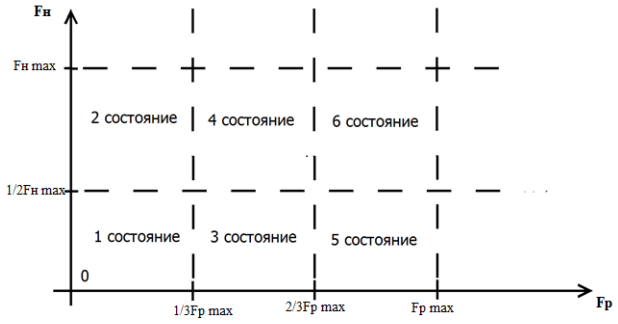

Рисунок 2 – Карта состояний

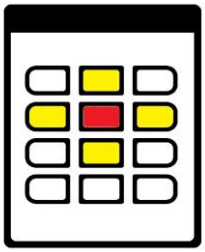

Рисунок 3 – Демонстрация работы состояний 1-4

ВЫВОДЫ

В ходе написания данной статьи были изучены основные особенности функционирования нейроинтерфейса, а также разработана модель управления, основанная на совокупности состояний, которые необходимы для создания программно-аппаратного комплекса для бесконтактного управления мобильным устройством. Говоря об управлении, следует упомянуть о том, что программно-аппаратный комплекс в потенциале дает полную возможность использования как мобильного устройства, включая управление набором символов и номеров, так и больших комплексов устройств, для которых фактор времени не является значимым (например, управление «умным домом»). Для реализации данного программно-аппаратного комплекса необходимо выполнение следующего ряда научных задач:

1. Формализация задачи построения когнитивных пользовательских мультипредметных информационных интерфейсов.
2. Исследование возможности применения нейроинтерфейса для реализации задачи управления синтетической клавиатурой.
3. Разработка механизмов ускорения процесса получения управляющих нейроимпульсов от пользователя.
4. Разработка программно-аппаратного комплекса синтезирования речи с использованием нейроинтерфейса.

СПИСОК ЛИТЕРАТУРЫ

1. Нейроинтерфейсы потребительского класса. Особенности и области применения [Электронный ресурс]. – URL: http://neuromatix.ru/news-ru/neyrointerfeysy-potrebitelskogo-klassa.-osobennosti-i-oblasti-primeneniya.html (дата обращения 24.03.2016).
2. Нейроинтерфейс NeuroSky MindWave [Электронный ресурс]. – URL: http://neurosky.com (дата обращения 24.03.2016).
3. BLUETOOTH – частота, скорость и другая информация [Электронный ресурс]. – URL: http://wireless-on.com.ua/bluetooth.html (дата обращения 24.03.2016).

Калинин Павел Валерьевич
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент
Email: kalinipasha@yandex.ru

Воюцкая Юлия Юрьевна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент
Email: vojulia1@yandex.ru

Тарасов Максим Евгеньевич
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Аспирант
Email: fessmax@gmail.com

P.V. KALININ *(Student)*

Yu.Yu. VOYuCKAYa *(Student)*
Orel State University named after I.S. Turgenev, Orel

M.E. TARASOV *(Post-graduate Student)*
Belgorod National Research University, Belgorod

DEVELOPING AN APPLICATION FOR TOUCHLESS CONTROL OF THE MOBILE DEVICE

The article discusses the issue of building a device that is capable of processing brain activity and generates control signals for the mobile device on the Android platform.

Keywords: *neurointerface; application for mobile devices on the Android platform.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Nejrointerfejsy’ potrebitel’skogo klassa. Osobennosti i oblasti primeneniya [E’lektronny’j resurs]. – URL: http://neuromatix.ru/news-ru/neyrointerfeysy-potrebitelskogo-klassa.-osobennosti-i-oblasti-primeneniya.html (data obrashheniya 24.03.2016).
2. Nejrointerfejs NeuroSky MindWave [E’lektronny’j resurs]. – URL: http://neurosky.com (data obrashheniya 24.03.2016).
4. BLUETOOTH – chastota, skorost’ i drugaya informaciya [E’lektronny’j resurs]. – URL: http://wireless-on.com.ua/bluetooth.html (data obrashheniya 24.03.2016).

УДК 004

Д.С. МИШИН, В.Т. ЕРЁМЕНКО, Я.Д. МИШИН

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ДИАГНОСТИРОВАНИЯ КОМПОНЕНТОВ СИСТЕМ ПОЛУЧЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ В ПОРТАЛАХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

В статье рассмотрена совокупность методов, с помощью которых возможно осуществление процесса диагностирования компонентов автоматизированных систем получения и обработки информации в порталах органов исполнительной власти. Приведены соответствующие этапы, подробным образом раскрывающие суть методов, а также принципы их воплощения и оценка пригодности процесса для полноценной реализации в автоматизированных системах.

Ключевые слова: *получение и обработка информации; диагностирование; процедурный подход; процессорный подход; автоматизированная система.*

ВВЕДЕНИЕ

В современном обществе наблюдается повсеместное развитие и внедрение средств вычислительной техники. Широкое использование информационно-телекоммуникационных технологий потребовало повышение качества и оперативности протекания информационных процессов. Решение этих вопросов стало возможным после разработки и распространения средств автоматизации планирования и управления практически всеми видами деятельности. Специальные комплексы, представляющие собой совокупность программных, технических, информационных, организационно-технологических средств под управлением специалистов получили название автоматизированные системы управления (АСУ).

Одним из основных требований к автоматизированным системам управления, используемым в порталах органов исполнительной власти, является обеспечение бесперебойной работы всего комплекса. Внедрение системы в деятельность любого подразделения или службы сопровождается необходимостью постоянного контроля компонентов, процессов получения и обработки информации. С этой целью для каждого случая разрабатывается методика диагностирования, позволяющая своевременно и качественно контролировать состояние. Проводимый мониторинг позволяет оперативно выявить неисправный компонент, что сокращает сроки устранения неисправностей.

МЕТОДОЛОГИЯ АВТОМАТИЗИРОВАННОГО ДИАГНОСТИРОВАНИЯ ПРОЦЕССОВ ПОЛУЧЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

Методологические основы разработки и создания АС позволяют значительно повысить эффективность современных управляющих систем получения и обработки информации в социальных и экономических системах [1]. Сама по себе методология автоматизированного диагностирования процессов циркуляции информации заключается в совершенствовании стратегии разработки автоматизированных систем контроля технологического процесса, использовании научных методов исследования протекающих процессов, создании математической модели автоматизированных систем, диагностических моделей, методов, алгоритмов и средств обнаружения отказов. Все это в соответствии с принципами диагностики развивается от процесса постановки проблемы и анализа объекта диагностирования до работоспособной модели и эффективных средств диагностирования посредством использования специализированных алгоритмов.

Методология диагностирования процессов получения и обработки информации в автоматизированном режиме основывается на использовании современных научных методов, инженерно-технических подходов и аппаратно-программной реализации. Комплексный подход в диагностировании заключается в (рис. 1):

1) совершенствовании методов технической диагностики и формировании принципов технологической диагностики на основе действующих стандартов;

2) использовании методов процессорного подхода с учетом требований системы менеджмента качества и теории параллельных вычислений;

3) построении теоретико-множественной модели на основе математического описания процесса технологического диагностирования объекта;

4) разработке операторных схем протекающих процессов, основыванных на формальных описаниях и программно-аппаратных средствах автоматизированной обработки и визуализации;

5) формировании диагностических процессов на базе положений теории технической диагностики;

6) разработке процедур диагностирования с использованием методов дискретной математики;

7) широком использованием теории вычислительных систем при создании АСУ с использованием в своем составе аппаратно-программных средств автоматизированных систем диагностики;

8) внедрении АСУ с комплексной оценкой эффективности на основании процедур автоматизированного технологического диагностирования протекающих процессов.

Рисунок 1 – Методология диагностирования в автоматизированном режиме

Характерными чертами циркуляции информации в порталах органов исполнительной власти является многоаспектность (обработка различных информационных потоков), многооперационность, нормируемость, повторяемость, совершенствование процедур, многообразие событий [2]. Основным направлениями в развитии систем диагностики являются процедурный и процессорный подходы.

Использование процедурного подхода является перспективным и определяет следующие направления работ:

– применение традиционных и современных программно-аппаратных комплексов контроля над системами электроснабжения;

– применение BP- и ERP-систем на основе программных платформ;

– контроль и повышение показателей качества протекающих процессов электроснабжения с учетом внедрения системы менеджмента качества.

Эффективность процессорного подхода к системе контроля автоматизированных систем подтверждается внедрением системы менеджмента качества, основывающейся на запросах потребителей и требованиях технических регламентов.

Автоматизированная система получения и обработки информации в порталах органов исполнительной власти включает в свой состав не только технические устройства, но и целый комплекс подсистем, контролирующих информационное, программное, организационное, правовое и лингвистическое обеспечения.

Основу диагностического обеспечения автоматизированной системы диагностики процесса получения и обработки информации составляют описания используемых технологий и процессов. То есть техническая диагностика основывается на знаниях об объекте контроля, сформированных и формализованных в результате исследования. При проведении диагностирования в контролируемом процессе признается отсутствие отказов или сбоев в случае его соответствия совокупности отношений, полученных из модели [3].

Решение задач автоматизированной диагностики циркуляции информации целесообразно основывать на связях между процессами, так как в этих случаях отражаются характерные черты типовых отказов и сбоев, а также повышается вероятность выявления нарушений распределенных во времени.

Обобщенные требования к правильному выполнению мониторинга возможно представить посредством интерпретации фундаментальных свойств алгоритмических систем из [4, 5] в виде требований к процессу получения и обработки информации (табл. 1). Невыполнение этих требований задает список отказов и сбоев.

Таблица 1 – Требования к правильному выполнению мониторинга посредством интерпретации фундаментальных свойств алгоритмических систем

Требования	**Отказы**	**Сбои**
Процесс избирателен: определен на конечном множестве операций и предикатов	Выход значений некоторых технических параметров за пределы допусков	Не выполняется одна из операций из-за незначительных ошибок
Процесс упорядочен: задан технологией, инструкцией, алгоритмом, схемой или иным методом	Нарушение показателей качественных признаков	Нарушение алгоритма работы объекта
Процесс результативен: приводит к требуемому преобразованию исходных материалов в конечную продукцию	Операции не приводят к результату при работоспособном состоянии объекта	Остановка компонента АСУ
Процесс распределен в пространстве	Качественные признаки, указывающие на нарушение нормальной работы объекта	Нарушение работы комплекса средств автоматизации
Процесс своевременен: имеет начало и предельные времена выполнения операций, этапов и всей технологии	В течение заданного контрольного времени не выполняется операция, этап или технология	Нарушение работы комплекса средств автоматизации

Поток операций правильного технологического процесса получения и обработки информации можно выразить в виде следующего соотношения:

$$O_{i,t} \in O_t \subseteq O_t^r \subseteq O, \quad (1.1)$$

где, O – множество операций технологии; $O_{i,t}$ – i-я операция, выполняемая в момент времени t; O_t – подмножество операций, выполняемых в момент t; O_t^r – подмножество операций, для которых готовы все требуемые ресурсы.

Для каждого процесса существует максимально производительный (в терминах параллельных вычислений – параллельный асинхронный) поток операций с выполнение следующего равенства:

$$O_t = O_t^r. \quad (1.2)$$

Основываясь на представленных выражениях, предложим диагностические соотношения в потоке операций для последовательного и параллельного процесса (табл. 2).

Таблица 2 – Диагностические соотношения в потоке операций для последовательного и параллельного процесса

Требования	Отказы	Сбои
$\forall t \exists O_{i,t} \in O_t^r, \lvert O_t \rvert = 1$	$\exists t \exists O_{i,t} \in O_t^r, \lvert O_t \rvert \neq 1$	
$\forall t \exists O_t \in O_t^r, \lvert O_t \rvert \geq 1$	$\exists t \exists O_t \in O_t^r, \lvert O_t \rvert = 0$	

Данный подход позволяет охватить конвейерные процессы, которые являются частностью параллельных процессов с произвольным внутренним параллелизмом и методом управления. К системам с подобным процессом можно отнести большинство АСУ. В то же время накопительный характер отказов и сбоев с высокой вероятностью потерь используемых виртуальных ресурсов значительно повышает актуальность задачи выявления отказов и сбоев, а также неисправностей распределенных во времени [6].

РАЗРАБОТКА ТЕОРЕТИКО-МНОЖЕСТВЕННОЙ ОПЕРАЦИОННО-СОБЫТИЙНОЙ МОДЕЛИ ПРОЦЕССОВ ПОЛУЧЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

Содержательное описание технологий в автоматизированных систем получения и обработки информации включает: назначение и общие параметры; оборудование, программно-технические комплексы и используемые виртуальные ресурсы; состав и характеристики выполняемых операций; параметры управления; связи между виртуальными операциями и процедуры обмена промежуточными результатами; характеристика результата. Формами представления технологий выступают технологические карты, инструкции и т.д., подготовленные в соответствии с действующими нормативными правовыми актами, техническими регламентами, утвержденными руководством и исполняемыми персоналом.

В целях разработки модели технологических процессов представим ее совокупностью упорядоченных операций с управляющими и ресурсными связями (рис. 2). В этом случае O_1 – O_4 – операции технологии, а S и T – координаты пространства и времени.

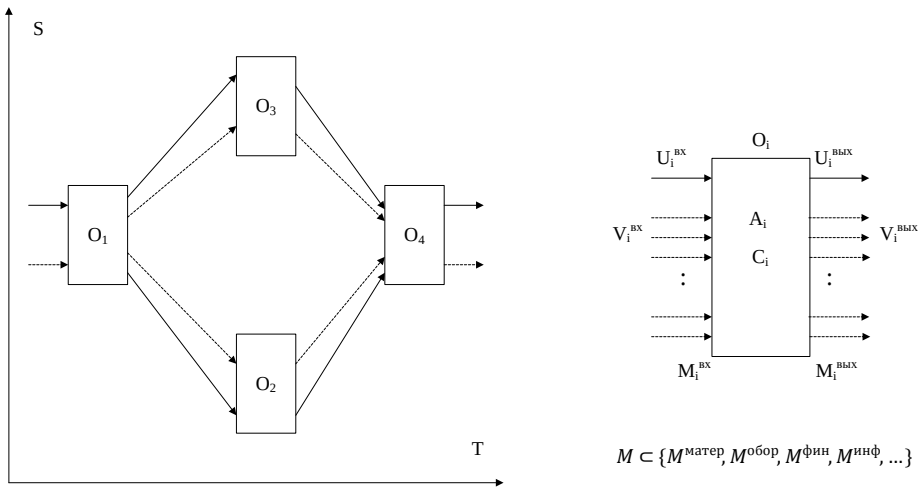

Рисунок 2 – Обобщенная модель технологических процессов получения и обработки информации

Предложим следующие основные множества модели:

– O – множество операций технологии, $O_i \in O$, i – порядковый номер операции, i=1, 2, …, i_k;

– $O \subseteq A \times C \times M$, где A – множество актов операций технологии, $A_i \epsilon A$; C – множество назначений операций, $C_i \in C$; M – множество ресурсов (материальных, финансовых, информационных и др.), используемых в операциях;

– P – множество предикатов, характеризующих условия выполнения технологии, $P_l \in P$, l= 1, 2, …,l_k;

– R – множество связей между операциями, $R = U \cup V$;

– U – множество управляющих связей между операциями, $U \subseteq O \times O \times P$;

– V – множество ресурсных связей между операциями, $V = O \times O \times M$;

– S – множество пространственных координат операций, $S_i \in S$;

– T– множество координат операций во времени, $T_i \in T$.

Используемые символы соответствуют общепринятым терминам operation, predicate, relation, space, time.

Теоретико-множественное представление рассматриваемой технологии (technology) можно отразить следующей моделью:

$$TL =< O, P, R, S, T >. \quad (2.1)$$

В целом оно соответствует содержательному определению технологии представленного в виде типового регламентированного порядка операций (действий) над заданными исходными ресурсными переменными с целью получения конечной информации.

При построении предлагаемой модели целесообразно определить технологию как план процесса получения и обработки информации, а также ввести в создаваемое выражение модели процесса дополнительные множества, например, реализация технологии и события в протекающем процессе. В этом случае модель процесса можно представить в виде следующей функционально-структурной модели:

$$TP =< TL, RL, E >, \quad (2.2)$$

где реализацию RL можно отобразить как

$$RL: TL \times TL \to E, \quad (2.3)$$

где E – совокупность событий, характеризующих процесс получения и обработки информации.

Объединенная модель изменяющихся процессов $ТР^{изм.проц.}$ при фиксированной технологии является множеством моделей, отличающихся по таким компонентам, как реализации и события:

$$TP^{изм.проц.} = \{TP_n\}, TP_n =< TL, RL_n, E_n >, \quad (2.4)$$

где n=1,2,…,n_k – порядковый номер реализации и процессов получения и обработки информации.

В дальнейшем при применении индексации нижние индексы будут обозначать номер элементов во множествах, а верхние – принадлежность к множеству путем указания символа множества или сокращенной русскоязычной записи.

Объединенная модель процессов с изменяемой технологией $ТР^{изм.тех.}$ включает в себя множество моделей, которые различаются по всем компонентам:

$$TP^{изм.тех.} = \{TP_{m.n}\}, TP_{m,n} =< TL_m, RL_{m,n}, E_{m,n} >, \quad (2.5)$$

где m=1,2,…,m_k – порядковый номер технологии.

Представленные выражения (2.2), (2.4) и (2.5) в общем виде отображают АСУ на процессорном уровне и представляют собой систему, которая многократно выполняет заданную технологию в изменяемых условиях жизненного цикла.

Однократная реализация технологического процесса по заданной технологии является уникальной по совокупности событий, параметров и результатов, она обуславливает целесообразность использования представлений (2.1-2.5) для моделирования изменяемых технологий и процессов получения и обработки информации.

Проблемы идентификации и сопоставления реализаций технологии получения и обработки информации целесообразно решать посредством определения и исследования свойств совокупности событий для множества реализаций [7].

Естественным способом определения совокупности событий E_nявляется ее представление в виде активации элементов теоретико-множественного представления (2.1), а именно – изменений в пространстве и времени значений соответствующих признаков:

$$E_n \subseteq g_n \times s_n \times t_n, \quad 2.6)$$

где g_n – множество, включающее признаки активации виртуальных операций, предметов, ресурсов и связей; s_n – множество признаков активации пространственных координат событий; t_n – множество признаков активации временных координат событий.

К признакам активации можно отнести:

- a_i – признак активизации операции, $a_i \in a$;
- p_l – признак активизации предиката, $p_l \in p$;
- u_{ij} – признак активизации управляющей связи, $u_{ij} \in u$;
- v_{ij} – признак активизации ресурсов связи, $v_{ij} \in v$;
- другие признаки в соответствии с основными множествами в (2.1).

Элементарное событие в модели процесса получения и обработки информации можно описатьследующим образом:

$$e_y = (g_i, s_i, t_i), \quad (2.7)$$

где $e_y \in E_n$, y=1,2,…,y_k.

То есть $g_i = a_i$ описывает активизацию i-ой операции.

Введем понятие пространственно-временной реконфигурации для оценки изменений процесса, опираясь на определение конфигурации как взаимного расположения его операций.

Реализация RL_n осуществляется с учетом порядка S_n событий E_n по пространственным координатам и порядок T_nсобытий E_nпо координатам времени.

Конфигурация характеризуется предикатом, указывающим на неизменность порядков при разных реализациях:

$$CF_q(RL_n, S^q, T^q): RL_n \subset RL^q \Leftrightarrow (S_n = S^q) \wedge (T_n = T^q), \quad (2.8)$$

где RL^q – реализации с конфигурацией q.

Конфигурация является мерой оценки изменений в повторяющихся (в течение эксплуатационного цикла АСУ) реализациях технологии получения и обработки информации. При этом отражается совпадение процессов с точностью до взаимного расположения признаков событий.

Конфигурация определяет множество процессов TP^q, совпадающих с точностью до порядков событий, для которых верно соотношение:

$$RL_n \subset RL^q \Leftrightarrow TP_n \subset TP^q. \quad (2.9)$$

Реконфигурация технологического процесса представляет собой упорядоченную пару конфигураций:

$$RC_r =< CF_r, CF_{r+1} >, \quad (2.10)$$

где CF_rиCF_{r+1} – текущая и следующая конфигурации, r=1,2,…,r_k.

Множеством реконфигураций процесса является декартово произведение

$$RC \subseteq CF \times CF, \quad (2.11)$$

где $RC_r \in RC$.

С учетом (2.4) и (2.8) множество реконфигурируемых процессов получения и обработки информации можно представить следующим образом:

$$TP^{\text{рск}} = TP^q \cup TP^{\text{рск.}q}, \quad (2.12)$$

где $TP^{\text{рск.}q}$ – подмножество процессов, реконфигурируемых относительно TP^q.

Анализ существующих методов управления технологическим процессом получения и обработки информациив АСУ отражает их многообразие и возможность совместного применения не только в рамках одной системы, но и для одной технологии. К типовым методам управления процессами можно отнести следующие:

– координатный, указывающий на время и место протекания процесса и его операций;

– событийный, в том числе по готовности виртуальных ресурсов, используемых в операции.

Определим перечень видов реализации технологии в соответствии с методологией и методами управления указанными ранее:

– координатная реализация, когда операции распределены по пространственным и временным координатам;

– алгоритмическая реализация, для которой операции имеют предшественников и последователей по управляющим связям;

– асинхронная реализация в случаях запуска операции по готовности используемых ресурсов либо по факту выполнения операций, поставляющих ресурсы.

Для указанных реализаций введем такие обозначения, как координатная $RL^{\text{коор}}$, алгоритмическая $RL^{\text{алг}}$, асинхронная $RL^{\text{ас}}$ реализации.

Вид модели процесса обозначается с обязательным указанием состава теоретико-множественной модели и технологии типа реализации и состава признака событий. Например, модель процесса выполнения формализованного алгоритма можно представить в виде нотации $TP =< TL(A,U,V), RL^{\text{алг}}, E(a,u,v) >$. При частичном использовании в модели состава признаков событий, например, признаков активности управляющей связи, нотация будет иметь вид $TP =< TL(A.U,V), RL^{\text{алг}}, E(u) >$.

Многовекторная теоретико-множественная модель технологического процесса получения и обработки информации может быть представлена выражением

$$TP =< TL(A,C,M,P,U,V,S,T), RL, E(a,c,m,p,u,v) > \quad (2.13)$$

и по отличительным признакам названа операционно-событийной.

Суть многоаспектности модели заключается в:

– отражении совокупности и отражении операций, методов управления и связи между операциями, пространственных и временных параметров, являющихся компонентами технологического процесса получения и обработки информации;

– описании используемых ресурсов, входящих в технологический базис, посредством включения подмножеств, соответствующих типам ресурсов, к которым можно отнести оборудование, финансы, информацию и т.д. Отсюда можно вывести основные множества:

$$M = M^{\text{обор}} \cup M^{\text{фин}} \cup M^{\text{инф}} \cup \ldots$$
$$V = V^{\text{обр}} \cup V^{\text{фин}} \cup V^{\text{инф}} \cup \ldots$$

Многоаспектность основной модели может сужаться. В этом случае частичные модели формируются по следующим компонентам:

– множества в модели технологии TL;
– подмножества ресурсов и связей в M и V;
– тип реализации RL;
– состав признаков в совокупности событий E.

Возможные варианты состава операционно-событийных моделей процессов получения и обработки информации представлены в таблице 2.1. Возможность различных комбинаций элементов в модели формирования видов моделей можно получить из выражения 2.13 и таблицы 2.1.

Таблица 2.1 – Состав операционно-событийных моделей процессов получения и обработки информации

Элементы модели		**Варианты использования**			
Технология	операции	комплексные	назначения	акты	
	ресурсы	все	выборочно	отсутствуют	
	предикаты	есть	отсутствуют		
	связи	все	управляющие	ресурсные	отсутствуют
	координаты	все	пространства	времени	отсутствуют
реализация		координатная	алгоритмическая	асинхронная	
события		все признаки активности	часть признаков		

Возможность определения соответствий частичных моделей и формальных описаний позволяет говорить об общности моделей. В зависимости от элементов, используемых при построении многоаспектной теоретико-множественной модели технологического процесса (2.13), можно получить следующие модели:

– $TP =< TL(A,C,P,S,T), RL^{\text{коор}}, E(a,c,p) >$ – модель сетевого графика;

– $TP =< TL(A,S,T), RL^{\text{коор}}, E(a) >$ – график Гранта;

– $TP =< TL(A,C,P,U), RL^{\text{алг}}, E(a,c,p,u) >$ – стандартные схемы программ;

– $TP =< TL(A,M,P,V), RL^{\text{ас}}, E(a,m,p,v) >$ – асинхронные вычисления [8].

Предложенная теоретико-множественная многоаспектная операционно-событийная модель предоставляет возможность описать технологический процесс получения и обработки информации на уровне операций, связей и координат. Отличие заключается в базировании на базе «технология-реализация-совокупность событий», что позволяет отразить на операционном уровне изменения в технологии (посредством использования множеств) и в процессах (посредством использования конфигурации и реконфигурации), а также методов управления процессами. Кроме того, модель обладает возможностью сужения многоаспектности и формирования частичных моделей.

В целом обладающий универсальностью теоретико-множественный подход требует дальнейшего развития в направлении разработки графовых форм моделей процессов получения и обработки информации по следующим причинам:

1) сложность разработки теоретико-множественных моделей конкретных процессов получения и обработки информации, особенно с потенциальной возможностью изменений в них и технологиях;

2) несоответствие стандартам в системе получения и обработки информации в порталах органов исполнительной власти;

3) недостаточная подготовленность инженерно-технического персонала;

4) трудности в имитационном моделировании и визуализации.

ЗАКЛЮЧЕНИЕ

Для осуществления диагностирования компонентов АСУ необходимо провести целый комплекс мер. Во-первых, необходимо определить общие принципы реализации процесса получения и обработки информации, добавить теоретическую основу его организации и структуры. Во-вторых, подготовить математическое описание реализации процесса, систематизирующее все приведенные ранее принципы в общую математическую модель. В-третьих, необходимо определить, каким образом возможно осуществление полученной модели, как организовать структуру управления, что приближает к воплощению процесса диагностирования компонентов системы получения и обработки информации. Однако стоит заметить, что завершающим этапом данного комплекса мер является определение целесообразности разработки, выявления имеющихся плюсов и минусов, оценка положительных и отрицательных сторон по степени своей значимости. Данная процедура позволяет как выявить недостатки полученной модели процесса, что дает возможность его усовершенствовать, так и выявить новые направления исследования данного вопроса, осуществить поиск новых способов реализации процесса диагностирования.

В целом же только совокупность всех мер как единого метода позволяет наиболее полно способствовать решению вопроса повышения эффективности получения и обработки информации в органах исполнительной власти. Только обобщение теоретических основ вопроса с оценкой его практического применения позволяет не только разработать данный механизм, но и принять решение о его целесообразности.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении: учебное пособие / под ред. А.А. Емельянова. – М.: Финансы и статистика, 2002. – 368 с.: ил.
2. Еременко В.Т., Полянский И.С., Беседин И.И. Методологические аспекты синтеза оптимальной древовидной структуры в системах сбора и обработки информации // Вестник компьютерных и информационных технологий, 2013. – № 11. – С. 15-21.
3. Еременко В.Т., Тютякин А.В. Методологические аспекты выбора профилей сбора и обработки данных в системах неразрушающего контроля и диагностики технических объектов // Контроль. Диагностика, 2013. – № 1. – С. 24-31.
4. Основы технической диагностики. – В 2-х книгах. Книга 1. Модели объектов, методы и алгоритмы диагноза / под ред. П.П. Пархоменко. – М.: «Энергия», 1976. – 464 с., ил.
5. Успенский В.Д., Семенов А.Л. Теория алгоритмов; основные открытия и приложения. – М.: Наука. Главная редакция физико-математической литературы. Б-чка программиста, 1987. – 288 с.
6. Еременко В.Т., Фисенко В.Е., Фисун А.П. Методы и модели оценки надежности распределенных систем обмена данными: монография. – Орел: Издательство «Госуниверситета – УНПК», 2014. – 197 с.
7. Еременко В.Т., Тютякин А.В., Кондрашин А.А. Выбор профилей обработки данных в системах контроля и диагностики технических объектов на основе их качественного анализа // Информационные системы и технологии, 2014. – № 5. – С. 88-97.
8. Котов В.Е., Сабельфельд В.К. Теория схем программ. – М.: Наука. Главная редакция физико-математической литературы, 1991. – 248 с.

Мишин Дмитрий Станиславович
ФГКОУ ВО «Орловский юридический институт МВД России им. В.В. Лукьянова», г. Орел
Кандидат юридических наук, доцент кафедры «Информационные технологие в деятельности органов внутренних дел»
Тел.: 8 903 880 23 45
E-mail: mishinds@mail.ru

Ерёменко Владимир Тарасович
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Доктор технических наук, профессор, профессор кафедры «Электроника, вычислительная техника, информационная безопасность»
Тел.: 8 920 812 65 64
E-mail: wladimir@orel.ru

Мишин Ярослав Дмитриевич
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент кафедры «Электроника, вычислительная техника, информационная безопасность»

D.S. MIShIN *(Candidate of Juridical Sciences,*
Associate Professor of the Department «Information Systems in activity Ministry of Internal Affairs»)
Law Institute of the Russian Interior Ministry named V.V. Luk'yanov, Orel

V.T. ERYoMENKO *(Doctor of Engineering Sciences, Professor,*
Professor of the Department «Electronics, Computer Engineering, Information Security»)

Ya.D. MIShIN *(Student of the Department «Electronics, Computer Engineering, Information Security»)*
Orel State University named after I.S. Turgenev, Orel

METHODOLOGICAL ASPECTS OF DIAGNOSIS OF COMPONENTS OF PRODUCTION AND PROCESSING OF INFORMATION IN THE PORTALS OF EXECUTIVE AUTHORITY

The article describes a set of methods by which the possible implementation of the process of diagnosing the components of the automated systems of reception and processing of information in the portals of the executive power. The corresponding steps detailed manner revealing the essence of the methods and principles of their implementation and evaluation of the suitability of the process for the full implementation of automated systems.

Keywords: *acquisition and processing of information; diagnosis; procedural approach; process approach; the automated system.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Anfilatov B.C., Emel'yanov A.A., Kukushkin A.A. Sistemny'j analiz v upravlenii: uchebnoe posobie / pod red. A.A. Emel'yanova. – M.: Finansy' i statistika, 2002. – 368 s.: il.
2. Eremenko V.T., Polyanskij I.S., Besedin I.I. Metodologicheskie aspekty' sinteza optimal'noj drevovidnoj struktury' v sistemax sbora i obrabotki informacii // Vestnik komp'yuterny'x i informacionny'x texnologij, 2013. – № 11. – S. 15-21.
3. Eremenko V.T., Tyutyakin A.V. Metodologicheskie aspekty' vy'bora profilej sbora i obrabotki danny'x v sistemax nerazrushayushhego kontrolya i diagnostiki texnicheskix ob''ektov // Kontrol'. Diagnostika, 2013. – № 1. – S. 24-31.
4. Osnovy' texnicheskoj diagnostiki. – V 2-x knigax. Kniga 1. Modeli ob''ektov, metody' i algoritmy' diagnoza / pod red. P.P. Parxomenko. – M.: «E'nergiya», 1976. – 464 s., il.
5. Uspenskij V.D., Semenov A.L. Teoriya algoritmov; osnovny'e otkry'tiya i prilozheniya. – M.: Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury'. B-chka programmista, 1987. – 288 s.
6. Eremenko V.T., Fisenko V.E., Fisun A.P. Metody' i modeli ocenki nadezhnosti raspredelenny'x sistem obmena danny'mi: monografiya. – Orel: Izdatel'stvo «Gosuniversiteta – UNPK», 2014. – 197 s.
7. Eremenko V.T., Tyutyakin A.V., Kondrashin A.A. Vy'bor profilej obrabotki danny'x v sistemax kontrolya i diagnostiki texnicheskix ob''ektov na osnove ix kachestvennogo analiza // Informacionny'e sistemy' i texnologii, 2014. – № 5. – S. 88-97.
8. Kotov V.E., Sabel'fel'd V.K. Teoriya sxem programm. – M.: Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury', 1991. – 248 s.

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК: 65.011.56

М.В. ГУСЕВ, В.А. ХОЛОПОВ

МЕТОД ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОЕКТИРОВАНИЯ АСУТП ПУТЕМ ОПТИМИЗАЦИИ КОНФИГУРАЦИИ ПРОМЫШЛЕННЫХ ETHERNET-СЕТЕЙ

В статье рассматривается метод повышения эффективности разработки АСУТП путем оптимизации конфигурации промышленных Ethernet-сетей. Представлено описание этапов проектирования промышленной сети, а именно алгоритмических и математических моделей. Наличие этих моделей позволяет сопоставить метрики промышленной сети с факторами, влияющими на них, а также разработать целевую функцию. Ввиду большого количества комбинаций при решении оптимизационной задачи (минимизации целевой функции) метод прямого перебора не может быть использован. В связи с вышесказанным в статье предложен вариант решения задачи комбинаторной оптимизации с помощью метода отжига по Больцмановской схеме. Согласно результатам исследования, данный метод является одним из наиболее подходящих в решении подобного рода задач. После описания решения оптимизационной задачи рассмотрены преимущества разработанного метода оптимизации конфигурации промышленных Ethernet-сетей.

Ключевые слова: *автоматизация производства; промышленная сеть; автоматизированная система управления; математические модели; алгоритмические модели; метод отжига; целевая функция; комбинаторная оптимизация.*

Проектирование промышленной сети как части АСУТП является сложным, многоэтапным процессом, состоящим из следующих обязательных частей: формализация требований к системе, соединение и размещение оборудования (выбор топологий), выбор технологий резервирования, расчет максимальной загрузки и выбор оборудования.

Согласно декомпозиции общей задачи, мы имеем набор подзадач, решение которых должно сформировать метод, позволяющий оптимизировать конфигурации промышленных Ethernet-сетей. Для достижения цели требуется разработать математическую модель промышленной сети, поставить оптимизационную задачу и решить ее. Первый этап подразумевает представление каждой подзадачи проектирования промышленной сети в математическом виде, придерживаясь итерационного подхода.

Процесс формализации требований к системе требуется для сбора всех входных данных, необходимых для достижения заданной цели и, как правило, каждый проект обладает уникальным набором таких требований. Однако есть ряд общих предъявляемых к сети и системе в целом требований [1]:

- высокие рабочие характеристики системы;
- быстрая реакция;
- высокая надежность;
- высокая производительность;
- модульная сетевая организация, информационная доступность в любой точке системы;
- легкость наращивания и изменения программно-технических данных;
- гибкость структуры.

Данные требования в представленном виде не могут быть использованы и должны выражаться в виде метрик промышленной сети и факторов, влияющих на них. Прежде чем перейти к описанию этих метрик, важно определить алгоритм, который будет лежать в основе метода оптимизации конфигурации промышленных Ethernet-сетей. К данному алгоритму предъявляются следующие требования:

– сеть должна быть работоспособной;
– сеть должна удовлетворять требованиям к характеристикам, важным для АСУТП;
– среди всех работоспособных вариантов сети нужно выбрать оптимальный;
– алгоритм должен предоставлять возможности по модификации.

Алгоритм включает два основных процесса: выбор топологии сети и выбор параметров оборудования. Структурный синтез промышленной сети выполняется путем выбора топологии среди множества определенных базовых. При этом базовая топология представляет собой правило, по которому строится топология реальной сети. Множество базовых топологий может быть расширено новыми.

Таким образом, для каждой базовой топологии будет решена задача выбора оборудования и соединительных линий. Оборудование и соединительные линии выбираются среди множества реально существующих экземпляров, которое может быть изменено.

Обеспечение соответствия требованиям к промышленной сети АСУТП предприятия достигается за счет введения ограничений на характеристики промышленной сети, для расчета которых используется соответствующая математическая модель. Работоспособность сети обеспечивается за счет введения ограничений на параметры оборудования. Эти ограничения определяют допустимое множество, из которого может быть выбрана каждая единица оборудования.

Для выбора оптимального варианта конфигурации сети сформулирован критерий оптимальности, который дает количественную оценку эффективности конфигураций.

Для описания общего алгоритма проектирования промышленной сети АСУТП необходимо ввести следующие объекты, свойства которых представлены в виде векторов [2]:

1. Конечное устройство – объект сети, подключенный как конечное устройство к коммутатору промышленной сети.

$$\bar{e} = [e_1, e_2, \dots, e_e]^T$$

Множество конечных устройств образует множество E:

$$E = \{\bar{e}\}$$

2. Коммутационные устройства – это устройства, к которым могут быть подключены конечные устройства и другие коммутационные устройства.

$$\bar{c} = [c_1, c_2, \dots, c_c]^T$$

Множество коммутационных устройств образует множество C:

$$C = \{\bar{c}\}$$

3. Связь – это соединение между двумя любыми устройствами, обладающая набором таких свойств, как тип, скорость, длина соединения.

$$\bar{l} = [l_1, l_2, \dots, l_l]^T$$

Множество связей образует множество L:

$$L = \{\bar{l}\}$$

4. Узел сети (УС) – это конечное или коммутационное устройство, т.е. любое устройство, принимающее участие в отправке и получении потоков данных. Узел сети h образует множество узлов сети H, т.е.

$$h \in H.$$

5. Сеть – это граф N [3]:

$$N = (H, V),$$

где $V \subset H^2$ – бинарное отношение на множестве H, характеризующее физическое соединение между устройствами.

6. Набор метрик – набор значений параметров сети, описанных в первой главе и формирующих ТТ для построения промышленной сети АСУТП. В математическом виде набор метрик представлен виде вектора $\bar{y} = [y_1, y_2, \dots, y_n]^T$, а ТТ – в виде системы неравенств:

$$\begin{cases} y_1^- \le y_1 \le y_1^+ \\ \dots \\ y_n^- \le y_n \le y_n^+ \end{cases}.$$

7. Технология резервирования – это технология, позволяющая при наличии между двумя устройствами резервного маршрута переключать поток данных между ними на резервный маршрут в случае недоступности основного [4].

$$\bar{r} = [r_1, r_2, \dots, r_r]^T$$

8. Базовая топология – это отображение множества конечных устройств на сеть:

$$\tau_i : 2^E \to \{N_i\},$$

где $i = \overline{1:n_\tau}; n_\tau = |T|$ – количество заданных базовых топологий; $T = \{\tau_i\}$ – множество базовых топологий; 2^E – множество всех подмножеств E; $\{N_i\}$ – множество всех сетей.

$\varphi: H \to C$

φ – ставит в соответствие коммутационному устройству конкретную модель коммутатора.

В качестве общего алгоритма проектирования промышленной сети АСУ ТП выбран следующий:

Шаг 1. Для каждой топологии τ_i из множества базовых топологий n_τ выполнить шаги 2-4.

Шаг 2. Создать реальную топологию на основании базовой: $T_i = \tau_i(E)$

Шаг 3. Рассчитать максимальную загрузку сети: $W, \bar{w}$

Шаг 4. Найти оптимальные значения $\varphi = \varphi^*$:

$$\begin{cases} \varphi_i^* = f_0(\varphi) \to min \\ y_j^- \le y_j(\varphi) \le y_j^+, j = \overline{1:n_y} \end{cases}$$
$$C_i = f_0(\varphi_i^*)$$

Шаг 5. Выбираем φ_k^*, N_k:

$$C_k = \min(C_1, \dots, C_{n\tau}),$$
$$k = \overline{1:n_\tau}$$

Общий алгоритм проектирования промышленной Ethernet сети АСУТП состоит из трех этапов (шаг 2-шаг 4), которые повторяются в цикле для каждой топологии из множества заданных.

Возвращаясь к метрикам промышленной сети, важно отметить, что для их представления в виде зависимостей важно провести анализ требований к промышленным сетям АСУ ТП, выявить характеристики и факторы, влияющие на них [5]. По результатам такого анализа сформирована таблица 1.

Таблица 1 – Метрики промышленной сети и факторы, влияющие на них

Метрика	**Влияющие факторы**
Максимально допустимые задержки (Delay) [6]	Длина кабеля Время обработки пакета коммутационным оборудованием Занятая емкость (Utilization)) (бит/с) Размер пакета (байт) Скорость интерфейса (бит/с) Скорость распространения сигнала (с)
Максимально допустимое	Время обработки пакета коммутационным оборудованием (с)

изменение задержки (Delay Jitter) [6]	Время обработки пакета конечным устройством Точность синхронизации времени между устройствами
Емкость каналов связи [6]	Скорости интерфейса коммутатора (бит/с)
Доступность сети [6]	MTBF\ (MTBF+MTTR)
Максимальные потери пакетов на канале [6]	Время конвергенции протоколов резервирования Ожидаемая загрузка

Определив алгоритм проектирования и метрики промышленных сетей, возникает задача соединения и размещения оборудования, которую решаем внутри одного здания. Модель здания представляет собой совокупность параллельных плоскостей, каждая из которых соответствует этажу здания. Внутри здания могут быть определены области для размещения коммутационного оборудования. Местоположение объектов внутри здания задается декартовыми координатами на этаже и номером этажа.

Входными данным этого этапа будут несколько отображений (биекций), которые ставятся в соответствие каждому устройству его положение в пространстве и порядковый номер. Подзадача соединения оборудования решается с применением метода одиночных связей, являющимся одним из методов иерархической кластеризации. Путем модификации алгоритма используемого метода сформирован следующий [7]:

Шаг 1. Каждой точке присваивается свой кластер, каждый из которых содержит один элемент. Расстояние между кластерами равно расстоянию между точками.

Шаг 2. Находится ближайшая пара кластеров, которая объединяется в один при условии, что расстояние между ними менее 100 м и общее количество кластеров больше двух. Расстоянием между кластерами считается расстояние между ближайшими точками.

Шаг 3. Вычисляются расстояния между новым кластером и каждым из существующих.

Шаг 4. Этапы 2 и 3 повторяются до тех пор, пока количество кластеров не перестанет уменьшаться.

Для решения подзадачи размещения оборудования здание должно быть представлено как трехмерное пространство. Для этого к каждой точке мы добавляем третью координату, равную высоте этажа. Задача размещения решается следующим образом:

Шаг 1. Для каждого кластера определяется центр масс.

Шаг 2. Соответствующий коммутатор каждого кластера помещается в ближайшую серверную относительно определенного центра масс.

Шаг 3. Центральный коммутатор помещается в ближайшую серверную к центру масс всех устройств.

По итогам размещения мы получаем отображение, которое ставит в соответствие каждой связи длину, равную евклидову расстоянию между точками в пространстве.

После решения описанных выше задач наступает этап расчета максимальной загрузки. Этот этап имеет ключевое значение при выборе оборудования и каналов связи. Максимальную загрузку сети имеет смысл искать среди тех состояний сети, при которых каждое устройство участвует в обмене данными. Каждое такое состояние S_k соответствует максимальному паросочетанию в полном графе с вершинами, соответствующими конечным устройствам. Для решения задачи разработан следующий алгоритм:

Шаг 1. Для каждого остовного дерева графа T выполнить шаги 2-4. Перебрать остовные деревья можно путем последовательного удаления сочетаний цикломатического числа ребер. Цикломатическое число определяется по следующей формуле:

$$V(x) = m - n + p,$$

где m – количество ребер, n – количество вершин, p – количество связных частей графа.

Шаг 2. Для каждого состояния сети S_k выполнить шаг 3.

Шаг 3. Рассчитать максимальную загрузку всех ребер остовного дерева. Последовательно рассматриваем пути между парами взаимодействующих устройств в

ориентированном графе, прибавляя каждому ребру соответствующее значение максимального потока данных каждого конечного устройства. Находим значение максимального потока данных на коммутаторе, равного входящей степени вершины.

Шаг 4. Для каждого ребра остовного дерева назначаем вес, равный максимальному среди весов для каждого состояния этого дерева.

Шаг 5. Для каждого ребра графа T назначаем максимальных вес из весов всех остовных деревьев.

По итогам выполнения алгоритма для каждой из базовых топологий имеем набор взвешенных графов. Далее требуется для каждой конфигурации подобрать оборудование и выбрать оптимальную конфигурацию из полученного множества, т.е. имеем задачу комбинаторной оптимизации. Выбор оборудования происходит среди объектов множества *F*, $F \subset C$. Множество *F* включает в себя устройства, соответствующие требованиям производства, таким, как: класс защищенности, рабочие температуры, допустимая влажность и т.д. С математической точки зрения, задачей данной этапа является поиск такого φ, что выполняются следующие ограничения:

$$\begin{cases} C(\varphi) \to \min - \text{стоимость сети} \\ A(\varphi) \geq A^{-} - \text{доступность сети} \\ D(\varphi) \leq D^{+} - \text{максимальные задержки} \\ J(\varphi) \leq J^{+} - \text{максимальный джитерр} \\ L(\varphi) \leq L^{+} - \text{максимальные потери} \end{cases}$$

$\varphi: H \to F$, φ ставит в соответствие коммутационному устройству (*H*) конкретную модель коммутатора (*F*), соответствующую требованиям производства.

Для решения оптимизационной задачи разработана целевая функция, которая определяет критерии оптимального выбора. Такими критериями будет стоимость, т.е. будет выполняться поиск такой конфигурации сети, при которой, не жертвуя параметрами качества сети, будет оптимизирована стоимость оборудования. В математическом виде целевая функция примет следующий вид: $C = \sum_j C_2^{(j)}$, где $C_2^{(j)}$ – стоимость коммутатора.

Для решения задачи комбинаторной оптимизации необходимо представить все метрики промышленной сети в математическом виде.

Односторонняя задержка зависит от задержки распространения сигнала (propogation delay), задержки передачи пакета в сеть (serialization delay), задержки очередности на интерфейсе (queuing delay)[8]. Для произвольного участка сети формула расчет задержки будет выглядеть следующим образом:

$$D = \sum_i \left[\frac{8 \cdot PS}{l_1^{(i)}} + \frac{8 \cdot PS}{l_1^{(i)} - U_1} + l_2^{(i)} \cdot l_3^{(i)} \right],$$

где PS – размер пакета (байт); l_1 – максимальный поток данных, который может быть обработан на интерфейсе (бит/с); U_1 – текущий поток данных на канале связи (бит/с); l_2 – скорость распространения сигнала (с); l_3 – длина кабеля (м).

Доступность промышленной сети рассчитывается по формуле:

$$A_{net} = \frac{MTBF_{net}}{MTBF_{net} + CT_N},$$

где $MTBF_{net}$ – среднее время между сбоями промышленной сети; CT_N – время конвергенции протокола резервирования при заданной конфигурации сети.

Джиттер возникает из-за очередей на интерфейсах коммутационного оборудования. Для кольцевой топологии максимальный джиттер рассчитывается по формуле [8]:

$$J_r = CT_N + n_h \cdot pd_N,$$

где n_h – количество устройств в кольцевой топологии; pd_N – вносимая дополнительная задержка каждым коммутационным устройством сети ко времени конвергенции протокола резервирования.

Для топологии «зарезервированная звезда» максимальный джиттер будет рассчитываться по формуле [8]:

$$J_s = \max(CT_N^{(i)}),\ i = \overline{1:n_{rl}},$$

где n_{rl} – количество зарезервированных связей.

Максимальные потери на канале – разница между отправленным количеством пакетов и полученным количеством пакетов [9]. Как правило, выражается в процентном соотношении.

$$L_k = \frac{\sum_i L_{ci}\left(CT_N, l_{4j}^{(i)}, C_{1i}\right)}{\sum_i CT_N \cdot \sum_i l_{4j}^{(i)}},$$

$$L_{ci}\left(CT_N, l_{4j}^{(i)}, C_{1i}\right) = \begin{cases} 0 \text{ при } C_{1i} > CT_N \cdot \sum_j l_{4j}^{(i)} \\ CT_N \cdot \sum_j l_{4j}^{(i)} - C_{1i} \text{ при } C_{1i} \le CT_N \cdot \sum_j l_{4j}^{(i)} \end{cases},$$

где $j = \overline{1:n_l}$, где n_l количество смежных с вышедшим из строя коммутаторов; $i = \overline{1:n_j}$, где n_j количество инцидентных связей для смежных вышедшему из строя коммутаторов; C_{1i} – размер буфера *i*-ого коммутатора (бит).

Причем ожидаемую загрузку l_4 инцидентных связей вышедшего из строя коммутатора считаем равной нулю.

Данная формула представляет собой отношение количества пакетов, суммарный размер которых превышает размер буфера коммутатора к сумме всех передаваемых пакетов за время конвергенции CT_N.

$$L = \max(L_k),\ k = \overline{1:n_c},$$

где n_c количество коммутационных устройств.

Решение полученной оптимизационной задачи не представляется возможным простым перебором, так как при превышении определенного количества комбинаций на поиск оптимального решения будут уходить месяцы и годы. В связи с этим был проведен анализ техник оптимизаций и выбран метод отжига как наиболее походящий для решения имеющейся задачи метод. Метод отжига – это техника оптимизации, использующая упорядоченный случайный поиск на основе аналогии с процессом образования в веществе кристаллической структуры с минимальной энергией при охлаждении [10].

Метод отжига служит для поиска глобального минимума некоторой функции $f(x)$, заданной для x из некоторого пространства S, дискретного или непрерывного. Элементы множества S представляют собой состояния воображаемой физической системы (энергетические уровни), а значение функции f в этих точках используется как энергия системы $E = f(x)$. В каждый момент предполагается заданной температура системы T, как правило, уменьшающаяся с течением времени. После попадания в состояние x при температуре T следующее состояние системы выбирается в соответствии с заданным порождающим семейством вероятностных распределений $G(x;T)$, которое при фиксированных x и T задает случайный элемент $G(x;T)$ со значениями в пространстве S. После генерации нового состояния $x' = G(x;T)$, система с вероятностью $h(\Delta E, T)$ переходит к следующему шагу в состояние x', в противном случае процесс генерации x'повторяется. Здесь ΔE обозначает приращение функции энергии $f(x') - f(x)$. Величина $h(\Delta E, T)$ называется вероятностью принятия нового состояния.

Как правило, в качестве функции $h(\Delta E, T)$ выбирается точное значение соответствующей физической величины.

В качестве функции $h(\Delta E, T)$ будет использоваться:

$$h(\Delta E, T) = e^{-\frac{\Delta E}{T}}$$

Таким образом, если ΔE будет меньше 0, то $h(\Delta E, T)$ будет больше 1, а тогда соответствующая вероятность считается равной 1. В результате, если новое состояние дает

лучшее значение оптимизируемой функции, то переход в это состояние произойдет в любом случае [21].

Итак, конкретная схема метода отжига задается следующими параметрами:

- выбором закона изменения температуры $T(k)$, где k – номер шага.
- выбором порождающего семейства распределений $G(x;T)$.
- выбором функции вероятности принятия $h(\Delta E,T)$.

Алгоритм:

1. Случайным образом выбирается начальная точка $x = x_0$, $x_0 \in S$. Текущее значение энергии E устанавливается в значение $f(x_0)$.

2. k -я итерация основного цикла состоит из следующих шагов:

– сравнить энергию системы E в состоянии x с найденным на текущий момент глобальным минимумом. Если $E = f(x)$ меньше, то изменить значение глобального минимума;

– сгенерировать новую точку $x' = G(x;T(k))$;

– вычислить значение функции в ней $E' = f(x')$;

– сгенерировать случайное число α из интервала [0; 1];

– если $\alpha < h(E' - E,T(k))$, то установить $x \leftarrow x'$, $E \leftarrow E'$ и перейти к следующей итерации. Иначе повторить шаг (2), пока не будет найдена подходящая точка x'.

Оптимизируемая система представляет собой граф с n вершин, каждой вершине которого может быть поставлена в соответствие модель коммутатора. Нужно искать отображение, ставящее в соответствие каждому элементу графа соответствующий коммутатор. Данное отображение может быть представлено в виде n-мерного вектора $x = [x_0 \dots x_{n-1}]$, в котором каждый элемент представляет собой идентификатор модели соответствующего узла. Все возможные значения x образуют пространство S. Энергия системы соответствует суммарной стоимости всех коммутаторов сети.

$$E = \sum_{i=0}^{n-1} C_2^{(i)}$$

Согласно Больцмановской схеме, изменение температуры задается формулой [10]:

$$T(k) = \frac{T_0}{\ln(1+k)}, k > 0,$$

где T_0 – начальная температура; k – номер шага.

Семейство распределений $G(x,T)$ выбирается как семейство нормальных распределений с математическим ожиданием x и дисперсией T, т.е. задается плотностью [10]:

$$g(x',x,T) = (2\pi T)^{-\frac{D}{2}} \cdot e^{-\frac{|x'-x|^2}{2T}},$$

где D – размерность пространства состояний.

Данное распределение является частью Больцмановской схемы, для которой доказано, что при достаточно больших T_0 и общем количестве шагов k гарантируется нахождение глобального минимума.

Данный метод оптимизации проектирования промышленной сети позволяет многократно ускорить процесс разработки проекта промышленной сети и предоставить проектировщику системы готовое техническое решение.

Очевидные выгоды использования метода – уменьшение числа ошибок на этапе создания рабочего проекта, структуризация процесса проектирования, четкая формализация требований, экономия времени квалифицированных сотрудников при составлении топологии, спецификаций и других проектных документов. Разработанный метод является перспективным решением, позволяющим повысить эффективность разработки АСУ ТП.

СПИСОК ЛИТЕРАТУРЫ

1. Офицеров А.И. Проектирование сетей передачи данных автоматизированных систем управления промышленных предприятий: дис. … канд. тех. наук: 05.13.06. – Орел, 2010. – 110 с.
2. Золотарев А. Методы оптимизации распределительных процессов. – М.: Инфра-Инженерия, 2014. – 160 с.
3. Хаггати Р. Дискретная математика для программистов, 2-е издание, исправленное. – М.: Техносфера, 2012. – 400 с.
4. Cisco Systems Inc. Руководство по технологиям объединенных сетей: пер. с англ. – М: ООО ИД «Вильямс», 2005. – 76 с.
5. Каллан Р. Основные концепции нейронных сетей. – М.: ООО ИД «Вильямс», 2003. – 288 с.
6. .Cisco Systems Inc. Руководство по технологиям объединенных сетей: пер. с англ. – М: ООО ИД «Вильямс», 2005. – 76 с.
7. Жамбю М. Иерархический кластер-анализ и соответствия. – М.: Финансы и статистика, 1988. – 345 с.
8. Sean R. Cisco Systems Inc. Designing for Cisco Internetwork Solutions (DESGN) Foundation. – USA: Cisco Press, 2011. – 576 p.
9. Cisco Systems inc. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство: пер. с англ. – М.: ООО ИД «Вильямс», 2007. – 439 с.
10. Лопатин А.С. Метод отжига. – СПБ: Санкт-Петербургский государственный университет, 2005. – 149 с.

Гусев Максим Викторович
ФГБОУ ВО «Московский технологический университет», г. Москва
Аспирант
Тел.: 8 (495) 525-31-13, 8 917 572 78 00

Холопов Владимир Анатольевич
ФГБОУ ВО «Московский технологический университет», г. Москва
Кандидат технических наук, доцент
Тел.: 8 (495) 483-97-50, 8 903 521 03 86
E-mail: holopov@gmail.com

M.V. GUSEV *(Post-graduate Student)*

V.A. XOLOPOV *(Candidate of Engineering Sciences, Associate Professor)*
Moscow Technological University, Moscow

APCS DESIGNING EFFICIENCY-INCREASING METHOD BY INDUSTRIAL ETHERNET-NETWORK CONFIGURATION OPTIMIZATION

In this article discussed APCS designing efficiency-increasing method by industrial Ethernet network configuration optimization. Provided industrial network designing stages description and related algorithmic and mathematic models. This models show dependencies between industrial network metrics and factors influencing them. Also it provides ability to create cost function but due to huge amount of variants we can't use brute force method and in this article discussed approach based on simulated annealing. Statistic says that it is one of most effective methods to resolve such kind of tasks. After describing cost function minimization discussed advantages of developed method.

Keywords: *automatization of production; industrial network; automated control system; mathematic model; algorithmic model; simulated annealing method; cost function; combinatorial optimization.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Oficerov A.I. Proektirovanie setej peredachi danny'x avtomatizirovanny'x sistem upravleniya promy'shlenny'x predpriyatij: dis. … kand. tex. nauk: 05.13.06. – Orel, 2010. – 110 s.
2. Zolotarev A. Metody' optimizacii raspredelitel'ny'x processov. – M.: Infra-Inzheneriya, 2014. – 160 s.
3. Xaggati R. Diskretnaya matematika dlya programmistov, 2-e izdanie, ispravlennoe. – M.: Texnosfera, 2012. – 400 s.
4. Cisco Systems Inc. Rukovodstvo po texnologiyam ob''edinenny'x setej: per. s angl. – M: OOO ID «Vil'yams», 2005. – 76 c.
5. Kallan R. Osnovny'e koncepcii nejronny'x setej. – M.: OOO ID «Vil'yams», 2003. – 288 s.
6. .Cisco Systems Inc. Rukovodstvo po texnologiyam ob''edinenny'x setej: per. s angl. – M: OOO ID «Vil'yams», 2005. – 76 c.
7. Zhambyu M. Ierarxicheskij klaster-analiz i sootvetstviya. – M.: Finansy i statistika, 1988. – 345 s.
8. Sean, R. Cisco Systems Inc. Designing for Cisco Internetwork Solutions (DESGN) Foundation. – USA: Cisco Press, 2011. – 576 p.
9. Cisco Systems inc. Programma setevoj akademii Cisco CCNA 3 i 4. Vspomogatel'noe rukovodstvo: per. s angl. – M.: OOO ID «Vil'yams», 2007. – 439 s.
10. Lopatin A.S. Metod otzhiga. – SPB: Sankt-Peterburgskij gosudarstvenny'j universitet, 2005. – 149 s.

УДК 631.350.2

А.И. ФРОЛОВ, А.О. ЧЁРНАЯ,
Л.О. РОЖКОВА, Д.А. РОСЛЯКОВ

МЕТОДИКА ПРИМЕНЕНИЯ МУЛЬТИРОТОРНОГО БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА ДЛЯ АВТОМАТИЗИРОВАННОЙ БИОТЕХНИЧЕСКОЙ ОБРАБОТКИ ПОЧВЫ И РАСТЕНИЙ

В статье приводятся обоснование необходимости использования мультироторного беспилотного летательного аппарата (БПЛА) в сельском хозяйстве. Раскрываются основные положения методики применения мультироторного БПЛА для автоматизированного внесения удобрений в почву и обработки растений. Приводятся конструктивные особенности и характеристики БПЛА с учетом специфики задач обработки растений.

Ключевые слова: *БПЛА; обработка растений; внесение удобрений в почву; автоматизация.*

ВВЕДЕНИЕ

Современное сельское хозяйство невозможно представить без механизированных средств повышения эффективности труда. В последнее время на первый план выходят биотехнологические методы, которые значительно влияют на урожайность. Объединение данных подходов позволит выйти на качественно новый уровень сельского хозяйства. С другой стороны, исследования показывают, что чрезмерное механическое воздействие на почву приводит к развитию процессов засоления и является причиной эрозии почв [1]. Поэтому решение данной проблемы является одной из самых актуальных задач сельского хозяйства.

Применение БПЛА снижает до минимума механические воздействия на почву в ряде сельскохозяйственных операций. Одной из таких операций является биотехнологическая обработка почвы и растений, включая сады и лесные массивы. Кроме того, применение БПЛА в данной операции существенно эффективней, чем ручная обработка, так как БПЛА сам определяет место, самостоятельно осуществляет перемещение для распыления и полностью исключает повреждение растений, так как распыление происходит с воздушного аппарата, не имеющего точек опоры на земле.

МЕТОДИКА ПРИМЕНЕНИЯ МУЛЬТИРОТОРНОГО БПЛА ДЛЯ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ПОЧВЫ И РАСТЕНИЙ

Для организации автоматизированной обработки почвы и растений с использованием мультироторного БПЛА необходимо поэтапное выполнение следующих шагов:

1. Определение общего состояния почвы или растительности на данном сельскохозяйственном участке, который может включать в себя как низкорослые насаждения, так и деревья. Данный шаг необходим для оценки интенсивности первоначальной обработки.

2. При помощи БПЛА в автоматическом режиме осуществляется построение актуального фотоплана местности с привязкой к глобальным спутниковым координатам [2]. Полученные данные обрабатываются и сохраняются на рабочей станции с использованием специального программного обеспечения (ПО). Данный шаг необходим для оценки объема работ.

3. С использованием БПЛА в автоматическом режиме осуществляется построение карты состояния почвы и активности растений на основе индекса вегетативности. Так как на БПЛА может устанавливаться различная аппаратура для получения индекса вегетативности, область захвата данных может быть существенно снижена по сравнению с областью захвата при построении фотоплана местности, что приводит к избыточным перемещениям БПЛА.

Поэтому рекомендуется уточнить области сканирования на основе данных, полученных на шаге 2, используя визуальное восприятие, если это возможно, для уменьшения времени работы БПЛА. Данный этап необходим для уточнения состояния почвы и растительности с целью построения оптимального плана использования БПЛА и реагентов при дальнейшей обработке. Полученные данные обрабатываются и сохраняются на рабочей станции.

4. На основе данных, полученных на предыдущем шаге, ПО автоматически производит построение плана полета (рис. 1). Оператор при необходимости имеет возможность внесения незначительных корректировок в план полета по таким параметрам, как:

- интенсивность обработки;
- площадь захвата;
- высота обработки;
- маршрут;
- и т.п.

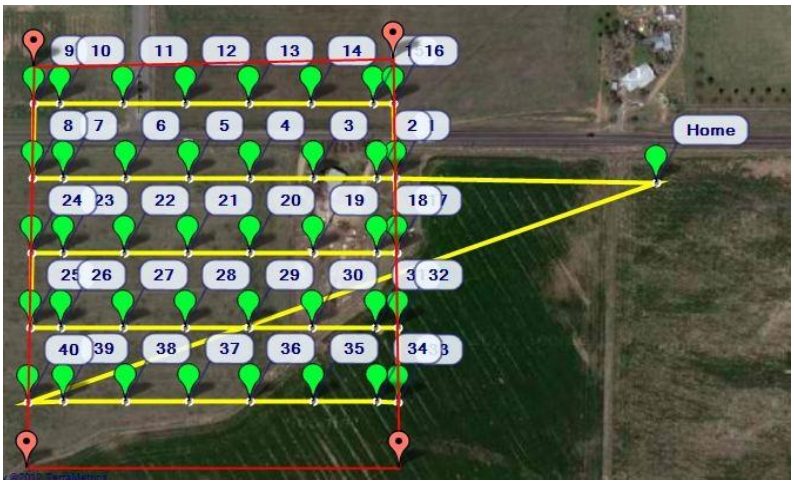

Рисунок 1 – Пример визуального представления плана полета БПЛА при обработке растительности

5. Оператор производит заправку БПЛА реагентами и отправляет в полет. БПЛА в соответствии с планом полета производит подлет к точке обработки, производит зависание или задействует режим равномерного движения и, открывая форсунки, производит распыление реагента, после чего перемещается к следующей контрольной точке. Миссия БПЛА прекращается в случае:

- опустошения баков с реагентами;
- выработки батареи;
- прохождения последней контрольной точки;
- возникновения иной нештатной ситуации.

После устранения проблемы предусматривается возможность продолжения прерванной миссии с той же точки. Во время выполнения данного шага также происходит сканирование активности растений, а данные используются для построения графика динамики развития растительности. Во время движения оператор имеет право вмешаться в действия БПЛА при необходимости, используя обратную видеосвязь [3].

6. Для достижения необходимого эффекта от воздействия биохимических реагентов необходимо периодическое выполнение этапов 1-5.

ПРИНЦИП ПОСТРОЕНИЯ МУЛЬТИРОТОРНОГО БПЛА

Основной чертой применяемого БПЛА является мультироторность, что предполагает наличие набора из N (четное число) винтомоторных групп (ВМГ), вектор тяги которых

направлен перпендикулярно вверх к плоскости поверхности земли. Данная особенность существенно упрощает конструкцию за счет минимизирования подвижных элементов по сравнению с БПЛА вертолетного типа позволяет осуществлять вертикальный взлет и посадку, а также зависание в воздухе. При N>=6 существенно повышается отказоустойчивость мультироторного БПЛА, которая выражается в сохранении полетных характеристик до 100% при отказе одной ВМГ. Высокий КПД достигается за счет применения бесколлекторных двигателей с неодимовыми магнитами, что позволит загружать БПЛА большим количеством полезного груза.

Для автоматизации процесса обработки растений мультироторный БПЛА должен быть оснащен следующим оборудованием:

1. Полетный контроллер обеспечивает преобразование входных сигналов управления в выходные сигналы для моторов, задающие их мощность.
2. Приемник сигналов с пульта управления.
3. Комплекс технического зрения для обратной связи с оператором и корректировки движения.
4. Аппарат фотофиксации с двухосевым гироскопическим подвесом для ортогональной съемки местности.
5. Гироскоп определяет положение БПЛА в пространстве и удержания его в горизонтальном положении.
6. Барометрический сенсор определяет высоту БПЛА с точностью до 0,05 м относительно точки взлета.
7. Ультразвуковой сенсор определяет расстояние до земли БПЛА с точностью до 0,005 м, используется при приближении к земле.
8. GPS/ГЛОНАСС приемник – определяет положение БПЛА в глобальной координатной системе с точностью до 0,05м;
9. Компас определяет вектор направления БПЛА.
10. Датчик NDVI индекса определяет в режиме реального времени индекс вегетативности растений.
11. Два распылителя с баками.

Указанное оборудование позволит использовать мультироторный БПЛА в автоматическом режиме с минимальным участием оператора. Комплекс сенсоров сможет сканировать поверхность и, соблюдая высоту, подбирать оптимальный расход и равномерность покрытия. Автопилот позволяет точно позиционировать БПЛА в заданной точке, удерживать его на время обработки или задавать равномерную скорость линейного перемещения, оптимально расходуя запас энергии. Логика управления автопилотом предусматривает внесение корректировок со стороны оператора при необходимости.

Для реализации требуемых функциональных особенностей БПЛА должен обладать следующими полетными характеристиками:

- время полета: 25 мин (при полной взлетной готовности);
- максимальная рабочая скорость: 8 м/с;
- максимальная скорость полета: 22 м/с;
- максимальная скорость распыления: 0,5 л/мин;
- зона распыления: 4-6 м;
- запас реагентов: два бака по 5 л;
- максимальная зона покрытия: до 162000-242000 $м^2$.

КОНСТРУКТИВНЫЕ ОСОБЕННОСТИ МУЛЬТИРОТОРНОГО БПЛА ДЛЯ БИОХИМИЧЕСКОЙ ОБРАБОТКИ ПОЧВЫ И РАСТЕНИЙ

Применение БПЛА в сельскохозяйственной отрасли подразумевает тяжелые условия эксплуатации, такие, как:

- полет в условиях сильной запыленности воздуха;

– полет в дождливую и туманную погоду;
– полет в ветреную погоду.

Исходя из этого, конструкция БПЛА должна быть спроектирована таким образом, чтобы обеспечить максимальную прочность при минимальном весе, что предполагает использование сверхпрочных материалов, а также защиту от попадания пыли и влаги в электрическую систему и подвижные элементы.

Беспилотный летательный аппарат будет оснащаться двумя баками по 5 литров. Это позволит распылять два разных вида удобрения одновременно.

Система опрыскивания состоит из:

– разветвленной системы трубок, ведущих к системе разбрызгивания;
– спринклеров (оросителей).

Перед каждой отдельной линией монтируют электромагнитный клапан, обслуживаемый запрограммированным электронным прибором. Именно этот блок в установленное время открывает подачу удобрения в одном или одновременно в нескольких направлениях. В этот же момент автоматически включается насос, отвечающий за давление в системе, благодаря которому двигается по трубам жидкость и подаётся на разбрызгиватели – так орошается поле. Блок управления разрешает включение и выключение клапанов в определенное время в течение всей обработки.

ВЫВОДЫ

Сельскохозяйственные БПЛА могут быть использованы в системах точного земледелия и помогут значительно увеличить их эффективность по сравнению с традиционными методами. Согласно замыслу авторов, БПЛА должны собирать информацию о состоянии полей и одновременно распылять жидкость, чтобы повысить уровень урожайности, а также вносить полученные данные в электронную карту. Благодаря этому точность полученной информации повысится в несколько раз, а трудозатраты на составление подобной карты, наоборот, значительно сократятся.

Благодаря высокой производительности БПЛА можно оперативно контролировать активность культур, предотвращать появление болезней, бороться с сорняками в ситуациях невозможности работы наземной техники, повышать качество урожая с помощью поздних подкормок, не повреждая растения. Кроме того, БПЛА остается незаменимой в борьбе с особо опасными вредителями – саранчой и луговым мотыльком, а также на десикации высокостебельных растений, например, подсолнечника [4].

Для реализации программно-аппаратного комплекса биотехнической обработки почв и растений с применением БПЛА необходимо решить ряд научных задач, таких, как:

1. Разработка системы автоматизированного распознавания контуров полей и произрастающих культур при помощи механизмов компьютерного зрения.

2. Разработка алгоритма построения оптимального плана полета на основе летных характеристик БПЛА, свойств используемых реагентов и погодных условий.

СПИСОК ЛИТЕРАТУРЫ

1. Сельское хозяйство мира [Электронный ресурс]. – URL: http://hitagro.ru/selskoe-xozyajstvo-mira/ (дата обращения 22.03.2016).
2. Агроинвестор. Защита с воздуха [Электронный ресурс]. – URL: http://www.agroinvestor.ru/technologies/article/14782-zashchita-s-vozdukha/ (дата обращения 22.03.2016).
3. Бизин И.В. и др. Возможности применения мультироторных беспилотных летательных аппаратов при неуверенном приеме сигналов ГНСС / И.В. Бизин, Ю.В. Василенко, В.В. Власов, А.В. Демидов, Н.В. Канатников, М.В. Смоляков // Информационные системы и технологии, 2014. – № 6(86). – С. 148-153.

4. Власов В.В. и др. К вопросу о применении беспилотных летательных аппаратов в сфере точного земледелия / В.В. Власов, Н.А. Власова, А.В. Демидов, Н.В. Канатников, М.В. Смоляков // Информационные системы и технологии, 2015. – № 5(91). – С. 72-77.

Фролов Алексей Иванович
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат технических наук, доцент
E-mail:aifrolov@mail.ru

Чёрная Анастасия Олеговна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Магистрант
E-mail: Chernayaanastasya@yandex.ru

Рожкова Лидия Олеговна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Студент
E-mail: lidiyarozhkova@yandex.ru

Росляков Дмитрий Андреевич
ПОУ «Орловский банковский колледж Центрального банка Российской Федерации», г. Орел
Студент
E-mail: mr.roslyakov57@mail.ru
Тел.: 8 910 208 69 90

A.I. FROLOV *(Candidate of Engineering Sciences, Associate Professor)*

A.O. ChYoRNAYa *(Master Student)*

L.O. ROZhKOVA *(Student)*
Orel State University named after I.S. Turgenev, Orel

D.A. ROSLYAKOV *(Student)*
Orel Banking College of the Central Bank of the Russian Federation, Orel

THE METHOD OF APPLICATION MULTIROTOR UAV FOR AUTOMATED BIOTECHNICAL TREATMENT OF SOIL AND PLANTS

The paper presents the rationale for the use multirotor unmanned aerial vehicle (UAV) in agriculture. Disclosed are methods of applying the basic provisions of multirotor UAV for the automated application of fertilizers in the soil and plant treatment. We give the design features and characteristics of the UAV-specific plant processing tasks.

Keywords: *UAV; processing plants; fertilizing the soil; automation.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Sel'skoe xozyajstvo mira [E'lektronny'j resurs]. – URL: http://hitagro.ru/selskoe-xozyajstvo-mira/ (data obrashheniya 22.03.2016).
2. Agroinvestor. Zashhita s vozduxa [E'lektronny'j resurs]. – URL: http://www.agroinvestor.ru/technologies/article/14782-zashchita-s-vozdukha/ (data obrashheniya 22.03.2016).
3. Bizin I.V. i dr. Vozmozhnosti primeneniya mul'tirotorny'x bespilotn'yx letatel'ny'x apparatov pri neuverennom prieme signalov GNSS / I.V. Bizin, Yu.V. Vasilenko, V.V. Vlasov, A.V. Demidov, N.V. Kanatnikov, M.V. Smolyakov // Informacionny'e sistemy' i texnologii, 2014. – № 6(86). – S. 148-153.
4. Vlasov V.V. i dr. K voprosu o primenenii bespilotny'x letatel'ny'x apparatov v sfere tochnogo zemledeliya / V.V. Vlasov, N.A. Vlasova, A.V. Demidov, N.V. Kanatnikov, M.V. Smolyakov // Informacionny'e sistemy' i texnologii, 2015. – № 5(91). – S. 72-77.

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

УДК 65.011.56

О.М. ПОЛЕВАЯ

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИНТЕЗА ФОРМУЛИРОВОК СТРАТЕГИЧЕСКИХ ЦЕЛЕЙ И ЗАДАЧ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПОДДЕРЖКИ ПРОЦЕССОВ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ

Рассмотрены проблемы, связанные с синтезом текста стратегических целей и стратегии их достижения на естественном языке. Рассмотрены методы автоматической генерации текста на естественном языке. Разработана модель и методы для синтеза формулировок стратегических целей и задач для различных групп пользователей с учетом изменяющихся требований к формулировкам, а также с учетом изменяющейся предметной области.

Ключевые слова: *автоматическая генерация текста на естественном языке; модель синтеза текста; методы синтеза стратегических целей и задач.*

ВВЕДЕНИЕ

При выборе решения из множества стратегических альтернатив лицо, принимающее решение, сталкивается с проблемой формулирования стратегии: необходимо, чтобы стратегия была целостна, непротиворечива, релевантна окружающей обстановке и динамике ее развития, конкретна и понятна всем участникам процесса. При формулировании целей и задач стратегического уровня зачастую возникает неоднозначность в интерпретации используемых понятий для различных групп, а также упускаются обязательные составляющие при формулировке цели, что делает дальнейшее оперирование текстом стратегических целей и стратегии невозможным из-за потери семантической составляющей.

Цель – это конечный желаемый результат, который определяется в процессе планирования и регулируется функциями управления [1].

На сегодняшний день, согласно [2], цель должна удовлетворять SMART-критериям, т.е. быть конкретна, достижима, измерима, выгодна и ограничена во времени.

При формулировании цели используются либо прямые, либо опосредованные постановки. В первом случае ставится цель, затем определяются способы ее достижения. В случае опосредования цели наличествует некоторый протекающий процесс. Субъект этого процесса намечает некоторое состояние объекта процесса, которое определяет как удовлетворяющее смыслу процесса. Тогда это состояние называется целью процесса. Для простоты в данной работе будут формализованы только прямые постановки. Но для оптимальности управления необходимо учитывать и опосредованные цели.

При разработке системы поддержки процессов стратегического управления возникают проблемы, связанные с синтезом текста на естественном языке стратегических целей и стратегии их достижения:

– формулирования целостной непротиворечивой конкретной стратегии (задача прагматики и семантики ЕЯ). При формулировании целей зачастую возникает неоднозначность в интерпретации используемых понятий для различных групп, а также упускаются обязательные составляющие при формулировке цели, что делает дальнейшее оперирование текстом стратегических целей и стратегии невозможным из-за потери семантической составляющей;

– однозначной интерпретируемости текстов стратегических целей и стратегии на различные ЕЯ. Если компания ведет бизнес в нескольких языковых регионах, то для

однозначной интерпретации цели необходимым условием является одинаковое понимание формулировки цели для разных языковых групп;

– применения и комбинации требований к формулируемым целям (задача применения динамических шаблонов);

– поиска оптимального дискурса. При формулировании целей необходимо учитывать глубину детализации: для того, чтобы определить стратегическую цель всей компании, необходимо дать целостное и полное описание механизма ее реализации на концептуальном уровне.

Актуальной является задача разработки методов и моделей для формулирования текста стратегии для различных групп пользователей с учетом изменяющихся требований к тексту стратегии и изменяющейся структуры предметной области.

ОБЗОР МЕТОДОВ АВТОМАТИЧЕСКОЙ ГЕНЕРАЦИИ ТЕКСТА НА ЕСТЕСТВЕННОМ ЯЗЫКЕ

Существуют несколько подходов синтеза естественно-языковых текстов в информационных системах [3]:

– генерация текста на основе шаблона. Шаблонная система использует готовые реплики или комбинирует готовые фрагменты текста таким образом, что они занимают заданные позиции в дискурсе или стереотипном тексте. Более сложные шаблонные системы дополнительно проводят ограниченную лингвистическую и риторическую обработку результата – позволяют задавать отдельные грамматические параметры текста или комбинировать шаблонные высказывания в связный текст, используя определенные лексические и грамматические знания о ЕЯ;

– системы автоматической генерации текстов (ГЕЯ) [4]. Генерация на естественном языке занимается созданием компьютерных систем, производящих тексты на естественном языке (ЕЯ) из некоторого нелингвистического (нетекстового) представления информации. Источником содержания являются данные, представленные в виде БД, БЗ или в виде выражений на формализованных языках. Считается, что генератор на входе должен принимать систему знаний, из которой будет конструироваться текст, коммуникативную цель порождаемого текста, модель адресата текста и контекст повествования.

Системы ГЕЯ имеют ряд преимуществ над шаблонными системами [5]. К ним относятся: сопровождаемость, лучшее качество создаваемых текстов, многоязыковой выход и гарантированное соответствие стандартам.

Таким образом, системы ГЕЯ решают три описанные выше проблемы: однозначной интерпретируемости текстов стратегических целей и стратегии на различные ЕЯ; применения и комбинации требований к формулируемым целям; поиска оптимального дискурса.

Общая схема генерации без детализации происходящих процессов в системах ГЕЯ состоит из трех основных блоков:

1. Планирование содержания текста – решение, какая именно информация из входных данных попадет в текст и как она будет организована. Этот этап работает исключительно с предметным знанием и общими способами организации содержания в тексте. Результатом является план текста в терминах последовательности событий, метафункций, например, запрос информации, предоставление информации или риторических отношений.

2. Микропланирование – это интерфейсный блок, который позволяет от предметных знаний перейти к языковым. В нем решается, каким образом выбранная информация будет реализована языковыми средствами в виде предложений на ЕЯ. Результатом этого процесса являются представления предложений в виде структур семантических и/или синтаксических отношений.

3. Реализация на ЕЯ – производство грамматически правильных предложений текста, основанное на лингвистических знаниях. Этот блок часто выделяется как универсальный и включает в себя либо только морфологический синтез словоформ, либо переход от семантических представлений к поверхностно синтаксическим и синтез словоформ.

Основной проблемой в системах ГЕЯ является моделирование структуры текста – планирование содержание текста и микропланирование. Поэтому в данной работе будет решаться проблема моделирования структуры текста при синтезе формулировок стратегических целей и задач.

Для решения данной задачи будет разработана модель и набор методов, позволяющий на основе предложенной модели смоделировать структуру текста формулировок стратегических целей и задач.

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИНТЕЗА ФОРМУЛИРОВОК СТРАТЕГИЧЕСКИХ ЦЕЛЕЙ И ЗАДАЧ

Математическое обеспечение синтеза формулировок стратегических целей в информационной системе поддержки процессов стратегического управления состоит из модели для синтеза формулировок и множества методов (рис. 1).

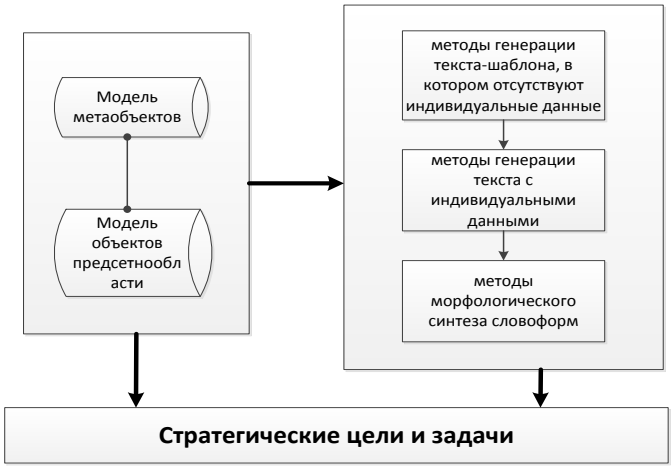

Рисунок 1 – Схема работы модели для синтеза формулировок стратегических целей

Модель, по которой будет происходить синтез формулировок, состоит из двух уровней – уровня метаобъектов и связанного с уровнем метаобъектов уровня объектов предметной области, для которой принимается стратегическое решение.

Множество методов для синтеза формулировок стратегических целей образует следующие группы:

1. Методы генерации текста-шаблона, в котором отсутствуют индивидуальные данные.

2. Методы генерации текста с индивидуальными данными. Эта группа методов подразумевает подстановку в выбранный шаблон значений объектов или их свойств, характеризующихся индивидуальными данными.

3. Методы морфологического синтеза словоформ. Поскольку сгенерированный текст и подставленные в него данные содержит слова в своей первоначальной форме, то необходимо выполнить их морфологическую обработку. На данный момент разработано множество методов морфологического синтеза словоформ [6].

Процесс синтеза формулировок – это последовательное применение вышеописанных групп методов в указанном порядке.

Опишем подробнее модель и группу методов генерации текста-шаблона, в котором отсутствуют индивидуальные данные.

МОДЕЛЬ ДЛЯ СИНТЕЗА ТЕКСТА СТРАТЕГИИ

В качестве модели будет рассмотрена система, состоящая из следующих компонентов:

StrategyFormulaModel = <MetaModel, Model, ConnectionFunction, TransformationFunction>, где

MetaModel – модель метаобъектов и связей между ними;

Model – модель предметной области, в которой принимается решение;

ConnectionFunction – множество правил, задающее отношение полиморфизма между объектами модели MetaModel и Model;

TransformationFunction – множество правил изменения множества ConnectionFunction.

Опишем подробнее каждый компонент данной модели.

MetaModel. На уровне метаобъектов определяются основные категорийные (базовые) понятия, применяемые для стратегического управления:

– объект – некоторая сущность, обладающая определенным состоянием и поведением, имеет заданные значения свойств и атрибутов;

– императив – действие, которое можно выполнять над объектом;

– субъект – производитель действия или носитель состояния;

– целевой показатель – количественное значение уровня, которому должен соответствовать тот или иной показатель объекта. Он подразумевает определенные действия, необходимые для достижения цели, и указывают на то, как стратегия будет реализована на операционном уровне;

– сроки – время, за которое планируется достичь конечного состояния;

– ресурсы – то, что необходимо для достижения цели.

Эти понятия могут представлять собой сложные сущности, но для задачи формулирования стратегии, удовлетворяющей определенным критериям, нет необходимости явно определять внутренние операции или элементы структур: они могут изменяться с течением времени.

Обозначение:

Пусть модель метаобъектов и связей между ними задается четверкой:

MetaModel = <MetaObj, AttributeMetaObj, ConnectionMetaObjFunction, TransformationMetaObjFunction, TransformationConnectionFunction>, где

MetaObj – конечное множество метаобъектов.

AttributeMetaObj – множество атрибутов метаобъекта.

ConnectionMetaObjFunction – множество правил, задающее отношение полиморфизма между объектами из MetaObj.

TransformationMetaObjFunction – множество правил изменения множества MetaObj

TransformationConnectionFunction – множество правил изменения множества ConnectionMetaObjFunction.

Пусть объекты x, y ϵ MetaObj.

Определим на множестве MetaObj следующие отношения:

Отношение строгого порядка: $x < y$. Отношение строгого порядка – это бинарное отношение на множестве MetaObj, обладающее свойствами транзитивности, антисимметричности и антирефлексивности.

Отношение строгого порядка задает последовательность вхождения метаобъектов в конечный текст.

Функцию определения степени вхождения элемента из множества MetaObj в текст: $f_n(x)$: MetaObj $\rightarrow \mathbb{N}$.

$f_n(x) = n,\ n \epsilon \mathbb{N}$.

Функция определения степени вхождения задает максимальное количество раз вхождения метаобъекта в конечный текст.

Определение:

Элемент $x \epsilon \text{MetaObj}$ называется начальным, если $\forall y \epsilon \text{MetaObj}, y \neq x$ выполняется $x < y$.

Определение:

Элемент $x \epsilon \text{MetaObj}$ называется конечным, если $\nexists y \epsilon \text{MetaObj}$ выполняется $x < y$.

На рисунке 2 приведена диаграмма связей метаобъектов. В желтый прямоугольник помещены метаобъекты, которые обязательно должны присутствовать в стратегической цели по методологии SMART [2].

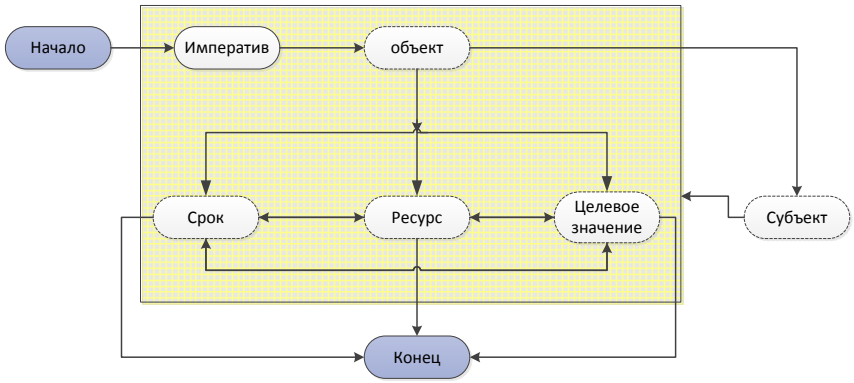

Рисунок 2 – Диаграмма связей метаобъектов модели MetaObj согласно методологии SMART

Model. Вторым уровнем модели для синтеза формулировок стратегических целей является модель предметной области. Предметная область для информационной системы синтеза формулировок стратегических целей является суммой предметных областей стратегического управления, операционного управления предприятием и специфической модели предметной области, в которой предприятие ведет свой бизнес.

Определение:

Пусть модель предметной области, в которой принимается решение, задается системой:

Model = <Obj, Attribute, ConnectionFunction (Obj, Obj), ConnectionFunction (Obj, Attr), ConnectionFunction (Attr, Attr), TransformFunction (Obj), TransformFunction (Attribute), TransformFunction (ConnectionFunction (Obj, Obj)),TransformFunction (ConnectionFunction (Obj, Attr)), TransformFunction (ConnectionFunction (Attr, Attr))>, где

Obj – конечное множество объектов предметной области

Attribute – конечное множество атрибутов объектов предметной области

ConnectionFunction (Obj, Obj) – множество правил связи между объектами предметной области. Для задачи синтеза текстовых формулировок понадобятся 2 типа связи:

– is_parent (x,y). Данная связь означает, что объект x является родителем к объекту y.

– относятся к цели (x,N).Данная связь означает, что объект x включен в множество объектов, относящихся к одной и той же цели N.

ConnectionFunction (Obj, Attr) – множество правил связи между объектами предметной области и их атрибутами.

ConnectionFunction (Attr, Attr) – множество правил связи между атрибутами объектов предметной области.

TransformFunction (Obj) – множество правил изменения объектов предметной области.

TransformFunction (Attribute) – множество правил изменения атрибутов объектов предметной области.

TransformFunction (ConnectionFunction (Obj, Obj)) – множество правил изменения правил связи между объектами предметной области.

TransformFunction (ConnectionFunction (Obj, Attr)) – множество правил изменения правил связи между объектами предметной области и их атрибутами.

TransformFunction (ConnectionFunction (Attr, Attr)) – множество правил изменения множество правил связи между атрибутами объектов предметной области.

ConnectionFunction. Каждое понятие предметной области связано с соответствующим ему метаобъектом. За счет этого при синтезе текста стратегии достигается соответствие текста определенным семантическим критериям (например, SMART-критериям).

Один и тот же объект предметной области может быть связан с несколькими метаобъектами.

Одному метаобъекту может соответствовать несколько объектов предметной области.

Таким образом, множество ConnectionFunction задает отношение полиморфизма между объектами модели MetaModel и Model.

Определение:

Пусть $x \in MetaObj, y \in Obj.$ Отношением связанности метаобъекта x и объекта y называется отношение эквивалентности.

Будем обозначать это отношение следующим образом: $x \rightsquigarrow y$

Определение:

Функция $f_{connection}(x,y) = \begin{cases} 1, \text{если в } x \rightsquigarrow y, x \in MetaObj, y \in Obj \\ 0, \text{иначе} \end{cases}$ определяет отношение связанности метаобъекта x и объекта предметной области y.

TransformationFunction. С развитием знаний о предметной области изменяется как сама предметная область, для которой необходимо сформулировать стратегическую цель, так и требования к формулировке целей. Поэтому модель для синтеза текста стратегической цели предусматривает множество правил изменения связей между объектами модели предметной области и метаобъектами.

Определим операции изменения связей:

- удалить связь;
- добавить связь.

Определение операции «изменить связь» автор считает лишней, так как она определяется через последовательное применение функций удаления и добавления связи.

МЕТОДЫ ГЕНЕРАЦИИ ТЕКСТА СТРАТЕГИИ

Множество методов для синтеза формулировок стратегических целей образует следующие группы:

- методы генерации текста-шаблона, в котором отсутствуют индивидуальные данные;
- методы генерации текста с индивидуальными данными;
- методы морфологического синтеза словоформ.

Опишем подробнее каждую из этих групп методов.

Методы генерации текста-шаблона без индивидуальных данных. Методы генерации текста-шаблона, в котором отсутствуют индивидуальные данные, включают:

- методы разработки шаблонов стратегических целей;
- методы изменения шаблонов стратегических целей;
- методы задания (выбора) шаблона цели, в который в конечном итоге будут подставлены индивидуальные данные.

Методы разработки шаблонов стратегических целей. Алгоритм синтеза шаблонов формулировок стратегии состоит из следующих этапов:

– синтез шаблона формулировки стратегической цели, содержащего только категорийные понятия (метаобъекты) по модели метаобъектов – синтез шаблона текста;

– подстановка в сгенерированный шаблон объектов предметной области на место соответствующих метаобъектов. Подстановка осуществляется за счет связи между метаобъектом и объектом предметной области;

– разбиение полученного шаблона на предложения с учетом связей между метаобъектами и объектами предметной области;

– ранжирование сгенерированных шаблонов с учетом весов связей между метаобъектами.

Опишем подробнее каждый этап.

Этап 1. Синтез шаблона текста

Определение:

Стратегия = текст = конечная последовательность элементов множества MetaObj, построенная с учетом отношения порядка и функции определения степени вхождения каждого элемента в последовательность.

Опишем алгоритм разработки шаблона текста стратегии:

1. На множестве MetaObj находим начальный и конечный элементы. Эти элементы всегда существуют в единственном экземпляре.

2. Далее ищем всевозможные пути от начального до конечного элемента в графе, заданном отношением строго порядка с ограничением, задающимся функцией определения степени вхождения элемента. Для этого модифицируем алгоритм поиска в ширину:

2.1. Поместить начальный элемент в изначально пустую очередь.

2.2.. Счетчик (x) = значение функции определения степени вхождения элемента в текст.

2.3 Уменьшить счетчик начального элемента на единицу.

2.4. Извлечь из начала очереди элемент x. Если счетчик(x) = 0, то необходимо пометить извлеченный элемент как развёрнутый.

2.4.1. Если элемент является конечным элементом, то завершить поиск с результатом «успех».

2.4.2. В противном случае в конец очереди добавляются все преемники элемента x, которые еще не развернуты. Уменьшить счетчик этих элементов на единицу.

2.5. Если очередь пуста, то все узлы связного графа были просмотрены, следовательно, целевой узел недостижим из начального; завершить поиск с результатом «неудача».

2.6. Вернуться к п. 2.

3. Множество шаблонов – это множество найденных таким образом путей.

Этап 2. Подстановка в сгенерированный шаблон объектов предметной области

После получения множества шаблонов текста стратегических целей в виде последовательности метаобъектов необходимо заменить метаобъекты объектами предметной области. Подстановка осуществляется за счет связи между метаобъектом и объектом предметной области.

Поскольку стратегические цели и задачи формулируются по результатам проведенного анализа, то на вход алгоритму поступает некоторое конечное подмножество объектов предметной области. Возможны следующие случаи:

– одному метаобъекту соответствует ровно один объект предметной области. В этом случае в шаблон текста стратегии подставляется этот объект;

– одному метаобъекту соответствует более одного объекта предметной области. В этом случае в шаблон подставляется несколько объектов с пометкой, что эти объекты соответствуют одному и тому же метаобъекту. На следующем этапе такую ситуацию необходимо обработать;

– одному метаобъекту не соответствует ни один объект предметной области. Если метаобъект является обязательным, то подобного рода ситуация должна вызвать ошибку. Если метаобъект не является обязательным, то метаобъект удаляется из шаблона;

– нескольким метаобъектам соответствует один и тот же объект предметной области. Данная ситуация является ошибочной.

Этап 3. Разбиение на предложения

На третьем этапе происходит разбиение полученного шаблона на предложения. Для этого определяются метаобъекты, которым соответствует несколько объектов предметной области. Обработка этих ситуаций происходит следующим образом:

1. В шаблоне отсутствуют метки повторяющихся метаобъектов. В этом случае текст шаблона не разбивается на предложения. Конец алгоритма.

2. Если в шаблоне присутствует только одна метка повторяющегося метаобъекта…

2.1. …выделяем связи между объектами предметной области с типом is parent. Если связь между повторяющимися метками найдена, то разбиваем шаблон на N+2 связанных предложения, где N – число потомков. В первое предложение помещаем все объекты, являющиеся родителем, и все неповторяющиеся элементы в заданном шаблоном порядке. Следующее предложение – это фраза «Цель может быть достигнута путем достижения смежных целей», следующие N предложений – это последовательность, заданная шаблоном, из неповторяющихся элементов и одного из потомка. Для каждого предложения перейти на шаг 1.

2.2. Иначе необходимо соединить объекты предметной области через запятую, а последнюю пару через союз «и». Конец алгоритма.

3. В шаблоне присутствует несколько меток повторяющихся метаобъектов.

Выделяем связи между объектами предметной области с типом «относятся к цели N», где N – номер цели, присвоенной на этапе анализа. Разбиваем текст-шаблон на N однотипных предложений. Каждое предложение должно состоять из объектов, объединенных одной связью, и неповторяющихся элементов. Для каждого предложения перейти на шаг 1.

Этап 4. Ранжирование сгенерированных шаблонов

На четвертом этапе происходит ранжирование сгенерированных шаблонов. Поскольку разным пользователям необходима разная детализация, то при выборе шаблона текста стратегической цели необходимо учитывать модель адресата текста. При определении адресата текста должна быть задана степень детализации синтезируемого текста. Она может быть задана как точным числом, так и лингвистической переменной. Степень детализации определяется как сумма числа метаобъектов в шаблоне текста стратегии и числа предложений в тексте. Если под заданную степень детализации попадают несколько шаблонов, то эти шаблоны ранжируются по сумме весов связей между метаобъектами в шаблоне текста, полученного на первом этапе.

Методы изменения шаблонов стратегических целей

Изменение шаблона синтезируемых целей может быть осуществлено при выполнении следующих условий:

– изменяется модель метаобъектов. Изменение категорийных понятий предметной области и\или связей между ними неизбежно приводит к изменению синтезируемого шаблона текста стратегии, так как меняется структура шаблона;

– изменяется модель предметной области. Данное изменение повлечет изменение семантической структуры стратегической цели (за счет изменения представлений о предметной области);

– изменяются связи между метаобъектами и объектами предметной области. Данное изменение может привести к изменению структуры текста стратегии.

Описанные выше изменения задаются множествами правил трансформации TransformFunction (), задаваемых моделью. При выполнении одного из правил трансформации шаблон стратегической цели будет изменен.

Методы выбора шаблона цели

После того как сгенерированы шаблоны стратегических целей, необходимо выбрать шаблон, в который в конечном итоге будут подставлены индивидуальные данные. В данной работе предлагается выбрать первый в соответствии с рангом сгенерированный шаблон стратегической цели.

ПРИМЕР ГЕНЕРАЦИИ ТЕКСТА СТРАТЕГИИ

Пусть модель MetaModel задается графом на рисунке 2, а пример модели предметной области Model задается графом на рисунке 3. Зеленым выделены объекты предметной области, которые попали на вход алгоритму генерации текста стратегических целей.

Условные обозначения на рисунке 3 (связь метаобъекта и объекта): круг – объект; прямоугольник – императив; скошенный прямоугольник – определение; ромб – показатель, трапеция – срок, перевернутая трапеция – ресурс.

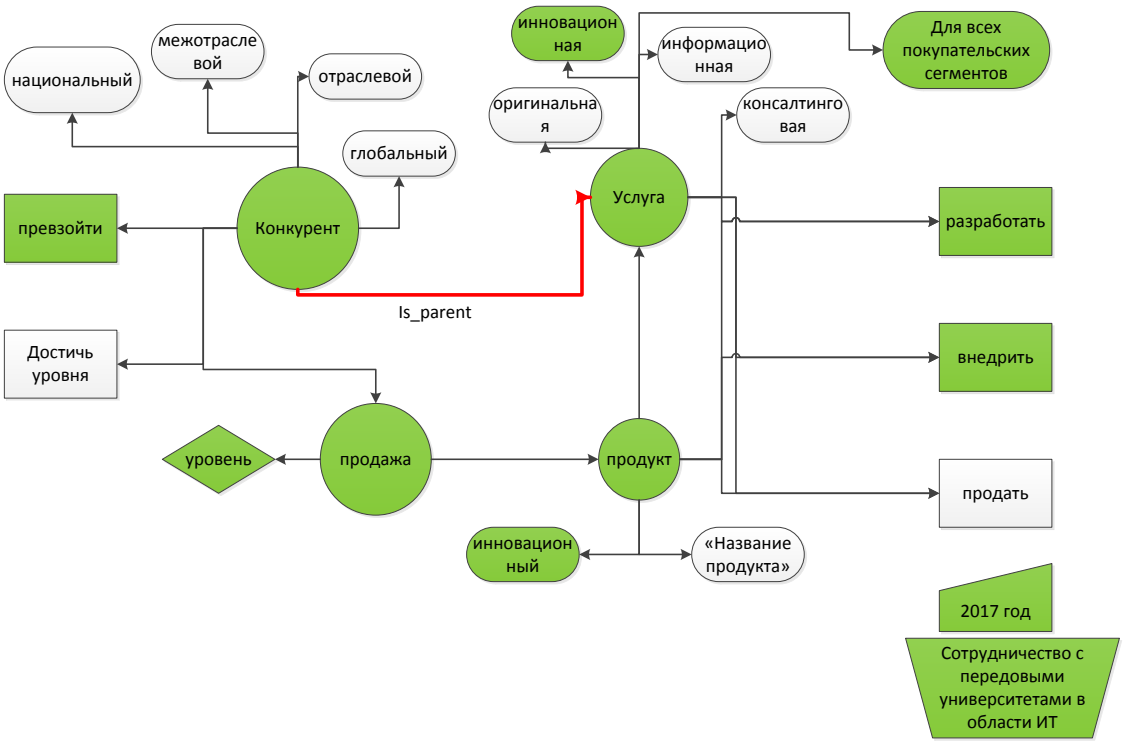

Рисунок 3 – Пример части модели предметной области

При синтезе шаблона текста по модели, заданной графом (рис. 2) могут быть получены следующие шаблоны:

1. Императив – объект – срок – ресурс – целевое значение.
2. Императив – объект – ресурс – срок – целевое значение.
3. Императив – объект – ресурс – целевое значение – срок.
4. Императив – объект – срок – целевое значение – ресурс.
5. Императив – объект – целевое значение – срок – ресурс.
6. Императив – объект – целевое значение – ресурс – срок.
7. Императив – объект – субъект – срок – ресурс – целевое значение.
8. Императив – объект – субъект – ресурс – срок – целевое значение.
9. Императив – объект – субъект – ресурс – целевое значение – срок.
10. Императив – объект – субъект – срок – целевое значение – ресурс.
11. Императив – объект – субъект – целевое значение – срок – ресурс.
12. Императив – объект – субъект – целевое значение – ресурс – срок.

После подстановки объектов предметной области и разбиения на предложения можно получить следующие стратегические цели:

1. Превзойти конкурентов по уровню продаж инновационных продуктов и услуг для всех покупательских сегментов к 2017 году. Цель может быть достигнута путем достижения смежных целей. Необходимо разработать и внедрить инновационные продукты и услуги для всех покупательских сегментов путем сотрудничества с передовыми университетами в области ИТ.

2. Превзойти конкурентов по уровню продаж продуктов и услуг для всех покупательских сегментов к 2017 году путем сотрудничества с передовыми университетами в области ИТ. Цель может быть достигнута путем достижения смежных целей. Необходимо разработать и внедрить инновационные продукты и услуги за счет сотрудничества с передовыми университетами в области ИТ к 2017 году.

3. Превзойти конкурентов к 2017 году по уровню продаж инновационных продуктов и услуг за счет сотрудничества с передовыми университетами в области ИТ. Цель может быть достигнута путем достижения смежных целей. Необходимо разработать и внедрить инновационные продукты и услуги для всех покупательских сегментов.

ЗАКЛЮЧЕНИЕ

В данной работе были рассмотрены проблемы, связанные с синтезом текста на естественном языке стратегических целей и стратегии их достижения: формулирование целостной непротиворечивой конкретной стратегии; однозначная интерпретируемость текстов стратегических целей и стратегии на различные естественные языки; применение и комбинации требований к формулируемым целям; поиск оптимального дискурса для различных групп пользователей.

После проведения анализа существующих подходов к автоматической генерации текста на естественном языке было предложено использовать подход, используемый в системах ГЕЯ. Основной задачей в подобных системах является моделирование структуры текста.

В данной работе была разработана двухуровневая модель для синтеза текста стратегических целей. Модель учитывает как изменяющиеся требования к формулировке цели, так и изменения в предметной области.

В статье также описаны разработанные автором методы для синтеза стратегических целей, особое внимание уделено группе методов по моделированию структуры текста: планированию содержания текста и микропланированию.

Разработанный математический аппарат может быть использован для синтеза текста, соответствующего некоторым заранее заданным критериям.

СПИСОК ЛИТЕРАТУРЫ

1. Энциклопедия менеджеров [Электронный ресурс]. – URL: http://www.e-xecutive.ru/wiki/index.php/%D0%A6%D0%B5%D0%BB%D0%B8_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8 (дата обращения 07.11.2015).
2. Литвак Б.Г. Управленческие решения. – М., 2012. – 512 с.
3. Судаков Б.Н., Маленкин А.С. Методы синтеза естественно-языковых текстов в экспертных системах // Вестник НТУ ХПИ, 2012. – № 38 [Электронный ресурс]. – URL: http://cyberleninka.ru/article/n/metody-sinteza-estestvenno-yazykovyh-tekstov-v-ekspertnyh-sistemah (дата обращения 30.10.2015).
4. Соколова Е.Г., Болдасов М.В. Автоматическая генерация текстов на ЕЯ (портрет направления) // Компьютерная лингвистика и интеллектуальные технологии, 2004 [Электронный ресурс]. – URL: http://www.dialog-21.ru/Archive/2004/Sokolova.htm (дата обращения 07.11.2015).
5. Reiter E. NLG vs. Templates // Proceedings of the Fifth European Workshop on Natural-Language Generation (ENLGW-1995), 1995.

6. Пруцков А.В., Розанов А.К. Методы морфологической обработки текстов // Прикаспийский журнал: управление и высокие технологии, 2014. – № 3(27). – С. 119-133.

Полевая Ольга Михайловна
ФГАОУ «Российский университет дружбы народов», г. Москва
Аспирант кафедры информационных технологий.
Тел.: 8 965 304 62 04
E-mail: o.m.balakhonova@gmail.com

O.M. POLEVAYA *(Post-graduate Student of the Department of Information Systems)*
Peoples' Friendship University of Russia, Moscow

MATHEMATICAL SOFTWARE FOR STRATEGY TEXT SYNTHESIS IN INFORMATION SYSTEMS FOR STRATEGIC MANAGEMENT

This document enumerates problems concerning strategy text synthesis in natural language and gives the description of developed model and methodology for strategy text synthesis. Developed mathematical software makes possible to synthesize text for different user's groups and it takes under consideration possible requirement changes to strategy goal format and changes in knowledge domain.

Keywords: *automatic text synthesis in natural language; text synthesis model; strategy goal synthesis methods.*

BIBLIOGRAPHY (TRANSLITERATED)

1. E'nciklopediya menedzherov [E'lektronny'j resurs]. – URL: http://www.e-xecutive.ru/wiki/index.php/%D0%A6%D0%B5%D0%BB%D0%B8_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8 (data obrashheniya 07.11.2015).
2. Litvak B.G. Upravlencheskie resheniya. – M., 2012. – 512 s.
3. Sudakov B.N., Malenkin A.S. Metody' sinteza estestvenno-yazykovy'x tekstov v e'kspertny'x sistemax // Vestnik NTU XPI, 2012. – № 38 [E'lektronny'j resurs]. – URL: http://cyberleninka.ru/article/n/metody-sinteza-estestvenno-yazykovyh-tekstov-v-ekspertnyh-sistemah (data obrashheniya 30.10.2015).
4. Sokolova E.G., Boldasov M.V. Avtomaticheskaya generaciya tekstov na EYa (portret napravleniya) // Komp'yuternaya lingvistika i intellektual'ny'e texnologii, 2004 [E'lektronny'j resurs]. – URL: http://www.dialog-21.ru/Archive/2004/Sokolova.htm (data obrashheniya 07.11.2015).
5. Reiter E. NLG vs. Templates // Proceedings of the Fifth European Workshop on Natural-Language Generation (ENLGW-1995), 1995.
6. Pruckov A.V., Rozanov A.K. Metody' morfologicheskoj obrabotki tekstov // Prikaspijskij zhurnal: upravlenie i vy'sokie texnologii, 2014. – № 3(27). – S. 119-133.

УДК 575.112:004

П.П. СИЛАЕВ

О МЕТОДАХ СБОРКИ ГЕНОМНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА ГРАФИЧЕСКОМ УСКОРИТЕЛЕ

В данной статье рассматриваются различные подходы к сборке геномной последовательности. В частности, приводится алгоритм сборки ДНК с использованием графа Де Брюйна и способы его распараллеливания на векторном графическом ускорителе.

Ключевые слова: *сборка ДНК; графический ускоритель; секвенирование.*

ВВЕДЕНИЕ

В настоящее время исследование генома является наиболее быстроразвивающимся направлением биомедицины, но его популяризация осложняется крайне высокой ресурсоемкостью получения промежуточных результатов. С применением векторных вычислителей графических процессоров персональных компьютеров молекулярная биология получает новый виток развития.

Использование результатов расшифровки ДНК в медицине и других отраслях народного хозяйства является одной из самых актуальных задач человечества. Процесс расшифровки подразумевает точное определение последовательности нуклеотидов и запись их в машинно-читаемом виде (оцифровку). Повышение эффективности в изучении ДНК возможно благодаря полной «оцифровке» структуры молекул. Формирование машинного представления исходной структуры ДНК является наиболее ресурсоемкой операцией во всей цепочке преобразований [1].

Современные секвенаторы, используя метод de novo, позволяют существенно повысить эффективность «оцифровки» молекул ДНК.

СБОРКА ГЕНОМНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Процесс секвенирования геномной последовательности в целом можно разделить на следующие этапы:

1) планирование эксперимента;
2) сбор и подготовка образцов ДНК;
3) секвенирование;
4) предварительная обработка;
5) сборка геномной последовательности;
6) анализ результатов после сборки.

Современные технологии вычислений на графических процессорах персональных компьютеров могут заметно проявить себя на этапе сборки геномной последовательности.

Данный процесс относится к классу задач высокой вычислительной сложности, которая зависит от объема входных данных и длиной непрерывно читаемого участка (рида). Существует условное различие между собираемыми ДНК по размеру [1]:

- маленькие (несколько мегабаз – бактериальные геномы);
- средние (несколько сотен мегабаз – геномы некоторых растений);
- крупные (гигабазы – геномы млекопитающих и растений).

Входные данные для сборки формируются на этапе секвенирования. На выходе образуется множество ридов R, представленных в цифровом виде.

Задача дальнейшей сборки ДНК сводится к выстраиванию всего множества ридов в единую последовательность D, которая повторяет структуру исходной ДНК.

Отдельно взятый рид получается в результате среза ДНК определенной длины в случайном месте последовательности. Поэтому последовательность, полученную в результате сборки ридов, можно считать достоверной лишь с определенной вероятностью,

которая зависит от множества факторов, одним из которых является степень покрытия каждого участка ДНК ридами. Для повышения точности определения нуклеотидной последовательности повышают уровень покрытия, за счет избыточности данных секвенирования большого множества идентичных копий ДНК (рис. 1).

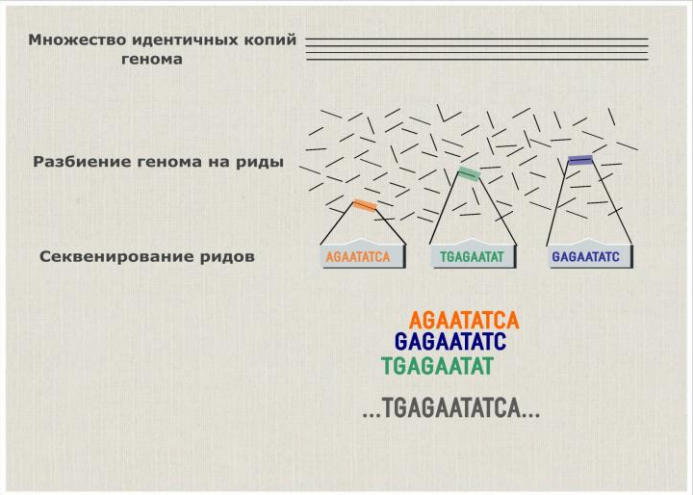

Рисунок 1 – Процесс сборки геномной последовательности

Основываясь на методе секвенирования De novo можно выявить следующие свойства ридов:

1. Один рид r ∈R представляет собой последовательность символов s ∈A, где A = {‘A’, ‘T’, ‘C’, ‘G’} – четырехбуквенный алфавит с мощностью $V_A = 4$, каждая буква которого ставится в соответствии с одним из четырех азотитистых оснований, входящих в состав ДНК;
2. $\mu(len(r)) = N$. В зависимости от типа секвенатора N различно. Малые значения N существенно снижают C (стоимость получения ридов);
3. $\sum_{t=1}^{m} len(r_t) \approx m \cdot N \approx P(N) \cdot len(D)$, где m – количество ридов, P(N) – функция определения степени избыточности информации в зависимости от N (при N = 100, P(N) ≈ 70). Такое равенство обусловлено обеспечением необходимого уровня покрытия для сборки исходной последовательности D;
4. Позиция каждого рида относительно исходной ДНК неизвестна;
5. Процесс секвенирования допускает возникновение ошибок в ридах.

Указанные свойства ридов, полученных на выходе секвенатора, делают решение задачи нетривиальным. При самых оптимистичных оценках сложность алгоритма сборки равна $O(P(N) \cdot len(D))$ или $O(m \cdot N)$, а количество затраченной памяти равно $m \cdot N \cdot log_2 V_A$ бит. В действительности ресурсоемкость процесса вычисления будет сильно больше ввиду нелинейности алгоритмов.

АЛГОРИТМЫ ВОССТАНОВЛЕНИЯ ИСХОДНОЙ НУКЛЕОТИДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА ВЕКТОРНЫХ ВЫЧИСЛИТЕЛЯХ ГРАФИЧЕСКИХ ПРОЦЕССОРОВ ОБЩЕГО НАЗНАЧЕНИЯ

Один из способов решения поставленной задачи в условиях ряда ограничений заключается в нахождении наибольшей общей подпоследовательности (далее НОП) всех пар пересекающихся ридов и определении их смежности и порядка расположения в исходной последовательности. Для поиска НОП требуется применение частных методик, имеющих

возможность параллельной реализации на векторных вычислителях с целью ускорения вычислений, анализ которых представлен ниже.

Нахождение максимального перекрытия между парой ридов обеспечивает наиболее высокую вероятность того, что данная пара в результате склейки будет являться фрагментом исходной последовательности.

Дальнейшая сборка исходной последовательности может проводиться одним из двух способов:

1. Фрагменты, полученные путем склейки пары ридов с НОП, проходят очередную итерацию для поиска перекрытия, максимально используя данные, полученные на предыдущих прогонах, пока не будут собраны в единую последовательность.

2. В случае, если L(НОП) > 0, где L – длина подпоследовательности, для двух произвольных ридов производится склеивание, запоминая L(НОП) для каждой склеенной пары. Далее производится переклеивание ридов, если найдется рид, где L`(НОП) > L(НОП), после чего возвращается рид со «слабым притяжением» в общую коллекцию ридов.

Очевидным фактом является то, что самой частой операцией для всего набора входных данных является нахождение наибольшей общей подпоследовательности для пары строк. Данное утверждение дает возможность для повышения быстродействия использовать векторные параллельные вычислители графических процессоров (GPU), построенные по принципу SIMD (одиночный поток команд, множественный поток данных), который позволяет обеспечить параллелизм на уровне данных (рис. 2).

Вектором вычислений выступает один из алгоритмов поиска максимальной общей подстроки. Потоком данных является набор ридов. На вход вектора подается пара ридов, а на выходе получаем наибольшую общую подстроку для данных ридов.

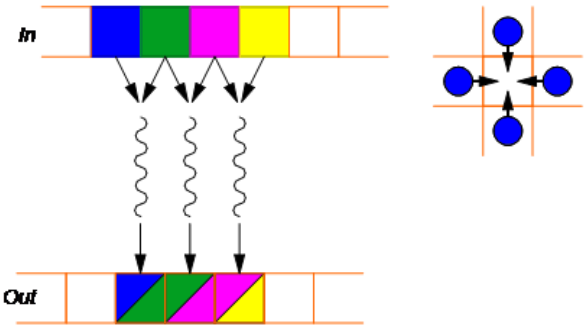

Рисунок 2 – Редуцирование данных при параллельной обработке

Алгоритм Нидлмана-Вунша является первым примером приложения динамического программирования в области сравнению биологических последовательностей. Для поиска НОП необходимо построить массив *F*, содержащий столько же строк, сколько символов в последовательности *A*, и столько же столбцов, сколько символов в последовательности *B*. Таким образом, при решении задачи, для строк с размерам *n* и *m* количество требуемой памяти будет *O(mn)*. Псевдокод для вычисления матрицы:

```
For i=0 to length(A)
    F(i,0) ← d*i
for j=0 to length(B)
    F(0,j) ← d*j
for i=1 to length(A)
for j = 1 tolength(B)
    {
      Match ← F(i-1,j-1) + S(Ai, Bj)
      Delete ← F(i-1, j) + d
```

```
        Insert ← F(i, j-1) + d
        F(i,j) ← max(Match, Insert, Delete)
    }
```

После вычисления матрицы F ее элемент F_{ij} дает максимальную оценку среди всех возможных совпадений. Для вычисления подпоследовательности, которое получило такую оценку, нужно начать с правой нижней клетки и сравнивать значения в ней с тремя возможными источниками (соответствие, вставка или делеция), чтобы увидеть, откуда оно появилось.

Алгоритм Хиршберга имеет схожий принцип работы и решает поставленную задачу, используя $O(n+m)$ количество памяти, но примерно вдвое большее время счета.

Суффиксный автомат (или ориентированный ациклический граф слов) – это мощная структура данных, которая позволяет решать множество строковых задач. Например, с помощью суффиксного автомата можно искать все вхождения одной строки в другую или подсчитывать количество различных подстрок данной строки – обе задачи он позволяет решать за линейное время.

На интуитивном уровне суффиксный автомат можно понимать как сжатую информацию обо всех подстроках данной строки. Впечатляющим фактом является то, что суффиксный автомат содержит всю информацию в настолько сжатом виде, что для строки длины n он требует лишь $O(n)$ памяти. Более того, он может быть построен также за время $O(n)$ (если мы считаем размер алфавита константой).

Суффиксным автоматом для данной строки s называется такой минимальный детерминированный конечный автомат, который принимает все суффиксы строки s.

Расшифруем это определение.

1. Суффиксный автомат представляет собой ориентированный ациклический граф, в котором вершины называются состояниями, а дуги графа – это переходы между этими состояниями.

2. Одно из состояний t_0 называется начальным состоянием, оно должно быть истоком графа (т.е. из него достижимы все остальные состояния).

3. Каждый переход в автомате – это дуга, помеченная некоторым символом. Все переходы, исходящие из какого-либо состояния, обязаны иметь разные метки. С другой стороны, из состояния может не быть переходов по каким-либо символам.

4. Одно или несколько состояний помечены как терминальные состояния. Если мы пройдем из начального состояния t_0 по любому пути до какого-либо терминального состояния и выпишем при этом метки всех пройденных дуг, то получится строка, которая обязана быть одним из суффиксов строки s.

5. Суффиксный автомат содержит минимальное число вершин среди всех автоматов, удовлетворяющих описанным выше условиям. Минимальность числа переходов не требуется, т.к. при условии минимальности числа состояний в автомате не может быть «лишних» путей, иначе это нарушило бы предыдущее свойство.

Для решения задачи будем осуществлять проход по строке T, для каждого префикса будем искать наидлиннейший суффикс этого префикса, встречающийся в S. Иными словами, мы для каждой позиции в строке T хотим найти наидлиннейшую общую подстроку S и T, заканчивающуюся именно в этой позиции. Для этого будем поддерживать две переменные – текущее состояние W и текущую длину l. Эти две переменные будут описывать текущую совпадающую часть – ее длину и состояние, которое соответствует ей (без хранения длины нельзя обойтись, поскольку одному состоянию может соответствовать сразу несколько строк разной длины).

Изначально $p=t_0$, $l=0$, т.е. совпадение пустое.

Пусть теперь мы рассматриваем символ $T[i]$ и хотим пересчитать ответ для него.

1. Если из состояния W в автомате есть переход по символу $T[i]$, то мы просто совершаем этот переход и увеличиваем l на единицу.

2. Если же из состояния *W* нет требуемого перехода, то мы должны попытаться укоротить текущую совпадающую часть, для чего надо перейти по суффиксной ссылке: *W = link(W)*.

3. При этом текущую длину надо укоротить, но оставить максимально возможной. Очевидно, для этого надо присвоить *l = len(W)*, поскольку после прохода по суффиксной ссылке нас удовлетворит подстрока любой длины, соответствующая этому состоянию: *l = len(W)*.

4. Если из нового состояния вновь не будет перехода по требуемому символу, то мы снова должны пройти по суффиксной ссылке и уменьшить *l*, и так далее, пока не найдем переход (тогда перейдем к пункту 1) или мы не попадем в фиктивное состояние *-1* (что означает, что символ *T[i]* вообще не встречается в *S*, поэтому присваиваем *W=l=0* и переходим к следующему *i*).

Ответом на задачу будет максимум из значений *l* за все время обхода.

Асимптотика такого прохода составляет *O(len(T))*, поскольку за один ход мы можем либо увеличить на единицу *l*, либо сделать несколько проходов по суффиксной ссылке, каждый из которых будет строго уменьшать значение *l*. Следовательно, уменьшений не могло быть больше *len(T)*, что и означает линейную асимптотику.

Следует также отметить, что приведенные алгоритмы поддаются распараллеливанию, и существуют их отдельные реализации для GPU.

Недостаток алгоритма Нудлмана-Вунша и использование суффиксных массивов заключается в квадратичной арифметической сложности относительно исходных данных. При больших объемах входных (муммарный объем ридов человеческой ДНК ~700GB) данных приведенные алгоритмы не применимы.

Граф Де Брюйна. Предположим, что мы имеем исходную ДНК *TAATGCCATGGGATGTT*. Найдем все возможные *k-меры* (срезы длины *k*) данной последовательности при *k=3* и построим вырожденный направленный граф, ребрами которого будут являться *3-меры*.

Для каждого 3-мера найдем два возможных *(k-1)-мера*, которые будут являться префиксом и суффиксом *k-мера* соответственно. Преффикс и суффикс каждого k-мера становится начальным и конечным узлом соответствующего ребра.

Объединяя одинаковые узлы графа так, как если бы эти узлы были образованы покрытием ридов, можно добиться существенного упрощения. Например, есть три узла *AT*, и их можно объединить в один узел (рис. 3). Аналогично можно проделать с узлами *TG* и *GG*.

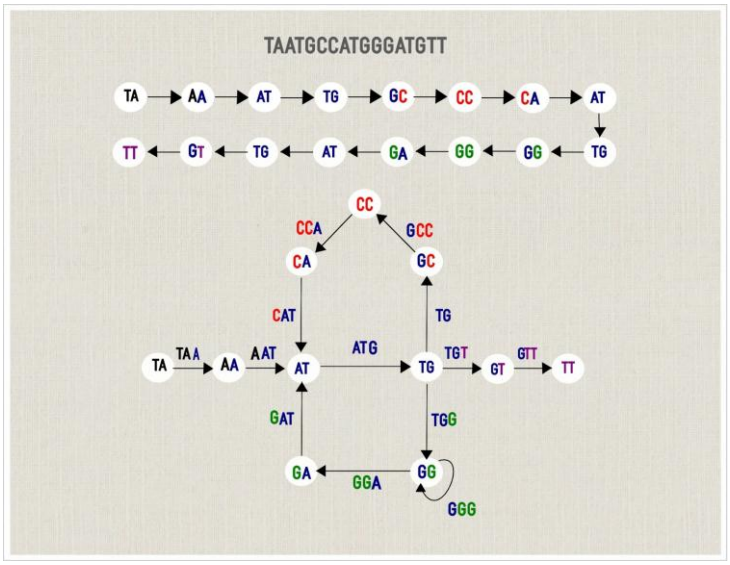

Рисунок 3 – Граф Де Брюйна

Полученный граф называется графом де Брюйна от *TAATGCCATGGGATGTT* и обозначается DeBruijn3(*TAATGCCATGGGATGTT*). Заметим, что граф де Брюйна имеет три различных ребра, соединяющие *AT* и *TG*, что свидетельствует о наличии трех одинаковых путей проходящих через две вершины, которые можно объединить в одно, указав соответствующий вес ребра.

Для реконструирования исходной ДНК необходимо найти Эйлеров путь в графе, то есть пройтись по всем вершинам ровно один раз. Одно из свойств графа де Брюйна доказывает наличие в нем Эйлерового пути или цикла. Начало и конец графа можно определить по нечётной степени

Применительно к ридам граф де Брюйна строится аналогичным образом. При достаточном уровне покрытия граф получается идентичным, как если бы строили его из исходной последовательности [2-3].

Неоптимальные входные данные для построения графа де Брюйна могут привести к следующим проблемам при определении нуклеотидной последовательности исходной ДНК:

1. Проблема определения Эйлерова пути во фрагментированном графе из-за недостаточного уровня покрытия;
2. Проблема усовершенствования алгоритмов коррекции ошибок секвенирования для игнорирования ошибочных ребер графа;
3. Проблема выбора оптимального значения *k*. Ошибка ведет к невозможности построения целостного графа.

ПАРАЛЛЕЛЬНОЕ ПОСТРОЕНИЕ ГРАФА ДЕ БРЮЙНА

Несмотря на высокую эффективность данного алгоритма при сборке геномной последовательности, комбинаторная сложность решения задачи остается на высоком уровне из-за сверх большого объема входных данных.

Ускорение построения графа Де Брюйна возможно благодаря распараллеливанию отдельных подзадач на GPU. Для применения графических процессоров необходимо сузить круг задач, для потенциальной параллельной реализации выполняющейся на векторном вычислителе. К таким задачам можно отнести:

1. Построение *k-меров* для каждого рида.
2. Вычисление префикса и суффикса*k*-мера.
3. Индексирование уникальных узлов графа для его более компактного хранения.

На начальном этапе построения графа обязательным действием, которое затрагивает весь поток ридов, является выделение *k-меров*. Вектором вычислений для данной подзадачи будет выступать алгоритм получения всех срезов входной последовательности длины k и разбора на префиксы, а потоком данных будет являться набор ридов. На выходе получается поток k-меров.

На следующем этапе при упрощении графа необходим быстрый поиск одинаковых узлов. С этой целью необходимо построить хэш для каждого узла графа.

Таким образом, представляется возможным полностью распараллелить построение графа. Поиск пути в графе удастся распараллелить частично, но основной поток выражен неделимым циклом обхода графа, оптимизировать который довольно трудно.

ВЫВОДЫ

В данной статье были рассмотрены основные этапы секвенирвания ДНК методом de novo. Была обозначена проблема сборки и пути ее решения. Предложны основные подходы к параллельной сборке геномной последовательности. В результате решения поставленной задачи возник ряд проблем, требующих детального анализа для их решения:

1. Проблема определения Эйлерова пути во фрагментированном графе из-за недостаточного уровня покрытия.

2. Проблема усовершенствования алгоритмов коррекции ошибок секвенирования для игнорирования ошибочных ребер графа.

3. Проблема выбора оптимального значения *k*. Ошибка ведет к невозможности построения целостного графа.

СПИСОК ЛИТЕРАТУРЫ

1. Konrad Paszkiewicz and David J. Studholme (2010) De novo assembly of short sequence reads. BRIEFINGS IN BIOINFORMATICS. page 1 of 16 doi:10.1093/bib/bbq020.
2. Phillip E. C. Compeau and Pavel A. Pevzner (2010) Genome Reconstruction: A Puzzle with a Billion Pieces. http://zhurnal.ape.relarn.ru/articles/2004/199.pdf (accessed 10 January 2016).
3. Ben Langmead, Cole Trapnell, Mihai Pop and Steven L Salzberg (2009) Ultrafast and memory-efficient alignment of short DNA sequences to the human genome. Genome Biology 2009, 10:R25 doi:10.1186/gb-2009-10-3-r25.

Силаев Павел Павлович
ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
Аспирант
Email: kaktyzzz89@gmail.com

P.P. SILAEV *(Post-graduate Student)*
Belgorod National Research University, Belgorod

METHODS FOR ASSEMBLY GENOMIC SEQUENCES OF GRAPHIC ACCELERATORS

This article discusses various approaches to the assembly of genomic sequences. In particular, given the DNA collection algorithm using the Graph De Bruijn and methods for parallelization on the vector graphics accelerator (GPU).

Keywords: *assembling DNA; graphics accelerator; GPU; sequencing.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Konrad Paszkiewicz and David J. Studholme (2010) De novo assembly of short sequence reads. BRIEFINGS IN BIOINFORMATICS. page 1 of 16 doi:10.1093/bib/bbq020.
2. Phillip E. C. Compeau and Pavel A. Pevzner (2010) Genome Reconstruction: A Puzzle with a Billion Pieces. http://zhurnal.ape.relarn.ru/articles/2004/199.pdf (accessed 10 January 2016).
3. Ben Langmead, Cole Trapnell, Mihai Pop and Steven L Salzberg (2009) Ultrafast and memory-efficient alignment of short DNA sequences to the human genome. Genome Biology 2009, 10:R25 doi:10.1186/gb-2009-10-3-r25.

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СЕТИ

УДК 621.396

Ч.Д. ЛЕ, О.А. СИМОНИНА

МЕХАНИЗМ ПРИОРИТЕЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ МИНИМИЗАЦИИ ЗАДЕРЖКИ В УСЛОВИЯХ КОНКУРЕНТНОЙ СРЕДЫ В СЕТЯХ WI-FI С ПЛОТНЫМ РАСПРЕДЕЛЕНИЕМ УСТРОЙСТВ

В статье предложено использовать приоретизацию в сетях Wi-Fi с плотным распределением устройств. Сначала производится классификация трафика по типам, после – объединение точек доступа по группам в зависимости от обслуживаемого типа трафика. Приоритезация выполнена в два этапа – конкуренция между станциями, принадлежащими одной точке доступа, которая дифференцирует разные типы трафика с разными требованиями к задержке, и конкуренция между точками доступа в одной группе.

Ключевые слова: *QoS; WLAN; IEEE 802.11; приоритезация; распределенный сценарий.*

ВВЕДЕНИЕ

В настоящее время растет спрос на функциональность и масштабируемость беспроводных локальных сетей (WLAN), связанный с распространением новых приложений и сетевых устройств. Большинство беспроводных устройств ориентированы на поддержку технологии Wi-Fi в нелицензируемом диапазоне 2.4 ГГц. Нехватка частотного ресурса и отсутствие планирования сети в совокупности с тенденцией быстрого возрастания количества устройств вызывают серьезную проблему конкуренции и взаимовлияния между устройствами. В случае высокой плотности сетевых устройств возникают коллизии из-за использования перекрывающихся частот. При этом полученные пакеты отбрасываются без восстановления данных, осуществляется повторная передача, что увеличивает вероятность порождения новых столкновений. Таким образом, явление интерференции приводит к уменьшению пропускной способности сети, являющейся одним из ключевых показателей качества обслуживания (QoS). Это приводит к существенному увеличению потерь и задержек [2] (вплоть до критических). На рисунке 1 представлено количество попыток передачи при 3, 6, 15 точек доступа (при обращении 3-4 станций на одну точку доступа). Легко видеть, что чем больше количество устройств, тем больше попыток передачи в сетях.

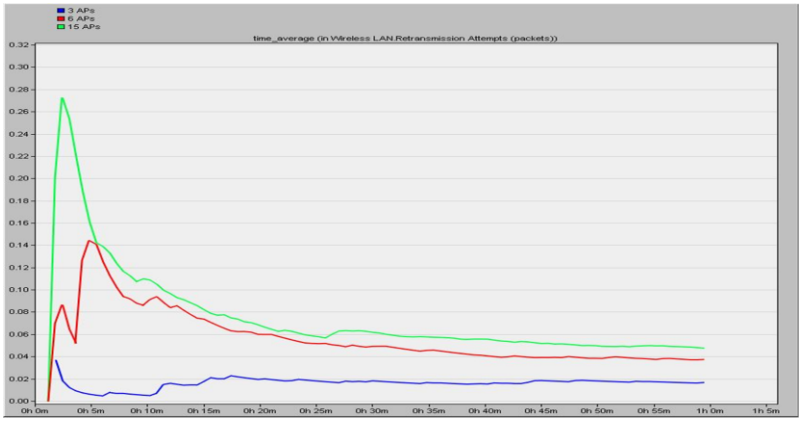

Рисунок 1 – Количество попыток передачи для 3, 6, 15 точек доступа

Существуют два сценария развертывания WLAN-сетей в условиях высокой плотности: централизованный и распределенный. Централизованный сценарий применятся в корпоративных сетях, когда все точки доступа подключаются к одной проводной сети и контролируются одним сетевым оператором. Распределенный сценарий характерен для сетей

домового сегмента, торговых центров, когда точки доступа принадлежат разным владельцам и могут иметь различные административные домены.

Большинство существующих механизмов обеспечения качества обслуживания ориентированы на сети с одной точкой доступа или ad hoc [1, 20, 21]. Существует также несколько решений централизованного сценария, т.е. ориентированного на одного оператора [9, 10, 12, 16, 18, 19]. Большинство этих решений предлагается производителем устройств и реализуется вендорами [4-9, 17]. Недостатком этих решений является неадекватность их применения для распределенного сценария из-за отсутствия координации и связи между отдельными беспроводными сетями.

Кроме механизмов обеспечения QoS, существует ряд исследований, связанных с назначением частот точкам доступа в плотных средах. Они основываются на использовании теории графов или статусов физического уровня и группах неперекрывающихся каналов [11, 13-15, 22]. Однако такие группы каналов ограничены, а количество устройств и точек доступа в случае плотного распределения большое. Также эти решения крайне слабо обеспечивают QoS в WLAN-сетях.

Предлагаемый механизм обеспечения QoS в WLAN-сети со многими точками доступа (APs) для распределенного сценария основывается на приоритезации трафика на основании требований к задержке. Также учитывается конкуренция между APs за право доступа аналогично режиму DCF (Distributed Coordination Function) в WLAN сети [3].

После процедуры конкуренции между APs точка доступа, которая захватила право доступа к среде, дает это право своему WLAN клиенту с самым большим приоритетом аналогично PCF (Point Coordination Function) в WLAN сети [3].

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ QoS ДЛЯ APs

Предлагается объединить режимы доступа PCF и DCF для назначения права доступа к среде точкам доступа (AP) и станции (STA). Механизм приоритезации APs состоит из следующих этапов (рис. 2):

Рисунок 2 – Этапы механизма приоритезации Aps

1. Механизм PCF_in: выполняется в рамках одной AP. Использует список опроса и механизм опроса, чтобы выдавать право доступа к среде каждой конкретной станции STA. В целях поддержки QoS используется модифицированный список опроса.

2. Механизм DCF_out: выполняется для обеспечения конкуренции точек доступа за право доступа к среде.

3. PCF_in использует механизм опроса для передачи данных.

Механизм PCF_in создает список опроса для выдачи права доступа к среде каждой конкретной STA. Процесс создания списка опроса в PCF_in похож на этот процесс в PCF IEEE 802.11: для подключения к BSS (Basic Service Set) отправляется кадр запроса с подполем CF_Pollable, в котором устанавливается значение True. Для реализации поддержки QoS в список опроса введена возможность приоритезации.

Весь трафик разделен на 4 типа: голос (voice), видео (video), эластичный (Best Effort), фоновый (Background), и каждому типу сопоставлены значения задержки (табл. 1) [23-26].

Таблица 1 – Требование параметра задержки для каждого типа трафика

Приориет *m*	**Тип трафика**	**Допустимое значение задержки (*d*, мс)**
1	Voice	< 150
2	Video	150 – 250
3	Best Effort	250 – 400
4	Background	> 400

Выбор задержки в качестве критерия обусловлен конкуренцией между точками доступа: право доступа к среде станциям, имеющим трафик с жестким требованием к задержкам, обеспечивается как первоочередное.

Пусть d – значение предела задержки. Тогда чем меньше d, тем ранее находится в списке данный тип трафика. В случае, если значения d для разных потоков равны, то они помещаются в одну группу m, где m – приоритет группы, m = 1, 2, 3, 4.

Если две STA имеют тип трафика, принадлежащий одной группе, то в списке они располагаются с приоритетом по времени подключения. Пусть k – количество станций STAs в одной группе m. Значение k используется для конкуренции DCF_out и рассматривается как один из параметров для обеспечения QoS. Например, для сети, представленной на рисунке 3, можно создать список опроса для каждой AP, согласно таблице 2.

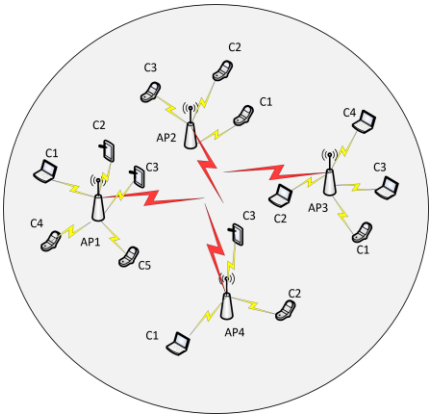

Рисунок 3 – Пример сети для распределенного сценария

Таблица 2 – Список опроса точек доступа для сети рисунка 3

m	**AP1**	**AP2**	**AP3**	**AP4**
1	C1, C2 (k=2)	C1 (k=1)	C1, C2, C3 (k=3)	-
2	C3 (k=1)	-	-	C1, C2 (k=2)
3	C4 (k=1)	C2, C3 (k=2)	-	C3
4	C5 (k=1)	-	C4 (k=1)	-

В целом механизм DCF_out аналогичен DCF в IEEE 802.11 и EDCA в IEEE 802.11n, то есть также использует различные IFS (Inter Frame Spacing) для конкуренции за среду. Однако в данном случае конкуренция происходит между точками доступа, а не между станциями, и доступ основывается на значениях m и k (рис. 4).

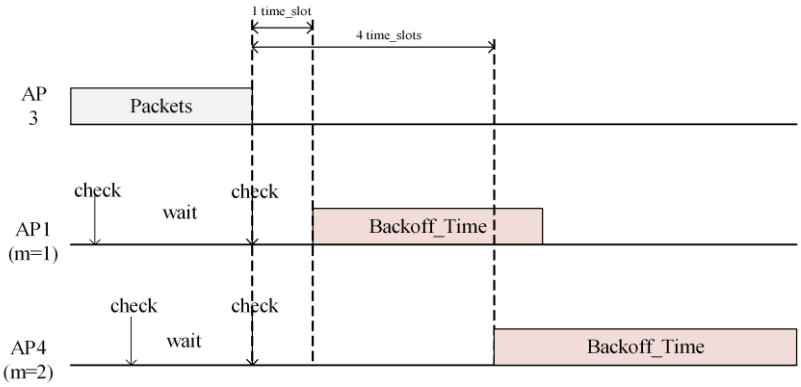

Рисунок 4 – Пример формирования ODIFS(m) в DCF_out для сети рисунка 3

1. Точка доступа AP проверяет на занятость (busy).
2. В случае не занятой среды точки доступа продолжают ждать в течение времени

$$\text{ODIFS}(m), = m_{min} \times slot\_times,$$

где m_{min} – наименьшее значение m в списке опроса, $slot\_times$ = 9 или 20 мс в зависимости от реализации.

Таким образом, приоритезация по времени ожидания ODIFS(m) позволяет трафик чувствительных к задержкам приложений передать быстрее, чем остальной.

Рассмотрим случай, когда много точек доступа имеют одинаковое значение m, то есть одновременно конкурируют доступ к среде. Тогда возможна ситуация, когда две APs предполагают, что среда свободна, и одновременно передают, что приводит к коллизии. Для купирования этой проблемы в механизме DCF_out вводится значение k – количество станций STAs в одной группе m.

ПРИОРИТЕЗАЦИЯ ПРИ КОНКУРЕНЦИИ МЕЖДУ ТОЧКАМИ ДОСТУПА С ОДИНАКОВЫМ ЗНАЧЕНИЕМ *m*

Для того, чтобы сократить задержку из-за конкуренции, предлагается всем STAs в одной группе m выполнить все передачи без конкуренции заново.

Например, в рассматриваемом примере (рис. 3, табл. 2) AP1 имеет m = 1 с двумя STAs (k = 2): C1, C2. Предположим, что AP1 получила доступ к среде. Тогда сначала передаются пакеты C1, затем последовательно передаются пакеты C2. После того, как C2 успешно заканчивает передачи (ACK успешно получено), другие точки доступа могут конкурировать за доступ. Значение k используется для конкуренции между точками доступа по принципу наименьшего: чем меньше значение k, тем быстрее точка получает право доступа к среде. После ожидания ODIFS(m) запускается процедура обратного отсчета Backoff_Time (k):

$$\text{Backoff\_Time}\ (k) = Random()*slot\_time.$$

Random () является произвольным значением в диапазоне значений [x, y], где [x, y] зависит от k, и n – количество одновременно конкурирующих Aps. На рисунке 5 приведен пример для рассматриваемой сети рисунка 3. Для упрощения на рисунке не указываются сообщения ACK.

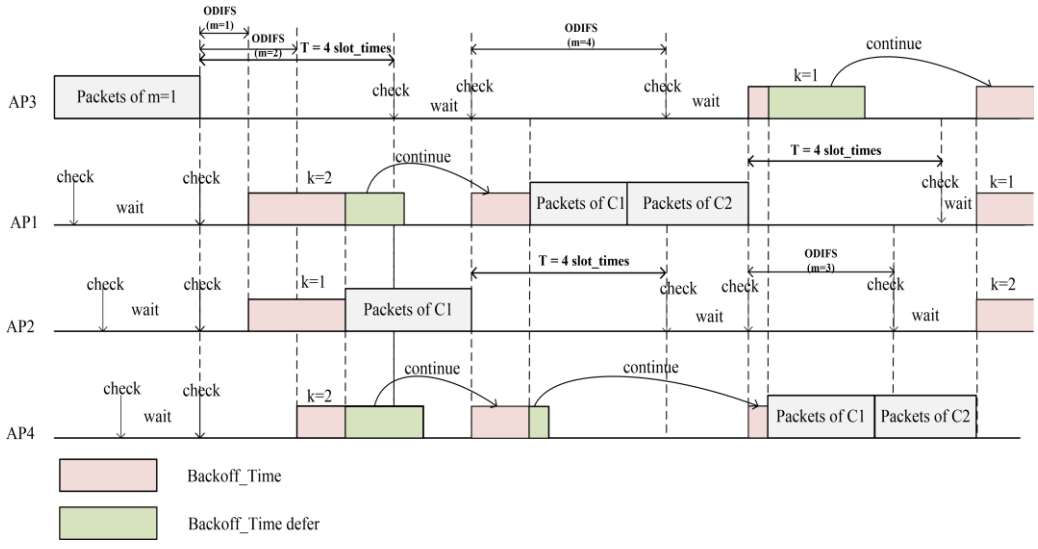

Рисунок 5 – Пример реализации приоритезации при конкуренции между точками доступа с одинаковым значением m для сети рисунка 3

Чтобы гарантировать успешную передачу пакетов в случае коллизии или потери ACK пара [x, y_j], где j – порядковый номер попытки, j_{max}= 7, меняется на [x, y_j + q], где $q \in N^*$, и передача пробуется в следующий раз.

ПРОЦЕДУРА ОПРЕДЕЛЕНИЯ ЗНАЧЕНИЙ [*x, y*]

Пусть S – количество APs, у которых есть возможность конкурирования; n – количество одновременно конкурирующих APs, $n \geq 2$; q – количество значений *Random*() в [*x, y*], $q \in N^*$. Вероятность, что n APs выбирают одно и то же значение *Random*() в [*x, y*]:

$$P_{(n)} = \frac{C_S^n \times q \times 1^{n-1}}{C_S^n \times q^n} = \frac{1}{q^{n-1}}, \quad (1)$$

откуда необходимо найти $q(n)|P_{(n)\to min}$, тогда:

$$q = \sqrt[n-1]{\frac{1}{P_{(n)}}}. \quad (2)$$

Примем, что $P_{(n)}$ имеет следующий приближенный вид:

$$P_{i(n)} = 10^{-i}, \text{ где } i \in N, i \geq 2. \quad (3)$$

Из выражений (2) и (3) следует:

$$q_{i(n)} = 10^{\frac{i}{n-1}}, \text{ где } i \in N, n \in N, i \geq 2, n \geq 2. \quad (4)$$

Здесь $q_{i(n)}$ является искомым количеством значений *Random()* в [*x, y*] в случае, когда n одновременно конкурирующих APs выбрали одно и то же значение *Random()* с вероятностью $P_{i(n)}$. Классификация интервалов значений k не влияет на вероятность и выбор [*x, y*], однако удобства классификации k разделено на 7 групп по 5 значений в одной группе. Распределение диапазонов представлено в таблице 3.

Таблица 3 – Диапазон значений [x, y]

k	**[*x, y*]**
1 - 5	[0,q_i-1]
6 - 10	[q_i, 2q_i -1]
11 - 15	[2q_i, 3q_i-1]
16 - 20	[3q_i, 4q_i -1]
21 - 25	[4q_i, 5q_i -1]
26 - 30	[5q_i, 6q_i -1]
>30	[6q_i, 7q_i -1]

На рисунке 6 представлена зависимость количества $q_{i(n)}$ в интервале [*x, y*] от количества n при i=2,3,4,5,6. График позволяет определить отношение между n, $P_{(n)}$ и q. Например, пусть q=32, тогда $P_{(n)} = \frac{1}{32^{n-1}}$. Кроме случая n = 2, т.е. P(n) ≈ 0,03, при $n \geq 3$, вероятности $P_{(n)} << 10^{-3}$ (рис. 7).

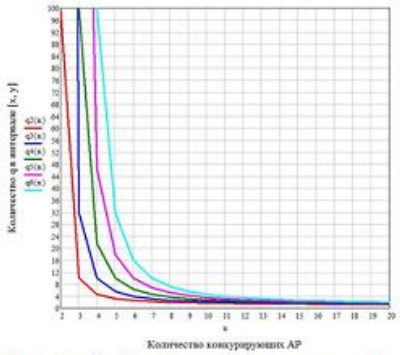

Рисунок 6 – Зависимость количества q_i в интервале [x, y] от количества одновременно конкурирующих APs

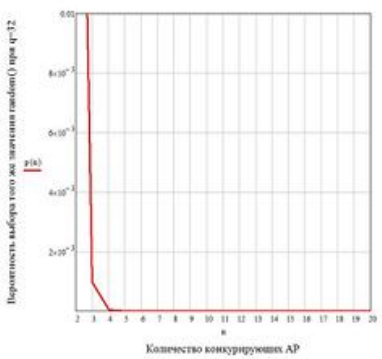

Рисунок 7 – Вероятность, что n конкурирующих APs выбирают одно и то же значение Random() при q=32

Это значит, что при q=32 вероятность, что n конкурирующих APs выбирают одно и то же значение *Random()* очень мала.

ЗАКЛЮЧЕНИЕ

Предложенный механизм использует приоритезацию на двух этапах для повышения способности обеспечения QoS в сетях с высокой плотностью APs. Первый этап: в конкуренции между станциями, принадлежащими одной точке доступа. Эта приоритезация дифференцирует разные типы трафика с разными требованиями к задержке. Второй этап: в конкуренции между точками доступа в одной группе. Эта приоритезация дифференцирует точки доступа с одинаковым значением группы согласно приоритету трафика и позволяет освободить среду как можно быстрее, что приводит к уменьшению задержки. Однако требуется разработка механизма обновления списка опроса, разработка модели формирования задержки и анализ производительности для предложенного механизма.

СПИСОК ЛИТЕРАТУРЫ

1. Malik A. and other. QoS in IEEE 802.11-based wireless networks: A contemporary review // Journal of Network and Computer Applications, 2015. – № 55. – P. 24-46.
2. Lavrukhin V., Simonina O., Volodin E. An experimental study of the key QoS parameters in public Wi-Fi networks // Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on. – IEEE, 2014. – C. 198-203.
3. IEEE Std 802.11™-2012. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012.
4. Florwick J. and other. Wireless LAN design guide for high density client environments in higher education // User Guide, 2011. – P. 1-41.
5. Raniwala A., Chiueh T. Deployment issues in enterprise wireless LANs, 2003 [Электронный ресурс]. – http://www.ecsl.cs.sunysb.edu/tr/wlandeployment.pdf.
6. Enterprise Data Communication Products – Feature Description – WLAN // Huawei Technologies Co. L., 2013. – № 2.
7. Best Practices for High Density Wireless Network Design In Education and Small/Medium Businesses // Netgear, 2014.
8. AutoCell – The Self-Organizing WLAN // Propagate Networks, 2003 [Электронный ресурс]. – URL: http://www.forsitegroup.com/pdf/WP_Propagate-AutoCell-WLAN.pdf.
9. ONEAir1-High Density Business WLAN Access Point // OneAccess Network [Электронный ресурс]. – URL: http://rally.webzona.hu/One%20Access/DATASHEETS/Router/Mobile%20Access%20Router/ONEAir1/datasheets_oneair1.pdf
10. Ali-Ahmad H. and other. An SDN-based network architecture for extremely dense wireless networks // Future Networks and Services (SDN4FNS). – Nov. 2013. – pp. 1-7
11. Drieberg M. Channel Assignment Strategies for Throughput Enhancement in High Density Wireless Local Area Networks // PhD diss., Victoria University. – Jun. 2010.
12. Ahmed N. Interference Management in Dense 802.11 Networks // PhD diss., University of Waterloo. - 2009.
13. Leith D.J. and other. WLAN channel selection without communication // Computer Networks? 2012. – № 56. – Issue 4. – P. 1424-1441.
14. Villegas E., Ferro R., Aspas J. Implementation of a distributed dynamic channel assignment mechanism for IEEE 802.11 networks // Personal, Indoor and Mobile Radio Communications, 2005. – Vol. 3. – P. 1458-1462.
15. Ali G.G.N., Shahin R., Mowna N. Fair Slots Assignment Mechanisms of IEEE 802.11 Networks for Multiple Access Points // Computers and Information Technology, ICCIT'09, 12th International Conference, 2009. –P. 94-99.
16. Zhao D., Zhu M., Xu M. Leveraging SDN and OpenFlow to Mitigate Interference in Enterprise WLAN // Journal of Networks, 2014. – № 9. – Issue 6. – P. 1526-1533.
17. Lee J., Suh Y. J., Yu C. Evaluation on enterprise WLAN techniques // Network of the Future (NOF), 2013 Fourth International Conference on the. – IEEE, 2013. – P. 1-3.

18. Panda M., Kumar A. Cell-level modeling of IEEE 802.11 WLANs // Ad Hoc Networks. – Sep. 2015. – № 25. – P. 84-101.
19. Dely P. and other. CloudMAC – An OpenFlow based architecture for 802.11 MAC layer processing in the cloud // Globecom Workshops, 2012. – P. 186-191.
20. Charfi E., Chaari L., Kamoun L. PHY/MAC enhancements and qos mechanisms for very high throughput WLANs: A survey // Communications Surveys & Tutorials, IEEE 15, 2013. – № 4. – P. 1714-1735.
21. Micó F., Cuenca P., Orozco-barbosa L. QoS Mechanisms for IEEE 802.11 Wireless LANs // High Speed Networks and Multimedia Communications, Springer Berlin Heidelberg, 2004. – P. 609-623.
22. Chickadel A. Interference Reduction in Wireless Networks Using Graph Coloring Methods // Computer Science Research Symposium, 2007. – № 3. – P. 22-29.
23. Xiao, XiPeng. Technical, commercial and regulatory challenges of QoS: An internet service model perspective // Morgan Kaufmann, 2008.
24. Rec ITU G. 114. One way transmission time // International Telecommunication Union, Geneva, 1993. – T. 2003.
25. MAC Bridges, ISO/IEC 10038, ANSI/IEEE Std 802.1D, 1993.
26. Rec. ITU Y. 1541: Network Performance Objectives for IP-Based Services // International Telecommunication Union, Geneva, 2003.

Ле Чан Дык
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург
Аспирант кафедры сетей связи и передачи данных
Тел.: 8 (812) 305-12-65
E-mail: letranduc.telecom@gmail.com

Симонина Ольга Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург
Кандидат технических наук, доцент кафедры сетей связи и передачи данных
Тел.: 8 (812) 305-12-65
E-mail: olga.simonina@spbgut.ru

Ch.D. LE *(Post-graduate Student of the Department of Communication Networks and Data Transmission)*

O.A. SIMONINA *(Candidate of Engineering Sciences, Associate Professor of the Department of Communication Networks and Data Transmission)*
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg

THE MECHANISM OF PRIORITIZATION TO MINIMIZE DELAY IN A COMPETITIVE ENVIRONMENT IN THE WI-FI NETWORKS WITH DENSE DISTRIBUTION OF DEVICES

In the article we suggest to use the prioritization in Wi-Fi networks with dense distribution of devices. At first, traffic classification is performed by types, then associate access points into groups depending on the type of traffics. The prioritization is executed in two stages: the competition between stations belonging to one access point, which differentiates between different types of traffic with different delay requirements, and the competition between access points in the same group.

***Keywords**: QoS; WLAN; IEEE 802.11; prioritization; distributed scenario.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Malik A. and other. QoS in IEEE 802.11-based wireless networks: A contemporary review // Journal of Network and Computer Applications, 2015. – № 55. – P. 24-46.
2. Lavrukhin V., Simonina O., Volodin E. An experimental study of the key QoS parameters in public Wi-Fi networks // Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014

6th International Congress on. – IEEE, 2014. – S. 198-203.

3. IEEE Std 802.11™-2012. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012.
4. Florwick J. and other. Wireless LAN design guide for high density client environments in higher education // User Guide, 2011. – P. 1-41.
5. Raniwala A., Chiueh T. Deployment issues in enterprise wireless LANs, 2003 [E'lektronnyj resurs]. – http://www.ecsl.cs.sunysb.edu/tr/wlandeployment.pdf.
6. Enterprise Data Communication Products – Feature Description – WLAN // Huawei Technologies Co. L., 2013. – № 2.
7. Best Practices for High Density Wireless Network Design In Education and Small/Medium Businesses // Netgear, 2014.
8. AutoCell – The Self-Organizing WLAN // Propagate Networks, 2003 [E'lektronnyj resurs]. – URL: http://www.forsitegroup.com/pdf/WP_Propagate-AutoCell-WLAN.pdf.
9. ONEAir1-High Density Business WLAN Access Point // OneAccess Network [E'lektronnyj resurs]. – URL: http://rally.webzona.hu/One%20Access/DATASHEETS/Router/Mobile%20Access%20Router/ONEAir1/datasheets_oneair1.pdf
10. Ali-Ahmad H. and other. An SDN-based network architecture for extremely dense wireless networks // Future Networks and Services (SDN4FNS). – Nov. 2013. – pp. 1-7
11. Drieberg M. Channel Assignment Strategies for Throughput Enhancement in High Density Wireless Local Area Networks // PhD diss., Victoria University. – Jun. 2010.
12. Ahmed N. Interference Management in Dense 802.11 Networks // PhD diss., University of Waterloo. - 2009.
13. Leith D.J. and other. WLAN channel selection without communication // Computer Networks? 2012. – № 56. – Issue 4. – P. 1424-1441.
14. Villegas E., Ferro R., Aspas J. Implementation of a distributed dynamic channel assignment mechanism for IEEE 802.11 networks // Personal, Indoor and Mobile Radio Communications, 2005. – Vol. 3. – P. 1458-1462.
15. Ali G.G.N., Shahin R., Mowna N. Fair Slots Assignment Mechanisms of IEEE 802.11 Networks for Multiple Access Points // Computers and Information Technology, ICCIT'09, 12th International Conference, 2009. –P. 94-99.
16. Zhao D., Zhu M., Xu M. Leveraging SDN and OpenFlow to Mitigate Interference in Enterprise WLAN // Journal of Networks, 2014. – № 9. – Issue 6. – P. 1526-1533.
17. Lee J., Suh Y. J., Yu C. Evaluation on enterprise WLAN techniques // Network of the Future (NOF), 2013 Fourth International Conference on the. – IEEE, 2013. – P. 1-3.
18. Panda M., Kumar A. Cell-level modeling of IEEE 802.11 WLANs // Ad Hoc Networks. – Sep. 2015. – № 25. – P. 84-101.
19. Dely P. and other. CloudMAC – An OpenFlow based architecture for 802.11 MAC layer processing in the cloud // Globecom Workshops, 2012. – P. 186-191.
20. Charfi E., Chaari L., Kamoun L. PHY/MAC enhancements and qos mechanisms for very high throughput WLANs: A survey // Communications Surveys & Tutorials, IEEE 15, 2013. – № 4. – P. 1714-1735.
21. Micó F., Cuenca P., Orozco-barbosa L. QoS Mechanisms for IEEE 802.11 Wireless LANs // High Speed Networks and Multimedia Communications, Springer Berlin Heidelberg, 2004. – P. 609-623.
22. Chickadel A. Interference Reduction in Wireless Networks Using Graph Coloring Methods // Computer Science Research Symposium, 2007. – № 3. – P. 22-29.
23. Xiao, XiPeng. Technical, commercial and regulatory challenges of QoS: An internet service model perspective // Morgan Kaufmann, 2008.
24. Rec ITU G. 114. One way transmission time // International Telecommunication Union, Geneva, 1993. – T. 2003.
25. MAC Bridges, ISO/IEC 10038, ANSI/IEEE Std 802.1D, 1993.
26. Rec. ITU Y. 1541: Network Performance Objectives for IP-Based Services // International Telecommunication Union, Geneva, 2003.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ

УДК 621.391

В.Е. ДЕМЕНТЬЕВ

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОТОКОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

В статье рассматриваются методики оценки защищенности информационно-телекоммуникационной сети различным воздействиям с использованием уязвимостей протоколов информационного обмена и обмена данными. Для этого конкретизируется понятие протокольного воздействия и протокольной защищенности информационно-телекоммуникационной сети. Вводится и показана зависимость оценки протокольной защищенности от информативности признаков протоколов. В качестве основного подхода используется метод анализа иерархий и распределения ресурса защиты. В качестве примера приводятся результаты оценки защищенности протоколов ИТКС в различных условиях. Делается вывод, что внедрение предлагаемого подхода позволит изменить существующие общепринятые взгляды и подходы к защите ИТКС.

Ключевые слова: *протокол; защита; протокольная защищенность; информативность; оценка; стратегия воздействия; рейтинг; метод анализа иерархий.*

Информационно-телекоммуникационные сети (ИТКС) являются результатом конвергенции компьютерных и телекоммуникационных сетей, их функционирование осуществляется в условиях воздействия некоторой совокупности угроз технологической природы, направленные на элементы и негативно влияющие на эффективность функционирования ИТКС. В связи с этим важной задачей является обеспечение достаточной степени защищенности ИТКС, для чего, в свою очередь, необходимо наличие адекватного аппарата, позволяющего оценить возможные технологические воздействия на ИТКС.

В последнее время вектор воздействия на ИТКС смещается от информационного воздействия, т.е. воздействия на информацию, НСД к информации, к воздействию на технологические процессы, протекающие в ИТКС, в т.ч. и процессы обмена данными. Об этом свидетельствуют отчеты различных аналитических компаний за 2014-2015 годы. К примеру, данные отчетов компаний Positive Technologies, Eset, Kaspersky и других утверждают, что количество инцидентов, связанных с нарушением технологических циклов ИТКС, выросло до 20 раз [1]. Причем подобные воздействия не обнаруживаются традиционными способами защиты информации, а ИТКС функционирует штатно, однако требуемого результата функционирования не достигается. Также необходимо отметить, что технологии построения современных ИТКС претерпели существенные изменения. Современные ИТКС представляют собой результат конвергенции локальных сетей и телекоммуникационных систем, что и приводит к расширению спектра угроз.

В ряду наиболее актуальных угроз, существенно влияющих на общий уровень защищенности ИТКС, стоят различные информационные воздействия (ИВ). По своей сути эти воздействия сводятся к эксплуатации общеизвестных принципов и способов обработки данных, т.е. протокольного взаимодействия между различными элементами сети. В общем виде протокол – это совокупность процедур, определяющих взаимодействие и обмен данными между устройствами, абонентами и уровнями ИТКС. Тогда протокольное воздействие – заранее спланированное целенаправленное воздействие на протоколы информационного обмена, обмена данными, функционального и другого назначения через установление соединения или попытки установления соединения на уровнях эталонной модели взаимодействия открытых систем или других известных моделях Интернета с объектом данного воздействия с определенной целью (задачей воздействия). Цель протокольного воздействия – организация канала утечки информации, модификация,

уничтожение различных данных, блокирование (перевод во внештатный режим работы) ИТКС, а также изменение ее штатного функционирования, приводящее к нарушению или блокированию обмена данными.

В случае, когда речь идет о протокольной защищенности, имеется в виду не состояние ИТКС, которое влияет на уровень ее защиты, а о некоторой совокупности признаков, наличие которых позволяет говорить о возможных ИВ на ИТКС. Наличие или отсутствие подобных ИВ определяется совокупностью признаков, характерных для того или иного протокола ИТКС. Каждый из признаков обладает определенным уровнем информативности, по которому определяется степень опасности протокола для ИТКС. Таким образом, первоначально определяется совокупность критически важных признаков и их степень информативности.

Кроме того, немаловажное значение имеет уровень ИТКС (в соответствии с уровнем ЭМВОС) и набор протоколов соответствующего уровня. Для определения априорной и апостериорной иерархичности ИВ в рамках методологического подхода проводится оценка важности уровней ИТКС и протоколов, соответствующих определенным уровням, что в дальнейшем позволит получить исходные данные для прогнозирования вероятностей воздействия на ИТКС.

В итоге полученные исходные данные используются для оценки протокольной защищенности ИТКС путем определения рейтингов надежности и стойкости каждого протокола ИТКС и формирования матриц защищенности, позволяющих спрогнозировать общий уровень эффективности защиты ИТКС от протокольных воздействий.

В рамках методологической основы протокольной защиты ИТКС рассматривается подход по определению вероятностей протокольных воздействий на ИТКС, который включает:

- методику оценки информативности признаков ИТКС;
- методику оценки комплексного информационного воздействия на протоколы ИТКС;
- методику оценки протокольной защищенности ИТКС;
- алгоритм модификации и идентификации признаков протокольных воздействий на ИТКС;
- устройство программного изменения параметров протокола.

Каждая последующая методика использует исходные данные, полученные в результате расчетов по предыдущей методике. В общем виде научно-методический аппарат обеспечения протокольной защиты представлен на рисунке 1.

Методика оценки комплексного информационного воздействия на протоколы ИТКС предназначена для прогнозирования распределения воздействий на протоколы ИТКС с учетом места и роли этих протоколов в информационном обмене, определения очередности воздействия на них и формирования исходных данных для обоснования мер защиты элементов и ИТКС в целом.

В основе данной методики лежит метод анализа иерархии и распределения ресурса защиты ИТКС [2, 3], которые используются для получения итоговых значений распределения вероятностей воздействия на протоколы ИТКС. В результате применения данной методики решена задача определения наиболее критичных протокольных воздействий (ПВ) для каждого протокола ИТКС.

Для нейтрализации опасных протокольных воздействий необходим их мониторинг, основу которого составляет методика оценки информативности признаков протоколов ИТКС, предназначенная для формирования совокупного пространства признаков протокольных воздействий на ИТКС, распределения признаков в соответствии с уровнем их информативности, а также формирования матриц информативности протоколов в соответствии с признаками протокольных воздействий [4].

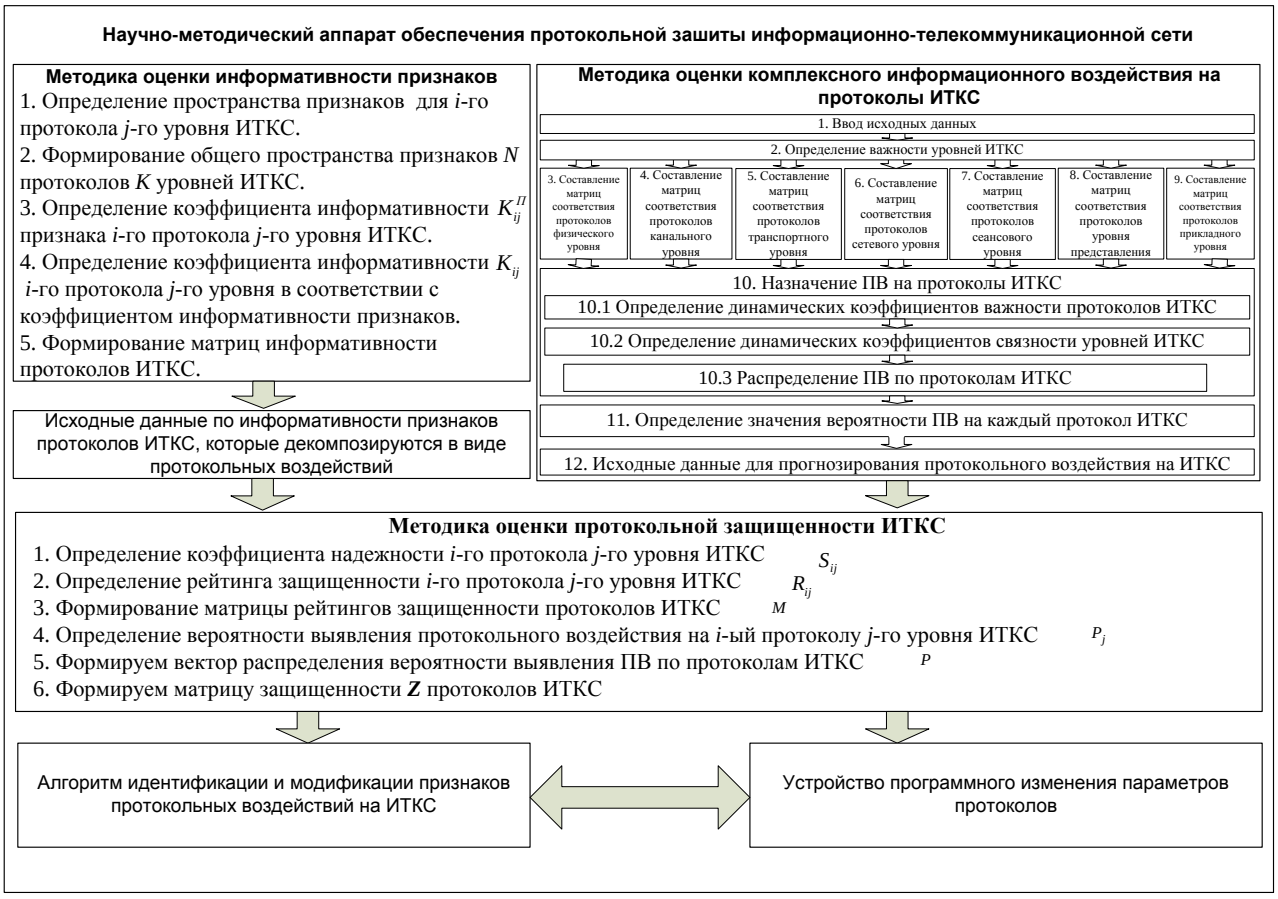

Рисунок 1 – Методологические основы протокольной защиты ИТКС

В основе данной методики лежит способ определения индивидуальных и типовых признаков протоколов ИТКС. В качестве примера рассмотрены некоторые признаки, полученные в результате анализа протоколов ИТКС, и определены значения информативности индивидуальных и типовых признаков.

Для разработки мер защищенности ИТКС необходимо оценить ущерб от ПВ, для чего предлагается методика оценки протокольной защищенности ИТКС, предназначенная для формирования промежуточных рейтингов стойкости и защищенности протоколов ИТКС и определения итогового рейтинга защищенности ИТКС от протокольных воздействий. Представленная методика использует в качестве исходных данных результаты расчетов, полученные по предыдущим методикам. В результате расчета информативности признаков протоколов и защищенности ИТКС, полученные для исходных данных (рис. 2, 3) и для случая, когда информативность признаков протоколов приведена к единому уровню, т.е. отсутствуют индивидуальные признаки, получен итоговый уровень защищенности ИТКС (рис. 4, 5).

Для реализации на практике предлагаемого подхода был разработан алгоритм модификации идентификационных признаков протокольных воздействий на ИТКС, который реализован в рамках разработанного устройства программного изменения параметров протокола. Предполагается, что данное устройство будет размещено на всех элементах ИТКС, что позволит организовать мониторинг параметров (признаков ПВ) ИТКС.

Таким образом, представленная совокупность методик, алгоритма и устройства представляют собой методологические основы протокольной защиты. Однако современные системы защиты ИТКС не рассчитаны на внедрение предлагаемых решений.

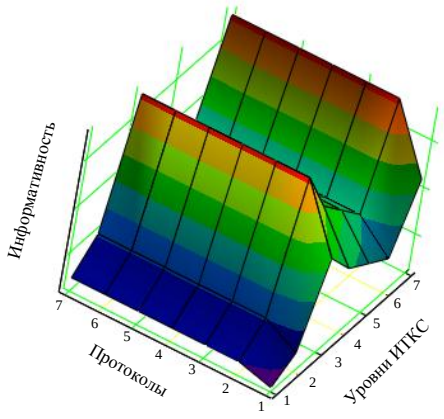

Рисунок 2

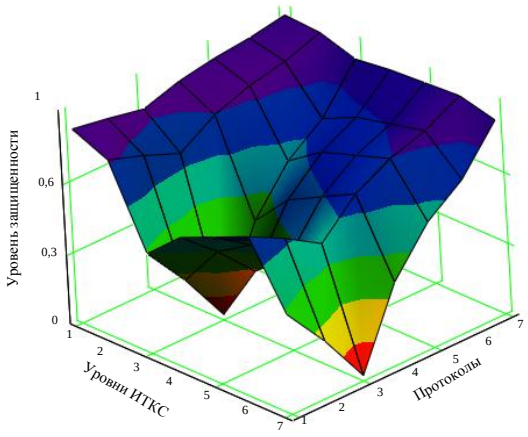

Рисунок 3

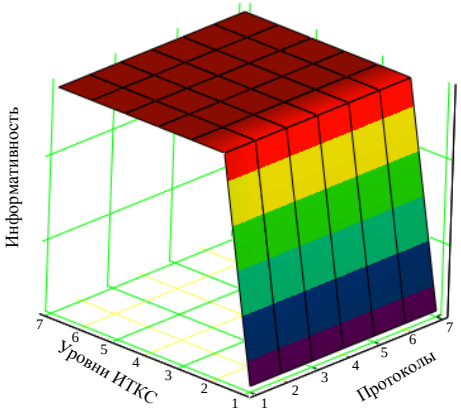

Рисунок 4

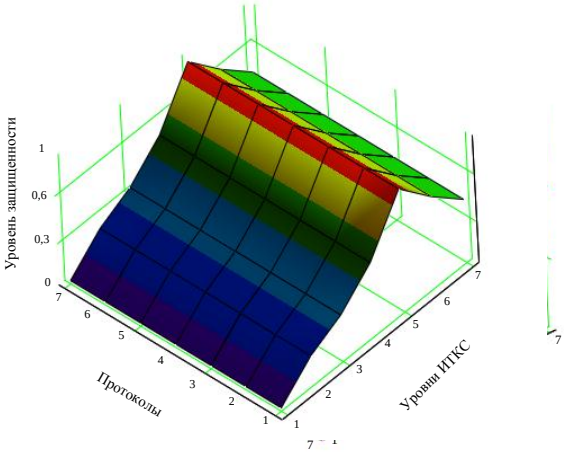

Рисунок 3.
Рисунок 5

Результаты анализа современных средств и методов защиты ИТКС показывают, что в них практически не затронуты возможности противодействия протокольным воздействиям. Большинство известных подходов обнаружения и пресечения ПВ не учитывают специфику функционирования самой ИТКС и решаемых ею задач. Практически отсутствуют комплексные методы и алгоритмы, на основе которых возможно построение средств обнаружения и пресечения ПВ и взаимосвязанных процессов, протекающих в ходе функционирования ИТКС. Недостаточно проработаны методы поддержки и принятия решений в ходе разработки замысла, планов и сценариев противодействия ПВ. Применение нового класса систем протокольной защиты должно существенно повысить защищенность ИТКС и дать адекватный ответ в ходе противодействия ПВ.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Research 2015. Сборник исследований по практической безопасности [Электронный ресурс]. – URL: www.ptsecurity.ru.
2. Берзин Е.А. Оптимальное распределение ресурсов и элементы синтеза систем / под ред. Е.В. Золотова. – М.: «Советское радио», 1974. – 304 с.
3. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 278 с.
4. Коцыняк М.А. и др. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М.А. Коцыняк, А.И. Осадчий, М.М. Коцыняк, О.С. Лаута, В.Е. Дементьев, Д.Ю. Васюков. – Спб.: ЛО ЦНИИС, 2015. – 126 с.

Дементьев Владислав Евгеньевич
Военная академия связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург
Кандидат технических наук, докторант
E-mail: dem-vlad@rambler.ru

V.E. DEMENT'EV *(Candidate of Engineering Sciences, Doctoral Student)*
Military Academy of Telecommunications named after Marshal S.M. Budyonny, Saint Petersburg

METHODOLOGICAL FOUNDATION FOR THE PROTOCOL PROTECTION OF INFORMATION AND TELECOMMUNICATION NETWORK

The article examines the methods of security assessment information-telecommunication networks of different influences with the use of vulnerabilities of protocols of information exchange and sharing. To do this, specified the concept of Protocol impacts and Protocol security information and telecommunications network. You enter and shows the evaluation of Protocol security from the information of the signs of protocols. As the main approach uses a method of analysis of hierarchies and the distribution of resource protection. As an example of the results of the security analysis protocols in various conditions. It is concluded that the implementation of the proposed approach will allow to change the existing common perceptions and approaches to the protection of ITS.

Keywords: *protocol; protection; protocol security; information value; estimation; impact strategy; ranking; analytic hierarchy process.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Positive Research 2015. Sbornik issledovanij po prakticheskoj bezopasnosti [E'lektronny'j resurs]. – URL: www.ptsecurity.ru.
2. Berzin E.A. Optimal'noe raspredelenie resursov i e'lementy' sinteza sistem / pod red. E.V. Zolotova. – M.: «Sovetskoe radio», 1974. – 304 s.
3. Saati T. Prinyatie reshenij. Metod analiza ierarxij. – M.: Radio i svyaz', 1993. – 278 s.
4. Kocy'nyak M.A. i dr. Obespechenie ustojchivosti informacionno-telekommunikacionny'x setej v usloviyax informacionnogo protivoborstva / M.A. Kocy'nyak, A.I. Osadchij, M.M. Kocy'nyak, O.S. Lauta, V.E. Dement'ev, D.Yu. Vasyukov. – Spb.: LO CNIIS, 2015. – 126 s.

УДК 004.942

С.С. КОЗУНОВА, А.А. БАБЕНКО

МОДЕЛЬ ПОСТРОЕНИЯ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОРПОРАТИВНОГО ТИПА

Обоснована актуальность построения защищенной информационной системы корпоративного типа. Сформирован профиль угроз нарушения информационной безопасности, характерный для информационных систем корпоративного типа, и приведена классификация этих угроз. Описаны источники угроз. На базе профиля угроз разработана уникальная модель защищенной информационной системы корпоративного типа, содержащая различные уровни информационной безопасности и специальную контрмеру.

Ключевые слова: *информационная система корпоративного типа; обеспечение информационной безопасности; защищенность; угроза нарушения информационной безопасности; уязвимость; уровни информационной безопасности.*

ВВЕДЕНИЕ

Деятельность по защите информации (ЗИ) в информационных системах корпоративного типа приобретает большую популярность в современном обществе научно-технологического прогресса. В настоящее время актуальность построения защищенной ИС повышается, исходя из роста малых и больших предприятий, а также из-за увеличения потребности в процедурах объединения организаций и предприятий в корпорации.

Корпоративные ИС (далее КИС) обрабатывают информационные ресурсы, содержащие не только коммерческую, государственную тайны, но и данные, повышающие конкурентоспособность компании. Современное развитие информационной безопасности (ИБ) показывает, что проблема обеспечения ИБ систем корпоративного типа стала новым индивидуальным направлением, сформированным множеством частных проблем отдельных организаций. Это обусловлено тем, что информационные системы являются инструментом управления производственными, технологическими и бизнес-процессами.

Процесс формирования защищенной информационной системы (далее ИС) является трудоемким. Для осуществления такого процесса необходимы большие временные, ресурсные и финансовые средства. Одной из основной проблем, с которой сталкиваются специалисты по ЗИ, является осуществление непрерывного взаимодействия штатных (встроенных) систем защиты информации (СЗИ) в ИС и добавочной (сторонней) СЗИ. В качестве решения проблемы обеспечения ИБ в ИС корпоративного типа мы предлагаем две модели: модель построения защищенной ИС корпоративного типа и модель профиля угроз нарушения ИБ ИС корпоративного типа.

Несмотря на немалое количество СЗИ, в настоящее время проблема комплексного обеспечения ИБ ИС корпоративного типа не решена. Исследования в областях проектирования защищенных ИС корпоративного типа, обеспечение ИБ в КИС, разработка и внедрение СЗИ КИС проводились следующими российскими авторами: А.М. Блинов, Е.Н. Горбачевская, Н.В. Машкина, А.Ю. Сенцова, В.Е. Кладов, В.М. Нечунаев и другие. Большинство ученых предлагают проведение оценки рисков ИБ КИС, однако механизмов и инструментов снижения рисков ИБ очень мало. Существующие механизмы снижения рисков нарушения ИБ ИС корпоративного типа не способны снизить все риски и провести развернутую классификацию рисковых событий ИБ, являющимися инцидентами. Поэтому из-за отсутствия универсального решения задач классификации рисков ИБ ИС корпоративного типа затрудняется выбор способов снижения таких рисков. Некоторые авторы описывают угрозы нарушения ИБ КИС, но такое описание носит общий характер. При обобщении угроз ИБ КИС отсутствует какая-либо карта угроз. Без специализированных характеристик угроз ИБ невозможно сформировать векторы атак и спрогнозировать

инциденты ИБ. Открытыми является ряд таких вопросов, как: совмещение информационных и функциональных процессов ИС корпоративного типа (отсутствие большого влияния на них СЗИ), взаимодействие и обмен данными между СЗИ различных классов КИС.

Одним из требований, предъявляемых к обеспечению ИБ ИС, является обеспечение доверенной среды. Это означает, что ИС принимает (оказывает доверие) информационно-телекоммуникационной среде, в которой она находится. При принятии решения о выборе такой среды применяют многокритериальный анализ, подробно описанный в [1]. Так, основываясь на дерево-карте, можно построить не только отношение качество-эффективность о доверенной среде, но и выстроить способ организации данных в ИС. Согласно [1], диаграмма «Дерево-карта» – это способ визуализации иерархических данных в виде двухмерной прямоугольной карты.

ИС – система, обеспечивающая функции управления, распределенную обработку данных на основе многоплатформенной информационно-технологической архитектуры [2]. Само понятие ИС включает в себя всю инфраструктуру предприятия и управление информационными потоками [2]. При реализации СЗИ для ИС корпоративного типа необходимо, чтобы СЗИ не влияла на функционирование и работоспособность ИС.

В настоящее время можно выделить два основных класса в области ЗИ в ИС корпоративного типа: разработка комплексной системы защиты информации и разработка систем обеспечения ИБ (СОИБ). Однако данные теоретико-практические предпосылки обладают некоторыми минусами. Так, для первого класса характерно то, что при построении комплексной СЗИ ИС корпоративного типа элементы ИС хоть и занимают главную позицию, но рассматриваются совместно с другими компонентами. Примерами таких компонент служат: распределенные ИС, телекоммуникационная сеть, системы управления и иные коммуникационные технологии. При построении такой СЗИ применяется комплексный подход, однако такой подход уязвим на этапе проектировании. Так как на этапе проектирования СЗИ команда разработчиков ориентируется на набор угроз ИБ и учитывает риски, актуальные на момент проектирования, то комплексное СЗИ не обладает гибкостью и адаптивностью. Недостатками применения СОИБ являются: длительное внедрение по временному показателю, отсутствие учета деструктивных воздействий в полной мере, отсутствие средств централизованного управления ИБ.

Автором [2] термин «защищенность» определен как совокупность правовых, научно-технических, специальных, организационных мер, направленных на своевременное выявление, предупреждение и пресечение неправомерного получения и распространения защищаемой информации, осуществляемых органами законодательной, исполнительной и судебной власти, общественными и иными организациями и объединениями, гражданами, принимающими участие в обеспечении безопасности в соответствии с законодательством, регламентирующим отношения в информационной сфере. Поддержание стабильной защищенности необходимо для обеспечения ИБ. В связи тем, что при осуществлении ИБ в КИС учитываются все процессы, рассмотрим защищаемый процесс.

Защищаемый процесс – это процесс, который используется в ИС для обработки защищаемой информации с требуемым уровнем защищенности [3]. Уровень защищенности и требования, предъявляемые к нему, обеспечиваются СЗИ.

На рисунке 1 представлены результаты аналитических исследований инцидентов ИБ, полученные компанией Positive Technologies. Так, по [4] для исследования было выбрано 63 крупные российские компании из следующих отраслей: транспорт, государственные организации, энергетика, телекоммуникации, банковская сфера. Всего было выявлено восемь инцидентов, меньшая частота инцидента – это потеря мобильных устройств (2%), наибольшую частоту появления занял инцидент отказ в обслуживании (23%), также 21% составили атаки на внешние веб-приложения.

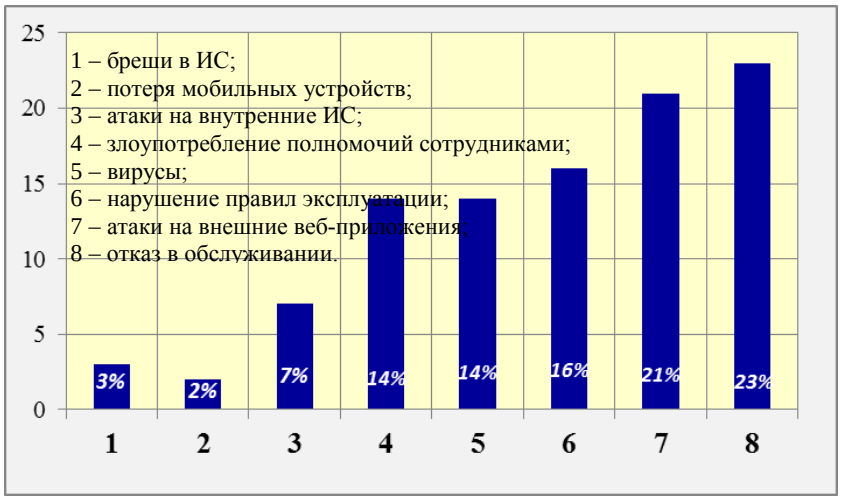

Рисунок 1 – Инциденты ИБ компаний, использующие КИС (2013 год)

В 2014 году компания INFOWATCH проводила исследование утечек корпоративной информации. По данным, опубликованным в [5], 2014 год обладал критическими потерями важной информации. Утечка персональных данных и платежной информации составила 91,8%, коммерческой тайны – 4,3%, государственной тайны – 1,7%, потеря некатегорированной (иной) информации составила 2,2%. В [8] приведена следующая статистика об инцидентах ИБ корпоративных компаний на 2015 год. К ним относятся такие, как: доступ к корпоративным информационным ресурсам (58%), перехват частичного контроля над КИС (26%), атаки на границе сети (16%).

Можно сделать вывод о том, что сейчас решены частные задачи обеспечения ИБ ИС корпоративного типа, а именно: разработаны методы оценки информационных рисков, предложены подходы к определению эффективности ИБ корпоративных ИС, описаны риски с помощью формализованной модели, сформированы когнитивные карты рисков ИБ, предложены методы обеспечение целостности ИР с использованием шифрования файлов и метаданных. Однако, обобщив данные проведенных исследований, невозможно описать единое решение проблемы обеспечения ИБ ИС корпоративного типа. Анализируя открытые статистические данные об обеспечении ИБ, можно подчеркнуть, что в настоящее время уровень ИБ ИС корпоративного типа нуждается в повышении.

УГРОЗЫ ИБ, ХАРАКТЕРНЫЕ ДЛЯ ИС КОРПОРАТИВНОГО ТИПА

Угроза безопасности информации – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения ИБ [3]. Угроза ИБ организации (предприятия) определена как совокупность факторов и условий, создающих опасность нарушения ИБ организации (предприятия), вызывающую или способную вызвать негативные последствия (ущерб, вред) для организации [3]. Процесс реализации угрозы называется атакой [2].

Для каждого объекта защиты модель угроз является уникальной. Согласно [3], модель угроз безопасности информации – это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Анализируя работы авторов [2, 6, 7], была определена необходимость формирования профиля угроз ИБ (рис. 1), являющимся общим для КИС. Такое решение принято, исходя из того, что в большинстве исследований указан обычно перечень угроз без концентрации на особенностях воздействий угроз и указания их направленности.

При разработке профиля угроз ИБ не определялось взаимодействие в классическом понимании объектов угроз с целью угрозы. Данные понятия определены обобщенно. Так, объектом угроз является ИС корпоративного типа и все ее составляющие (включая ЛВС), цель реализации угроз ИБ – это нарушение ИБ ИС. Иными словами, целью реализации угроз

(как единичной угрозы, так и совокупности угроз) является вывод из строя механизмов ЗИ ИС корпоративного типа. Исходя из этого, можно выделить основную цель функционирования модели защищённой ИС корпоративного типа: противодействие угрозам безопасности КИС.

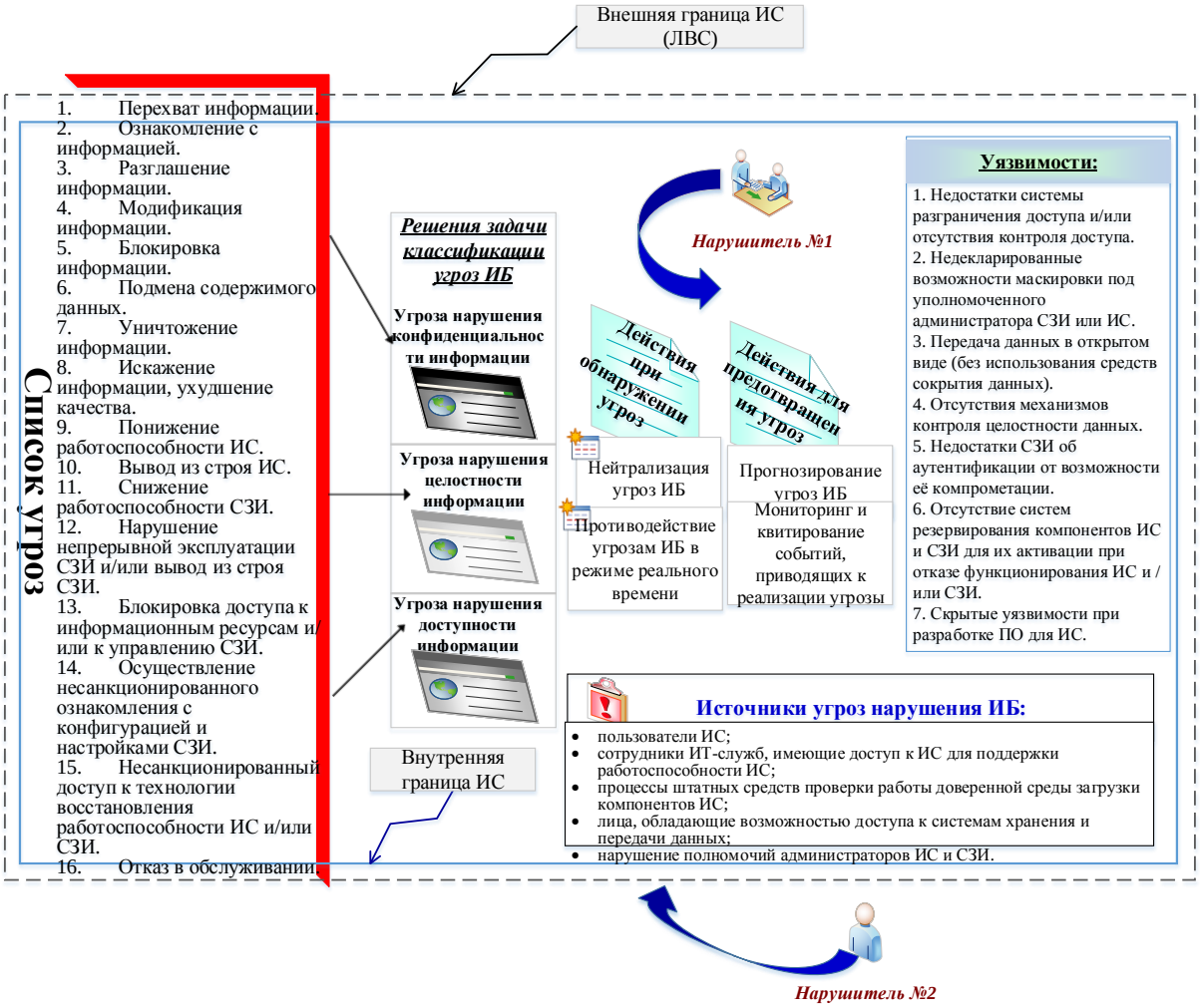

Рисунок 2 – Модель профиля угроз нарушения ИБ ИС корпоративного типа

Профиль угроз нарушения ИБ содержит шестнадцать актуальных угроз, характерных для ИС корпоративного типа. Данным угрозам сопоставимы семь уязвимостей, отталкиваясь от которых злоумышленник может совершить атаку на ИС, ее компоненты и сеть, в которой она функционирует. Профиль угроз имеет поэтапное описание действий при необходимости обнаружить и предотвратить угрозы.

Злоумышленником в сфере ИБ является лицо, способное нанести урон безопасности защищаемой информации. Согласно [3], под нарушителем ИБ принято понимать физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение ИБ организации. В модели определены два нарушителя: нарушитель № 1 – «внутренний», нарушитель № 2 – «внешний». Внутренний нарушитель ИБ в ИС корпоративного типа – это лицо, являющееся пользователем или администратором этой ИС. Внешним нарушителем ИБ в ИС корпоративного типа могут быть сотрудники предприятия, не являющиеся пользователями ИС, или иные лица, не входящие в состав рабочего персонала предприятия. Нарушитель № 2 находится за пределами границы КИС или за пределами ЛВС. Нарушитель № 1 находится внутри периметра КИС, то есть во внутренней среде функционирования КИС. На рисунке 1 область действия злоумышленников показана стрелкой. Атакующие действия внешнего

злоумышленника направлены на внешнюю границу ИС, то есть в основном на ЛВС, ИКТ и на СЗИ, расположенные на границе сети для образования защищенной связи между ЛВС и КИС. Атакующие воздействия внутреннего злоумышленника производятся внутри ИС, а именно на компоненты ИС, программные средства, прикладные приложения, БД, ИР и СРД.

Уязвимость ИС (или «брешь») – это свойство ИС, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации [3]. Использование нарушителем уязвимости как свойство ИС может привести к реализации атаки на ИС.

Направленность угроз ИБ формируется источником угроз. Для ИС корпоративного типа характерны несколько таких источников, при разработке профилей защиты их было выделено пять:

– пользователи информационной системы корпоративного типа (или информационных систем, объединенные в единое звено управления);

– сотрудники подразделений ИТ-служб, имеющие доступ к поддержке работоспособности ИС;

– функциональные процессы встроенных (штатных) средств проверки работы доверенной среды загрузки компонентов ИС;

– лица, обладающие возможностью доступа к системам хранения и передачи данных;

– нарушение полномочий, которыми наделены администраторы ИС и СЗИ.

Применение профиля угроз ИБ позволяет решить задачу классификации угроз ИБ путем их деления на три типа: нарушение целостности, доступности и конфиденциальности информации.

Угроза нарушения конфиденциальности является угрозой раскрытия информации с точки зрения ее разглашения [2]. Таким образом, после осуществления такой угрозы лицо, необеспеченное полномочным доступом, располагает данными конфиденциального характера, обрабатываемыми в ИС. Согласно сформированному профилю угроз для ИС выделены следующие угрозы нарушения конфиденциальности информации: НСД к ИР, ознакомление с информацией, разглашение информации и ее перехват, а также отказ в обслуживании.

Угроза нарушения целостности информации – угроза, наступающая в результате НСД или санкционированного доступа к ИР с последующим изменением свойств ИР, которое приводит к изменению внутреннего содержимого ИР. Основными угрозами нарушения информации являются модификация информации, блокировка информации, подмена информации (ее содержимого), искажение информации или ухудшения ее качества и другие. Также к нарушению целостности может привести ошибка, возникшая при функционировании ИС или СЗИ.

Отсутствие специальных действий по восстановлению данных с целью устранения нарушений целостности может привести к тому, что доступ к ИР, целостность которого не соответствует эталону, становится запрещен. То есть активация угроз нарушения целостности ИР приводит к реализации второй угрозы – нарушения доступности к ИР.

Угроза нарушения доступности информации – это блокирование доступа к ИР для пользователей ИС, обладающим легальным доступом [2]. К классу таких угроз относятся уничтожение информации, отказ в обслуживании, подмена содержимого данных, блокировка информации. Также к наличию таких угроз могут привести отказ функционирования служб ИС, то есть снижение работоспособности ИС и вывод из строя СЗИ (или ИС).

При построении систем обеспечения ИБ предприятий необходимо разрабатывать проект ИБ. Область, исследованная в данной статье, указывает на то, что проектирование защищенной ИС корпоративного типа является проектной деятельностью. Однако она может являться как самостоятельным проектом, так подпроектом построения ИБ предприятия. Развитие и внедрение таких проектов осуществляется с использованием вложенных финансовых средств. Принятие решений об инвестировании ИБ предприятий подробно описано и систематизировано в [9].

Наличие угроз или уязвимостей в ИС корпоративного типа говорит о возможности подвержения КИС рисковым событиям, способным привести к потере конфиденциальных данных, обрабатываемых в ИС. Авторы [10] отмечают, что риск является действием в ситуации неопределенности с желанием реализовать самый положительный прогноз (или результат). Значение риска указывает на необходимость использования средств и механизмов, противодействующих каждой угрозе [11], и определение уровня ИБ, в котором функционирование подсистемы защиты информации нарушено.

ПОСТРОЕНИЕ ЗАЩИЩЕННОЙ ИС КОРПОРАТИВНОГО ТИПА

В качестве решения мы предлагаем модель защищенной ИС корпоративного типа (рис. 3), которая описывает основные процедуры обеспечения ИБ. Данная модель построена на основе пяти уровней ИБ, характерных для КИС и содержит один компонент «контрмера».

Рисунок 3 – Модель защищенной ИС корпоративного типа

На уровне системного анализа исследуется проблема обеспечения ИБ ИС, результатом работ, проведенных на данном уровне, является формирование объекта защиты (ОЗ). На стратегическом уровне ЗИ осуществляется выбор стратегии ИБ, регламентирующей разграничение доступа к ИР, и определение поведения предложенной модели. Организационные меры по ЗИ реализуются на организационном уровне ЗИ, именно на этом уровне производится установление режима ИБ. Управление данной моделью осуществляется на уровне управления ИБ по результатам проведения мониторинга ИБ и фиксации инцидентов ИБ. Аудит ИБ защищаемой ИС проводится на уровне контроля примененных мер обеспечения ИБ. Операции определения уровня и повышение эффективности ИБ объединены в контрмеру.

Таким образом, исходя из структуры предложенной модели, можно сделать вывод, что такая модель учитывает все уровни ИБ, характерные для ИС корпоративного типа. На базе применения данной модели можно получить описание объекта защиты и его уникальные характеристики, что облегчит решение такой задачи такой, как подбор механизмов защиты информации. Особенностью разработанной модели является

возможность формирования стратегии ИБ, а также возможность полностью придерживаться выбранных стратегических принципов в защите информации.

ВЫВОДЫ

Особенности решения прикладной области защиты информации в КИС, а именно – ИС корпоративного типа, является наличие модели профиля угроз ИБ. Такой профиль является унифицированным, что означает его полноту в описании угроз ИБ, источников угроз, решения задачи классификации угроз нарушения ИБ. Именно эти характеристики позволяют сформировать сценарий обнаружения угроз ИБ ИС корпоративного типа и определение алгоритма действий при предотвращения угроз. Определение действий злоумышленников, а также объектов, на которые они направлены, позволяет сформировать портреты нарушителей (№ 1 и № 2), что делает модель профиля угроз актуальным для любых условий, в которые попадают ИС корпоративного типа.

Результат проведенного исследования показал, что модель защищенной ИС корпоративного типа может быть развернутой, гибкой и управленческой. Это означает, что процедуры обеспечения ИБ не ограничены, они могут проводиться на различных уровнях ИБ, так не будет возникать сложность во взаимодействии встроенной СЗИ в КИС и добавочных механизмов защиты.

Перспективами дальнейшего развития данного направления являются: формализованное описание объекта защиты и их динамических характеристик, разработка системы управления защищенной ИС корпоративного типа, система мониторинга процессов защищённой ИС корпоративного типа, системный анализ противодействия угрозам ИБ защищённой ИС корпоративного типа и другие.

СПИСОК ЛИТЕРАТУРЫ

1. Горбатов В.С., Кондратьева Т.А., Мещеряков А.А. Программный комплекс многокритериального выбора средств организации доверенной среды // Безопасность информационных технологий, 2015. – № 1 [Электронный ресурс]. – URL: http://pvti.ru/data/file/bit/2015_1/part_2.pdf (дата обращения 03.02.2016).
2. Блинов А.М. Информационная безопасность: учебное пособие. – Часть 1. – СПб.: Издательство СПбГУЭФ, 2010. – 96 с.
3. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // StandartGOST.ru – открытая база ГОСТов [Электронный ресурс]. – URL: http://standartgost.ru/g/ГОСТ_Р_53114-2008 (дата обращения 03.02.2016).
4. Positive Technologies. Инциденты в информационной безопасности крупных российских компаний (2013 год) [Электронный ресурс]. – URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf (дата обращения 03.02.2016).
5. INFOWATCH Исследование утечек конфиденциальной информации в 2014 году [Электронный ресурс] – URL: http://www.infowatch.ru/report2014# (дата обращения 03.02.2016).
6. Горбачевская Е.Н. Исследование механизмов защиты данных в корпоративных информационных системах // Вестник волжского университета им. В.Н. Татищева, 2012. – № 4(20) [Электронный ресурс]. – URL: http://cyberleninka.ru/article/n/issledovanie-mehanizmov-zaschity-dannyh-v-korporativnyh-informatsionnyh-sistemah-1 (дата обращения 18.01.2016).
7. Машкина И.В. и др. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем / И.В. Машкина, А.Ю. Сенцова, Р.М. Гузаиров, В.Е. Кладов // Известия Южного федерального университета. Технические науки, 2011. – № 12 (том 125). – С. 25-35.

8. Итоги года в ИБ глазами экспертов Positive Technologies [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/results_year_cybersecurity (дата обращения 18.01.2016).
9. Козунова С.С., Бабенко А.А. Система принятия решений инвестирования информационной безопасности предприятий в условиях полной неопределенности // Информационные системы и технологии, 2015. – № 6(92). – С. 59-67.
10. Атапина Н.В. Сравнительный анализ методов оценки рисков и подходов к организации риск-менеджмента // Молодой ученый, 2013. – № 5(52). – С. 235-243.
11. Оладько В.С. Модель оценки защищённости автоматизированного рабочего места пользователя // Информационные системы и технологии, 2016. – № 1(93). – С. 92-99.

Козунова Светлана Сергеевна
ФГБОУ ВО «Волгоградский государственный технический университет», г. Волгоград
Аспирант кафедры системы автоматизированного проектирования и поискового конструирования
Тел.: 8 (8442) 24-81-00
E-mail: one1100on@gmail.com

Бабенко Алексей Александрович
ФГБОУ ВО «Волгоградский государственный технический университет», г. Волгоград
Кандидат педагогических наук, доцент, доцент кафедры информационной безопасности
Тел.: 8 (8442) 46-03-68
E-mail: ba_benko@mail.ru

S.S. KOZUNOVA *(Post-graduate Student of the Department of Computer-aided Design and Search Construction)*

A.A. BABENKO *(Candidate of Pedagogic Sciences, Associate Professor, Associate Professor of the Department of Information Security)*
Volgograd State Technical University, Volgograd

MODEL OF CONSTRUCTION PROTECTED INFORMATION SYSTEM OF CORPORATE STYLE

The relevance is substantiated of building a secure information system of corporate type. The profile of violations of information security threats is formed, which characteristic information systems of corporate type and the classification is shown of these threats. We describe the sources of threats. On the basis of the profile of the threats it has developed a unique model of a secure information system of corporate type, containing various levels of information security and special countermeasure.

Keywords: *information system of corporate type; provision of information protected; the security; threat of violation of information security; vulnerability; levels of information security.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Gorbatov V.S., Kondrat'eva T.A., Meshheryakov A.A. Programmny'j kompleks mnogokriterial'nogo vy'bora sredstv organizacii doverennoj sredy' // Bezopasnost' informacionny'x texnologij, 2015. – № 1 [E'lektronny'j resurs]. – URL: http://pvti.ru/data/file/bit/2015_1/part_2.pdf (data obrashheniya 03.02.2016).
2. Blinov A.M. Informacionnaya bezopasnost': uchebnoe posobie. – Chast' 1. – SPb.: Izdatel'stvo SPbGUE'F, 2010. – 96 s.
3. GOST R 53114-2008. Zashhita informacii. Obespechenie informacionnoj bezopasnosti v organizacii. Osnovny'e terminy' i opredeleniya // StandartGOST.ru – otkry'taya baza GOSTov [E'lektronny'j resurs]. – URL: http://standartgost.ru/g/GOST_R_53114-2008 (data obrashheniya 03.02.2016).
4. Positive Technologies. Incidenty' v informacionnoj bezopasnosti krupny'x rossijskix kompanij (2013 god) [E'lektronny'j resurs]. – URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf (data obrashheniya 03.02.2016).
5. INFOWATCH Issledovanie utechek konfidencial'noj informacii v 2014 godu [E'lektronny'j resurs] – URL: http://www.infowatch.ru/report2014# (data obrashheniya 03.02.2016).
6. Gorbachevskaya E.N. Issledovanie mexanizmov zashhity' danny'x v korporativny'x informacionny'x sistemax // Vestnik volzhskogo universiteta im. V.N. Tatishheva, 2012. – № 4(20) [E'lektronny'j resurs].

– URL: http://cyberleninka.ru/article/n/issledovanie-mehanizmov-zaschity-dannyh-v-korporativnyh-informatsionnyh-sistemah-1 (data obrashheniya 18.01.2016).
7. Mashkina I.V. i dr. Ispol'zovanie metodov sistemnogo analiza dlya resheniya problemy' obespecheniya bezopasnosti sovremenny'x informacionny'x sistem / I.V. Mashkina, A.Yu. Sencova, R.M. Guzairov, V.E. Kladov // Izvestiya Yuzhnogo federal'nogo universiteta. Texnicheskie nauki, 2011. – № 12 (tom 125). – S. 25-35.
8. Itogi goda v IB glazami e'kspertov Positive Technologies [E'lektronny'j resurs]. – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/results_year_cybersecurity (data obrashheniya 18.01.2016).
9. Kozunova S.S., Babenko A.A. Sistema prinyatiya reshenij investirovaniya informacionnoj bezopasnosti predpriyatij v usloviyax polnoj neopredelennosti // Informacionny'e sistemy' i texnologii, 2015. – № 6(92). – S. 59-67.
10. Atapina N.V. Sravnitel'ny'j analiz metodov ocenki riskov i podxodov k organizacii risk-menedzhmenta // Molodoj ucheny'j, 2013. – № 5(52). – S. 235-243.
11. Olad'ko V.S. Model' ocenki zashhishhyonnosti avtomatizirovannogo rabochego mesta pol'zovatelya // Informacionny'e sistemy' i texnologii, 2016. – № 1(93). – S. 92-99.

УДК 004.056

А.В. НИКИШОВА, Р.Н. АРТЮХОВ, Е.А. ВИТЕНБУРГ

СТЕГАНОГРАФИЧЕСКИЕ СИСТЕМЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последние годы стеганография часто применяется в области защиты информации. Разработано большое число стеганографических систем, позволяющих осуществить скрытую передачу конфиденциальной информации. В данной статье проанализированы методы сокрытия информации. Определены базовые методы для различных групп методов сокрытия информации. Создан программный комплекс для оценки эффективности выбранных методов с точки зрения размера встраиваемого сообщения. Проведены экспериментальные исследования с использованием данного программного комплекса. Сделан вывод о наиболее эффективной группе методов сокрытия информации.

Ключевые слова: *стеганография; информационная безопасность; пропускная способность; кодер; скрытность; контейнер.*

На сегодняшний день все большую популярность в информационной безопасности приобретают стеганографические методы защиты информации. Методы стеганографии позволяют решить ряд задач: скрытая передача данных, защита авторского права, контроль целостности данных, отслеживание источника утечки информации, решение задач помехоустойчивой аутентификации [1].

Рост объемов обрабатываемой в цифровой форме информации, а также упрощение доступа к ней приводят к повышению популярности применения методов сокрытия данных. Исследования и разработки в области стеганографии становятся распространенными наряду с использованием цифровых форматов мультимедиа [2, 3]. В связи с этим появилось большое количество стеганографических систем, осуществляющих скрытую передачу данных.

При построении стеганосистемы должны учитываться следующие положения [4, 5]:

1) стеганосистема должна иметь приемлемую вычислительную реализацию;
2) должна обеспечиваться пропускная способность;
3) методы скрытия данных должны обеспечивать аутентичность и целостность секретной информации;
4) злоумышленник не имеет возможности определить факт передачи сообщения.

На рисунке 1 представлена структурная схема стеганосистемы [4].

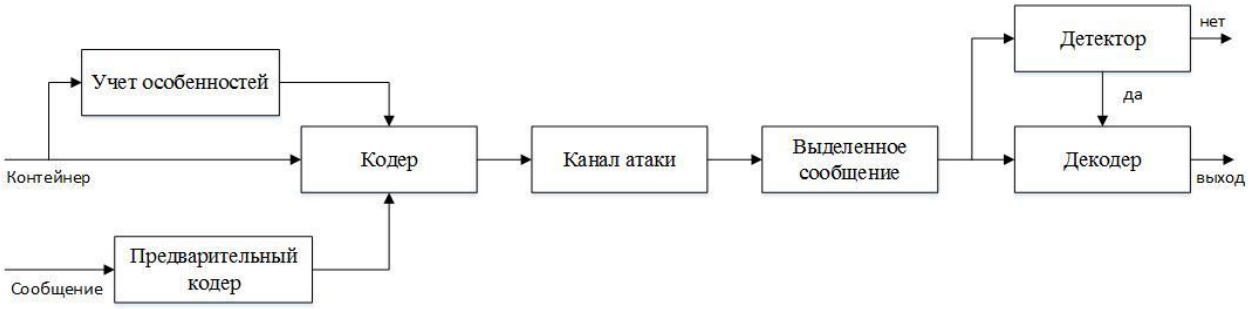

Рисунок 1 – Структурная схема стеганосистемы

Предлагаются следующие критерии для оценки качества программных продуктов сокрытия данных – стеганографических систем [6]: надежность стеганографической системы как программного продукта; скрытность, то есть определение вероятности обнаружения встроенного сообщения; устойчивость контейнеров к искажениям; пригодность применения

стеганографической системы для различных форматов контейнеров; применяемый метод встраивания; размер встраиваемого сообщения.

1. Для оценки уровня надежности программного продукта используют модель последовательности испытаний Бернулли [7]. Пространство элементарных событий в этой модели содержит 2^n точек, где n – число запусков программы. Пусть вероятность ошибочного запуска p, а вероятность правильного – (1-p). Вероятность того, что из n запусков k приведут к неправильному результату, определяется формулой биномиального распределения:

$$B(p,n,k) = C(n,k) * pk * (1-p)(n-k),$$

где C(n, k) – число сочетаний. Вероятность p неизвестна, но по результатам запусков известны n и k. Величина B как функция p имеет максимум при

$$p = \frac{k}{n}.$$

В качестве критерия надежности программного продукта можно принять величину R:

$$R = 1 - \frac{k}{n} = \frac{n-k}{n},$$

значения которой определяют уровень надежности: если все запуски завершились ошибочно (k=n), то надежность нулевая. Величина погрешности при оценке надежности R зависит от количества запусков n.

2. Критерий скрытности. Методы стеганографии в основном используют избыточность мультимедийных каналов хранения и передачи информации. В связи с этим возникает вопрос об оценке уровня скрытности защищаемой информации. Для оценки уровня скрытности более удобно использовать критерий оценки, основанный на коэффициенте группирования α-серий [8, 9]. Под α-серией длины m будем понимать последовательность, состоящую из одинаковых бит, вида:

ααα…α, где α∈{0 или 1}, m=1, 2, …, M.

Тогда

$$К_{гр} = (s_{ср} - 1)/s_{ср},$$

где $s_{ср}$ – среднее значение длины α-серии.

Коэффициент группирования $К_{гр}$, принимающий значения в интервале от 0 до 1, позволяет определить количественную оценку уровня.

3. Критерий устойчивости к искажениям. Большинство показателей искажения, которые используются при визуальной обработке информации, относятся к группе разностных показателей контейнера. Эти показатели базируются на отличии между контейнером-оригиналом (неискаженный сигнал) и контейнером-результатом (искаженный сигнал) [10]. Для оценки качества восстановленного контейнера можно использовать меру среднеквадратичного искажения СКО, определяемую как [11]:

$$СКО = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2,$$

где N – число элементов в контейнере; x_i, $\hat{x}_i$ – значения пикселей исходного и восстановленного контейнера.

Этот показатель базируется на анализе отдельных элементов контейнера, то есть практически не адаптирован к человеческой зрительной системе.

4. Критерий пригодности применения стеганографической системы для различных контейнеров. Одним из ключевых критериев оценки качества стеганографической системы является критерий пригодности стеганографической системы для различных контейнеров,

так как в значительной степени эффективность применения контейнера в стеганографии зависит от формата его хранения.

5. Применяемый метод встраивания. Важным отличием различных стеганографических систем является применяемый метод встраивания, который влияет на вычислительные преобразования контейнера.

6. Использование контейнера для хранения информации определяется в первую очередь максимальным возможным размером встраиваемого сообщения. Как правило, данный критерий определяется соотношением между размером данных и исходным размером контейнера.

Данные могут быть сокрыты стеганосистемой в контейнерах различных форматов, но на практике только некоторые из них способны хранить дополнительную сокрытую информацию с возможностью ее восстановления. Такие контейнеры можно разделить на три группы, а именно: текстовые файлы, мультимедиа-файлы (аудио и видео), изображения.

Целью стеганографии является скрытость встраивания, поэтому наилучшим контейнером для задач стеганографии является наиболее распространенный контейнер.

Для выбора наиболее распространенного контейнера была использована статистика сайта alexa.com (рис. 2) о сотне самых посещаемых сайтов в сети Интернет.

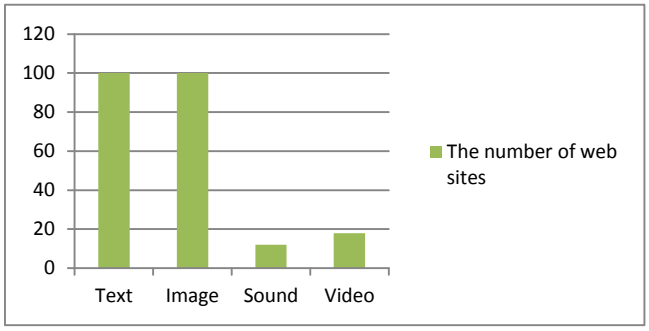

Рисунок 2 – Статистика использования контейнеров на сайтах сети Интернет

Статистика по использованию возможных контейнеров в сотне самых посещаемых веб-сайтов была набрана с главной страницы каждого из них. Выяснилось, что каждый сайт использует изображения и текст на главной странице, в то время как звуковые файлы и видеофайлы используются только на 12 и 18 сайтах соответственно.

Сделан вывод о дальнейшем использовании двух наиболее распространенных контейнеров. Наиболее распространенным текстовым форматом является DOC. DOC-файл, созданный с помощью текстового процессора, полностью сохраняет форматирование. Формат DOC включает широкие возможности обработки и форматирования текста. Полноценно и корректно все возможности реализованы в MS Word. DOC «понимают» и другие программы, хотя корректность распознавания другими программами сравнительно ниже, чем у MS Word. DOC является бинарным форматом, что делает его нечитабельным в простых текстовых редакторах.

Для сокрытия информации в текстовых файлах используют три основных метода:

1. Методы произвольного интервала, они осуществляют встраивание путем манипуляции с пробелами. Существует две причины, почему манипуляции с «белым пространством» в особенности дают полезные результаты. Во-первых, изменение числа завершающих пробелов имеет малую вероятность изменить значение фразы или предложения. Во-вторых, обычный читатель не замечает небольшого изменения «белого пространства».

К данным методам относятся: метод изменения интервалов между предложениями, метод изменения количества пробелов в конце текстовых строк, метод изменения количества пробелов между словами выровненного по ширине текста. Данная группа методов

предполагает использование свободного пространства в текстовом документе. Использование свободного пространства не вносит изменений в содержание текста и не вызывает подозрений у читателя.

Методом, который позволяет встроить наибольшее количество информации в текстовый контейнер, является метод изменения количества пробелов между словами выровненного по ширине текста. Он заключается в сокрытии данных в свободных местах текста, выровненного по ширине. Биты данных встраиваются путем управляемого выбора позиций, в которых размещены дополнительные пробелы.

Данные кодируются регулированием того, где будет помещен дополнительный пробел. Один пробел между словами интерпретируется как «0», а два пробела – как «1». В результате этот метод скрывает несколько бит на каждой строчке (рис.3).

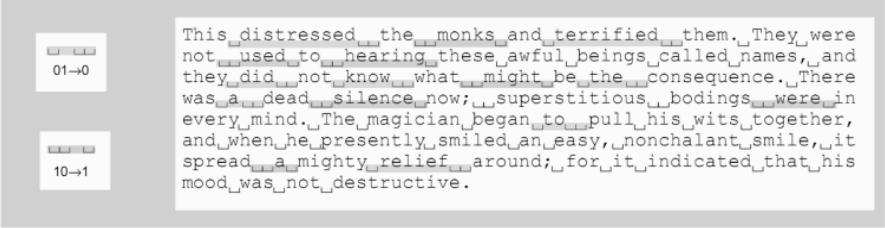

Рисунок 3 – Кодирование данных методом изменения количества пробелов между словами выровненного по ширине текста

Из-за ограничений на выравнивание не всякое пространство между словами может быть использовано как данные. Чтобы определить какое пространство представляет скрытые данные, а какое является частью исходного текста, необходимо применить метод Манчестерского кодирования. Манчестерские кодовые группы по два бита интерпретируются следующим образом: «01» как «1» и «10» как «0». Битовые строки «00» и «11» игнорируются. Например, закодированное сообщение «1000101101» уменьшается до «001», тогда как «110011» является null-строкой.

Алгоритм работы метода изменения количества пробелов между словами выровненного по ширине текста представлен на рисунке 4. Блок-схема данного алгоритма состоит из следующих блоков:

– блок 2. Осуществляется выбор контейнера и ввод скрываемого сообщения;

– блок 3. Осуществляется перевод скрываемого сообщения в биты;

– блок 4. Цикл, используемый для прохода по всем строкам;

– блок 5. Если t/2<max(L)-Li, где t – количество пробелов в строке, max(L) – максимальная длина строки, Li – длина конкретной строки, то переходим на блок 6, в противном случае на блок 7;

– блок 6. Подсчет количества бит, которые можно встроить в текущую строку, подсчет осуществляется с помощью формулы CountSp=Целая часть(t/2)-1, где t – количество пробелов в строке;

– блок 7. Подсчет количества бит, которые можно встроить в текущую строку, подсчитываем с помощью формулы CountSp=max(L)-Li, где max(L) – максимальная длина строки, а Li – длина конкретной строки;

– блок 8. Изменение количества пробелов в зависимости от битов секретного сообщения, один пробел между словами интерпретируется как «0», а два пробела – как «1»;

– блок 9. Вывод заполненного контейнера.

2. Синтаксические методы – алгоритмы, относящиеся к этой группе, работают с пунктуацией, структурой и стилем текста. Внесение дополнительных изменений в текст для сокрытия информации может стать заметным только в том случае, если данные изменения исказили смысл текста-контейнера [1].

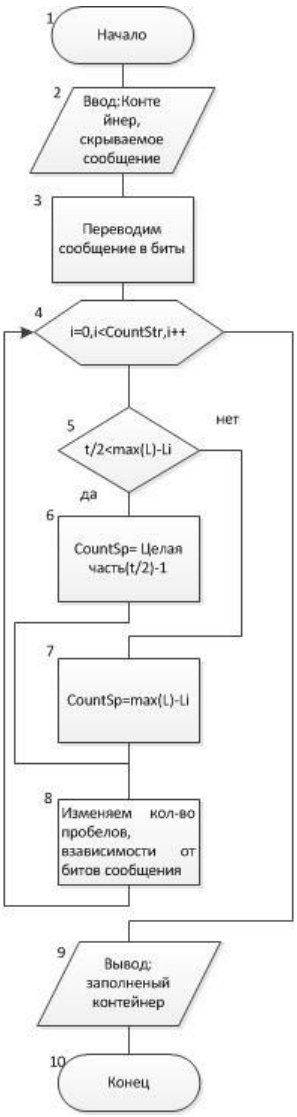

Рисунок 4 – Алгоритм работы метода изменения количества пробелов между словами выровненного по ширине текста

3. Семантические методы. В основу таких методов положено манипулирование словами, зависимое от скрываемых бит данных. Для проведения сокрытия семантическим методом необходимо наличие таблицы синонимов. Проблемы могут возникнуть, когда желанию встроить бит информации препятствует значение слова [1].

Для определения наиболее распространенного графического формата исследовались статистические данные, представленные проектом HTTPArchive, собирающим техническую информацию с более чем 17 тысячами наиболее популярных сайтов [12]. В период с 1.10.2014 по 1.02.2015 статистика имеет вид, представленный на рисунке 5.

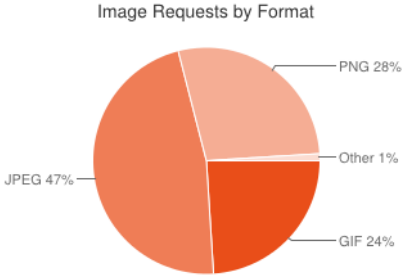

Рисунок 5 – Форматы изображений, использующиеся в сети Интернет

Согласно статистике, наиболее распространенным форматом является JPEG. Это графический формат, используемый для хранения фотоизображений, изображений растрового типа, с глубиной цвета 8 или 24 и форматом сжатия JPEG.

За последние время разработано достаточно много методов сокрытия информации в изображениях, это позволяет произвести их классификацию и выделить две основные группы методов:

1. Методы замены в пространственной области. Алгоритмы, относящиеся к этой группе, встраивают скрываемое сообщение в область первичного изображения. Их преимущество в том, что нет необходимости выполнять вычислительно сложные и длительные преобразования. К данной группе относятся следующие методы: метод замены наименьшего значащего бита, методы замены палитры, метод квантования изображения, метод Куттера-Джордана-Боссена и другие. Метод, который является базовым для данной группы, – метод замены наименее значащего бита (LSB), он построен на работе с пространственной областью изображения [2]. Алгоритм работы метода LSB представлен на рисунке 6. Блок- схема данного алгоритма включает в себя:

– блок 2. Осуществляется выбор контейнера и ввод скрываемого сообщения;

– блок 3. Получение значения размера изображения (его длины и высоты в пикселях);

– блок 4. Осуществляется перевод скрываемого сообщения в биты;

– блоки 5, 6. Циклы по ширине и высоте изображения, используемые для обращения к каждому пикселю изображения;

– блок 7. Получение значения RGB для текущего пикселя;

– блок 8. Изменение значения RGB пикселя путем встраивания в наименее значащий бит бита скрываемого сообщения;

– блок 9. Вывод заполненного контейнера.

Смысл метода замены наименее значащего бита заключается в замене последних значащих бит изображения на биты скрываемого сообщения. Для органов восприятия человека разница между пустым и заполненным контейнером должна быть неощутима.

Один пиксель 24-битного растрового RGB-изображения в этом формате кодируется тремя байтами, каждый из них отвечает за интенсивность одного из трех цветов. В результате смешения цветов из красного (R), зеленого (G) и синего (B) каналов пиксель получает нужный оттенок. Замена одного или двух младших, наименее значащих бит на другие произвольные биты незначительно исказит оттенок пикселя, так что человек просто не сможет заметить изменения.

Занимая один бит из восьми на каждый канал, можно спрятать три бита скрываемого сообщения в одном пикселе изображения.

Преимущества метода – неизменяемый размер контейнера и возможность изменять пропускную способность, изменяя количество заменяемых бит. Главным недостатком метода является неустойчивость к преобразованиям заполненного контейнера.

2. Методы сокрытия в частотной области изображения. Алгоритмы, входящие в состав данной группы, представляют изображения в частотной области, основываясь на различных методах, например, ДКП (дискретном косинусном преобразовании), вейвлет-преобразовании. Эта группа алгоритмов является более стойкой к искажениям, чем методы предыдущей группы. Однако эти методы имеют большую вычислительную сложность и менее распространены, чем методы замены в пространственной области.

Для оценки такого критерия, как размер встраиваемого сообщения для выбранных стеганографических методов, был разработан программный комплекс.

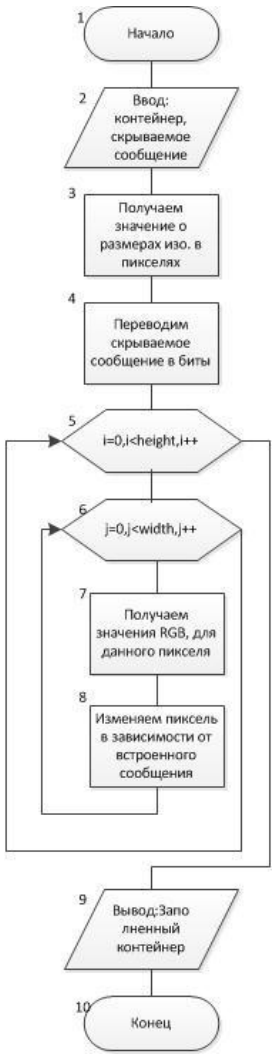

Рисунок 6 – Алгоритм работы метода LSB

Интерфейс разработанной программы имеет вид, изображенный на рисунке 7, и содержит основные элементы:

1 – текстовое поле служит для ввода скрываемого сообщения;

2 – текстовое поле для вывода пути к файлу, при применении метода lsb;

3 – кнопка, служащая для выбора файла, при использовании метода lsb;

4 – кнопки для извлечения и скрытия информации методом lsb;

5 – текстовое поле для вывода пути к файлу при применении метода изменения количества пробелов между словами выровненного по ширине текста;

6 – кнопка, служащая для выбора файла при использовании метода изменения количества пробелов между словами выровненного по ширине текста;

7 – кнопки для извлечения и скрытия информации методом изменения количества пробелов между словами выровненного по ширине текста;

8 – текстовое поле для вывода извлеченного сообщения;

9 – группа текстовых полей для вывода информации, необходимой для оценки пропускной способности.

Используя разработанный программный комплекс, были проведены 10 испытаний для каждого метода. В ходе испытаний в качестве контейнеров выбирались изображения и текстовые файлы различного размера. Была построена зависимость между количеством встроенных бит данных и количеством элементов контейнера (пикселей, символов). Результаты для LSB представлены на рисунке 8, для метода изменения количества пробелов

между словами выровненного по ширине текста – на рисунке 9. По оси Oy отложено количество скрытой информации в битах, по Ox – количество элементов контейнера.

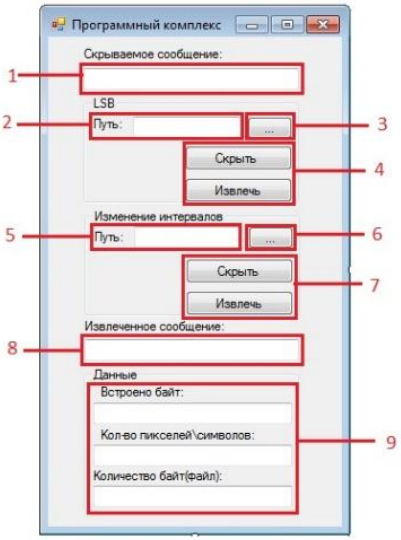

Рисунок 7 – Пользовательский интерфейс программы определения пропускной способности выбранных стеганографических методов (экранная копия)

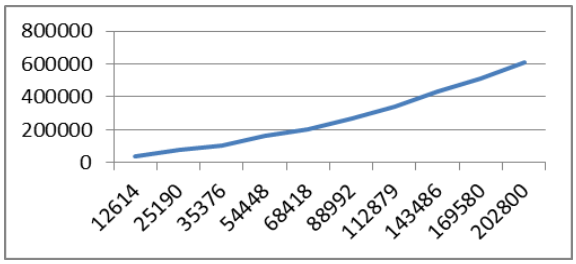

Рисунок 8 – Зависимость между количеством встроенных бит и количеством элементов контейнера для метода LSB

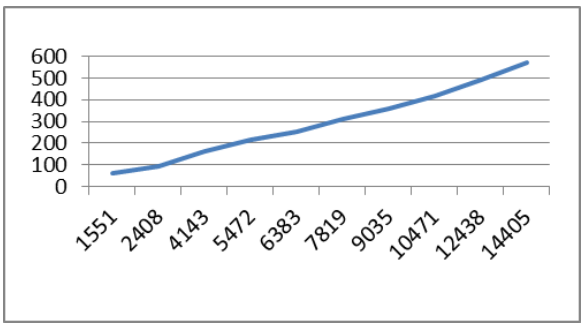

Рисунок 9 – Зависимость между количеством встроенных бит и количеством элементов контейнера для метода изменения количества пробелов между словами выровненного по ширине текста

Также была рассчитана эффективность сокрытия данных для каждого из исследуемых методов, представляющая собой отношение потенциального эффекта работы метода к его ресурсоемкости.

Для рассмотренного исследования потенциальный эффект представляет собой объем встроенных данных, а в качестве затрачиваемых ресурсов принимается объем контейнера:

$$C = \frac{m}{k},$$

где m – количество бит встраиваемого сообщения; k – количество элементов контейнера.

Для метода LSB – C=3 бит/пиксель, а для метода изменения количества пробелов между словами выровненного по ширине текста – C=0,039 бит/символ.

Исследование показало, что наибольшей пропускной способностью обладает метод LSB, по этому показателю превосходящий метод изменения количества пробелов между словами выровненного по ширине текста в 77 раз.

СПИСОК ЛИТЕРАТУРЫ

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.
2. Кувшинов С.С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии. – Санкт-Петербург, 2010.
3. Генне О.В. Основные положения стеганографии. Журнал «Защита информации. Конфидент», 2000. – № 3 [Электронный ресурс]. – URL: http://citforum.ru/internet/securities/stegano.shtml.
4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
5. Хорошко В.О. и др. Основы компьютерной стеганографии: учебное пособие для студентов и аспирантов / В.О. Хорошко, О.Д. Азаров, М.С. Шелест, Ю.С. Яремчук. – Винница: ВДТУ, 2003. – 143 с.
6. Никишова А.В., Корняков О.А. Оценка качества стеганографических систем // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы III Всероссийской научно-практической конференции, г. Волгоград, 24-25 апреля 2014 г. – В.: Издательство ВолГУ, 2014. – С. 210-214.
7. Усенко О.А. Модели и методы оценки надежности программного обеспечения информационных систем: учебное пособие. – Таганрог: Издательство ТТИ ЮФУ, 2008. – 40 с.
8. Барсуков В.С., Романцов А.П. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации // Специальная техника, 2000. – № 6.
9. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра. – Специальная техника, 1998. – №4-5.
10. Казарян А.Л. Оценка стойкости разнотипных стеганографических систем // Seventh International Conference on Computer Science and Information Technologies. – Ереван, 2009.
11. Ажбаев Т.Г., Ажмухамедов И.М. Анализ стойкости современных стеганографических алгоритмов // Астрахань: Вестник АГТУ, 2008. – № 1.
12. Interestingstats [Электронный ресурс] – URL: http://httparchive.org/interesting.php (дата обращения: 21.05.2014).

Никишова Арина Валерьевна
ФГАОУ ВПО «Волгоградский государственный университет», г. Волгоград
Кандидат технических наук, доцент кафедры «Информационная безопасность», Тел.: 8 904 777 50 03
E-mail: arinanv@yandex.ru

Артюхов Роман Николаевич
ФГАОУ ВПО «Волгоградский государственный университет», г. Волгоград
Студент
Тел.: 8 903 478 21 49
E-mail: infsec@volsu.ru

Витенбург Екатерина Александровна
ФГАОУ ВПО «Волгоградский государственный университет», г. Волгоград
Студент
Тел.: 8 906 408 65 73
E-mail: kalinina573@bk.ru

A.V. NIKIShOVA *(Candidate f Engineering Sciences, Associate Professor of the Department «Information Security»)*

R.N. ARTYuXOV *(Student)*

E.A. VITENBURG *(Student)*
Volgograd State University, Orel

STEGANOGRAPHIC SYSTEMS IN INFORMATION SECURITY

In recent years, steganography is often used in the field of information security. A large number of steganographic systems which allows carrying out a hidden transmission of confidential information were developed. This article analyzes the methods of information hiding. It defines basic methods for different groups of information hiding methods. A software package was developed to assess the effectiveness of selected methods from the point of view of the embedded message size. Experimental studies were carried out using this software package. The conclusion about the most effective group of information hiding methods was made.

Keywords*: steganography; information security; bandwidth; coder; concealment; container.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Konaxovich G.F., Puzy'renko A.Yu. Komp'yuternaya steganografiya. Teoriya i praktika. – K.: «MK-Press», 2006. – 288 s.
2. Kuvshinov S.S. Metody' i algoritmy' sokry'tiya bol'shix ob''emov danny'x na osnove steganografii. – Sankt-Peterburg, 2010.
3. Genne O.V. Osnovny'e polozheniya steganografii. Zhurnal «Zashhita informacii. Konfident», 2000. – № 3 [E'lektronny'j resurs]. – URL: http://citforum.ru/internet/securities/stegano.shtml.
4. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaya steganografiya. – M.: Solon-Press, 2002. – 272 s.
5. Xoroshko V.O. i dr. Osnovy' komp'yuternoj steganografii: uchebnoe posobie dlya studentov i aspirantov / V.O. Xoroshko, O.D. Azarov, M.S. Shelest, Yu.S. Yaremchuk. – Vinnica: VDTU, 2003. – 143 s.
6. Nikishova A.V., Kornyakov O.A. Ocenka kachestva steganograficheskix sistem // Aktual'ny'e voprosy' informacionnoj bezopasnosti regionov v usloviyax globalizacii informacionnogo prostranstva: materialy' III Vserossijskoj nauchno-prakticheskoj konferencii, g. Volgograd, 24-25 aprelya 2014 g. – V.: Izdatel'stvo VolGU, 2014. – S. 210-214.
7. Usenko O.A. Modeli i metody' ocenki nadezhnosti programmnogo obespecheniya informacionny'x sistem: uchebnoe posobie. – Taganrog: Izdatel'stvo TTI YuFU, 2008. – 40 s.
8. Barsukov V.S., Romancov A.P. Ocenka urovnya skry'tnosti mul'timedijny'x steganograficheskix kanalov xraneniya i peredachi informacii // Special'naya texnika, 2000. – № 6.
9. Barsukov V.S., Romancov A.P. Komp'yuternaya steganografiya vchera, segodnya, zavtra. – Special'naya texnika, 1998. – №4-5.
10. Kazaryan A.L. Ocenka stojkosti raznotipny'x steganograficheskix sistem // Seventh International Conference on Computer Science and Information Technologies. – Erevan, 2009.
11. Azhbaev T.G., Azhmuxamedov I.M. Analiz stojkosti sovremenny'x steganograficheskix algoritmov // Astraxan': Vestnik AGTU, 2008. – № 1.
12. Interestingstats [E'lektronny'j resurs] – URL: http://httparchive.org/interesting.php (data obrashheniya: 21.05.2014).

УДК 004.056, 004.738.5

В.С. ОЛАДЬКО, А.А. БЕЛОЗЁРОВА

ФОРМАЛИЗАЦИЯ ПОДХОДА К ВЫБОРУ ВЕБ-БРАУЗЕРА

Рассмотрена проблема обеспечения информационной безопасности при использовании пользователем веб-браузера. Проанализированы существующие причины нарушения безопасности. Показано, что одной из основных причин нарушения безопасности являются уязвимости в веб-браузерах и плагинах к ним. Выделены и описаны типовые классы уязвимостей в веб-браузере, а также атаки, которые могут быть через них реализованы. Разработано формализованное описание и функциональная модель многокритериального выбора веб-браузера.

***Ключевые слова**: Интернет; угроза; безопасность; электронные платежи; уязвимость; злоумышленник.*

ВВЕДЕНИЕ

Информационная безопасность в глобальной сети Интернет является одной из проблем, с которой современное общество столкнулось в процессе использования различных автоматизированных средств и современных интерактивных технологий: электронная коммерция, социальные сети, информационные и аналитические порталы, государственные услуги, мультимедийные конференции. В процессе использования данных средств и технологий пользователи получают, обрабатывают и передают данные разного уровня конфиденциальности. Поэтому при работе в сети Интернет пользователи должны заботиться о безопасности информации, которая, в свою очередь, зависит от многих факторов. Одним из факторов, влияющих на безопасность и удобство работы пользователя в глобальной сети, является выбор наиболее безопасного веб-браузера [1]. Веб-браузеры, являясь прикладными программами, фактически стали главными соединяющими элементами между объектами и ресурсами сети Интернет и пользователями с разных концов мира. Являясь неотъемлемым участником взаимодействия, веб-браузеры часто становятся слабым звеном в цепи безопасности, так как существующие в них уязвимости – это легкий способ для злоумышленника похитить персональные данные пользователя и/или воспользоваться ресурсами персонального компьютера (ПК) и выполнить вредоносные действия, такие, как:

- несанкционированный доступ;
- распространение вредоносного программного обеспечения;
- фишинг и мошенничество;
- превращение ПК в участника бот-сети;
- кража платежных данных и электронных заместителей финансовых средств.

Поэтому одним из важных параметров при выборе браузера должен быть показатель безопасного использования браузеров и наличие в нем механизмов, позволяющих противодействовать различному спектру интернет угроз.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВЕБ-БРАУЗЕРА

Браузер позволяет пользователю быстро и просто получать информацию, размещенную на многих веб-страницах. На графике изображена статистика Liveinternet, которая показывает использование веб-браузеров на период 2013-2015 года (рис. 1).

Анализ данной статистики позволяет сделать вывод, что на сегодняшний день одним из самых популярных браузеров в сети Интернет является Google Chrome. На втором месте по популярности идет Mobile Safari от компании Apple, это, в первую очередь, обуславливается популярностью мобильных платформ от Apple и ежегодным увеличении количества пользователей, использующих мобильный Интернет. Третье место занимают браузеры от Firefox. Как показывает практика, популярность данных браузеров обусловлена

скоростью работы, удобным поиском, проверкой орфографии, переводом страниц на иностранный язык, наличием механизмов безопасности и ряда дополнительных плагинов и надстроек.

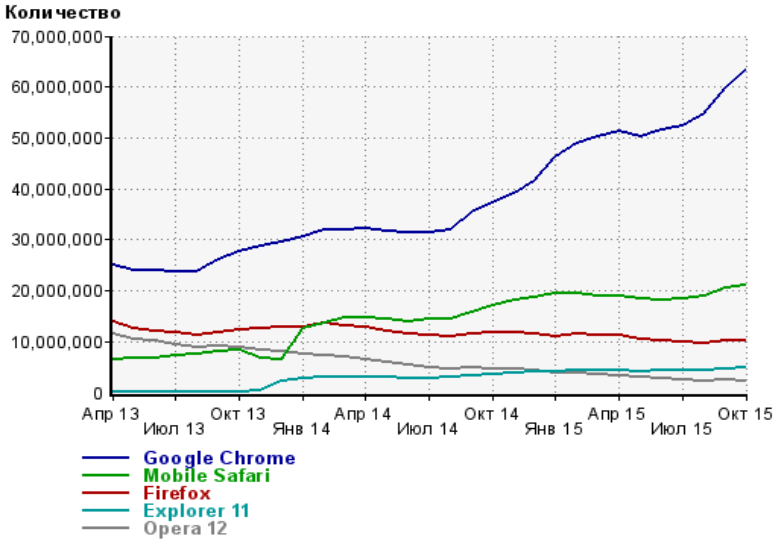

Рисунок 1 – Статистика веб-браузеров за 2013-2015 года

Однако анализ литературных источников [2-5] показывает, что ни один из существующих браузеров не является абсолютно безопасным и защищенным от всего спектра возможных угроз. Это подтверждается исследованиями Лаборатории Касперского [3], которые показывают, что при реализации злоумышленниками атак в 61% случаях использовались уязвимости в браузерах. Уязвимости в веб-браузерах можно отнести к следующим типам:

- Remote Code Execution (RCE), которые могут быть использованы атакующими для удаленного исполнения кода в веб-браузере или запуска на исполнение вредоносного скрипта, с помощью которого злоумышленник может похитить информацию с компьютера пользователя;
- ASLR bypass, которые могут использоваться злоумышленниками для обхода ASLR (случайное выравнивание адресного пространства);
- cross-origin обходы;
- use-after-free (UAF), представляющие собой способ передачи управления на свой код, в такой схеме легитимный исполняемый код должен содержать неправильную логику работы с памятью, которая заключается в том, что на каком-то этапе фрагмент кода обращается по указателю на тот блок памяти, который уже был освобожден ранее. Это может как вызвать аварийное завершение браузера, так и заставить уязвимый код передать управление по нужному адресу данных с заполнением их необходимыми злоумышленнику инструкциями;
- уязвимости нулевого дня, особенно опасны для популярных браузеров;
- уязвимости, связанные с favicon, обусловленные тем, что многие браузеры, такие, как Google Chrome, Firefox и Safari, не проверяют размер файла, что позволяет злоумышленнику забить всю доступную память, вызвав серьезные зависания. Internet Explorer не подвержен уязвимости;
- небезопасные прямые ссылки на объекты (Insecure Direct Object References), являющиеся также следствием недостаточной проверки пользовательских данных. При выводе каких-либо конфиденциальных данных для доступа к объекту используется идентификатор, который передается в открытом виде в адресной строке браузера, при этом проверка прав доступа к объектам не реализована.

Описанные уязвимости могут использоваться злоумышленником при реализации XSS-атак, SQL-инъекций, переполнении буфера, вызова исключительных ситуаций, заражения компьютера пользователя вредоносным программным обеспечением, спам-рассылок и фишинга. Поэтому разработчиками браузеров и плагинов проводиться регулярное исправление ошибок и закрытие обнаруженных уязвимостей. Кроме того, пользователям рекомендуется регулярно устанавливать обновленные версии браузеров, надстроек безопасности и плагинов к ним, не перегружать их плагинами и устанавливать плагины с официальных сайтов доверенных источников.

КРИТЕРИИ ВЫБОРА ВЕБ-БРАУЗЕРА

В связи с большим количеством существующих на сегодняшний день браузеров особенностями их реализации, функциональными возможностями и уровнем безопасности актуально решение задач, связанных с формализацией и автоматизацией процедур выбора наиболее удовлетворяющего требованиям пользователя веб-браузера. Для решения задачи выбора веб-браузера авторами предлагается использовать многокритериальную оценку, основанную на количественной нормированной шкале с элементами векторного анализа. Множество критериев оценки $K = \{K_1, K_2, K_3, K_4\}$ предлагается разбить на 4 группы:

1) Критерии безопасности браузера ($К_1$):
- возможность приватного просмотра ($К_{11}$);
- возможность очистки кэша ($К_{12}$);
- возможность защищенного просмотра и поддержка HTTPS-соединения ($К_{13}$);
- блокировка баннеров ($К_{14}$);
- блокировка всплывающих окон ($К_{15}$);
- фильтр фишинга и блокирование опасных сайтов ($К_{16}$);
- блокировка содержимого и скриптов ($К_{17}$);
- индикатор доверия сайтов ($К_{18}$);
- защита от слежения ($К_{19}$);
- автоматическое обновление ($К_{110}$).

2) Критерии функциональных возможностей браузера ($К_2$):
- создание вкладок ($К_{21}$);
- наличие менеджера закачки ($К_{22}$);
- наличие панели поиска ($К_{23}$);
- проверка орфографии ($К_{24}$);
- пропорциональное увеличение ($К_{25}$).

3) Критерии удобства эксплуатации ($К_3$):
- круглосуточная поддержка ($К_{31}$);
- поддержка нескольких операционных систем ($К_{32}$);
- поддержка веб-стандартов ($К_{33}$);
- потребление ресурсов ($К_{34}$);
- высокая скорость ($К_{35}$).

4) Цена ($К_4$):
- цена браузера ($К_{41}$);
- стоимость 1 года обслуживания ($К_{42}$).

При этом каждая группа критериев K_i будет иметь свой нормированный вес W_i в зависимости от степени значимости данной группы для пользователя. Все весовые коэффициенты нормированы в единицу $\sum_{i=1}^{4} W_i = 1$. А поскольку целью работы является выбор наиболее безопасного веб-браузера, то наибольший вес должна иметь группа критериев оценки, связанная с безопасностью. Значение каждого группового критерия K_i представляет собой сумму оценок по частным групповым критериям K_{ij} и в своем максимальном значение не превышает единицу (1).

$$K_i = \sum_{j=1}^{m} K_{i\,j} \le 1, \quad (1)$$

где m – число частных критериев в каждой группе.

Таким образом, при выборе наиболее удовлетворяющего требованиям пользователя браузера сначала для каждого браузера из списка альтернатив формируется оценочный вектор $K_A = \{K_1, K_2, K_{3,} K_4\}$, который сравнивается с эталонным вектором $KT = \{KT_1, KT_2, KT_{3,} KT_4\}$, составленным по требованиям пользователя к браузеру. Для проверки близости векторов в соответствии с [6] предлагается использовать метрику Манхэттена (2).

$$d(KT, K_A) = \|KT - K_A\| = \sum_{j=1}^{4} W_j \left| KT_i - K_{A\,i} \right|. \quad (2)$$

Наиболее подходящим будет являться тот браузер из списка альтернатив, вектор оценок K_A которого имеет наименьшее отклонение от эталонного вектора KT: $d(KT, K_A) \to \min$.

Правила выставления количественных оценок для частных критериев из каждой группы критериев представлены ниже.

Суммарная оценка по критериям безопасности браузера в соответствии с формулой 1 рассчитывается как $K_1 = \sum_{j=1}^{10} K_{1\,j}$. Для того, чтобы K_1=1, необходимо, чтобы в анализируемом браузере без применения дополнительных надстроек и плагинов были реализованы функциональные возможности, соответствующие всем частным критериям группы безопасности. Правила выставления оценки частным критериям представлены в (3).

$$K_{1j} = \begin{cases} 0, \text{если функция отсутсвует в браузере} \\ 0.05, \text{если функция отсутвует, но можно установить плагин} \\ 0.01, \text{если функция в наличии} \end{cases} \quad (3)$$

Суммарная оценка по критериям функциональные возможности в соответствии с формулой 1 рассчитывается так:

$$K_2 = \sum_{j=1}^{5} K_{2\,j}.$$

Для того, чтобы K_2=1, необходимо, чтобы в анализируемом браузере без применения дополнительных надстроек и плагинов были реализованы функциональные возможности, соответствующие всем частным критериям группы функциональные возможности. Правила выставления оценки частным критериям представлены в (4).

$$K_{2j} = \begin{cases} 0, \text{если функция отсутсвует в браузере} \\ 0.1, \text{если функция отсутвует, но можно установить плагин} \\ 0.2, \text{если функция в наличии} \end{cases} \quad (4)$$

Суммарная оценка по критериям удобство эксплуатации в соответствии с формулой 1 рассчитывается как

$$K_3 = \sum_{j=1}^{5} K_{3\,j}.$$

Для того, чтобы K_2=1, необходимо, чтобы оцениваемый браузер был максимально удобен в эксплуатации, имел высокую скорость и не требовал больших вычислительных

ресурсов. Правило выставления оценки по частному критерию K_{31} (круглосуточная поддержка) представлено на формуле 5.

$$K_{31} = \begin{cases} 0, \text{ если нет круглосуточной поддержки} \\ 0.2, \text{ если есть круглосуточная поддержка} \end{cases} \quad (5)$$

Правило выставления оценки по частному критерию K_{32} (поддержка операционных систем) представлено в (6).

$$K_{32} = \begin{cases} 0, \text{если браузер поддерживает 1 ОС} \\ 0.1, \text{если браузер поддерживает 2 ОС} \\ 0.2, \text{если браузер поддерживает более 2 ОС} \end{cases} \quad (6)$$

Правило выставления оценки по частному критерию K_{33} (поддержка веб-стандартов) представлено на формуле 7.

$$K_{33} = \begin{cases} 0, \text{ если поддерживает не все современные стандарты} \\ 0.2, \text{ если поддерживает все стандарты} \end{cases} \quad (7)$$

Правило выставления оценки по частному критерию K_{34} (потребляемые ресурсы) представлено на формуле 8.

$$K_{34} = \begin{cases} 0.1, \text{ если потребляет более 50\% вычислительных ресурсов компьютера} \\ 0.2, \text{ если потребляет менее 50\% больших вычислительных ресурсов компьютера} \end{cases} \quad (8)$$

Под потребляемыми браузером вычислительными ресурсами в данной работе понимается объем оперативной памяти компьютера и загрузка процессора.

При оценке браузера по частному критерию K_{35} (скорость) (под скоростью следует понимать относительный результат производительности браузера), получен с помощью специализированной программы тестирования, соотносящийся с возможностью компьютера пользователя (программная и аппаратная часть), качеством и скоростью сети Интернет. В данной работе при составлении правил выставления оценок использовалась программа тестирования браузера Peacekeeper [7]. Скорость определялась как высокая, если браузер набирал более 80% от максимально возможного числа баллов, средняя, если от 60% до 80%, и низкая, если меньше 60%. Правило выставления оценки по частному критерию K_{35} (скорость) представлено в формуле 9.

$$K_{35} = \begin{cases} 0, \text{если низкая скорость} \\ 0.1, \text{если скрость низкая при использовании плагинов} \\ 0.2, \text{если высокая скорость} \end{cases} \quad (9)$$

Суммарная оценка по критериям цена в соответствии с формулой 1 рассчитывается как:

$$K_4 = \sum_{j=1}^{2} K_{4j} .$$

Для того, чтобы K_2=1, необходимо, чтобы оцениваемый браузер требовал минимальных затрат на сопровождение и эксплуатацию. Правила выставления оценки частным критериям представлены на формуле 10.

$$K_{4j} = \begin{cases} 0.5, \text{если нет затрат} \\ 0, \text{если есть затраты} \end{cases} \quad (10)$$

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ВЫБОРА ВЕБ-БРАУЗЕРА

Разработанное формализованное описание процедуры выбора можно представить в виде функциональной модели, отображающей последовательность необходимых действий. Для разработки данной модели была выбрана нотация IDEF0. В соответствии с данной нотацией необходимо выделить входные и выходные данные, механизмы и управляющие воздействия на процесс выбора (рис. 2).

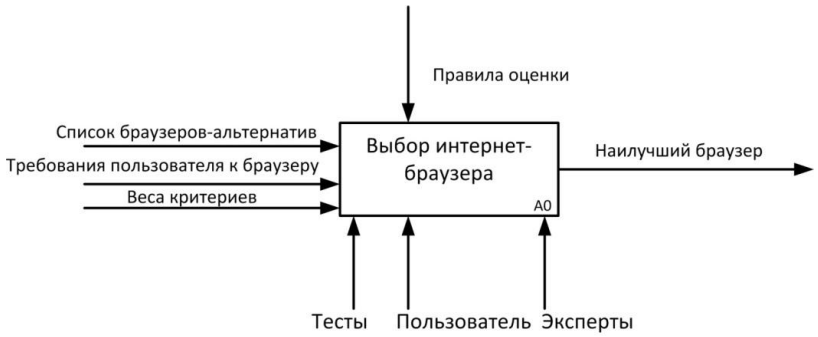

Рисунок 2 – Контекстная диаграмма выбора веб-браузера

В общем виде процесс выбора веб-браузера разбивается на следующие функции:

- сбор данных о характеристиках браузеров из списка альтернатив;
- формирование эталонного вектора на основе требований пользователя к веб-браузеру;
- выставление оценок по группам критериев для каждого браузера из списка альтернатив;
- формирование векторов оценок для каждого браузера из списка альтернатив;
- сравнение векторов оценок браузеров из списка альтернатив с эталонным вектором и выбор вектора с минимальным отклонением от эталона.

Связь между функциями и данными, используемыми в процесс выбора, представлены на схеме декомпозиции контекстной диаграммы (рис. 3).

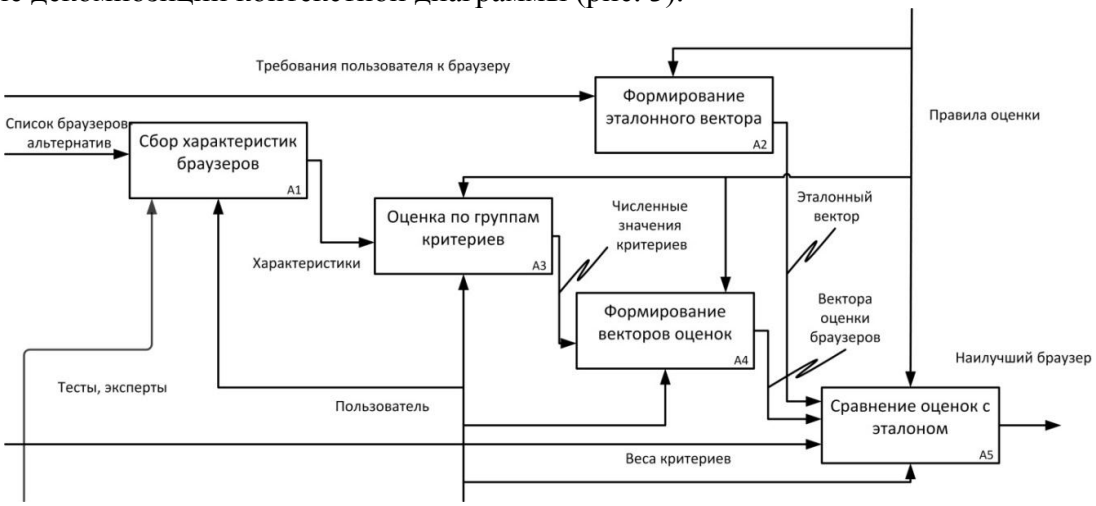

Рисунок 3 – Декомпозиция процесса выбора интернет-браузера

Данную функциональную модель можно использовать при разработке программы автоматизирующей процесс выбора веб-браузера.

ЗАКЛЮЧЕНИЕ

Предложенный подход может использоваться в качестве механизма поддержки принятия решений при выборе наиболее удовлетворяющего требованиям пользователя веб-браузера. Кроме того, формализованная модель может быть доработана и адаптирована для

использования в процессе планирования используемых средств защиты от атак злоумышленника и других интернет-угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Оладько В.С., Микова С.Ю., Нестеренко М.А. Технологии защиты интернет-технологий и web-приложений // Международный научный журнал, 2015. – № 8. – С. 81-86.
2. Шевченко А. Атака через браузер. Анализ вредоносных Flash-объектов и документов в формате PDF [Электронный ресурс]. – URL: http://nobunkum.ru/ru/flash (дата обращения 10.01.2015).
3. Новости кибербезопасности: Kaspersky Security Bulletin 2015 о хакерских атаках и не только // Тесты и обзоры лучшего софта для Windows [Электронный ресурс]. – URL: http://testsoft.su/novosti-kiberbezopasnosti-kaspersky-security-bulletin-2015-o-hakerskih-atakah-i-ne-tolko/ (дата обращения 10.01.2016).
4. OWASP TOP-10: практический взгляд на безопасность веб-приложений // Блог компании SimplePay [Электронный ресурс]. – URL: http://habrahabr.ru/company/simplepay/blog/258499/ (дата обращения 10.01.2016).
5. Идов Р. Уязвимости в плагинах и надстройках для браузеров // Доверие в сети [Электронный ресурс]. – URL: http://довериевсети.рф/article/51 (дата обращения 10.01.2016).
6. Хаханов В.И., Мищинко А.С., Вареца В.В. Метрики алгебры векторной логики для кибернетического пространства // Радиоэлектроника и информация, 2010. – № 3. – С. 39-42.
7. Программа тестирования веб-браузеров [Электронный ресурс]. – URL: http://peacekeeper.futuremark.com/results?key=CcEo&resultId=8350073 (дата обращения 10.01.2016).

Оладько Владлена Сергеевна
ФГАОУ ВО «Волгоградский государственный университет», г. Волгоград
Кандидат технических наук, доцент кафедры информационной безопасности
E-mail: oladko.vs@yandex.ru

Белозёрова Ангелина Андреевна
ФГАОУ ВО «Волгоградский государственный университет», г. Волгоград
Студент кафедры информационной безопасности

V.S. OLAD'KO *(Candidate of Engineering Sciences, Associate Professor of the Department of Information Security)*

A.A. BELOZYoROVA *(Student of the Department of Information Security)*
Volgograd State University, Volgograd

THE FORMALIZATION APPROACH TO THE CHOICE OF WEB-BROWSERS

The problem of information security when using the web browser user is investigated. There is a reason security breaches analyzed. The authors showed that one of the main causes of security breaches are vulnerabilities in web browsers and plug-ins to them. Typical classes of vulnerabilities in the Web browser are marked and identified the attack, which may be implemented through vulnerability. The formalized description and a functional model of multi-criteria choice of web browser developed.

Keywords: *Internet; threat; security; electronic payments; vulnerability; attacker.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Olad'ko V.S., Mikova S.Yu., Nesterenko M.A. Texnologii zashhity' internet-texnologij i web-prilozhenij // Mezhdunarodny'j nauchny'j zhurnal, 2015. – № 8. – S. 81-86.

2. Shevchenko A. Ataka cherez brauzer. Analiz vredonosny'x Flash-ob''ektov i dokumentov v formate PDF [E'lektronny'j resurs]. – URL: http://nobunkum.ru/ru/flash (data obrashheniya 10.01.2015).
3. Novosti kiberbezopasnosti: Kaspersky Security Bulletin 2015 o xakerskix atakax i ne tol'ko // Testy' i obzory' luchshego softa dlya Windows [E'lektronny'j resurs]. – URL: http://testsoft.su/novosti-kiberbezopasnosti-kaspersky-security-bulletin-2015-o-hakerskih-atakah-i-ne-tolko/ (data obrashheniya 10.01.2016).
4. OWASP TOP-10: prakticheskij vzglyad na bezopasnost' veb-prilozhenij // Blog kompanii SimplePay [E'lektronnyj resurs]. – URL: http://habrahabr.ru/company/simplepay/blog/258499/ (data obrashheniya 10.01.2016).
5. Idov R. Uyazvimosti v plaginax i nadstrojkax dlya brauzerov // Doverie v seti [E'lektronny'j resurs]. – URL: http://doverievseti.rf/article/51 (data obrashheniya 10.01.2016).
6. Xaxanov V.I., Mishhinko A.S., Vareca V.V. Metriki algebry' vektornoj logiki dlya kiberneticheskogo prostranstva // Radioe'lektronika i informaciya, 2010. – № 3. – S. 39-42.
7. Programma testirovaniya veb-brauzerov [E'lektronny'j resurs]. – URL: http://peacekeeper.futuremark.com/results?key=CcEo&resultId=8350073 (data obrashheniya 10.01.2016).

УДК 004.01; 621.391

А.П. ФИСУН, Ю.А. БЕЛЕВСКАЯ, Р.А. ФИСУН,
Р.А. БЕЛЕВСКИЙ, Д.А. ЕСЕННИКОВ

КОНЦЕПЦИЯ ФОРМИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В статье изложены результаты анализа и систематизации направлений, подходов классификации и формирования угроз информационной безопасности (ИБ) информационно-телекоммуникационных технологий (ИКТ), в том числе одного из базовых классов информационной системы, информационно-телекоммуникационные сетей (ИТКС) и их компонентов, являющихся информационной, технической, программно-аппаратной основой объектов информатизации (ОИ) современных материально-энергетических и информационных сфер и видов деятельности личности, общества и государства. Предложен концептуальный подход формирования классификационной структуры угроз ИБ ИКТ ОИ и их состав компонентов, характеризующихся значительным многообразием и разнообразием оснований классификации, показателей, критериев и характеристик, определяемых, в свою очередь, количественными, качественными показателями, и критериев эффективности ОИ и их ИКТ, функционирующих в сложных условиях неопределенности, риска, воздействия внешних и внутренних угроз.

Ключевые слова: *информационная безопасность (ИБ); информационно-телекоммуникационные технологии (ИКТ); информационные системы (ИС); информационно-телекоммуникационные сети (ИТКС); объекты информатизации (ОИ); системы; средства комплексного обеспечения информационной безопасности и защиты информации (СКОИБ); угрозы информационной безопасности.*

Исследования известных отечественных и зарубежных достижений в области обеспечения информационной безопасности (ИБ) социотехнических систем и их компонентов (СТС), прежде всего информационно-телекоммуникационных технологий (ИКТ), информационно-телекоммуникационных сетей (ИТКС), составляющих основу объектов информатизации (ОИ) всех материально-энергетических и информационных сфер и видов деятельности современного, информационного общества (ИО) [1-26], позволяет заключить, что проблема повышения эффективности обеспечения ИБ всегда остается актуальной и зависит от полноты учета угроз ИБ обусловленных объективным существованием, видоизменением, возникновением и ростом соответствующих дестабилизирующих факторов (ДФ), представляющих события, явления, процессы, оказывающие обуславливающие возможность потенциального негативного воздействия на информацию, системы ее обработки и способствующее возникновению соответствующих угроз этим объектам. Такими угрозами ИБ из рассмотренного множества [1-34], как нам видится, являются угрозы, несущие потенциальную опасность случайного или преднамеренного:

– нарушения безопасности информации (БИ), т.е. нарушения логической или физической целостности информации, несанкционированного доступа, модификации, копирования, блокирования информации;

– демаскирования ТКС, ИТКС и других ИС, их средств и комплексов обработки конфиденциальной информации;

– разрушающего воздействия на ОИ, их компоненты, в том числе ИКТ и ИТКС.

Исходя из проведенного анализа проблем обеспечения ИБ [1-26], известного определения безопасности информации и ИБ ОИ, их ИКТ, ИТКС [27-34], материально-энергетического и информационного содержания, характеристик и особенностей ОИ, ИКТ,

ИТКС, можно заключить, что содержание, свойства, особенности, угроз ИБ ОИ, ИКТ, ИТКС и дестабилизирующих факторов объективно обуславливается свойствами ОИ, ИКТ и ИТКС, их целевым назначением, функциональными возможностями, средой и условиями функционирования, а также субъективными намерениями и целями нарушителей. Необходимо заметить, что и любые – реальные и гипотетические – цели нарушителей, определяющие соответствующее содержание угроз, априори также будут зависеть от потенциальных, гипотетических свойств и характеристик ОИ их ИКТ, ИТКС. В целом формируемое множество угроз будет обуславливаться и определяться:

– потребительскими свойствами информационных потоков и ресурсов (ИР) ОИ и прежде всего показателями конфиденциальности;

– потенциальным множеством ОИ, на которое нацелены угрозы, их ИКТ, ИТКС;

– технико-эксплуатационными характеристиками и свойствами функционирующих, модернизируемых или проектируемых ОИ, ИКТ, ИТКС, а также физико-географическими условиями их функционирования;

– воздействием человеческого фактора, отражающего легитимную функциональную деятельность и непреднамеренные действия обслуживающего персонала, пользователей ОИ, ИКТ, ИТКС, т.е. так называемого «внутреннего нарушителя», а также преднамеренные противоправные целенаправленные воздействия злоумышленников («внешнего нарушителя») независимо от их функционального статуса (обслуживающий персонал, легитимные пользователи или противник).

При этом важной особенностью решения проблемы эффективного обеспечения ИБ ОИ, ИКТ, ИТКС, осуществляемой на основе выбора эффективных вариантов систем и средств комплексного обеспечения ИБ (СКОИБ) и реализации мероприятий обеспечения ИБ, является реализация требования полноты учета дестабилизирующих факторов и угроз ИБ ОИ, ИКТ и ИТКС. Это, безусловно, предполагает постановку и решение актуальной задачи классификации и формирования относительно полного множества известных, существующих и потенциально возможных дестабилизирующих факторов и угроз ИБ для объективной, количественной интегральной технико-экономической оценки эффективности используемых СКОИБ, их компонентов и реализации соответствующих мер и мероприятий обеспечения ИБ ОИ, ИКТ, ИТКС.

Анализ известных подходов формирования и классификации угроз ИБ [1-26] позволил выявить значительное многообразие и разнообразие оснований классификации, используемых в зависимости от решения конкретных прикладных задач обеспечения ИБ ОИ, используемых ИКТ, ИТКС и СКОИБ. Прикладная направленность формирования искомых оснований классификации множества угроз и дестабилизирующих факторов [1-26] вполне объяснима тем, что наряду с существованием некоторых статистических данных о ряде частных угроз и дестабилизирующих факторах, сколько-нибудь относительно полных и всесторонних априорных данных об угрозах, как было выявлено, не существует, да и не может существовать по определению в силу их случайного характера появления и воздействия. Поэтому на концептуальном уровне при формировании множества угроз и дестабилизирующих факторов необходимо учитывать реальную действительность, определяемую конкретными целями, предназначением, условиями функционирования, уровнем конфиденциальности обрабатываемой информации ОИ, используемыми их ИКТ, ИТКС и компонентами. С учетом этого при формировании угроз ИБ ОИ, ИКТ, ИТКС и дестабилизирующих факторов предлагается концептуальный подход, состоящий в реализации следующих, вполне очевидных посылок:

1) рассмотрение и формирование множества угроз и дестабилизирующих факторов ИБ как функционирующих, модернизируемых, так и проектируемых ОИ, ИКТ, ИТКС, необходимо осуществлять с учетом и в рамках реальной действительности и использования существующих, проектируемых и перспективных средств, систем, комплексов, компонентов ОИ, ИКТ, ИТКС;

2) в силу случайного характера возникновения и воздействия угроз, дестабилизирующих факторов, отсутствия относительно полных априорных данных о них, а также известных подходов и методов систематизации и классификации [35-41 и др.] необходимо в качестве одного из подходов первоначального формирования относительно полного множества угроз и дестабилизирующих факторов [1-34] использовать методы экспертных оценок, позволяющие сформировать относительно полный перечень возможных классов, групп и видов угроз и дестабилизирующих факторов, потенциально возможных источников образования угроз;

3) при формировании множества угроз и дестабилизирующих факторов учитывать количественную и качественную недостаточность ОИ, ИКТ, ИТКС, СКОИБ, определяемых заданными архитектурой, технологией, уровнем конфиденциальности обрабатываемой информации, условиями функционирования, отказами, сбоями, ошибками компонентов и элементов ОИ, ИКТ, ИТКС, физико-географическими условиями их функционирования, злоумышленными действиями, побочными явлениями, процессами, материально-энергетическими средствами, используемые ОИ и ИКТ, ИТКС;

4) рассматривать в качестве источников угроз и дестабилизирующих факторов внутренние источники, ОИ, обусловленные обслуживающим персоналом и легитимными пользователями ОИ, ИКТ, ИТКС, технологиями их функционирования (совокупность средств, приемов, правил, мероприятий и соглашений, используемых в процессе обработки информации, модели, алгоритмы и программы, а также внешние источники (физико-географическую среду, совокупность элементов, не входящих и входящий в состав ОИ (злоумышленники), оказывающие влияние на снижение ИБ [1-34].

С учетом этих концептуальных положений можно рассмотреть вариант классификации дестабилизирующих факторов и угроз ИБ по основаниям и показателям угроз, представленным в таблице 1, развернутое содержание которой включает следующие компоненты

1) Показатель «виды угроз» является основополагающим, определяющим целевую направленность по уровню обеспечения ИБ ОИ, его ИКТ, ИТКС, СКОИБ, включающую обеспечение:

– безопасности информации – защиту физической, логической целостности информации, защиту ее от несанкционированного доступа, копирования и модификации, блокирования;

– защиты ОИ, его ИКТ, ИТКС, осуществляющих обработку конфиденциальной информации и СКОИБ от демаскирования;

– защиты ОИ, его ИКТ, ИТКС, СКОИБ от разрушающего воздействия информации злоумышленников.

2) По природе происхождения множество возможных угроз, в том числе и определенных по целевому назначению (пункт 1), можно классифицировать по показателю мотивации действия человека и разделить на две группы: непреднамеренные угрозы обусловленные случайными, не зависящими от воли людей обстоятельствами, возникающими на ОИ в процессе функционирования ИКТ, ИТКС, и преднамеренные угрозы (табл. 1);

3) По предпосылкам появления угроз выделяют [1-36] объективные и субъективные:

а) объективные предпосылки:

– количественная недостаточность ИКТ, ИТКС – физическая нехватка одного или нескольких элементов, вызывающая нарушения технологического процесса обработки/защиты информации (или) перегрузку и сбои их элементов;

– качественная недостаточность – несовершенство конструкции, организации и условий размещения элементов и самого ОИ, а также состояние сложившихся окружающих физико-географических условий функционирования ОИ, влекущие появление возможностей

случайного или преднамеренного негативного воздействия на обрабатываемую конфиденциальную информации;

б) субъективными предпосылками являются:

– деятельность иностранных разведывательных и специальных служб – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами, ведение информационного противоборства (ИПБ) и информационных войн (ИВ) с использованием основных видов разведки: агентурной (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых недоброжелателей) и технической;

– промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или хищения, а также по созданию для себя благоприятных условий в целях получения максимальной выгоды;

– преступные действия отдельных групп, формирований и физических лиц – хищение, несанкционированное копирование, модификация, блокирование информации или программного обеспечения ИКТ, ИТКС в целях незаконного получения прибыли или разрушения в интересах конкурентов;

– злоумышленные действия недобросовестных (обиженных) сотрудников ОИ – хищение, несанкционированное копирование, модификация, блокирование информации или программного обеспечения ИКТ, ИТКС по эгоистическим или корыстным мотивам.

4) В качестве источника угроз принимается непосредственный так называемый «исполнитель», осуществляющий воздействие на ОИ и его компоненты с целью воздействия на обрабатываемую в нем информацию с использоапнием ИКТ, ИТКС, СКОИБ.

Таким образом, угрозы ИБ ОИ, обусловленные предпосылками их формирования, представляющими дестабилизирующие факторы, можно представить следующими показателями:

- нарушение физической целостности (НФЦ), $Y_{НФЦ}$;
- нарушение логической целостности (НЛЦ), $Y_{НЛЦ}$;
- несанкционированная модификация (НСМ), $Y_{НСМ}$;
- несанкционированное получение (доступа) (НСД), $Y_{НСД}$;
- несанкционированное размножение (копирования) (НСК), $Y_{НСК}$;
- демаскирование (расконспирация) ИКТ, ИТКС и их компонентов (ДМ), $Y_{ДМ}$;
- разрушающее воздействие на информацию, ИКТ, ИТКС (РВИ), $Y_{РВИ}$.

Таблица 1 – Системная классификация угроз безопасности информации

Основания классификации	**Значения показателей угроз**	**Критерии угрозы**
Виды угроз	Физической целостности	Уничтожение (искажение)
	Логической структуры	
	Содержания	Искажение структуры
	Конфиденциальности	Несанкционированное получение
		Несанкционированная модификация
	Права собственности	Присвоение чужого права
Природа происхождения угроз	Непреднамеренные	Отказы, ошибки, сбои, стихийные бедствия, побочные явления
	Преднамеренная	Злоумышленные действия людей
Предпосылки появления угроз	Объективные	Количественная недостаточность элементов ОИ
		Качественная недостаточность элементов ОИ
	Субъективные	Разведывательные органы иностранных государств

		Промышленный шпионаж Уголовные элементы Недобросовестные и обиженные сотрудники ОИ
Источники угроз	Люди Технические устройства Модели, алгоритмы, программы Технологические схемы обработки Внешняя среда	Пользователи ОИ Посторонние лица на ОИ Персонал ОИ. Регистрация передача, хранение, переработка и выдача. Общего назначения, прикладные, вспомогательные. Ручные, интерактивные, внутримашинные, сетевые. Состояние физико-географических условий Побочные шумы Побочные сигналы

Формируемое относительно полное множество реальных угроз может быть представлено выражением (1)

$$Y = \{Y_{НФЦ}, Y_{НЛЦ}, Y_{НСМ}, Y_{НСД}, Y_{НСК}, Y_{ДМ}, Y_{ИВ}\}. \quad (1)$$

Проявлению и возникновению этих угроз сопутствуют следующие причины:

$$Y^* = \{Y^*_{ПНЦ}, Y^*_{КНСД}, Y^*_{СНСК}\}. \quad (2)$$

где $Y^*_{ПНЦ}$ – причины нарушение целостности информации (ПНЦИ); $Y^*_{КНСД}$ – каналы несанкционированного доступа к информации (КНСДИ); $Y^*_{НСК}$ – способы несанкционированного размножения (копирования) информации (СНКИ).

Тогда с учетом условий возникновения угроз (табл. 1) систематизированных основных причин ПНЦИ, КНСДИ и СНКИ, способствующих формированию угроз на различных этапах обработки конфиденциальной информации и обеспечения ИБ ОИ и его компонентов, обобщенную модель формирования угроз ИБ можно представить, как показано на рисунке 1.

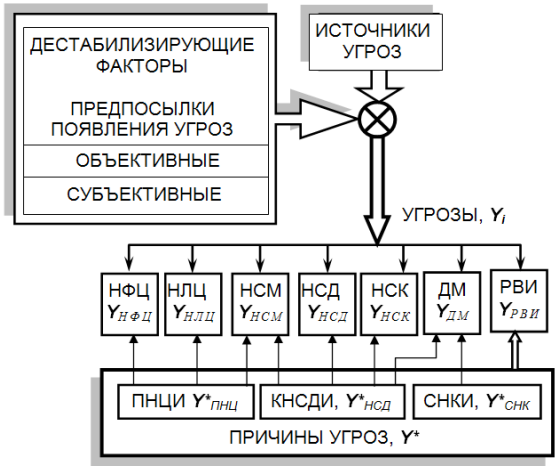

Рисунок 1 – Модель формирования показателей угроз ИБ

С учетом известных результатов исследований и работ ученых и специалистов [1-35] уточнено содержание составляющих компонентов этой модели.

Причины нарушения целостности информации (ПНЦИ) представляют ДФ, в результате воздействия которых может быть нарушение физическая или логическая целостности информации (искажение, уничтожение или блокирование) в результате:

– отказов, сбоев и ошибок в работе ИКТ, ИТКС, их основных (ОТСС) и вспомогательных технических средств и систем (ВТСС) обработки информации, программного обеспечения, носителей информации;

– ошибок, некомпетентных действий персонала и пользователей;

– хищения, утраты, подмены, модификации информации и ее носителей;

– чрезвычайных ситуаций природного и техногенного характера;

– умышленных действий человека на ОИ.

Каналы несанкционированного получения информации (КНДИ) представляют ДФ, способствующие несанкционированному получению конфиденциально информации или ее модификации без легитимных пользователей и обслуживающего персонала:

– безотносительно к обработке информации на ОИ;

– возникающие в силу объективных физических процессов и особенностей обработки конфиденциальной информации в ИКТ, ИТКС и их компонентов без непосредственного доступа злоумышленников этим средствам обработки информации на ОИ;

– проявляющиеся в процессе обработки конфиденциальной информации при определенных воздействиях злоумышленников на средства обработки и защиты информации без изменения их режимов функционирования или с изменением.

Способы несанкционированного размножения (копирования) информации (СНКИ) могут реализовываться за счет:

– сторонних, взаимодействующих с ОИ организаций и учреждений и используемых ими средствами обработки информации;

– непосредственных действий на ОИ пользователей или обслуживающего персонала;

– учреждений-разработчиков технических средств обработки и защиты информации, их программного обеспечения.

Проведенный анализ угроз ИБ и ДФ [1-34] показывает, что наиболее трудно определяемыми ДФ, обуславливающими угрозы ИБ ОИ, являются преднамеренные действия, мотивы деятельности, другие характеристики обслуживающего персонала, пользователей ОИ (внутренние нарушители) и непреднамеренные действия злоумышленников (внешние нарушители. В наиболее общем виде классификацию этих нарушителей можно осуществить по следующим основаниям:

– по уровню профессиональной подготовки N_1;

– используемым нарушителями методам и средствам N_2;

– времени действия N_3;

– месту действий N_4.

Тогда возможные действия нарушителя (внутреннего или внешнего) будут описываться множеством (3):

$$N = \{N_1, N_2, N_3, N_4\}. \quad (3)$$

В качестве обобщенных, но далеко не окончательных характеристик действий нарушителя, представляющих соответствующий функционал, могут быть следующие.

Нарушитель по уровню профессиональной подготовки N_1:

– знает функциональные особенности ОИ и их компонентов, обрабатываемые в них массивы информации, информационных ресурсов, потоки транзакций;

– знает структуру, функции и механизм действий средств комплексного обеспечения информационной безопасности ОИ, из ИКТ, ИТКС и других компонентов, их достоинства, недостатки;

– умеет пользоваться программно-аппаратными, техническими и другими средствами, комплексами и оборудованием для осуществления реализации угроз ОИ и их компонентам;

– владеет высоким уровнем знаний, опытом работы со средствами ИКТ, ИТКС, их компонентами, используемыми ОИ;

– обладает высоким уровнем знаний и умений в области программирования, разработки, эксплуатации ЭВМ, систем и сетей ЭВМ;

– другое.

Нарушитель по используемым нарушителями методам и средствам N_2 знает, владеет, умеет использовать и применять:

– агентурные методы добывания информации;

– технические средства и комплексы перехвата информации без модификации компонентов системы ее обработки на ОИ и его компонентах;

– штатные, компактные, носимые, возимые средства и комплексы, для скрытного преодоления рубежей обеспечения информационной безопасности, добывания конфиденциальной информации;

– методы, средства активного воздействия (модификация, подключение) на информацию, системы, комплексы и средства ее обработки;

– другие методы, средства и комплексы.

Нарушитель по времени действий (N3) может создавать угрозы ИБ ОИ:

1) в процессе функционирования ОИ, его ИКТ, ИТКС, КСОИБ, ОТСС, ВТСС;

2) в период неактивности компонентов ОИ:

– в нерабочее время;

– во время плановых перерывов;

– во время перерывов для обслуживания и ремонта;

3) в процессе обслуживания ОИ и его компонентов обработки информации и в период неактивности компонентов ОИ.

Нарушитель по месту действий (N_4) может создавать угрозы ИБ ОИ:

– без доступа на контролируемую территорию ОИ и его ИКТ, ИТКС;

– с контролируемой территории ОИ без доступа в здание и сооружения ОИ;

– внутри помещений ОИ, но без доступа к его ИКТ, ИТКС, другим программно-аппаратным техническим средствам обработки конфиденциальной информации;

– с рабочих мест пользователей ОИ;

– с доступом в зону обработки информации (базы данных, архивы и другие);

– с доступом в зону управления средствами комплексного обеспечения информационной безопасности ОИ;

– другие.

Таким образом, на основе выбора или разработки системы классификации угроз ОИ, их ИКТ, ИТКС и других компонентов можно определить некоторое начальное состояние категорируемого ОИ с заданным уровнем информационной безопасности ИБ, который зависит от эффективности систем и средств комплексного обеспечения ИБ. При построении таких СКОИБ можно использовать два пути: построение СКОИБ конкретно для каждого ОИ или построение СКОИБ для определенного класса ОИ, близких по какому-либо критерию. В качестве такого критерия может быть выбран обобщенный (интегральный) показатель ИБ, определяемый показателями, характеризующими БИ и показателями, характеризующими защищенность самого ОИ, ИКТ, ИТКС, их компонентов от демаскирования и разрушающего информационного воздействия злоумышленников на ОИ, ИКТ, ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Бушуев С.Н. и др. Теоретические основы информационно-технических систем. – СПб.: ВАС, 1998. – 404 с.
2. Герасименко В.А., Малюк А.А. Основы защиты информации: учебник. – М.: МОПО, МИФИ, 1997. – 537 с.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1998.
4. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России: учебное пособие. – Ч.1. Основные понятия и определения / под общ. ред. проф. А.А. Прохожева. – М.: РАГС при Президенте РФ, 1999. – 52 с.
5. Коваленко Б.В. и др. Национальная безопасность: информационная составляющая // под общ. ред. В.В. Еременко. МОСУ, 2000. – 311 с.
6. Зегжда П.Д. Обеспечение информационной безопасности. – М.: Яхтсмен, 1996. – 298 с.
7. Комарович В.Ф., Симонов М.В., Фролов В.Ю. Основы радиоэлектронной борьбы, радиоэлектронная защита, безопасность связи и АСУ // под ред. Симонова М.В. – Л.: ВАС, 1989. – 346 с.
8. Минаев В.А., Курушин В.Д., Компьютерные преступления информационная безопасность. – М.: Новый Юрист, 1998. – 256 с.
9. Хоффман Л.Дж. Современные методы защиты информации; перевод с англ. под ред. Герасименко В.А. – М.: Советское радио, 1980. – 263 с.
10. Шураков В.В. Обеспечение сохранности информации в системах обработки данных. – М.: Финансы и статистика, 1985. – 224 с.
11. Макаров В.Ф. Теоретические и организационно-технические основы защиты информации в органах внутренних дел; диссертация доктора технических наук, 1992. – М.: Академия МВД. – 289 с.
12. Ярочкин В.И. Безопасность информационных систем, 1996. – М.: «Ос-89». – 320 с
13. Ажмухамедов И.М. Решение задач обеспечения ИБ на основе системного анализа и нечёткого когнитивного моделирования: монография, 2012. – Астрахань, 2012. – 344 с.
14. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: ФАТРМ, 2007. – 6 с.
15. Статистика уязвимостей систем дистанционного банковского обслуживания. – М.: 2013. – 40 с. [Электронный ресурс]. – URL: http://www.opennet.ru/opennews/art.shtml?num=28338; http://www.exploit-db.com/exploits/15024/.
16. Желтов С.А. Общая методика практической апробации вычислительных систем в отношении рисков реализации угроз ИБ // Вестник РГГУ. Серия «Информатика, защита информации. Математика». – № 11(133). – М.: РГГУ, 2014. – С. 10-15
17. Тарасова Н.А. Структуризация организационных рисков в системах обеспечения информационной безопасности предприятий // Вестник РГГУ. Серия «Информатика, защита информации. Математика». – № 11(133). – М.: РГГУ, 2014. – С. 15-25
18. Ясенев В.Н. ИБ в экономических системах: учебное пособие. – Н. Новгород: Издательство ННГУ, 2006. – 253 с.
19. Черешкин Д.С. и др. Методика оценки рисков нарушения информационной безопасности в автоматизированных информационных системах / Д.С. Черешкин, А.А. Кононов, Е.Г. Новицкий. В.Н. Цыгичко; Институт систем анализа РАН. – М.: ИСА РАН, 1999
20. Ярочкин В.И. Информационная безопасность: учебник для студентов ВУЗов. – М.: Гаудеамус, 2004. – 2 изд.
21. Гладких А.А., Дементьев В.Е. Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов, обучающихся по специальностям 08050565, 21040665, 22050165, 23040165. – Ульяновск: УлГТУ, 2009. – 156 с.
22. Войтик А.И., Прожерин В.Г. Экономика информационной безопасности: учебное пособие. – СПб.: НИУ ИТМО, 2012. – 120 с.
23. Информационная безопасность: экономические аспекты. Информационный бюллетень № 10 (125)/2003. – М: Jet Info, 2003. – С. 1-23.
24. Анализ угроз информационной безопасности. – Тамбов: ТГТУ, 2007. – 10 с. [Электронный ресурс]. – URL: http://www.studfiles.ru/preview/4518611/page:2/.
25. Методы и средства защиты компьютерной информации [Электронный ресурс]. – URL: http://country-expert.narod.ru/index.html.
26. Классификация угроз информационной безопасности [Электронный ресурс]. – URL: http://country-expert.narod.ru/pages/3.htm.

27. Вихорев С.В. Классификация угроз информационной безопасности. – М.: ОАО «Элвис Плюс», 1998 [Электронный ресурс]. – URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?print.
28. Хорин В.В. Вопросы создания методологии системы защиты информации в АСУ // Сб. НТП и информация, 1993. – № 3. – М.: ВНИИМИ. – С. 23-32.
29. Фисун А.П. Моделирование и оценка угроз информационной безопасности. Сборник материалов 8-й Международной конференции «Информатизация правоохранительных систем» (МФИ-99), 1999. – Часть 2. – М.: Академия МВД РФ.
30. Фисун А.П., Лебедев В.Н. Определение и классификация угроз безопасности информационно-вычислительных сетей // Труды Академии управления МВД России «Компьютерные технологии и управление ОВД», 2000. – М.: Академия управления МВД РФ. – С. 67-78.
31. Фисун А.П., Минаев В.А., и др. Теоретические основы информатики и информационная безопасность: монография. – М.: Радио и связь, 2000. – 466 с.
32. Фисун А.П. Теоретические основы информационной безопасности информационных телекоммуникационных систем; диссертация доктора технических наук. – М.: ЦНИИРЭС, 2000. – 468 с.
33. Фисун Р.А. Моделирование угроз информационной безопасности информационно-телекоммуникационных систем. Дипломный проект, 2003. – Орел, Академия ФАПСИ.
34. Фисун А.П. и др. Моделирование угроз информационной безопасности человеко-компьютерных систем / А.П. Фисун, К.А. Джевага, Р.А. Фисун, Л.А. Гращенко // Сборник материалов 2-й Всероссийской НПК «Методы и средства технической защиты конфиденциальной информации» 7-9 июня 2005 года. – Обнинск: ГОУ ГЦИПК.
35. Фисун А.П. Повышение эффективности полевой сети правительственной связи на основе использования методов математического моделирования; диссертация кандидата технических наук. – М.: Академия МВД, 1992.
36. Макаров Б.Е., Фисун А.П. Постановка задачи классификации и оценки угроз информационной безопасности информационных систем // Сборник научных трудов ученых Орловской области, 1999. – Вестник науки. – Выпуск 5. – В 2-х томах. – Т. 1 – Орел: Орел ГТУ. – С. 24-27.
37. Жамбю М. Иерархический кластер-анализ и соответствия. – М.: Финансы и статистика, 1988. – 342 с.
38. Лейбкинд А.Р., Рудник Б.Л., Тихомиров А.А. Математические методы и модели формирования организационных структур управления. – М.: МГУ, 1982. – 232 с.
39. Мандель И.Д. Кластерный анализ; предисловие Б.Г. Миркина. – М.: Финансы и статистика, 1988. – 176 с.
40. Многокритериальные задачи принятия решений; под ред. Д.М. Гвышиани, С.В. Емельянова. – М.: Машиностроение, 1978. – 192 с.
41. Розова С.С. Классификационная проблема в современной науке. – Новосибирск: Наука, 1986. – 224 с.
42. Саати Т. Принятие решения. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.
43. Экспертные системы. Принципы работы и примеры: пер. с англ.; под ред. Р.Форсайта. – М.: Радио и связь, 1987. – 224 с.

Фисун Александр Павлович
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Доктор технических наук, профессор, профессор кафедры «Электроника, вычислительная техника, информационная безопасность»
Тел.: 8 910 307 0081
E-mail: fisun01@pisem.net

Белевская Юлия Александровна
ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», г. Орел
Кандидат юридических наук, доцент, магистрант направления «Конструирование и технология электронных средств»
Тел.: 8 (4862) 42-15-56
E-mail: furiya_ua@mail.ru

Фисун Роман Александрович
Отделение по Смоленской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу, г. Смоленск
Заместитель начальника отдела информационной безопасности
Тел.: 8 919 711 00 03

Белевский Роман Александрович
ФГКОУ ВО «Орловский юридический институт МВД Российской Федерации», г. Орел
Кандидат юридических наук, старший преподаватель кафедры «Гражданско-правовые и экономические дисциплины»
Тел.: 8 910 747 11 00
E-mail: belevskiy@gmail.com

Есенников Дмитрий Алексеевич
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, г. Москва
Слушатель по направлению «Бизнес-информатика»
Тел.: 8 903 968 71 11
E-mail: boxgen@mail.ru

A.P. FISUN *(Doctor of Engineering Sciences, Professor,*
Professor of the Department «Electronics, Computer Science, Information Security»)

Yu.A. BELEVSKAYa *(Candidate of Engineering Sciences, Associate Professor,*
Master Student of the Department «Civil, Law and Economic Disciplines»)
Orel State University named after I.S. Turgenev, Orel

R.A. FISUN *(Deputy Head of Department of Information Security)*
Department of the Smolensk Region of the Main Department of the Central Bank of the Russian Federation in the Central Federal District, Smolensk

R.A. BELEVSKIJ *(Candidate of Engineering Sciences,*
Senior Teacher of the Department «Civil, Law and Economic Disciplines»)
Orel Law Institute of the Russian Interior Ministry named V.V. Luk'yanov, Orel

D.A. ESENNIKOV *(Student of the Department «Business Informatics»)*
The Russian Presidential Academy of National Economy and Public Administration, Moscow

THE CONCEPT OF FORMING OF INFORMATION SECURITY THREATS INFORMATION-TELECOMMUNICATION NETWORKS INFORMATION OBJECTS

The article presents the results of the analysis and systematization of the directions, approaches to the classification and formation of threats to the information security (ISC) information and telecommunication technologies (ICT), including one of the base classes of the information system, information and telecommunication networks (ITN) formation and their components, which are informational, technical, software and hardware basis of the object information (OI) modern material and energy and information spheres and activities of the individual, society and the state. The conceptual approach of forming a classification structure of information security threats to the IS ITN OI and their components, characterized by a significant diversity and variety of classification bases, indicators, criteria and characteristics defined, in turn, the quantitative and qualitative indicators and criteria of efficiency of OI and they ICT, operating in difficult conditions of uncertainty, risk, impact of external and internal threats.

Keywords: *information security (ISC); information and telecommunication technologies (ICT); information systems (IS); information and telecommunication network (ITN) formation; the object information (OI); system; means an integrated information security and information protection (SCOB); threats to information security.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Bushuev S.N. i dr. Teoreticheskie osnovy' informacionno-texnicheskix sistem. – SPb.: VAS, 1998. – 404 s.

2. Gerasimenko V.A., Malyuk A.A. Osnovy' zashhity' informacii: uchebnik. – M.: MOPO, MIFI, 1997. – 537 s.
3. Gerasimenko V.A. Zashhita informacii v avtomatizirovanny'x sistemax obrabotki danny'x. – M.: E'nergoatomizdat, 1998.
4. Emel'yanov G.V., Strel'cov A.A. Informacionnaya bezopasnost' Rossii: uchebnoe posobie. – Ch.1. Osnovny'e ponyatiya i opredeleniya / pod obshh. red. prof. A.A. Proxozheva. – M.: RAGS pri Prezidente RF, 1999. – 52 s.
5. Kovalenko B.V. i dr. Nacional'naya bezopasnost': informacionnaya sostavlyayushhaya // pod obshh. red. V.V. Eremenko. MOSU, 2000. – 311 s.
6. Zegzhda P.D. Obespechenie informacionnoj bezopasnosti. – M.: Yaxtsmen, 1996. – 298 s.
7. Komarovich V.F., Simonov M.V., Frolov V.Yu. Osnovy' radioe'lektronnoj bor'by', radioe'lektronnaya zashhita, bezopasnost; svyazi i ASU // pod red. Simonova M.V. – L.: VAS, 1989. – 346 s.
8. Minaev V.A., Kurushin V.D., Komp'yuterny'e prestupleniya informacionnaya bezopasnost;. – M.: Novy'j Yurist, 1998. – 256 s.
9. Xoffman L.Dzh. Sovremenny'e metody' zashhity' informacii; perevod s angl. pod red. Gerasimenko V.A. – M.: Sovetskoe radio, 1980. – 263 s.
10. Shurakov V.V. Obespechenie soxrannosti informacii v sistemax obrabotki danny'x. – M.: Finansy' i statistika, 1985. – 224 s.
11. Makarov V.F. Teoreticheskie i organizacionno-texnicheskie osnovy' zashhity' informacii v organax vnutrennix del; dissertaciya doktora texnicheskix nauk, 1992. – M.: Akademiya MVD. – 289 s.
12. Yarochkin V.I. Bezopasnost' informacionny'x sistem, 1996. – M.: «Os-89». – 320 s
13. Azhmuxamedov I.M. Reshenie zadach obespecheniya IB na osnove sistemnogo analiza i nechyotkogo kognitivnogo modelirovaniya: monografiya, 2012. – Astraxan', 2012. – 344 s.
14. GOST R 51275-2006 Zashhita informacii. Ob''ekt informatizacii. Faktory', vozdejstvuyushhie na informaciyu. Obshhie polozheniya. – M.: FATRM, 2007. – 6 s.
15. Statistika uyazvimostej sistem distancionnogo bankovskogo obsluzhivaniya. – M.: 2013. – 40 s. [E'lektronny'j resurs]. – URL: http://www.opennet.ru/opennews/art.shtml?num=28338; http://www.exploit-db.com/exploits/15024/.
16. Zheltov S.A. Obshhaya metodika prakticheskoj aprobacii vy'chislitel'ny'x sistem v otnoshenii riskov realizacii ugroz IB // Vestnik RGGU. Seriya «Informatika, zashhita informacii. Matematika». – № 11(133). – M.: RGGU, 2014. – S. 10-15
17. Tarasova N.A. Strukturizaciya organizacionny'x riskov v sistemax obespecheniya informacionnoj bezopasnosti predpriyatij // Vestnik RGGU. Seriya «Informatika, zashhita informacii. Matematika». – № 11(133). – M.: RGGU, 2014. – S. 15-25
18. Yasenev V.N. IB v e'konomicheskix sistemax: uchebnoe posobie. – N. Novgorod: Izdatel'stvo NNGU, 2006. – 253 s.
19. Chereshkin D.S. i dr. Metodika ocenki riskov narusheniya informacionnoj bezopasnosti v avtomatizirovanny'x informacionny'x sistemax / D.S. Chereshkin, A.A. Kononov, E.G. Novickij. V.N. Cygichko; Institut sistem analiza RAN. – M.: ISA RAN, 1999
20. Yarochkin V.I. Informacionnaya bezopasnost': uchebnik dlya studentov VUZov. – M.: Gaudeamus, 2004. – 2 izd.
21. Gladkix A.A., Dement'ev V.E. Bazovy'e principy' informacionnoj bezopasnosti vy'chislitel'ny'x setej: uchebnoe posobie dlya studentov, obuchayushhixsya po special'nostyam 08050565, 21040665, 22050165, 23040165. – Ul'yanovsk: UlGTU, 2009. – 156 s.
22. Vojtik A.I., Prozherin V.G. E'konomika informacionnoj bezopasnosti: uchebnoe posobie. – SPb.: NIU ITMO, 2012. – 120 s.
23. Informacionnaya bezopasnost': e'konomicheskie aspekty'. Informacionny'j byulleten' № 10 (125)/2003. – M: Jet Info, 2003. – S. 1-23.
24. Analiz ugroz informacionnoj bezopasnosti. – Tambov: TGTU, 2007. – 10 s. [E'lektronny'j resurs]. – URL: http://www.studfiles.ru/preview/4518611/page:2/.
25. Metody' i sredstva zashhity' komp'yuternoj informacii [E'lektronny'j resurs]. – URL: http://country-expert.narod.ru/index.html.
26. Klassifikaciya ugroz informacionnoj bezopasnosti [E'lektronny'j resurs]. – URL: http://country-expert.narod.ru/pages/3.htm.
27. Vixorev S.V. Klassifikaciya ugroz informacionnoj bezopasnosti. – M.: OAO «E'lvis Plyus», 1998 [E'lektronny'j resurs]. – URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?print.
28. Xorin V.V. Voprosy' sozdaniya metodologii sistemy' zashhity' informacii v ASU // Sb. NTP i informaciya, 1993. – № 3. – M.: VNIIMI. – S. 23-32.
29. Fisun A.P. Modelirovanie i ocenka ugroz informacionnoj bezopasnosti. Sbornik materialov 8-j Mezhdunarodnoj konferencii «Informatizaciya pravooxranitel'ny'x sistem» (MFI-99), 1999. – Chast' 2. – M.: Akademiya MVD RF.

30. Fisun A.P., Lebedev V.N. Opredelenie i klassifikaciya ugroz bezopasnosti informacionno-vychislitel'ny'x setej // Trudy' Akademii upravleniya MVD Rossii «Komp'yuterny'e texnologii i upravlenie OVD», 2000. – M.: Akademiya upravleniya MVD RF. – S. 67-78.
31. Fisun A.P., Minaev V.A., i dr. Teoreticheskie osnovy' informatiki i informacionnaya bezopasnost': monografiya. – M.: Radio i svyaz', 2000. – 466 s.
32. Fisun A.P. Teoreticheskie osnovy' informacionnoj bezopasnosti informacionny'x telekommunikacionny'x sistem; dissertaciya doktora texnicheskix nauk. – M.: CNIIRE'S, 2000. – 468 s.
33. Fisun R.A. Modelirovanie ugroz informacionnoj bezopasnosti informacionno-telekommunikacionny'x sistem. Diplomnyj proekt, 2003. – Orel, Akademiya FAPSI.
34. Fisun A.P. i dr. Modelirovanie ugroz informacionnoj bezopasnosti cheloveko-komp'yuterny'x sistem / A.P. Fisun, K.A. Dzhevaga, R.A. Fisun, L.A. Grashhenko // Sbornik materialov 2-j Vserossijskoj NPK «Metody' i sredstva texnicheskoj zashhity' konfidencial'noj informacii», 7-9 iyunya 2005 goda. – Obninsk: GOU GCIPK.
35. Fisun A.P. Povy'shenie e'ffektivnosti polevoj seti pravitel'stvennoj svyazi na osnove ispol'zovaniya metodov matematicheskogo modelirovaniya; dissertaciya kandidata texnicheskix nauk. – M.: Akademiya MVD, 1992.
36. Makarov B.E., Fisun A.P. Postanovka zadachi klassifikacii i ocenki ugroz informacionnoj bezopasnosti informacionny'x sistem // Sbornik nauchny'x trudov ucheny'x Orlovskoj oblasti, 1999. – Vestnik nauki. – Vy'pusk 5. – V 2-x tomax. – T. 1 – Orel: Orel GTU. – S. 24-27.
37. Zhambyu M. Ierarxicheskij klaster-analiz i sootvetstviya. – M.: Finansy' i statistika, 1988. – 342 s.
38. Lejbkind A.R., Rudnik B.L., Tixomirov A.A. Matematicheskie metody' i modeli formirovaniya organizacionny'x struktur upravleniya. – M.: MGU, 1982. – 232 s.
39. Mandel' I.D. Klasterny'j analiz; predislovie B.G. Mirkina. – M.: Finansy' i statistika, 1988. – 176 s.
40. Mnogokriterial'ny'e zadachi prinyatiya reshenij; pod red. D.M. Gvy'shiani, S.V. Emel'yanova. – M.: Mashinostroenie, 1978. – 192 s.
41. Rozova S.S. Klassifikacionnaya problema v sovremennoj nauke. – Novosibirsk: Nauka, 1986. – 224 s.
42. Saati T. Prinyatie resheniya. Metod analiza ierarxij. – M.: Radio i svyaz', 1993. – 320 s.
43. E'kspertnye sistemy'. Principy' raboty' i primery': per. s angl.; pod red. R.Forsajta. – M.: Radio i svyaz', 1987. – 224 s.

ТРЕБОВАНИЯ
к оформлению статьи для опубликования в журнале
«Информационные системы и технологии»

ОБЩИЕ ТРЕБОВАНИЯ

Объем материала, предлагаемого к публикации, измеряется страницами текста на листах **формата А4** и содержит от **4 до 9 страниц**; все страницы рукописи должны иметь сплошную нумерацию.

В одном сборнике может быть опубликована только **одна** статья **одного** автора, включая соавторство.

Плата с аспирантов за публикацию рукописей не взимается.

Аннотации всех публикуемых материалов, ключевые слова, информация об авторах, списки литературы будут находиться в свободном доступе на сайте соответствующего журнала и на сайте Российской научной электронной библиотеки – РУНЭБ (Российский индекс научного цитирования).

ТРЕБОВАНИЯ К СОДЕРЖАНИЮ НАУЧНОЙ СТАТЬИ

Научная статья, предоставляемая в журналы, должна иметь следующие **обязательные** элементы:

- постановка проблемы или задачи в общем виде;
- анализ достижений и публикаций, в которых предлагается решение данной проблемы или задачи, на которые опирается автор, выделение научной новизны;
- исследовательская часть;
- обоснование полученных результатов;
- выводы по данному исследованию и перспективы дальнейшего развития данного направления;
- библиография.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ НАУЧНОЙ СТАТЬИ

Статья должна быть набрана шрифтом Times New Roman, размер 12 pt с одинарным интервалом, текст выравнивается по ширине; абзацный отступ – 1,25 см, правое поле – 2 см, левое поле – 2 см, поля внизу и вверху – 2 см.

Обязательные элементы:

- **УДК**
- **заглавие (на русском и английском языках)**
- **аннотация (на русском и английском языках)**
- **ключевые слова (на русском и английском языках)**
- **список литературы**, на которую автор ссылается в тексте статьи.

ТАБЛИЦЫ, РИСУНКИ, ФОРМУЛЫ

Все таблицы, рисунки и основные формулы, приведенные в тексте статьи, должны быть пронумерованы.

Формулы следует набирать в редакторе формул Microsoft Equation 3.0 с размерами: обычный шрифт – 12 pt, крупный индекс – 10 pt , мелкий индекс – 8 pt. **Формулы, внедренные как изображение, не допускаются!** Русские и греческие буквы, а также обозначения тригонометрических функций набираются прямым шрифтом, латинские буквы – *курсивом*.

Рисунки и другие иллюстрации (чертежи, графики, схемы, диаграммы, фотоснимки) следует располагать непосредственно после текста, в котором они упоминаются впервые. Рисунки, число которых должно быть логически оправданным, представляются в виде отдельных файлов в формате *.eps (Encapsulated PostScript) или TIF размером не менее 300 dpi.

СВЕДЕНИЯ ОБ АВТОРАХ

В конце статьи приводятся набранные 10 pt сведения об авторах в такой последовательности: фамилия, имя, отчество (полужирный шрифт); учреждение или организация, ученая степень, ученое звание, должность, адрес, телефон, электронная почта (обычный шрифт). Сведения об авторах также предоставляются отдельным файлом и обязательно дублируются на английском языке.