ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(29) / 2018

УЧРЕДИТЕЛИ

ФГБОУ ВПО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District Information security

ISSN 2225-5435

№ 3(29) / 2018

The journal « UrFR Newsletter. Information Security » is included in the List peer-reviewed scientific publications, in which should be published main scientific results of scientific dissertations degree of doctor and candidate of science

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

METHODS OF DATA ANALYSIS

ORGANIZATIONAL, TECHNICAL AND LEGAL PROTECTION OF INFORMATION

TOPICAL PROBLEMS OF CYBERSECURITY

THE PRACTICAL ASPECT

УДК 004.357

Вестник УрФО № 3(29) / 2018, с. 5–12

Асяев Г. Д., Антясов И. С.

DOI: 10.14529/SECUR180301

ИСПОЛЬЗОВАНИЕ УЛЬТРАЗВУКОВЫХ КОЛЕБАНИЙ ДЛЯ РЕАЛИЗАЦИИ ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

В статье рассмотрены физические основы образования технического канала утечки информации с применением ультразвуковых колебаний. Описана уязвимость, позволяющая обратить наушники в микрофон на программном уровне. Представлена атака типа «Дельфин». Исследована применимость данной уязвимости для скрытой передачи информации с помощью ультразвуковых колебаний. Рассмотрены основные сценарии реализации данной атаки и выявлены основные методы противодействия.

Ключевые слова: *защита информации, ультразвук, передача данных, отношение сигнал/шум.*

Asyaev G. D., Antyasov I. S.

USING ULTRASONIC VIBRATIONS TO IMPLEMENT A TECHNICAL INFORMATION LEAKAGE CHANNEL

The article discusses the physical basis for the formation of a technical information leakage channel using ultrasonic vibrations. Describes the vulnerability that allows the headphones turn into a microphone at the program level. Introduced attack type "Dolphin". The applicability of this vulnerability to hidden information transmission using ultrasonic vibrations is investigated. The main scenarios for the implementation of this attack are considered and the main methods of countering are identified.

Keywords: *information protection, ultrasound, data transmission, signal-to-noise ratio.*

В настоящее время существует большое многообразие возможных сценариев похищения данных с ПК. Установка антивирусного программного обеспечения, разграничение доступа, увеличение границ контролируемой зоны, отключение ПК от сети Интернет – вот неполный перечь мер, необходимый для защиты информации. Однако даже при выполнении вышеперечисленных критериев два размещённых рядом компьютера, которые имеют либо

встроенные динамики, либо микрофон образуют технический канал утечки информации.

В качестве объекта разведки в рассматриваемом ТКУИ выступает информация ограниченного распространения, обрабатываемой на СВТ (компьютер или ноутбук). Актуальной средой распространения в данном случае является только воздушная. В качестве технического акустического средства разведки выступает микрофон или наушники, которые подключены непосредственно к самому объекту разведки и вспомогательный ПК или ноутбук, находящийся в одном помещении с объектом разведки.

Основными задачами исследования являются:

• Рассмотреть атаку типа «Дельфин»;

• Определить возможные сценарии проведения рассматриваемой атаки;

• Определить эффективность применения рассматриваемой уязвимости для скрытой передачи информации с помощью ультразвуковых волн;

• Рассмотреть программную и техническую спецификацию функции «jack retasking» для расширения вариантов атаки;

• Определить методы противодействия данной уязвимости.

Исследователи по кибербезопасности из Чжэцзянского университета доказали, что с помощью ультразвуковых колебаний можно скрытно передавать команды системам с функцией голосового помощника. Данная атака получила название «Дельфин». Алгоритм работы системы представлен на рисунке 1. Злоумышленник преобразует стандартные команды, произнесённые человеком в ультразвук. Система распознавания речи реагирует на эти колебания и выполняет соответствующие команды. Так как ультразвуковые колебания не слышны человеческому уху, то атакующий ничего не услышит, что повышает опасность реализации данной атаки [1].

С помощью данной атаки можно заставить систему открыть вредоносный сайт, загрузить шпионскую программу, позвонить кому-либо, либо включить диктофон и отправлять голосовую информацию через Интернет.

Выделяют 2 типа систем голосовых помощников:

• те, которые зависят от голоса говорящего;

• те, которые не зависят от голоса говорящего.

Для реализации атаки в первом случае злоумышленникам требуется запись голоса владельца данной системы для активации. Впоследствии уже можно с помощью ультразвуковых команд, промодулированных человеческим голосом передавать команды для выполнения.

Для реализации атаки по втором случае достаточно сразу посылать системе команды с помощью ультразвука. Так как было доказано, что система понимает фразы для активации произнесённые на другой частоте (в ультразвуковом диапазоне). Данная атака работает в диапазоне 21000-40000 Гц, а максимальное расстояние между ультразвуковым излучателем и устройством, поддерживающим систему распознавания голоса, при котором удалось успешно реализовать вышеописанный алгоритм составило 2 метра.

Однако ультразвуковые колебания можно использовать не только для передачи команд голосовым помощником, но и для скрытой передачи данных. С помощью вредоносного программного обеспечения, которое может быть внедрено, например, внутренним нарушителем, можно настроить беспроводную передачу защищаемых сведений между двумя компьютерами посредством акустиче-

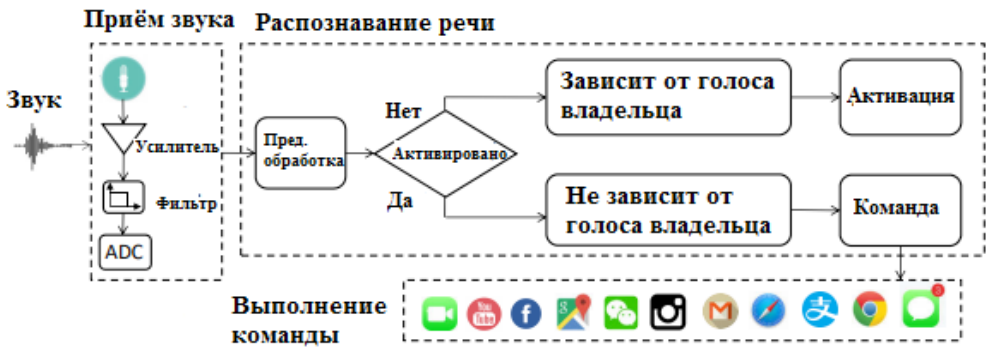


Рис. 1. Схема работы голосовых помощников

ских колебаний. В качестве акустических колебаний выступают ультразвуковые волны в диапазоне 17000-24000 Гц (данный диапазон частот выбран из функциональных возможностей динамиков и микрофонов). Так как ультразвук в большинстве случаев не способно воспринимать человеческое ухо, то рядовой пользователь никак не сможет на слух понять, что происходит утечка информации. Было проведено исследование в ходе которого происходила непрерывная запись в течение 5 часов всех шумов, циркулирующих в помещении, кроме того была открыта форточка откуда доносился индустриальный шум (рядом проходит оживлённая улица с большим количеством машин и людей).

Исходя из рисунка 2, видно, что речевая информация и индустриальные шумы, которые циркулируют в помещении, никаким образом не влияют на процесс записи и распознавания сигналов, которые ведутся при скрытой передачи с помощью ультразвуковых волн в силу отсутствия излучения в заданном диапазоне частот: 17000-20000 Гц, что повышает актуальность рассматриваемой угрозы.

Пусть в помещении имеются два компьютера (рис. 3). Компьютер А обрабатывает защищаемую информацию, оснащён внутренним динамиком и не имеет выход в Интернет. Компьютер В обрабатывает общедоступную информацию, оснащён микрофоном и имеет выход в сеть Интернет. С помощью заранее внедрённого вредоносного скрипта компьютер А преобразовывает информацию ограни-

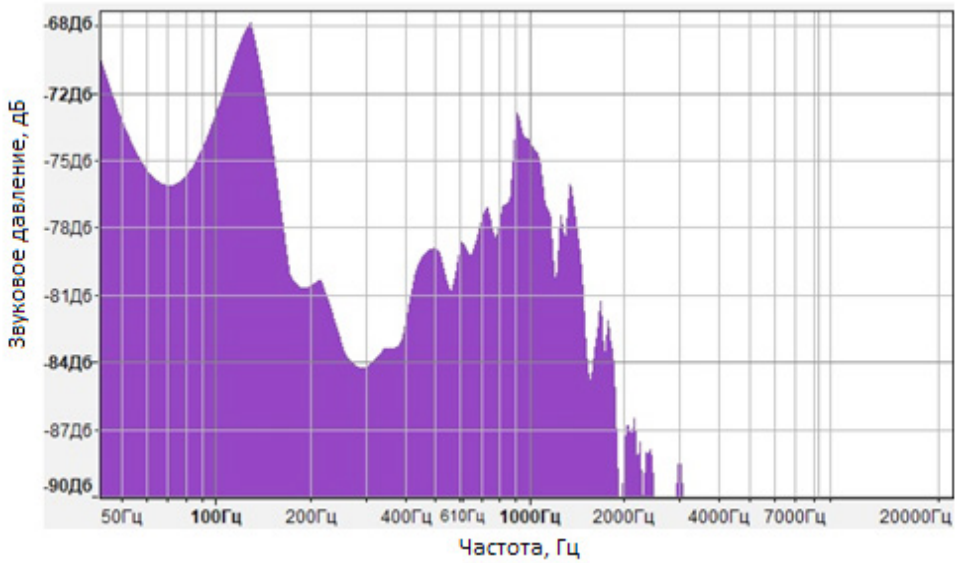


Рис. 2. АЧХ шума, циркулирующего в помещении в течении дня

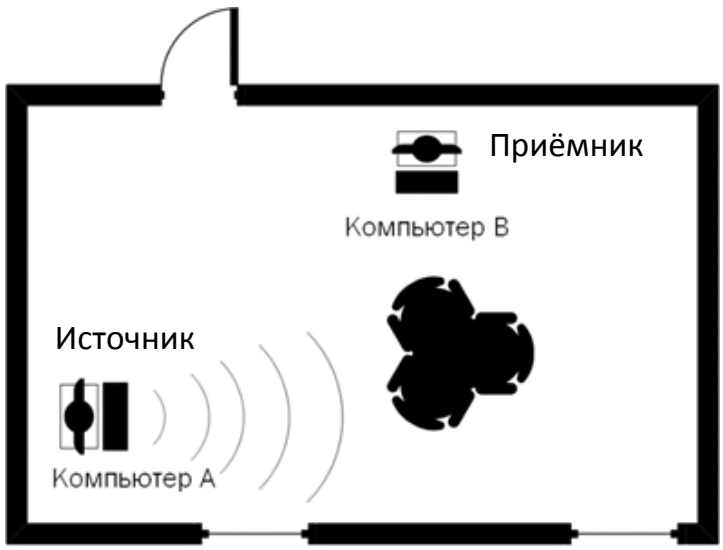
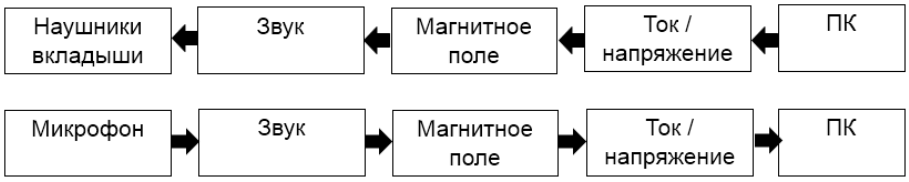


Рис. 3. Возможный сценарий атаки

ченного доступа в ультразвуковые колебания определённой частоты и излучает в эфир. Компьютер В с помощью микрофона прослушивает и записывает эфир в заданном диапазоне частот и, впоследствии, либо проводит демодуляцию полученных сигналов и получает исходные файлы, либо сразу передаёт данные в сеть Интернет.

Однако, принимать ультразвуковые колебания могут не только микрофоны, но и наушники. Стоит заметить, что микрофон и наушники на физическом уровне построены одинаково и отличаются лишь программной составляющей.



В чипах производителя звуковых карт Realtek есть функция под названием «jack retasking/ jack remapping», которая позволяет изменить функции/назначение порта на программном уровне. Эта особенность может использоваться в качестве реализации уязвимости для утечки речевой информации. Данное исследование было уже проведено автором в предыдущей статье. Злоумышленник может изменить назначение порта с выходного на входной без ведома пользователя и с помощью наушников записывать ультразвуковые колебания для последующей демодуляции и получения защищаемой информацией [2].

Существуют 4 возможных сценария реализации атаки. Исходные данные для всех ситуаций одинаковые:

• Имеется заражённый ПК, на котором обрабатывается защищаемая информация.

• Динамики (встроенные или переносные) излучают ультразвуковые колебания определённой частоты, формирующиеся путём перевода локальных файлов в неслышимый для человеческого уха сигнал.

1. Воздействие данного сигнала на ограждающие конструкции (окна), приводит к возникновению вибрационных колебаний промодулированных информативным сигналом. С помощью технических средств разведки возможна регистрация колебаний и дальнейшая расшифровка. Тем самым реализуется оптоэлектронный канал утечки информации.

2. В помещении имеется ещё один компьютер с подключённым к входному аудиогнезду микрофоном. С помощью данного записывающего устройства происходит регистрация акустических волн в заданном диапазоне частот, и отправка в сеть Интернет.

3. В помещении имеется ещё один компьютер с подключёнными к выходному аудиогнезду динамиками или наушниками. С помощью функции jack retasking злоумышленник переназначает выходной порт во входной выполняет все те же действия как в п. 2.

4. В помещении может находиться электронное устройство негласного получения информации, которое прослушивает эфир и при наличии акустических волн в заданном диапазоне частот записывает и отправляет данные по радиоканалу [3].

Для экспериментального исследования рассмотренной уязвимости были сгенерированы колебания с частотой 19000 Гц, которые излучались через встроенные динамики ноутбука HP 250 G6. Уровень громкости был выставлен на максимальный (64 дБ). Данные излучения были записаны на различном расстоянии с помощью стандартного средства звукозаписи Windows. В ходе проведения эксперимента в качестве приемной части ультразвуковых колебаний было исследовано звуковое оборудование, представленное в табл. 1.

Таблица 1

Экспериментальное оборудование

	Микрофон	**Наушники-вкладыши**	**Накладные наушники**
Название	OKLICK MP-M009B	PHILIPS SHE3550BK	PHILIPS SHL5000/00
Диапазон	50 – 23000 Гц	20 – 19000 Гц	9 – 24000 Гц
Чувствительность	58 дБ	95 дБ	104 дБ
Импеданс	—	32 Ом	24 Ом

Основными задачами исследования является определение применимости на практике данной уязвимости, а также определение максимальной дальности скрытой передачи информации при помощи ультразвуковых волн.

стотная характеристика ультразвукового сигнала записанного с помощью микрофона на расстоянии 1 метр.

Исходя из представленной выше таблицы видно, что данный канал утечки информации является актуальным и применимым на практике.

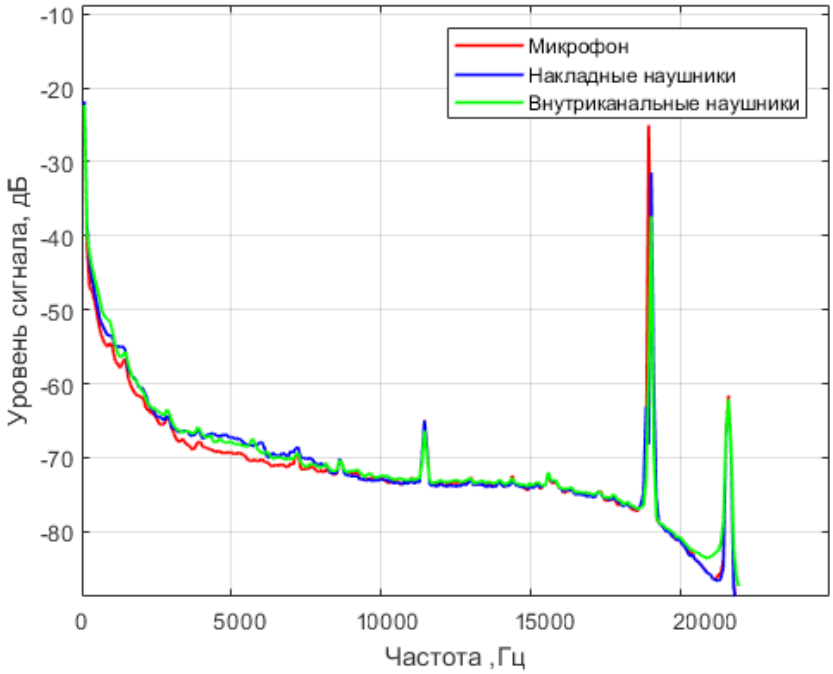


Рис. 4. Средний уровень сигнала на расстоянии 1 метр при записи через микрофон, накладные наушники, наушники-вкладыши

Исходя из рисунка 4, можно заметить, что более высоким качеством записи обладают накладные наушники по сравнению с наушниками-вкладышами. Разница в уровне сигнала от накладных наушников по сравнению с микрофоном составляет всего около 6 дБ. На рисунке 5 представлена амплитудно-ча-

Важным параметром при передаче различных сообщений является шаг частоты. Чем меньше этот шаг, тем больший объём информации можно будет передать. Стоит отметить, что при увеличении расстояния передачи увеличивается погрешность передачи частоты (рис. 6).

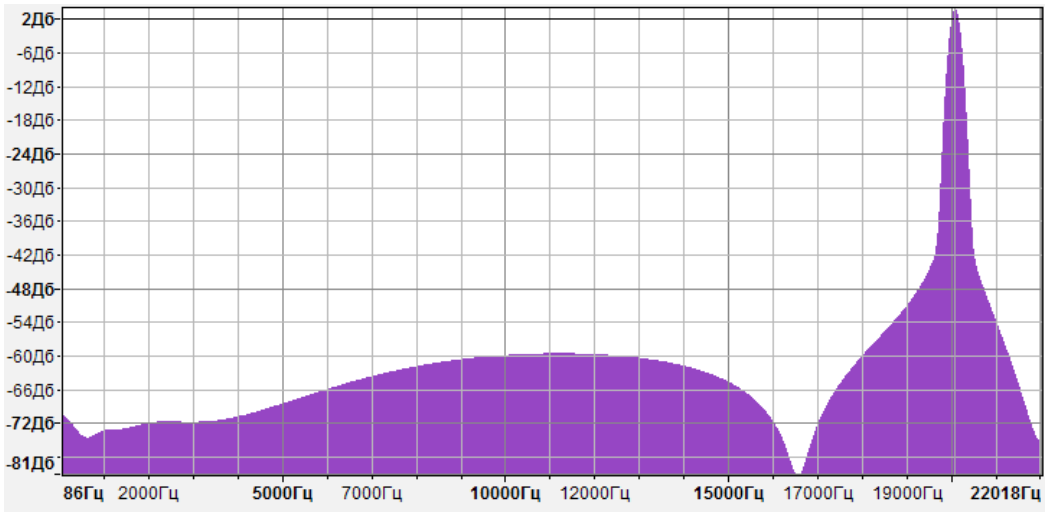


Рис. 5. АЧХ ультразвукового сигнала, сгенерированного на частоте 20200 Гц, записанная с помощью микрофона

Таблица 2

Зависимость расстояния от уровня сигнала

	Микрофон	Накладные наушники	Наушники вкладыши
1 метр	-25 дБ	-31 дБ	-38 дБ
3 метра	-30 дБ	-38 дБ	-46 дБ
5 метров	-40 дБ	-50 дБ	-68 дБ

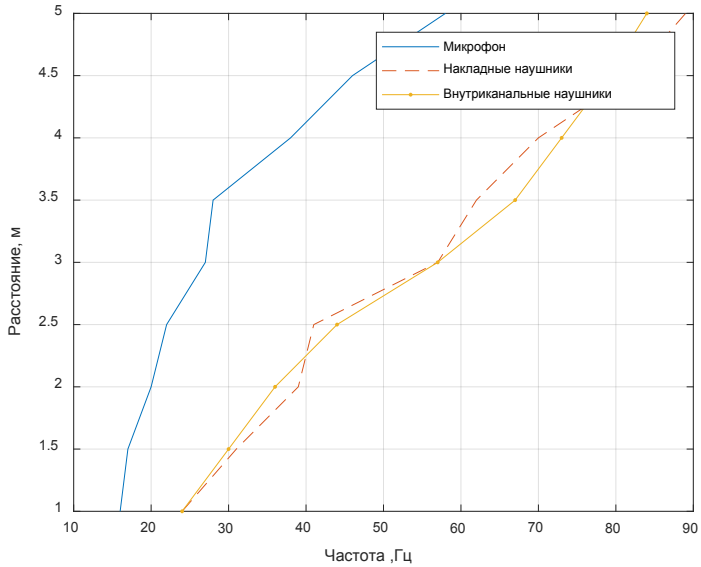


Рис. 6. Зависимость расстояния передачи от погрешности передачи частоты

Так при передаче ультразвуковых колебаний на расстоянии 1 метр средняя погрешность для микрофона составила ± 16 Гц, на расстоянии 3 метра ± 27 Гц, на расстоянии 5 метров ± 58 Гц. Экспериментальным путём было выявлено, что оптимальным шагом частоты, при котором достигается уверенное распознавание сигналов является 150 Гц. Данное числовое значение обеспечивает формирование полноценного алфавита. Таким образом, описанный технический канал утечки информации «Дельфин» является актуальным для большинства типовых офисных ситуаций, а вышеприведённые исследования доказали эффективность его реализации на практике.

Для противодействия данной атаке можно выделить 4 метода защиты:

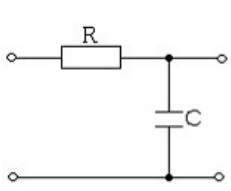
1. *Технический.* Доработка системы, регистрирующей акустические колебания, интегрирующей цепочкой, которая выполняет роль фильтра низких частот [4]. Следует ограничивать частотный диапазон до 20000 Гц.

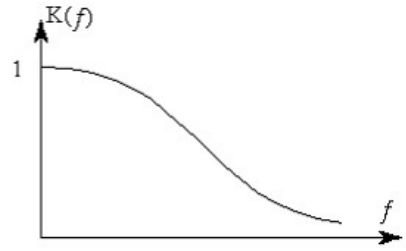
Рассчитаем значения сопротивления и ёмкости, при которых обеспечивается частота среза 20000 Гц. В качестве общего сопротивления возьмём 5 кОм. Входное напряжение = 1 В, а выходное = 0,7 В.

1) Определим входное напряжение Xc= $\frac{U_{вых} * R_{общ}}{U_{вх}} = \frac{0{,}7 * 5000}{1} = 3500$ Ом;

2) Определим сопротивление резистора *R=Робщ-Xc=5000-3500=1500 Ом;*

3) Определим ёмкость конденсатора: $X_c = \frac{1}{2\pi f c}$. Выразим ёмкость $C = \frac{1}{2\pi f X_c} = \frac{1}{2*3.14*20000*3500} = 2.23$ нФ;





4)Проверим частоту среза:

$$F_{ср} = \frac{1}{2\pi X_C C} = \frac{1}{2*3.14*3500*2.23*10^{-9}} \approx 20000 \text{ Гц}$$

Таким образом для построения фильтра низких частот, который будет ограничивать все частоты выше 20000 Гц, следует применить резистор сопротивлением 1.5 кОм (например, CF-50), а конденсатор ёмкостью 0.22 мкФ (например, К10-17А Н50). Данные значения конденсатора и резистора являются достаточно распространёнными и доступными в продаже, что повышает практическую реализацию данного метода.

2. *Организационный.* Запрет в организациях использования наушников, микрофонов, а также динамиков без предусилителей [5]. Во избежание переназначения портов, следует извлекать наушники из аудиогнезда, когда они не используются по назначению. Данный метод является одним из самых эффективных и наименее затратным.

3. *Программный.* Отключение звукового оборудования в настройках BIOS. Это может предотвратить вредоносный доступ аудиокодека из операционной системы. Однако, использование данной конфигурации является приемлемым методом только для организаций, так как отключение звукового оборудования ведёт к невозможности прослушивания аудиозаписи и ведения конференц-переговоров. Использование сертифицированных средств защиты информации от несанкционированного доступа [5].

4. *Использование ультразвукового подавителя в помещении.* Достоинством является бесшумный режим работы, не влияющий на психологическое состояние человека, однако данный метод является самым финансово затратным.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Catalin Cimpanu., Hackers can use ultrasounds to take control of Alexa, Siri, Cortana, others, [Электронный ресурс] // https://www.bleepingcomputer.com/news/security/hackers-can-use-ultrasounds-to-take-control-of-alexa-siri-cortana-others/. (Дата обращения 15.08.2018).

2. Asyaev G.D., Antyasov I.S. Using headphones to implement a technical channel for the leakage of voice information // 2018 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) / 2018, P. 229-232.

3. Макаров Ю.К., Хорев А.А. Методы защиты речевой информаци и оценки их эффективности // Защита информации. – Конфидент.: 2001. - № 4, С. 22-33.

4. Сапожков М.А. Акустика // Справочник. – М.: Радио и связь 1998. – С. 186-192.

5. Фучко М.М., Широких А.В., Захаров А.А., Несговоров Е.С., Оленников Е.А. Аудиовыход как скрытый канал утечки данных: технологии создания и методы защиты //Вестник УрФО. Безопасность в информационной сфере. – Челябинск: Изд. Центр ЮУрГУ, 2016. - № 3(21) С. 26-30.

References

1. Catalin Cimpanu., Hackers can use ultrasounds to take control of Alexa, Siri, Cortana, others, [Elektronnyy resurs] // https://www.bleepingcomputer.com/news/security/hackers-can-use-ultrasounds-to-take-control-of-alexa-siri-cortana-others/. (Data obrashcheniya 15.08.2018).

2. Asyaev G.D., Antyasov I.S. Using headphones to implement a technical channel for the leakage of voice information // 2018 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) / 2018, P. 229-232.

3. Makarov YU.K., Khorev A.A. Metody zashchity rechevoy informatsi i otsenki ikh effektivnosti // Zashchita informatsii. – Konfident.: 2001. - № 4, S. 22-33.

4. Sapozhkov M.A. Akustika // Spravochnik. – M.: Radio i svyaz' 1998. – S. 186-192.

5. Fuchko M.M., Shirokikh A.V., Zakharov A.A., Nesgovorov Ye.S., Olennikov Ye.A. Audiovykhod kak skrytyy kanal utechki dannykh: tekhnologii sozdaniya i metody zashchity //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – Chelyabinsk: Izd. Tsentr YUUrGU, 2016. - № 3(21) S. 26-30.

АСЯЕВ Григорий Дмитриевич, студент высшей школы электроники и компьютерных наук кафедры "Защита информации" Южно-Уральского Государственного Университета. Россия, 454080, г.Челябинск, проспект Ленина, д.76. E-mail: asyaev1996@mail.ru

ASYAEV Grigoriy, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

АНТЯСОВ Иван Сергеевич, руководитель, старший преподаватель кафедры "Защита информации научный " Южно-Уральского Государственного Университета. Россия, 454080, г. Челябинск, проспект Ленина, д.76. E-mail: antiasovis@susu.ru.

ANTYASOV Ivan, research manager, senior teacher Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: antiasovis@susu.ru.

УДК 004.056 Вестник УрФО № 3(29) / 2018, с. 13–17

Баранкова И. И., Михайлова У. В., Лукьянов Г. И. DOI: 10.14529/SECUR180302

РАЗРАБОТКА ДОКУМЕНТИРУЮЩЕГО МОДУЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИБРОАКУСТИЧЕСКОГО КАНАЛА

В данной статье рассмотрены основные функции и возможности разработанного программного обеспечения для автоматизации процесса оценки защищенности виброакустического канала объекта исследования. Представлен реализованный модуль документирования исходной информации об объекте исследования и выдачи заключения по результатам аттестационных испытаний для разработанного программного обеспечения «ASL». Рассмотрен процесс формирования базы данных об объекте исследования с возможностью дальнейшей загрузки данных для упрощения проведения повторной оценки. Представлена процедура внесения данных контрольных точек измерения изоляционных свойств ограждающих конструкций для работы модуля оценки виброакустической защищенности. Разобрана процедура формирования готовой документации в формате pdf. Рассмотрены планируемые модернизации ПО «ASL» с целью повышения защищенности данных формируемой БД.

Ключевые слова: *ПО «ASL», оценка защищенности виброакустического канала, модуль документирования и протоколирования, загрузка и выгрузка данных, база данных, шифрование данных.*

Barankova I. I., Mikhailova U. V., Lukianov G. I.

DEVELOPMENT OF A DATA COLLECTION MODULE FOR AN OBJECT WHEN ANALYZING THE INFORMATION SECURITY OF A VIBRO-ACOUSTIC CHANNEL

This article describes the main functions and capabilities of the developed software to automate the process of assessing the security of the study object vibro-acoustic channel. An imple-

mented information documentation module for the developed ASL software has been presented. The process of forming a database of the study object with the possibility of further data downloads to simplify the re-evaluation. A procedure for entering data from control points for measuring the insulating properties of enclosing structures for the operation of the module for evaluating vibro-acoustic protection is presented. The procedure for the formation of finished documentation in pdf format has been analyzed. The planned upgrades of the ASL software were considered in order to improve the security of the data of the formed database.

Keywords: *«ASL» software, security vibroacoustic channel estimation, documentation and logging module, data loading and unloading, database, data encryption.*

Обработка подлежащей защите информации предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации. Аттестация выполняется в несколько этапов, каждый из которых включает в себя определенный перечень работ, связанных со спецификой аттестуемых объектов: начиная от определения местоположения, технических характеристик объекта, и заканчивая проведением специальных исследований[1,2].

Для проведения аттестационных испытаний по требованиям безопасности информации от утечки по виброакустическому каналу на базе лабораторий кафедры информатики и информационной безопасности МГТУ им. Г.И. Носова разработан программный продукт «ASL» (рис.1). Разработанное ПО позволяет упростить процедуру аттестации и снизить затраты на приобретаемое оборудования организации проводящей аттестационные испытание[3,4]. Стоит отметить что ПО «ASL» может работать в режимах быстрого или точного сканирования. Отличие режимов заключает в наборе количества измерений для каждой октавной полосы. После проведения испытания в контрольной точке в любом режиме проводится анализ полученных данных с целью снижения ошибки полученных данных[5,6].

Для большей автоматизации процесса проведения аттестационных испытаний и анализа результатов экспертного обследования в программном обеспечении предусмотрен модуль формирования и ведения отчетной документации по проведенным испытаниям изоляционных свойств ограждающих конструкций.

На основе анализа требуемой документации для вынесения заключения по результатам аттестации, в разработанном модуле реализованы 3 пользовательских интерфейса. Первый - окно программы для сбора исходных данных по аттестуемому объекту (рис.2). Разработанный пользовательский интерфейс сбора исходных данных включает 4 раздела:

- общие данные (сведения об организации и АС);
- размещение (условия размещения аттестуемого объекта);

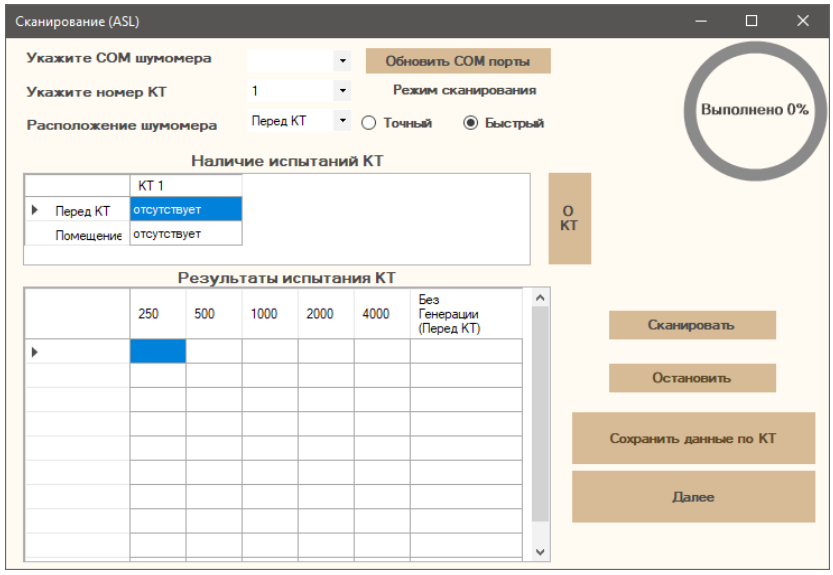


Рис.1. Пользовательский интерфейс ПО «ASL»

• документация (организационно-распорядительная и эксплуатационная документация);

• дополнительно (информация о руководителе организации и аттестационной комиссии).

пользуемых при аттестации. Стоит отметить, что добавленные КТ будут автоматически загружены в окно оценки ограждающих конструкций.

При разработке модуля ведения документации была реализована функция сохра-

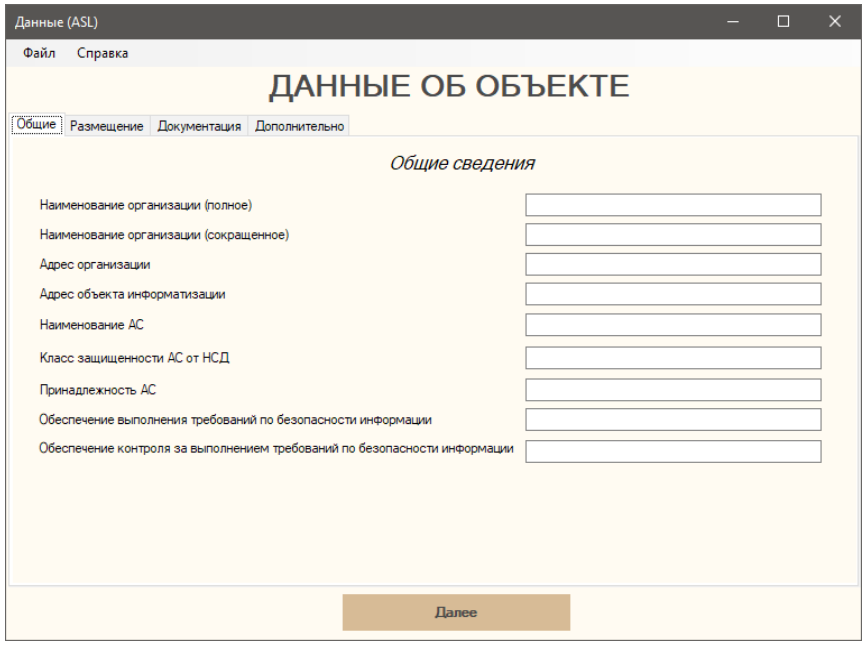


Рис.2. Пользовательский интерфейс сбора основных данных

После заполнения первого окна модуля пользователю предлагается второй пользовательский интерфейс (рис.3). Данный интерфейс служит для внесения данных о контрольных точках (КТ) и оборудовании, ис-

нения внесенных данных в формате *.pdf и дальнейшей печати, а также сохранения в формате *.ini для ведения БД аттестуемых объектов. Введение такой БД позволяет упростить процедуру внесения данных с помо-

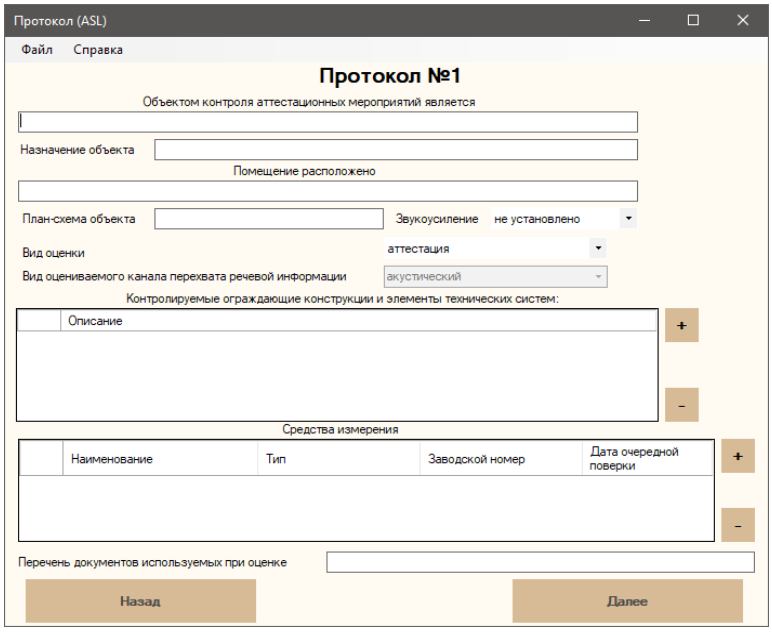


Рис.3. Пользовательский интерфейс ввода данных для испытаний КТ

щью функции загрузки данных. На рис.4 представлен интерфейс для сохранения и загрузки данных.

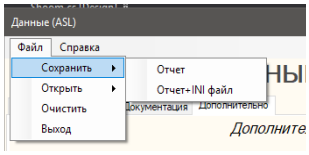


Рис.4. Интерфейс для сохранения БД и документа отчета

На рис. 5 представлен пример сформированного pdf документа включающего данные внесенные в окно сбора исходных данных. Для удобства восприятия данные представлены в табличном виде.

Общие сведения об объекте информатизации

Наименование	Содержание
Наименование организации (полное)	ФГБОУ ВО МГТУ им.Г.И. Носова
Наименование организации (сокращенное)	МГТУ им.Г.И. Носова
Адрес организации	Город Магнитогорск улица Калинина 40,
Адрес объекта информатизации	Город Магнитгорск улица Калинина 40, аудитория 2124
Наименование АС	Информационная система МГТУ Им.Носова
Класс защищенности АС от НСД	УЗ-2 К-1
Принадлежность АС	МГТУ им.Г.И. Носова
Обеспечение выполнения требований по безопасности информации	отсутствует
Обеспечение контроля за выполнением требований по безопасности информации	отсутствует

Условия размещения объекта информатизации

Наименование	Содержание
Место установки ОТСС	ауд.2124
Граница контролируемой зоны	По периметру здания
Смежные помещения и их функциональное назначение	Коридор,лестница,кабинет заведующего кафедрой
Выше этажом:	3 этаж
Ниже этажом:	1 этаж
Слева:	отсутствует
Справа:	отсутствует
Вход в помещение АС	Коридор
Расстояние от ОТСС до мест возможного размещения портативных средств разведки ПЭМИН	1 м
-возимых ВСР	10 м
-носимых НСР	5 м
Система охранно-пожарной сигнализации автоматизированной системы.	Пожарная сигнализация и охранная сигнализация
Система электропитания и заземления АС.	Центральная электросеть
Место нахождения трансформаторной подстанции относительно границ КЗ	За пределами
Наличие посторонних потребителей электроэнергии в пределах КЗ	Нет
Место нахождения заземлителей относительно границ КЗ	За пределами

Перечень организационно- распорядительной и эксплуатационной документации

Наименование	Содержание
Организационно - распорядительная документация	Положение о МГТУ им.Г.И. Носова
Схема контролируемой зоны	Представлена в приложении 1
Акт категорирования	Отсутствует
Акт классификации	Отсутствует
Описание технологического процесса обработки информации	Указано выше
Технический паспорт	Отсутствует
Другие документы:	Отсутствует
Эксплуатационная документация	Отсутствует
Сведения о спец. лабораторных проверках ТС импортного (совместного) производства	Отсутствует

1 / 2

Рис.5. Пример сформированного документа «Основные данные»

После проведения аттестационных испытаний ПО переходит в заключительный пользовательский интерфейс (рис.6) для анализа результатов аттестационных испытаний и выдачи заключения по результатам этих испытаний. Данное окно предоставляет возможность выполнить сохранение протокола и заключения отдельно. Однако при сохранении

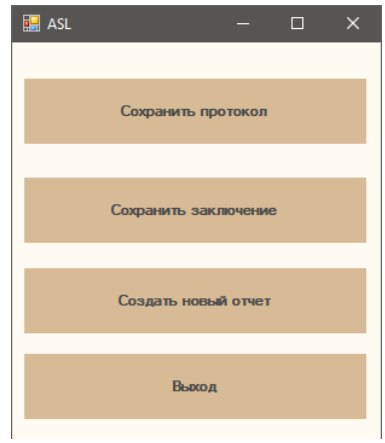


Рис 6. – Заключительный пользовательский интерфейс

заключения в него автоматически записывается протокол испытаний.

Использование внедренного модуля ведения документации позволит снизить затраты на ведении документации в процессе проведения аттестации. Однако ведение БД в открытом виде является не надежным. Поэтому дальнейшая модернизация ПО предполагает внедрение DES шифрования БД с использованием лицензионного ключа пользователя.

Заключение

Разработанное ПО «ASL» с добавлением модуля документирования данных оценки защищенности виброакустического канала утечки речевой информации помимо автоматизации процесса проведения испытаний позволит автоматизировать процедуру формирования отчетной документации и процесс выдачи заключения по результатам аттестационных испытаний. Кроме этого, благодаря ведению базы исходных данных об испытуемом объекте упрощается процедура заполнения данных для проведения повторных оценочных испытаний. Внедрение такого модуля позволит существенно сократить затраты человеко-часов на проведение аттестационных испытаний, что в свою очередь приведет к сокращению стоимости данных работ. Хранение результатов в незашифрованном виде снижает их безопасность, поэтому в дальнейшей модернизации ПО «ASL» планируется добавить шифрование БД и отчетной документации.

Литература

1. Михайлова У.В., Лукьянов Г.И. Защита информации в помещении от утечки по акустическому каналу // Актуальные проблемы современной науки, техники и образования Тезисы докладов 76-ой международной научно-технической конференции. 2018. С. 294.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Анализ методик оценки звукоизоляционных свойств ограждающий конструкций // Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 211-214.

3. Лукьянов Г.И., Михайлова У.В. Эффективность применения СЗИ от утечки по акустическим каналам // Вестник УрФО. Безопасность в информационной сфере. 2014. № 4 (14). С. 14-18.

4. Лукьянов Г.И., Михайлова У.В., Баранкова И.И., Коновалов М.В. Защита информации по виброакустическим каналам с использование СЗИ «СОНАТА» // Актуальные проблемы современной науки, техники и образования. 2015. Т. 2. С. 186-188.

5. Хусаинов А.А., Михайлова У.В. Особенности и проблемы, возникающие при разработке моделей угроз информационной безопасности // Безопасность информационного пространства. Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Научный редактор - Д.И. Дик. 2016. С. 72-75.

6. Коновалов М.В., Михайлова У.В., Хусаинов А.А., Санарбаев Р.Ж. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. - 2013. - Т. 2. - № 71. С. 159-161.

References

1. Mikhaylova U.V., Luk'yanov G.I. Zashchita informatsii v pomeshchenii ot utechki po akusticheskomu kanalu // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya Tezisy dokladov 76-oy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2018. S. 294.

2. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Analiz metodik otsenki zvukoizolyatsionnykh svoystv ograzhdayushchiy konstruktsiy // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2017. T. 1. S. 211-214.

3. Luk'yanov G.I., Mikhaylova U.V. Effektivnost' primeneniya SZI ot utechki po akusticheskim kanalam // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2014. № 4 (14). S. 14-18.

4. Luk'yanov G.I., Mikhaylova U.V., Barankova I.I., Konovalov M.V. Zashchita informatsii po vibroakusticheskim kanalam s ispol'zovaniye SZI «SONATA» // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2015. T. 2. S. 186-188.

5. Khusainov A.A., Mikhaylova U.V. Osobennosti i problemy, voznikayushchiye pri razrabotke modeley ugroz informatsionnoy bezopasnosti // Bezopasnost' informatsionnogo prostranstva. Sbornik materialov XV Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh. Nauchnyy redaktor - D.I. Dik. 2016. S. 72-75.

6. Konovalov M.V., Mikhaylova U.V., Khusainov A.A., Sanarbayev R.ZH. Algoritmy shifrovaniya dannykh // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. - 2013. - T. 2. - № 71. S. 159-161.

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой ИиИБ, МГТУ им. Г.И. Носова, 455000, г. Магнитогорск, пр. Ленина 38. E-mail: inna_barankova@mail.ru;

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры ИиИБ, МГТУ им. Г.И. Носова, 455000, г. Магнитогорск, пр. Ленина 38. E-mail: ylianapost@gmail.com;

ЛУКЬЯНОВ Георгий Игоревич, ст. преподаватель кафедры ИиИБ МГТУ им. Г.И. Носова, 455000, г. Магнитогорскпр. Ленина 38. E-mail: decorsi@mail.ru.

BARANKOVA Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc., Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru;

MIKHAILOVA Uliana, NMSTU, Ph.D., Associate Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com;

LUKIANOV Georgy, NMSTU, Assistant Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: decorsi@mail.ru.

УДК 004.934.2

Вестник УрФО № 3(29) / 2018, с. 18–22

Гаршина В. В., Степанцов В. А.

DOI: 10.14529/SECUR180303

ОНТОЛОГИЧЕСКИЙ ПОДХОД ДЛЯ АНАЛИЗА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье предлагается метод формирования комплекса мер по обеспечению безопасности корпоративных информационных систем на основе анализа рисков, проводимого с использованием онтологического подхода. Приводится анализ применения методов оценки уровня угроз в зависимости от анализируемой информации: источников, вида представления, объективности и надежности.

Ключевые слова: *онтология, анализ рисков, информационная безопасность, модель идентификации угроз STRIDE.*

Garshina V. V., Stepantsov V. A.

ONTOLOGICAL APPROACH FOR RISK ANALYSIS SECURITY OF INFORMATION SYSTEMS

The article proposes a method of forming a set of measures to ensure the security of corporate information systems based on a risk analysis carried out using an ontological approach. The analysis of the application of methods for assessing the level of risk is presented depending on the information analyzed: sources, type of representation, objectivity and reliability.

Keywords: *ontology, risk analysis, information security, STRIDE threat identification model.*

Одним из перспективных направлений в области формализации знаний и их эффективной компьютерной обработки, являются онтологии. Они представляют описание структурной спецификации предметной области, включающее словарь терминов этой области (концептов, понятий, классов), набор отношений между понятиями которые описывают, как эти термины соотносятся между собой и наборы функций интерпретации (аксиоматизация), на понятиях и/или отношениях [1].

Формально онтология определяется как

$$O = \langle X, R, F \rangle$$

где X – конечное непустое множество терминов (концептов, понятий, классов) предметной области, R – конечный набор отношений между понятиями; F – конечное множе-

ство функций интерпретации (аксиоматизация), на понятиях и/или отношениях.

Онтологии классифицируются по типам в зависимости от конкретной задачи:

Мета-онтологии (Top-level ontologies) – описывают наиболее общие понятия, которые не зависят от предметных областей.

Онтология предметной области (Domain-ontologies) – формальное описание предметной области, применяется для уточнения понятий, определённых в мета-онтологии и определяет общую терминологическую базу предметной области.

Онтология конкретной задачи (Task ontologies) – онтология, определяющая общую терминологическую базу, относящуюся к конкретной задаче.

Сетевые онтологии (Application ontologies) – часто используются для описания конечных результатов действий, выполняемых объектами предметной области или задачи.

В случае если набор *R* и множество *F* являются пустыми, то такая онтология представляет собой глоссарий. Если *R* состоит из единственного отношения типа «подкласс-класс», а *F* – пусто, то онтология представляет собой таксономию.

Рассмотрим возможность применения онтологического подхода для анализа рисков безопасности информационных систем. Для этого необходимо определить методологическую основу для проведения анализа рисков и разработать соответствующую онтологию, объединяющую онтологию предметной области и онтологию решения задачи определения методов и выбору технологий защиты.

Комплекс мер по обеспечению безопасности корпоративных информационных систем формируются на основе анализа рисков. Реальные риски являются интегральной оценкой способности имеющихся в наличии средств защиты эффективно противодействовать угрозам информационной безопасности. На практике принято использовать следующие группы методов оценки рисков безопасности:

1. Группа методов определяющих уровень риска с помощью оценки степени соответствия определенному набору требований по обеспечению информационной безопасности. Основаны на нормативно-правовых материалах организации; требованиях действующего законодательства РФ, руководящие документы ФСТЭК, СТР-К, требования ФСБ РФ, ГОСТы; рекомендации международных стандартов – ISO 17799, OCTAVE, CoBIT; рекомендации компаний-производителей программного и аппаратного обеспечения.

2. Методы оценки рисков информационной безопасности основываются на определении вероятности реализации атак, а также уровней их ущерба. Количественный показатель риска вычисляется отдельно для каждой атаки и в общем случае является произведением вероятности проведения атаки на величину возможного ущерба от этой атаки. Материальный и моральный ущерб определяется собственником информационной системы, а вероятность атаки вычисляется группой экспертов на основе процедуры аудита.

При использовании данных методов применяются как количественные, так и качественные шкалы на основе которых определяются величины риска информационной безопасности. В случае применения количественных шкал, вероятность реализации атаки выражается числом в интервале [0,1], а ущерб определяется денежным эквивалентом материальных и моральных потерь, которые может понести организация в случае успешного проведения атаки. В случае применения качественных шкал используются нечеткие смысловые уровни, причем каждому такому уровню ставится в соответствие определенный интервал количественной шкалы оценки. В зависимости от применяемых методик оценки рисков число уровней может быть различным.

Важнейшими задачами защиты данных в информационных системах являются:

1) обеспечение строго санкционированного доступа к данным (availability), 2) обеспечение конфиденциальности данных (confidentiality),

3) обеспечение целостности данных (integrity).

Мероприятия по предотвращению или снижению критичности угроз информационной системе реализуются на следующих этапах:

1) классификация угроз безопасности;

2) определение методов защиты;

3) выбор технологии защиты.

Реализация первого этапа может быть выполнена в соответствии с подходом фирмы Microsoft на основе модели идентификации угроз STRIDE (**S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) и мето-

дики DREAD (**D**amage potential, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability) для оценки рисков угроз [2].

В соответствии с моделью STRIDE осуществляется классификация угроз:

Spoofing identity (подмена сетевых объектов) – атаки подобного типа позволяют взломщику выдавать себя за другого пользователя путем воспроизведения транзакции, выполняющей аутентификацию пользователя, а также осуществлять подделку электронных сообщений и пакетов аутентификации.

Tampering with data (фальсификация данных) – несанкционированное изменение данных с целью атаки, в частности модификация аутентификационных файлов с целью добавления нового пользователя, подделка электронных сообщений, модификация данных, передаваемых по сети.

Repudiation (отказ от ответственности) – отсутствие фиксации в системных журналах действий, которые могут привести к нарушению безопасности, контрагент отказывается от совершенного им действия (или бездействия), пользуясь тем, что у другой стороны нет никакого способа доказать обратное.

Information disclosure (раскрытие информации) – несанкционированный доступ к конфиденциальной информации, публикация конфиденциальной информации.

Denial of service (отказ в обслуживании) – атаками такого типа взломщик пытается лишить доступа к сервису правомочных пользователей путем заполнения сети пакетами SYN и излишней загрузкой сетевых ресурсов фальшивыми пакетами ICMP.

Elevation of privilege (повышение привилегий) – несанкционированное присваивание прав системного администратора, присваивание прав администратора используя переполнение буфера, в результате чего непривилегированный пользователь получает привилегированный доступ, позволяющий ему взломать или даже уничтожить систему.

Для выбора методов защиты на втором этапе необходимо выполнить количественную оценку риска опасности для конкретной информационной системы по методике DREAD:

Damage potential (потенциальный ущерб) – мера реального ущерба от успешной атаки. Наивысшая степень опасности равная 10 означает практически беспрепятственный взлом средств защиты и выполнение практически любых операций.

Reproducibility (воспроизводимость) – мера возможности реализации опасности. Некоторые бреши доступны постоянно, при этом оценка равна 10, другие – только в зависимости от ситуации, их доступность не предсказуема.

Exploitability (подверженность взлому) – мера усилий и квалификации, необходимых для атаки. В случае, если атаку может реализовать пользователь невысокой квалификации с домашнего компьютера – оценка опасности 10. Если же для ее проведения надо потратить 100 000 000 долларов, оценка опасности – 1. Атака, для которой можно написать алгоритм и распространить в виде сценария среди непрофессионалов, также оценивается в 10 баллов.

Affected users (группы пользователей, попадающих под удар) – доля пользователей, работа которых нарушается из-за успешной атаки. Оценка выполняется на основе процентной доли, если нарушается работа 100 % пользователей, то оценка 10, а 10 % – 1 балл.

Discoverability (возможность раскрытия атаки) – в силу того, что любая опасность поддается реализации, то практически всегда оценивается в 10 баллов.

Суммарное значение риска рассчитывается по следующей формуле

$$Risk - DREAD = (DMG + R + E + AU + D)/5$$

где DMG – Damage, R – Reproducibility, E – Exploitability, AU – Affected users и D – Discoverability.

Оценка рисков является главной целью в процессе управления информационными системами. Для минимизации уровня рисков требуется анализировать риски информационной безопасности и на основе этого анализа принимать эффективные решения по определению методов и выбору технологий защиты.

Разработка онтологии анализа рисков проводилась в специализированном онтологическом редакторе Protégé, предназначенном для создания онтологий различных предметных областей. Protégé позволяет проектировать онтологии, раскрывая иерархическую структуру классов и проводить тестирование правильности структуры и системы выводов по онтологии. Этот инструмент поддерживает язык OWL (Web Ontology Language), позволяет генерировать HTML-документы, которые отражают структуру онтологии. OWL онтология содержит описания классов, их характеристики и связи. Исполь-

зуя формальную семантику OWL и указанные данные, возможно получение информации, которая не была явно описана в онтологии, но следует из семантики данных [3].

При проектировании классов онтологии были разработаны: Абстрактный класс *Атака*, содержащий все классы предметной области и задачи анализа рисков, представляет собой верхний уровень онтологии. Набор требований безопасности к информационной системе содержится в классе *Требования безопасности*, его атрибутами являются атрибуты обеспечения строго санкционированного доступа (availability), обеспечения конфиденциальности (confidentiality) и целостности данных (integrity) со своими приоритетами. Набор подклассов модели идентификации атак STRIDE включается в класс *Типы атак*. Класс *Анализ риска* содержит набор подклассов методики DREAD.

На основе поступающих сведений о ситуации угрозы, в онтологии генерируется экземпляры классов, свойства классов получают значения и на основе структурных и семантических отношений, описанных в онтологии строиться логический вывод об уровне риска и, соответственно, выборе методов и технологий защиты.

Заключение о безопасности анализируемой системы строится на основе разработанных и размещенных в онтологии правил. Для задания собственных правил логических выводов используется стандарт SWRL. Каждое правило состоит из двух частей – условия и вывода, который формируется, если условие выполнено. И условие, и вывод могут состоять из нескольких атомов – элементарных логических выражений. Каждый атом представляет собой предикат – утверждение о каких-либо объектах онтологии. Правила SWRL позволяют создавать гибкие условия для получения новых знаний. На основе таких правил строится вывод о защищенности системы.

Механизмы логического вывода обеспечивают вычисление значений логических выражений, оценку правильности модели, позволяют автоматически помещать в онтологию новую информацию в соответствии с правилами, оперировать именами классов, свойств и сущностей, и «задавать модели вопросы», абстрагируя пользователя от подробностей внутреннего строения модели.

Стандарт языка SPARQL [4] описывает синтаксис запросов к онтологическим моделям (является аналогом языка SQL). Применяется преимущественно для выборки необходимых данных с помощью SELECT-запросов с возможной их фильтрацией и сортировкой. SPARQL поддерживает вопросы, требующие однозначных ответов да или нет, сортировку, фильтрацию, сопоставление строк.

В целях информационной безопасности всегда требуется анализировать риски и принимать эффективные решения по определению методов и выбору технологий защиты. Предлагаемый онтологический подход позволит эффективно использовать полученные знаний для решения задачи комплексного анализа рисков безопасности информационных систем.

Литература

1. Semantic Web / [Электронный ресурс]. – Режим доступа: https://elite.polito.it/teaching/past-courses/360-01rrdiu-semantic-web, свободный (дата обращения 09.06.2018).

2. Ховард М., Лебланк Д. Защищенный код: Пер. с англ, – 2-е изд., испр. М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 с.

3. A. Herzog, N. Shahmehri, C. Duma, An Ontology of Information Security, International Journal of Information Security and Privacy, 1(4):1-23, 2007.

4. Стандарты W3C Консорциума / [Электронный ресурс]. – Режим доступа: https://www.w3.org/ , свободный (дата обращения 09.06.2018).

Refereces

1. Semantic Web / [EHlektronnyj recurs]. – Rezhim dostupa: https://elite.polito.it/teaching/past-courses/360-01rrdiu-semantic-web, svobodnyj (data obrashcheniya 09.06.2018).

2. K. Hovard M., Leblank D. Zashhishhennyj kod: Per. s angl, – 2-e izd., ispr. M.: Izdatel'sko-torgovyj dom «Russkaya Redaktsiya», 2004. – 704 s.

3. A. Herzog, N. Shahmehri, C. Duma, An Ontology of Information Security, International Journal of Information Security and Privacy, 1(4):1-23, 2007.

4. Стандарты W3C Консорциума / [EHlektronnyj recurs]. – Rezhim dostupa: https://www.w3.org/ , svobodnyj (data obrashcheniya 09.06.2018).

ГАРШИНА Вероника Викторовна, кандидат технических наук, доцент, доцент кафедры технологий обработки и защиты информации, федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет», Россия, 394018, г. Воронеж, Университетская пл., 1. E-mail: garshina@cs.vsu.ru.

СТЕПАНЦОВ Вячеслав Алексеевич, кандидат технических наук, доцент, доцент кафедры технологий обработки и защиты информации, федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет», Россия, 394018, г. Воронеж, Университетская пл., 1. E-mail: mrstep@yandex.ru

VERONIKA Garshina, Candidate of Engineering Science, Docent, Department of Processing Technology and Information Security in Voronezh State University. 1 Universitetskaya pl., Voronezh, 394018, Russia. E-mail: garshina@cs.vsu.ru

VYACHESLAV Stepantsov, Candidate of Engineering Science, Docent, Department of Processing Technology and Information Security in Voronezh State University. 1 Universitetskaya pl., Voronezh, 394018, Russia. E-mail: mrstep@yandex.ru

УДК 004.04 Вестник УрФО № 3(29) / 2018, с. 23–28

Гончаренко Ю. Ю., Паво Ф. Н.

DOI: 10.14529/SECUR180304

РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОГО ПРИЛОЖЕНИЯ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВОЙ ИДЕНТИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

В данной работе были проанализированы виды архитектур систем, выявлены их преимущества и недостатки. Приведены аргументы в пользу децентрализованных систем и способы достижения децентрализации. Одним из выявленных эффективных методов децентрализации является цепочка блоков – блокчейн. В работе был произведен анализ свойств и структуры блокчейна, исследованы методы обеспечения безопасности и достижения консенсуса между участниками сети. Рассмотрены преимущества децентрализованных приложений в сравнении с традиционными централизованными. Проанализированы популярные платформы для разработки децентрализованных приложений и выявлена наиболее оптимальная платформа для реализации приложения. Рассмотрены основные функции умного контракта Ethereum и методы взаимодействия с блокчейн-сетью средствами программного кода. Были исследованы популярные приложения на технологии блокчейн и направления их применения. В отличии от подобных статей с исследованием технологии блокчейн, в данной работе был представлен вариант реализации собственного приложения с использованием блокчейн платформы Ethereum. Разработанное приложение позволяет производить регистрацию и авторизацию пользователя. В данной работе были описаны основные функции и интерфейс приложения. Также его можно использовать как модуль для более сложных систем. Например, в системах голосования, контрольно-пропускных пунктов и других, где требуется идентификация пользователя и надежное хранилище учетных данных.

Ключевые слова: *блокчейн, децентрализации, Ethereum, идентификация, авторизация, умный контракт, приложений, цифровая подпись, QR-код.*

DEVELOPMENT OF A DECENTRALIZED APPLICATION FOR THE IMPLEMENTATION OF DIGITAL IDENTITY USING BLOCKCHAIN TECHNOLOGY

In this paper, the types of system architectures were analyzed, their advantages and disadvantages were revealed. The arguments in favor of decentralized systems and ways to achieve decentralization are presented. One of the effective methods of decentralization identified is the chain of blocks - block. In this work, the analysis of the properties and structure of the block was carried out, methods of ensuring security and achieving consensus between the participants of the network were explored. The advantages of decentralized applications are compared with traditional centralized ones. Analyzed popular platforms for the development of decentralized applications and identified the most optimal platform for implementing the application. The main functions of the smart contract Ethereum and the methods of interaction with the blockchain network by means of program code are considered. Popular applications on the technology of blockades and the direction of their application were investigated. Unlike similar articles with research on blockchain technology, in this paper we presented an implementation version of our own application using the Ethereum platform block. The developed application allows you to register and authorize the user. In this paper, the main functions and interface of the application were described. It can also be used as a module for more complex systems. For example, in voting systems, checkpoints and others, where you need to identify the user and a reliable store of credentials.

Keywords: *blocking, decentralization, Ethereum, identification, authorization, smart contract, applications, digital signature, QR code.*

В наше время, с ростом вычислительных мощностей открываются новые возможности и способы построения приложений. Растет и количество ценной информации, обрабатываемой приложениями. Появляется необходимость использовать новые, более защищенные системы для обработки и сохранения целостности данных.

Еще недавно, такая технология как Интернет в корне изменила подход к созданию программного обеспечения, заменив полностью клиентские приложения клиент-серверными. Теперь же, клиент-серверные приложения постепенно вытесняются децентрализованными. Централизованная архитектура имеет свои недостатки и проблемы безопасности. Децентрализованные приложения на основе технологии Блокчейн позволяют избавиться от посредников, обеспечить отказоустойчивость и предотвратить потерю или порчу данных.

Таким образом, выделяют три основных архитектуры систем: централизованная, распределенная децентрализованная [4]. В наше время наибольшей популярностью пользуются централизованные приложения. С появлением сети Интернет практически все приложения используют централизованную архитектуру.

Централизованные системы предполагают единый центр обработки и хранения данных – сервер. На стороне сервера, как правило, обрабатываются пользовательские данные и критически важные операции. Например, авторизация пользователя, хранение и

обработка его персональных данных, или различные финансовые транзакции.

Данный подход является наиболее распространенный и экономически выгодный в наше время. Существует, как правило, одна точка отказа которую несложно поддерживать и масштабировать. Но централизованные системы требуют от пользователя полного доверия, так как работают по принципу «черного ящика» и только владельцу сервиса известно, как именно обрабатываются пользовательские данные и не передаются ли они третьим лицам. Также подобные системы имеют множество уязвимостей и злоумышленник, получивший доступ к единому центру, получает контроль над всеми данными пользователей.

Децентрализованная архитектура подразумевает исключение центрального узла и равномерное распределение полномочий между всеми участниками сети. Подобные сети также называют одноранговыми или пиринговыми, где каждый узел выполняет роль сервера и клиента и функционирует независимо от других узлов. Данная структура позволяет сети продолжать работу даже при отключении или выходе из строя одного из узлов и обеспечивает масштабируемость сети в целом. Одной из важнейших характеристик децентрализованной архитектуры является полная открытость и прозрачность ее работы, что предотвращает различные скрытые действия на стороне сервера.

Можно выделить три основные преимущества децентрализации:

– отказоустойчивость – децентрализованные системы менее подвержены случайным ошибкам, так как они полагаются на множество отдельных компонентов, ошибка в которых менее вероятна;

– устойчивость к атакам – децентрализованные системы более массивные дорогостоящие, чтобы их атаковать, так как в них исключены центральные точки воздействия, которые можно атаковать с гораздо меньшими затратами, чем экономические размеры всей инфраструктуры;

– стойкость к сговору – участникам децентрализованных систем гораздо труднее вступать в сговор, чтобы получить выгоду от менее скоординированных участников.

Технология одноранговых сетей и их применение исследуется многими разработчиками. Но уже сейчас есть множество вариантов реализации технологии децентрализованных сетей.

Одна из областей применения децентрализованных сетей – это обмен файлами. В подобных торрент-сетях узел размещает файл, другие узлы получают возможность загрузить его. При этом загрузка может происходить сразу с нескольких источников. Наибольшую популярностью имеют цифровые валюты: Bitcoin, Ethereum, Litecoin и также реализации децентрализованного облачного хранилища – такие проекты как: Storj, Sia, MaidSafe, Decent, LBRY Credits, FileCoin и другие [3].

Большинство подобных проектов использует специальную технологию хранения данных и транзакций – цепочку блоков. Данная технология нашла свое применение в децентрализованных системах благодаря своим уникальным свойствам и характеристикам, что позволяет эффективно распределять информацию по всем узлам и обеспечивать ее целостность и подлинность.

Реализовать децентрализацию наиболее эффективно позволяет распределенный реестр – блокчейн.

Несмотря на новизну технологии, существует множество решений и блокчейн-платформ для реализации полноценных децентрализованных приложений. Количество приложений и их аудитория стремительно возрастает, все больше сфер услуг охватывают приложения с использованием данных платформ, которые постоянно совершенствуются с учетом недостатков своих предшественников Большинство из них решают многие проблемы централизованных приложений и предоставляют удобные интерфейсы для разработки. Чем больше узлов в сети, тем она безопаснее, в следствии большей децентрализации. Следовательно, для реализации децентрализованного приложения нет необходимости разрабатывать собственную блокчейн-сеть, достаточно использовать проверенные и более безопасные платформы.

Наиболее развитой структурой и сообществом обладают блокчейн-сети Ethereum и Bitcoin. В январе 2018 года группой ученых Корнеллского университета были опубликованы результаты исследования степени децентрализации перечисленных платформ [1]. Было выявлено, что сеть Bitcoin имеет большую пропускную способность, в отличии от Ethereum, но узлы первой более сконцентрированные и, вероятно, содержатся в датацентрах, что нарушает принципы децентрализации. По данным исследования около 56 процентов узлов Bitcoin сконцентрированы в

дата-центрах, в то время как у Ethereum 28 процентов.

Следовательно, для реализации децентрализованного приложения предпочтительней использовать наиболее распространенные платформы. Среди которых можно выделить блокчейн Ethereum.

Для взаимодействия с блокчейном Ethereum существует множество программных решений. Среди них различные библиотеки для интеграции блокчейна Ethereum в приложения. В разработке децентрализованного приложения была использована библиотека web3 и расширение браузера Metamask для доступа к учетным записям Ethereum и взаимодействия с умным контрактом.

Умный контракт состоит из хранилища учетных записей и функций для регистрации и извлечения данных учетных записей. В хранилище записываются такие данные как: имя, фамилия, пол, дата регистрации и публичный адрес в сети Ethereum с которого производилась регистрация.

Было разработано веб-приложение использующее расширение Metamask и функции умного контракта.

Интерфейс приложения представляет собой панель навигации и основные разделы:

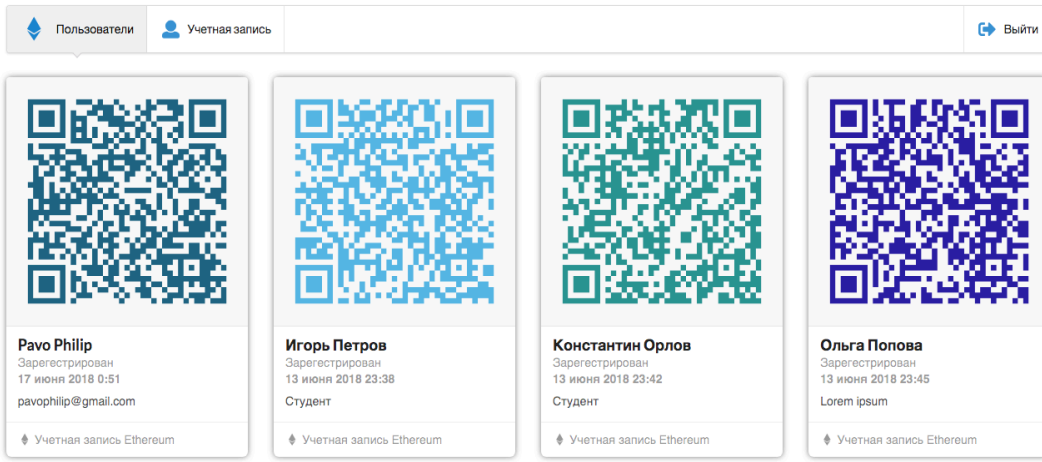


Рис. 1. Раздел с учетными записями пользователей

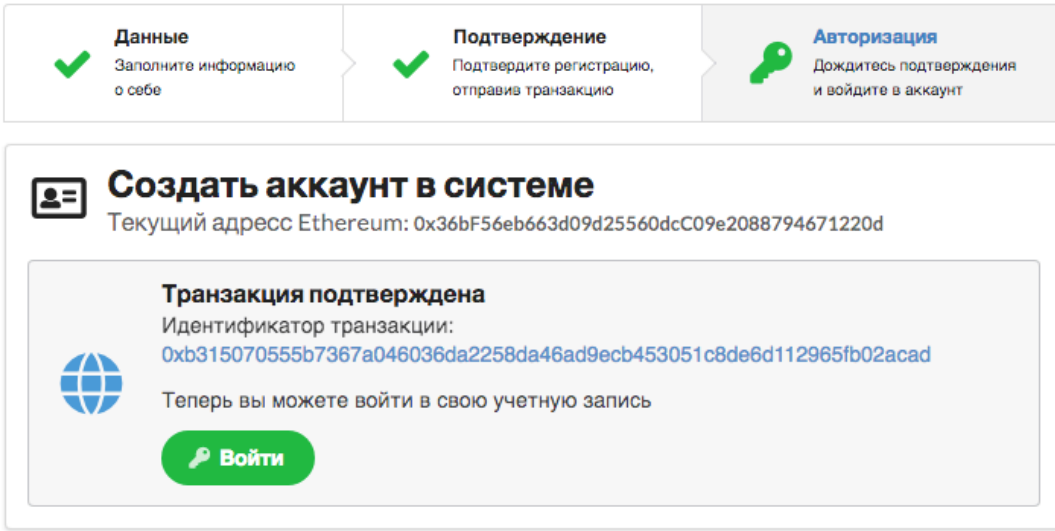


Рис. 2. Создание учетной записи.

– список зарегистрированных пользователей;

– форма создания учетной записи;

– форма авторизации;

– карточка пользователя.

На главной странице расположен список

зарегистрированных пользователей. Карточка учетной записи состоит из QR-кода (Quick Response Code) с уникальной ссылкой на учетную запись, имени пользователи, даты и времени регистрации, дополнительной информации, которая была указана при регистрации. Также присутствует ссылка на информацию о кошельке Ethereum с которого производилась регистрация (рис. 1) и ссылка на кошелек в etherscan.io [2].

После чего будет создана запись в хранилище умного контракта. Для каждого зарегистрированного пользователя генерируется QR со ссылкой на его учетную запись.

Для авторизации и идентификации пользователя необходимо выполнить цифровую подпись с использованием своего приватного ключа (рис. 3). Это делается также с помощью расширения Metamask.

Данное приложение позволяет создавать учетные записи и идентифицировать пользователя без использования сервера. Все данные хранятся децентрализовано в сети Ethereum.

В контракте можно реализовать хранение дополнительных данных, а также данных в зашифрованном виде либо файлов, что позволит пользователю надежно хранить важную информацию децентрализовано. Умный контракт может наследовать другие контракты, следовательно, данное приложение может быть использовано как модуль для других систем, таких как голосование, что обеспечит точный подсчет и невозможность подделки голосов или систему для проверки прав на владение цифровыми ресурсами и произведениями.

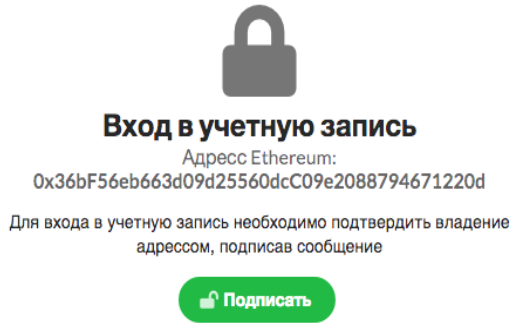


Рис. 3. Сообщение об успешной проверке подписи.

Литература

1. Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer. Decentralization in Bitcoin and Ethereum Networks [Электронный ресурс] / Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer // Financial Cryptography and Data Security 2018. – Режим доступа: URL: https://arxiv.org/abs/1801.03998v2. – (дата обращения: 03.04.2018).

2. Etherscan [Электронный ресурс] - URL: https://ethersan.io

3. Jay J.Wylie, Michael W., Bigrigg, John D. Strunk Survivable Information Storage Systems // Computer. 2000. Volume 33, Issue 8, p. 61-68

4. The Meaning of Decentralization [Электронный ресурс] - URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

References

1. Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer. Detsentralizatsiya v setyakh Bitcoin i Ethereum [Elektronnyy resurs] / Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer // Finansovaya kriptografiya i bezopasnost' dannykh 2018. - Rezhim dostupa: URL: https://arxiv.org /abs/1801.03998v2. - (data obrashcheniya: 03.04.2018).

2. Etherscan [Elektronnyy resurs] - URL: https://ethersan.io

3. Jay J.Wylie, Michael W., Bigrigg, John D. Strunk Survivable Information Storage Systems // Komp'yuter. 2000. Tom 33, vypusk 8, str. 61-68

4. Znacheniye detsentralizatsii [Elektronnyy resurs] - URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

ГОНЧАРЕНКО Юлия Юрьевна, доктор технических наук, доцент, про-фессор кафедры «Информационная безопасность» ФГАОУ ВО «Севасто-польский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская 33. E-mail: luliay1985@mail.ru.

ПАВО Филипп Николаевич, студент 1 курса магистратуры кафедры «Информационная безопасность» ФГАОУ ВО «Севастопольский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская 33. E-mail: pavophilip@gmail.com.

GONCHARENKO Julia, doctor of technical Sciences, associate Professor, Professor of "Information security" FSAEI HE "Sevastopol state University". Kurchatov street 7, Sevastopol, Russian, 299015. E-mail: Iuliay1985@mail.ru.

PAVO Philip, student of the 1st year of the master's degree of the "Information security" FSAEI HE "Sevastopol state University". Kurchatov street 7, Sevastopol, Russian, 299015. E-mail: pavophilip@gmail.com.

УДК 004.93.1 Вестник УрФО № 3(29) / 2018, с. 29–37

Ложников П. С.

DOI: 10.14529/SECUR180305

ИНТЕГРАЦИЯ БИОМЕТРИЧЕСКОЙ И ЭЛЕКТРОННОЙ ПОДПИСЕЙ С ПРИМЕНЕНИЕМ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ

В настоящей статье приводятся аргументы относительно возможности использования современных методов распознавания образов в задачах биометрической аутентификации: нечетких экстракторов, искусственных многослойных нейронных сетей, методов «глубокого обучения», а также сверточных, эволюционных, малых, «широких», гибридных нейронных сетей. Приводятся результаты собственных исследований по данному направлению. Предлагается два метода интеграции биометрической и электронной подписей на основе динамических параметров подписи, а также параметров лица и клавиатурного почерка.

Ключевые слова: *искусственные нейронные сети, биометрия, электронная подпись, распознавание образов.*

Lozhnikov P. S.

INTEGRATION OF BIOMETRIC AND ELECTRONIC SIGNATURES USING NEURAL NETWORK ALGORITHMS

The article provides arguments on the possibility of using modern pattern recognition methods in biometric authentication tasks: fuzzy extractors, artificial multilayer neural networks, "deep learning" methods, as well as convolutional, evolutionary, shallow, wide, hybrid neural networks. The results of our research in this area are given. Two methods of biometric and electronic signatures integration are proposed based on dynamic parameters of handwritten signature, as well as parameters of the face and keyboard handwriting.

Keywords: *artificial neural networks, biometrics, electronic signature, pattern recognition.*

Введение

Тенденции современного информационного общества связаны с переходом государств к цифровой экономике. Это приводит к тому, что целые сегменты документооборота (ДО) переносятся в цифровую среду: государственные услуги, банковское обслуживание, электронные закупки. Хотя документы создаются при помощи программного обеспечения, многие из них распространяются на бумажных носителях. Это связано с тем, что темпы повсеместного внедрения и освое-

ния современных технологий в организациях, а также развитие законодательства отстают от потенциальных возможностей, которые дают эти технологии. Поэтому в обозримом будущем во многих сферах деятельности документооборот будет смешанным, при этом электронные документы и транзакции будут превалировать.

В настоящей статье рассматривается решение проблемы интеграции биометрической и электронной подписей в среде гибридного документооборота [1]. Гибридный документ может находиться на электронном или бумажном носителе и содержать изображение автографа, защищенное с помощью электронной подписи (ЭП), а также тайных или открытых биометрических образов, благодаря чему можно быстро (за приемлемое время) проверить его целостность и аутентичность независимо от формы представления (бумажный или электронный). Ключевым атрибутом гибридного документа является ЭП, при формировании которой используется биометрический образ субъекта. При этом применяются нейросетевые алгоритмы преобразования биометрических признаков в секретный ключ ЭП. Для формирования ЭП из биометрических данных предложен гибридный преобразователь биометрия-код, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров пользователя в четкий однозначный код ключа (пароля).

В качестве биометрических образов предлагается использовать так называемую биометрическую рукописную подпись (автограф) либо образ лица и параметры клавиатурного почерка субъекта при вводе им парольной фразы. Основной акцент делается на динамические биометрические образы человека, изменяющиеся с течением жизни.

1. Динамические биометрические образы

Предлагается два варианта реализации технологии генерации секретных ключей ЭП на основе биометрических образов:

1. Первый вариант подразумевает использование в качестве биометрического образа рукописную подпись. В данном случае формирование ЭП из биометрической рукописной подписи не повлияет существенным образом на имеющиеся бизнес-процессы в организации, т.к. подпись является привычным способом подтверждения аутентичности бумажных документов.

2. Второй предлагаемый метод формирования ЭП заключается в использовании для выработки секретного ключа данных от стандартного оборудования: клавиатуры и вебкамеры. В этом случае задействуются параметры лица и клавиатурного почерка субъекта. На базе данного метода также предлагается «расширенная» технология защиты для электронных реализаций документов, которая заключается в следующем. После формирования гибридного документа его владелец может ограничить доступ других лиц к произвольным его частям, а также запретить определенные действия (печать, редактирование и т.д.). При этом содержание каждой из этих частей документа будет зашифровано на открытом ключе того субъекта, которому предоставляется доступ. Если к одной из частей документа имеют доступ более одного субъекта, создается несколько копий этой части, каждая из которых шифруется на соответствующем открытом ключе. При работе пользователя с электронной реализацией гибридного документа производится непрерывный мониторинг в реальном времени параметров его лица и клавиатурного почерка. Эти параметры используются для генерации закрытого ключа, применяемого в дальнейшем для расшифровки соответствующих частей документа (рис. 1). При фиксации изменений биометрических характеристик субъекта, регистрируемых в процессе работы, документ временно «изменяет» либо «скрывает» свое содержимое целиком или полностью, блокирует часть функций по его редактированию. Пользователь не сможет пойти «в обход» системы гибридного документооборота, т.к. вся конфиденциальная информация зашифрована на соответствующих криптографических ключах. Общедоступная для всех субъектов информация не шифруется. Такая техника активной защиты получила название технологии «живого документа».

Для повышения надежности генерации ключа можно использовать многофакторный метод, сочетающих оба предложенных варианта.

1.1. Параметры рукописной подписи

В компьютерном представлении подпись может состоять из функций положения пера на планшете $x(t)$, $y(t)$ и давления пера на планшет $p(t)$, где t – это время в дискретной форме. Каждый рукописный образ подвергается спектральному и корреляционному анализу с целью вычисления фиксированного коли-

чества информативных признаков. Данный вектор состоит как из величин, характеризующих внешний вид образа (расстояния между определенными точками изображения подписи, параметры ее наклона, ширины, длины), так и динамику его воспроизведения (амплитуды гармоник функций *x(t), y(t), p(t)*, соответствующих частоте колебания руки подписанта (около 1-10 Гц), коэффициенты корреляции между этими и производными функциями, коэффициенты вейвлет-преобразования Добеши D6). Подробнее процесс вычисления данных признаков описан в работе [2].

1.2. Параметры лица и клавиатурного почерка субъектов

В качестве параметров лица использовались некоторые характеристики из работ [3] и [4], в частности:

– Расстояния между глазами, центром лица, кончиком носа (в пикселях, значения нормировались по диагонали лица в кадре).

– Площади глаз, носа, рта (значения нормировались по площади лица).

– Коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) между всеми парами следующих областей лица: глаза, нос, рот. Данные признаки характеризуют асимметрию лица.

– Параметры, характеризующие цвет глаз и кожи.

В качестве признаков клавиатурного почерка использовались времена удержания и паузы между нажатием клавиш.

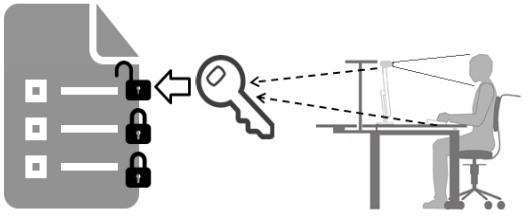


Рис. 1. Иллюстрация процесса получения доступа к фрагменту электронной реализации гибридного документа

2. Методы и технологии формирования секретного ключа электронной подписи из биометрических данных субъекта

Нечеткий экстрактор (fuzzy extractor) базируется на применении кодов, исправляющих ошибки. Криптографический ключ кодируется помехоустойчивым кодом, далее закодированная последовательность бит объединяется с биометрическими характеристиками субъекта, которые вычисляются по данным обучающей выборки. На выходе получается «открытая строка». В процессе аутентификации субъект повторно предъявляет биометрические данные, которые складываются с «открытой строкой» с помощью операции XOR. В результате высвобождается ключ, неверные биты которого корректируются. К фундаментальным недостаткам нечетких экстракторов относятся [1]:

1. Все классические коды вносят избыточность. Чем больше исправляющая способность кода, тем больше избыточности и меньше длина генерируемого ключа-пароля. В нечетком экстракторе длина ключа жестко зависит от исправляющей способности кода.

2. Классические коды не могут исправить большое количество ошибок, поэтому их невозможно использовать вместе с малоинформативными или коррелированными биометрическими параметрами (признаками).

3. Нечеткие экстракторы квантуют «сырые» (необработанные, необогащенные) биометрические данные и не учитывают параметры распределения значений признаков, в результате они должны давать более высокую долю ошибок по сравнению с нейросетевыми преобразователями биометрия-код, которые в свою очередь располагают этими данными, кодируя их весовыми коэффициентами нейронов.

Применение данного подхода по отношению к динамическим биометрическим образам не дало высоких результатов [5, 6].

Искусственные нейронные сети (ИНС) состоят из взаимосвязанных вычислительных элементов (нейронов), способных к обучению, приводящему к уличению качества решения задачи. Классические ИНС кодируют данные об особенностях признаков весовыми коэффициентами синапсов нейронов. Особое внимание в настоящее время уделяется технологиям «глубокого обучения». Популяризация данного направления поддерживается крупными организациями (NVIDIA Corporation, Intel Corporation, Google, Inc., Microsoft Corporation). На сегодняшний день под «глубоким» обучением обычно подразумевается итерационная настройка многослойных нейронных сетей прямого распространения, при которой в том или ином виде используется алгоритм «обратного распространения ошибки». Он имеет 2 типа реализации: пакетного или стохастического гради-

ентного спуска (во втором случае используются методы оптимизации ИНС) [7]. Предпринимаются попытки применения методов глубокого обучения для аутентификации субъектов по динамическим биометрическим характеристикам [8]. Однако использовать эти техники в реальной практике пока затруднительно, так как для достижения приемлемых показателей требуется значительный объем обучающей выборки (сотни примеров биометрического образа и более).

Помимо больших многослойных ИНС активные исследования ведутся в области, так называемых *малых сетей* (shallow networks). Эти ИНС способны к универсальной аппроксимации, но для этого требуется потенциально неограниченное число скрытых нейронов, которое играет роль сложности модели ИНС и является критическим фактором для практической реализации. Известен ряд работ, в которых выполнялась оценка ограничений малых ИНС и сформулирован ряд теорем [9]. Получены нижние оценки сложности неглубоких сетей в зависимости от соотношения между областью значений аппроксимируемой функции и размерностью входа [10]. Попытки создания процедур автоматической оценки минимально необходимого числа нейронов на основании данных обучающей выборки предпринимались и ранее. В [11] дана эмпирическая связь между числом примеров обучающей выборки и размером сети с целью определения верхнего порога числа нейронов скрытого слоя. Эти результаты являются важными для развития методов биометрической аутентификации, так как имеют отношение к обоснованию сложности ИНС в зависимости от ограничений на объем обучающей выборки. Малые сети могут обучаться на гораздо меньшем числе примеров.

Нейронные сети, в которых реализовано изменение весовых коэффициентов и топологии с помощью эволюционных алгоритмов, относятся к группе сетей TWEANNs (Topology & Weight Evolving Artificial Neural Networks). Данная стратегия построения и обучения ИНС относится к категории методов обучения с подкреплением и нашла применение в условиях, когда выполнить обучение с учителем практически невозможно. Эволюционная аугментация нейросетевой топологии (NeuroEvolution of Augmenting Topologies, NEAT) использует генетические алгоритмы для адаптации, как топологии, так и весов ИНС. Метод использует вариацию параметрической мутации, которая основана на эволюционных стратегиях и эволюционном программировании. Эволюция начинается с ИНС без скрытых нейронов и идет в направлении усложнения структуры. Такой подход находит применение в долго функционирующих и постоянно обучающихся ИНС на больших объемах данных (системы автопилотов автомобилей, обнаружения препятствий и др.) [12].

На сегодняшний день при сравнительно небольших обучающих выборках эволюционный подход успешно применяется для подбора топологий и весов в ИНС с одним скрытым слоем. Только с 2014 года доступность аппаратных ресурсов позволила применить нейроэволюцию к глубоким и сверточным нейронным сетям, но уже на очень больших выборках [13]. Эволюционный подход может быть положен в основу механизмов, позволяющих менять параметры ИНС пропорционально изменениям динамического биометрического образа пользователя со временем и в зависимости от его состояния.

В некотором смысле аналогом «малых» ИНС являются так называемые *«широкие» нейросети*. Эти ИНС представляют собой персептроны, которые состоят из большого количества нейронов, но малого числа слоев (один или два) и имеют принципиальные отличия от shallow networks. Главное отличие состоит в том, что для обучения «широких» ИНС не используется принцип «обратного распространения ошибки». Не итерационный и абсолютно устойчивый алгоритм обучения «широких» ИНС впервые предложен в России несколько лет назад для решения задач биометрической аутентификации [14]. Позже он лег в основу серии стандартов ГОСТ Р 52633. Обучение выполняется послойно, каждый нейрон обучается независимо от остальных нейронов сети, исходя из параметров закона распределения признаков, вычисляемых по данным обучающей выборки. Чтобы настроить автомат на распознавание определенного субъекта достаточно 20 примеров его образа. Высокая скорость работы позволяет реализовать данные алгоритмы на низкопроизводительном вычислительном устройстве.

В рамках теории «широких» ИНС стали применяться процедуры оценки информативности признаков (через площади пересечения функций плотностей вероятности) [15]. Впервые предложено создавать синапсы с учетом информативности признаков, а коли-

чество входов нейрона устанавливать, исходя из общей информативности признаков [16]. Это требование является логичным и позволяет обосновать выбор многих параметров ИНС. Теория «широких» ИНС имеет много общего с методами математической статистики и теории вероятностей. Комплексирование разных математических аппаратов позволило сдвинуться «с мертвой точки» в вопросах биометрической аутентификации.

«Широкие» нейронные сети могут быть настроены на генерацию фиксированной битовой последовательности при поступлении на вход образа, принадлежащего определенному классу, и случайной равномерно распределенной последовательности бит («белого» шума) при поступлении на вход неизвестного образа. Таким образом, данные сети могут быть использованы для интеграции биометрической и электронной подписей.

3. Гибридный подход к построению преобразователей биометрия-код, генерирующего секретный ключ электронной подписи

Активное развитие «широких» ИНС произошло в последние годы главным образом по пути гибридных нейросетевых алгоритмов. После отказа от «обратного распространения ошибки» появилась возможность менять не только активационную функцию нейрона, но и его функционал (в персептроне всегда использовался функционал взвешенного суммирования). В частности, для более эффективной обработки слабо коррелирующих биометрических параметров подходят квадратичные формы (1). Последние исследования показали, что многие функционалы обрабатывают данные гораздо эффективнее сумматоров персептрона и способны работать с сильно коррелирующими признаками [17]. Также эти исследования показывают, что сильно коррелирующие признаки позволяют создавать специальные нейроны, эффективность которых значительно выше, чем нейронов, ориентированных на обработку независимых признаков [18]. Например, такие нейроны можно построить на базе разностного (2) или гиперболического (3) многомерного Байесовского функционала. Таким образом, корреляционная зависимость между признаками может быть воспринята нейросетью как особый вид информации об образе. Это обстоятельство кардинально меняет подход: от малоинформативных и коррелированных признаков не нужно избавляться, они должны обрабатываться отдельными видами нейронов. Гибридные «широкие» ИНС имеют общие черты с сетями радиально-базисных функций, но являются более гибкими. Они могут состоять из нескольких слоев, формируемых из различных типов нейронов и иметь перекрестные связи.

$$\ddot{I} = \sqrt{\sum_{j=1}^{N} \frac{(m_j - a_j)^2}{\sigma_j^2}}, \quad (1)$$

где a_i – значение i-го биометрического параметра (входа нейрона), m_i и σ_i – математическое ожидание и среднеквадратичное отклонение i-ого признака (для образа «Свой»), соответственно, n – размерность функционала (число признаков, входов нейрона).

$$d_t = \sum_{j=1}^{N} \left| \frac{|m_t - a_t|}{\sigma_t} - \frac{|m_j - a_j|}{\sigma_j} \right|, \; j \neq t \quad (2)$$

$$g_{t-} = \sum_{j=1}^{N} \left(\frac{(m_t - a_t)^2}{\sigma_t^2} - \frac{(m_j - a_j)^2}{\sigma_j^2} \right), j \neq t, \quad (3)$$

где a_j – значение i-го параметра (входа нейрона) с высоким значением модуля корреляции $|ri,t|$ по отношению к t-му биометрическому признаку. То есть таблицы входных связей функционала Байеса должна формироваться таким образом, что бы обогащаемые им параметры были как можно сильнее коррелированны между собой.

После обогащения входных данных нейрона расчетное значение функционала поступает в функцию активации. В простейшем случае функция активации является пороговой. Именно такой случай рассматривается в рамках настоящей статьи.

Рассматриваемые гибридные ИНС ориентированы на распознавание образов при высокой размерности пространства признаков и наличии ограничений на объем обучающей выборки. Построение и обучение этих сетей детерминировано, при этом коррелированность биометрических параметров определяется только на основании малой обучающей выборки, а сами параметры определены заранее. Обучение «широкой» нейросети является послойным, т.е. каждый последующий слой обучается на выходных значениях нейронов предыдущего слоя, воспринимая их как значения признаков. Можно сказать, что каждый слой «широкой» сети состоит из нескольких подсетей, настройка нейронов каждой из которых имеет свою специфику.

При реализации преобразователя биометрия-код на практике важно позабо-

титься о том, чтобы биометрический образ и ключ пользователя не были скомпрометированы. Сегмент сети, представляющий собой персептрон, можно считать достаточно защищенным от этой угрозы [19]. Из весов нейронов нельзя за приемлемое время извлечь данные обучающей выборки и воссоздать эталон биометрического образа, как и извлечь личный ключ пользователя (это является вычислительно сложной и плохо формализуемой задачей). Однако квадратичные формы и Байесовские функционалы оперируют непосредственно параметрами законов распределения признаков, что ведет к необходимости хранения данных параметров. Если сервер, на котором хранится таблица нейросетевых функционалов, не является доверенным, то существует угроза восстановления фрагментов ключа и эталона биометрического образа пользователя по данным таблицы нейросетевых функционалов. В этом случае для защиты биометрического эталона на этапе хранения может быть применен механизм защищенного нейросетевого контейнера [19]. Данный механизм заключается в том, что параметры нейронов гибридной сети шифруются на выходах нейронов персептрона. При верной выдаче фрагмента ключа нейронами персептрона, параметры других нейронов будут расшифрованы. В противном случае, сеть сгенерирует шум, т.к. расшифрованные значения весовых коэффициентов не будут соответствовать эталону субъекта.

Корректирующие коды из работы [20] позволяют безопасно хранить синдромы ошибок и не дают возможности восстановить ключ без предъявления биометрического образа, достаточно близкого к аутентичному. В сочетании с механизмом защищенного нейросетевого контейнера [19] эти помехоустойчивые коды [20] решают проблему безопасного хранения таблицы нейросетевых функционалов. Однако открытым остается вопрос влияния механизма защищенного нейросетевого контейнера на вероятность ошибочных решений, принимаемых «широкой» нейронной сетью.

В работе [21] предлагается следующая модель гибридной сети, представленная на рисунке 2. Для каждого субъекта по данным его обучающей выборки формируется и обучается отдельная нейронная сеть. Каждая сеть способна генерировать ключ электронной подписи длиной до 2048 бит.

Надежность биометрической системы аутентификации (идентификации) определяется следующими показателями. Вероятность ошибки 2-ого рода («пропуска чужого», False Acceptance Rate, FAR) должна быть как можно ниже. При этом вероятность шибки 1-ого рода («ложный отказ в допуске своему», False Rejection Rate, FRR) должна быть приемлемой, т.к. частые отказы создают неудобства. FAR и FRR также возникают при генерации неверного ключа (при FAR=FRR говорят о Equal Error Rate, EER).

В настоящей работе нейросетевой преобразователь биометрия-код с указанной архи-

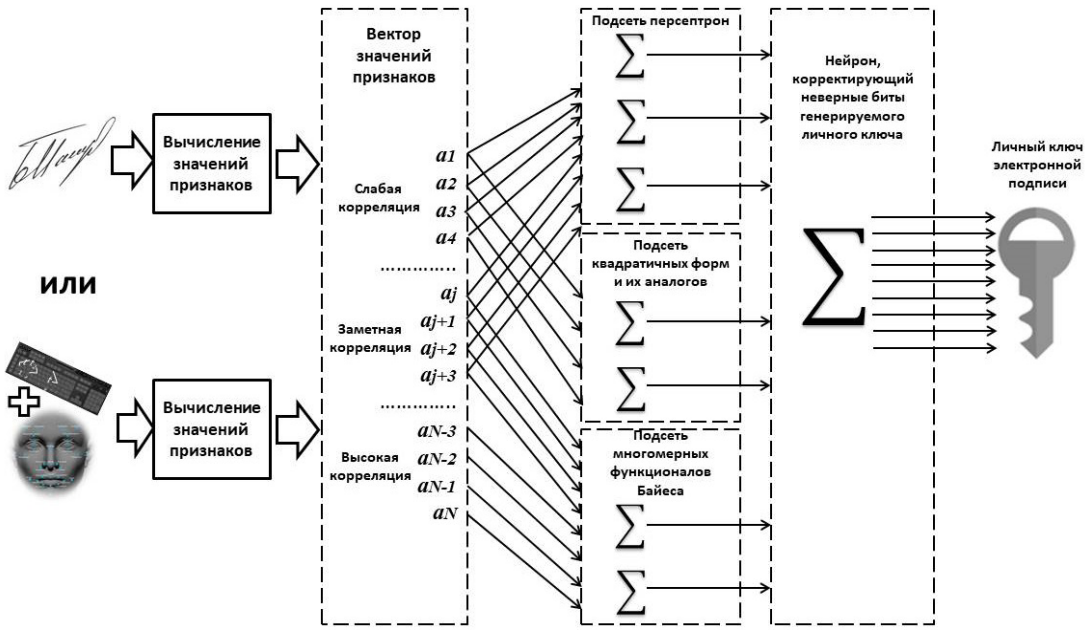


Рис. 2. Схема работы преобразователя биометрия-код на базе гибридных нейронных сетей

тектурой был реализован в виде программного комплекса с интерфейсами ввода подписей (рукописных паролей), лица и клавиатурного почерка (с использованием графического планшета, веб-камеры и клавиатуры). С использованием биометрических данных собранных в рамках исследования [21] гибридные сети (рис. 2) были перенастроены индивидуально под каждого субъекта. Далее были привлечены те же 90 испытуемых, что и в работе [21], которые многократно прошли процедуру биометрической идентификации (данные предъявлялись сразу всем нейросетевым преобразователям). Далее проводилась проверка корректности ключей, генерируемых с помощью 90 гибридных сетей (ключ должен быть корректен только в одном из 90 случаев). В результате достигнуты следующие вероятности ошибочных решений:

– при распознавании субъекта/генерации ключа по рукописным образам: FRR=18% при FAR<0,01% (EER=3,5%);

– при распознавании субъекта/генерации ключа по клавиатурному почерку и лицу: FRR=6,8% при FAR<0,01% (EER=1,7%);

– при распознавании субъекта/генерации ключа по рукописным образам, клавиатурному почерку и лицу: FRR=2,5% при FAR<0,01% (EER=0,9%).

При проведении эксперимента не применялся механизм защищенного нейросетевого контейнера, однако были учтены изменения динамического биометрического образа субъекта со временем (обучение преобразователя биометрия-код и его тестирование проводилось в различные дни с перерывом от одной до нескольких недель). В общей сложности совершено порядка 4500 попыток прохождения процедуры идентификации и последующей аутентификации.

Заключение

В рамках работы проведено аналитическое исследование методов построения преобразователей биометрия-код, используемых для интеграции биометрической и электронной подписей в качестве основы биометрических систем аутентификации и систем электронной подписи с биометрической активацией: нечетких экстракторов, искусственных многослойных нейронных сетей, методов «глубокого обучения», а также сверточных, эволюционных, малых, «широких», гибридных нейронных сетей. Протестирована модель гибридной нейронной сети на базе персептрона, сетей квадратичных форм и многомерных разностных и гиперболических функционалов Байеса. Экспериментально подтверждена высокая эффективность применения модели для решения задачи по интеграции биометрической и электронной подписей.

Литература

1. Ложников П.С. Биометрическая защита гибридного документооборота: монография / Новосибирск: Изд-во СО РАН, 2017. — 130 с.

2. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. – 2016. – №7(4). – P. 59; DOI: 10.3390/info7040059.

3. Васильев В.И., Ложников П.С., Сулавко А.Е., Жумажанова С.С. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования // Вопросы защиты информации. – 2016. – №1. – С. 12-20.

4. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. – 2017. – №3. – С. 24-34.

5. Lozhnikov P.S., Sulavko, A.E., Volkov D.A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information / Control and Communications (SIBCON), 21-23 May 2015, Omsk, Russia. – P.1-3; DOI: 10.1109/SIBCON.2015.7147126.

6. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Buraya E.V. Methods of Generating Key Sequences Based on Keystroke Dynamics // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 15-17 November, 2016, Omsk, Russia. – P. 1-5; DOI: 10.1109/Dynamics.2016.7819038.

7. Yasuoka Y., Shinomiya Y., Hoshino Y. Evaluation of Optimization Methods for Neural Network // Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems, 25-28 August 2016, Sapporo, Japan; DOI: 10.1109/SCIS-ISIS.2016.0032.

8. Hafemann L. G. et al. Writer-independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks // 2016 International Joint Conference on Neural Networks (IJCNN), 24-29 July 2016. – P. 2576-2583; DOI: 10.1109/IJCNN.2016.7727521.

9. Kůrková V., Sanguineti M. Probabilistic Lower Bounds for Approximation by Shallow Perceptron Networks // Neural Networks. – 2017. – Vol. 91.– P. 34-41.

10. Kůrková V., Sanguineti M. Model Complexities of Shallow Networks Representing Highly Varying Functions // Neurocomputing. – 2016. – Vol. 171. – P. 598-604.

11. Rogers L.L., Dowla F.U.: Optimization of Groundwater Remediation Using Artificial Neural Networks with Parallel Solute Transport Modeling //. Water Resources Research. – 1994. – Vol. 30(2). – P. 457–481.

12. Stanley K.O. Efficient Evolution of Neural Networks Through Complexification. PhD Thesis. Department of Computer Sciences, The University of Texas at Austin, 2004.

13. Koutn´ık J., Schmidhuber J., Gomez F. Evolving Deep Unsupervised Convolutional Networks for Vision-Based Reinforcement Learning // 2014 Annual Conference on Genetic and Evolutionary Computation. – 2014. – P. 541–548.

14. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза: Изд-во Пензенского государственного университета. – 2005. – С. 273.

15. Sulavko A.E., Fedotov A.A., Eremenko A.V. Users' Identification through Keystroke Dynamics Based on Vibration Parameters and Keyboard Pressure // XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 14-16 November, 2017, Omsk, Russia. – P. 1-7.

16. Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза: Изд-во ПНИЭИ. – 2016. – С. 133.

17. Иванов А.И., Ложников П.С., Сулавко А.Е. Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. – 2017. – Т. 41. – №5. – С.765-774; DOI: 10.18287/2412-6179-2017-41-5-765-774.

18. Ivanov A.I., Lozhnikov P.S., Vyatchanin S.E. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / Control and Communications (SIBCON), 29-30 June 2017, Astana, Kazakhstan. – P.1-3; DOI: 10.1109/SIBCON.2017.7998435.

19. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «Издательство LEM». – 2014. – С. 144.

20. Безяев А. В., Иванов А. И., Фунтикова Ю. В. Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хэш-функций // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 3(13). – С. 4 -13.

21. Lozhnikov P.S., Sulavko A.E. Generation of a Biometrically Activated Digital Signature Based on Hybrid Neural Network Algorithms // Journal of Physics: Conf. Series. –2018. – № 1050; DOI: 10.1088/1742-6596/1050/1/012047.

References

1. Lozhnikov P.S. Biometricheskaya zashchita gibridnogo dokumentooborota: monografiya / Novosibirsk: Izd-vo SO RAN, 2017. — 130 s.

2. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. – 2016. – №7(4). – P. 59; DOI: 10.3390/info7040059.

3. Vasil'yev V.I., Lozhnikov P.S., Sulavko A.Ye., Zhumazhanova S.S. Otsenka identifikatsionnykh vozmozhnostey biometricheskikh priznakov ot standartnogo periferiynogo oborudovaniya // Voprosy zashchity informatsii. – 2016. – №1. – S. 12-20.

4. Lozhnikov P.S., Sulavko A.Ye., Buraya Ye.V., Pisarenko V.YU. Autentifikatsiya pol'zovateley komp'yutera na osnove klaviaturnogo pocherka i osobennostey litsa // Voprosy kiberbezopasnosti. – 2017. – №3. – S. 24-34.

5. Lozhnikov P.S., Sulavko, A.E., Volkov D.A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information / Control and Communications (SIBCON), 21-23 May 2015, Omsk, Russia. – P.1-3; DOI: 10.1109/SIBCON.2015.7147126.

6. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Buraya E.V. Methods of Generating Key Sequences Based on Keystroke Dynamics // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 15-17 November, 2016, Omsk, Russia. – P. 1-5; DOI: 10.1109/Dynamics.2016.7819038.

7. Yasuoka Y., Shinomiya Y., Hoshino Y. Evaluation of Optimization Methods for Neural Network // Soft

Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems, 25-28 August 2016, Sapporo, Japan; DOI: 10.1109/SCIS-ISIS.2016.0032.

8. Hafemann L. G. et al. Writer-independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks // 2016 International Joint Conference on Neural Networks (IJCNN), 24-29 July 2016. – P. 2576-2583; DOI: 10.1109/IJCNN.2016.7727521.

9. Kůrková V., Sanguineti M. Probabilistic Lower Bounds for Approximation by Shallow Perceptron Networks // Neural Networks. – 2017. – Vol. 91.– P. 34-41.

10. Kůrková V., Sanguineti M. Model Complexities of Shallow Networks Representing Highly Varying Functions // Neurocomputing. – 2016. – Vol. 171. – P. 598-604.

11. Rogers L.L., Dowla F.U.: Optimization of Groundwater Remediation Using Artificial Neural Networks with Parallel Solute Transport Modeling //. Water Resources Research. – 1994. – Vol. 30(2). – P. 457–481.

12. Stanley K.O. Efficient Evolution of Neural Networks Through Complexification. PhD Thesis. Department of Computer Sciences, The University of Texas at Austin, 2004.

13. Koutn´ık J., Schmidhuber J., Gomez F. Evolving Deep Unsupervised Convolutional Networks for Vision-Based Reinforcement Learning // 2014 Annual Conference on Genetic and Evolutionary Computation. – 2014. – P. 541–548.

14. Volchikhin V.I., Ivanov A.I., Funtikov V.A. Bystryye algoritmy obucheniya neyrosetevykh mekhanizmov biometriko-kriptograficheskoy zashchity informatsii. Monografiya. Penza: Izd-vo Penzenskogo gosudarstvennogo universiteta. – 2005. – S. 273.

15. Sulavko A.E., Fedotov A.A., Eremenko A.V. Users' Identification through Keystroke Dynamics Based on Vibration Parameters and Keyboard Pressure // XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 14-16 November, 2017, Omsk, Russia. – P. 1-7.

16. Ivanov A.I. Mnogomernaya neyrosetevaya obrabotka biometricheskikh dannykh s programmnym vosproizvedeniyem effektov kvantovoy superpozitsii. Penza: Izd-vo PNIEI. – 2016. – S. 133.

17. Ivanov A.I., Lozhnikov P.S., Sulavko A.Ye. Otsenka nadezhnosti verifikatsii avtografa na osnove iskusstvennykh neyronnykh setey, setey mnogomernykh funktsionalov Bayyesa i setey kvadratichnykh form // Komp'yuternaya optika. – 2017. – T. 41. – №5. – S.765-774; DOI: 10.18287/2412-6179-2017-41-5-765-774.

18. Ivanov A.I., Lozhnikov P.S., Vyatchanin S.E. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / Control and Communications (SIBCON), 29-30 June 2017, Astana, Kazakhstan. – P.1-3; DOI: 10.1109/SIBCON.2017.7998435.

19. Akhmetov B.S., Ivanov A.I., Funtikov V.A., Bezyayev A.V., Malygina Ye.A. Tekhnologiya ispol'zovaniya bol'shikh neyronnykh setey dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa: Monografiya. / Almaty: TOO «Izdatel'stvo LEM». – 2014. – S. 144.

20. Bezyayev A. V., Ivanov A. I., Funtikova YU. V. Optimizatsiya struktury samokorrektiruyushchegosya biokoda, khranyashchego sindromy oshibok v vide fragmentov khesh-funktsiy // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2014. – № 3(13). – S. 4 -13.

21. Lozhnikov P.S., Sulavko A.Ye. Generation of a Biometrically Activated Digital Signature Based on Hybrid Neural Network Algorithms // Journal of Physics: Conf. Series. –2018. – № 1050; DOI: 10.1088/1742-6596/1050/1/012047

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-07-01204.

ЛОЖНИКОВ Павел Сергеевич, заведующий кафедрой «Комплексная защита информации» Омского государственного технического университета, кандидат технических наук, доцент. 644050, г. Омск, проспект Мира, д. 11. E-mail: lozhnikov@gmail.com.

LOZHNIKOV Pavel Sergeevich, Head of the "Complex Information Protection" Department, Omsk State Technical University, PhD, associate professor. 644050, Omsk, Mira av., 11. E-mail: lozhnikov@gmail.com.

УДК 004.7.056.53 Вестник УрФО № 3(29) / 2018, с. 38–42

Маслова М. А.

DOI: 10.14529/SECUR180306

ПРИНЦИПЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

В данной статье рассмотрены общие тенденции системы защиты интернет вещей и подробно рассмотрены четыре ее главных принципа: безопасность связи, защита устройств, контроль устройств и контроль взаимодействий в сети.

Ключевые слова: *интернет вещи, защита устройств, контроль устройств, сеть, безопасность связи.*

Maslova M. A.

PRINCIPY BEZOPASNOSTI INTERNETA VESHCHEJ

In this article we studied the general tendencies of the defence systems of the IoT (internet of things and reviewed (examined)) in detail four of its main principles: connection security, protection of the devices device protection), control of the devices and control of the interaction within the network.

Keywords: *Internet of Things, device protection, device monitoring, networking, communication security.*

При любом упоминании об интернет вещей, как правило, имеется в виду вещи для дома, которыми можно управлять через интернет, но если рассмотреть этот вопрос более глубже, то тема Internet of Things намного шире в своем применении. Под интернетом вещей в первую очередь понимается подключенные к вычислительной сети различные устройства: автомобили, телевизоры, камеры наблюдения, роботизированное производство, умное медицинское оборудование, сеть электроснабжения и бесчисленные промышленные системы управления. Все это современно и удобно, но необходимо помнить не только об удобстве в использовании, но и о ее безопасности и конфиденциальности. Безопасность интернета вещей можно построить на: безопасности связи, защите устройств, контроля устройств и контроля взаимодействий в сети. На этом фундаменте можно создать мощную и простую в развертывании систему безопасности, которая способна ослабить негативное воздействие большинства угроз безопасности для интернета вещей, включая целенаправленные атаки, что очень стало актуально в нынешнее время [1, 2].

Тема «Интернет вещей» очень актуальна в современном мире, т.к. «Интернет вещей» плотно вошел в нашу жизнь и миллиардов людей по всему миру. Однако рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования это могут быть даже трубопроводы, доменные печи и установки для выработки электроэнергии. Поскольку ряд таких объектов и систем интернета вещей уже подвергались нападению и был причинен внушительный ущерб, обеспечение их защиты выходит на первый план.

Необходимо рассмотреть, что же будет являться безопасностью связи и с помощью чего он будет реализован. Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, для того чтобы устройства знали, могут ли они доверять удаленной системе. Со-

временные криптографические технологии: Elliptic Curve Cryptography, работают в десять раз лучше предшественников в слабомощных чипах IoT 8-bit 8MHz.

Так же не менее важной задачей здесь является управление ключами для проверки подлинности данных и достоверности каналов их получения. Ведущие центры сертификации (CA) уже встроили «сертификаты устройств» в более чем миллиард устройств Internet of Things, предоставив возможность выполнять проверку подлинности широкого спектра устройств, включая сотовые базовые станции, телевизоры и многое другое [1].

Так же было разработано множество стандартов для упрощения развертывания надежной проверки подлинности всех звеньев цепи обмена данными. Существуют стандарты для форматов сертификатов, и надежные центры сертификации поддерживают как стандартные, так и кастомные форматы. С помощью стандартных протоколов, таких как Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) и Online Certificate Status Protocol (OCSP) во многих случаях сертификатами можно легко управлять удаленно.

Благодаря надежному центру сертификации, который предоставляет возможность обрабатывать сертификаты, ключи и учетные данные, фактическую проверку подлинности можно делать с помощью мощных стандартов Transport Layer Security (TLS) и Datagram TLS (DTLS) родственных SSL. Взаимная проверка подлинности, когда обе конечные точки проверяют друг друга, имеет решающее значение для качественной защиты систем IoT. В качестве дополнительного бонуса, однажды выполнив проверку подлинности по TLS или DTLS, две конечные точки могут обмениваться ключами шифрования или получать их для обмена данными, которые невозможно расшифровать подслушивающими устройствами. Для многих приложений IoT требуется абсолютная конфиденциальность данных, это требование легко выполняется использованием сертификатов и протоколов TLS/DTLS [1, 3].

Проверка подлинности информации, устройств и происхождения информации могут иметь решающее значение, так как данные зачастую хранятся, кэшируются и обрабатываются несколькими узлами, а не просто передаются из из одной точки в другую. Поэтому необходимо придерживаться правила, что данные всегда должны быть подписаны в тот момент, когда они были впервые зафиксированы и сохранены, что поможет снизить риски любого вмешательства в информацию. Подписание объектов данных, как только они были зафиксированы, и ретрансляция подписи с данными даже после их дешифрации является все более распространенной и успешной практикой [4].

Если рассматривать защиту устройств, то это в первую очередь обеспечение безопасности и целостности программного кода. Тема безопасности кода выходит за рамки этой статьи, заострим внимание на целостности. Подписание кода требуется для подтверждения правомерности его запуска, также необходима защита во время выполнения кода, чтобы атакующие не перезаписали его во время загрузки. Подписание кода криптографически гарантирует, что он не был взломан после подписания и безопасен для устройства. Это может быть реализовано на уровнях application и firmware и даже на устройствах с монолитным образом прошивки. Все критически важные устройства, будь то датчики, контроллеры или что-то еще, должны быть настроены на запуск только подписанного кода. Устройства должны быть защищены и на последующих этапах, уже после запуска кода, тут поможет защита на основе хоста, которая обеспечивает харденинг, разграничение доступа к системным ресурсам и файлам, контроль подключений, песочницу, защиту от вторжений, защиту на основе поведения и репутации. Также в этот длинный список возможностей хостовой защиты входят блокирование, протоколирование и оповещение для различных операционных систем IoT. В последнее время многие средства хостовой защиты были улучшены и адаптированы для IoT и теперь хорошо проработаны и отлажены, они не требуют доступа к облаку и бережно расходуют вычислительные ресурсы IoT-устройств [5].

Возможности удаленного обновления (Over the air) имеют решающее значение и должны быть встроены в устройства до того, как они покинут завод. OTA-обновления software и firmware очень важны для поддержания высокого уровня защищенности устройства. Тем не менее, обфускация, сегментированное подписание кода и OTA-обновления в конечном счете должны быть плотно объединены между собой для эффективной работы. Сегментированное подписа-

ние кода использует модель доверия на основе сертификатов, которое было описано в предыдущем разделе «Безопасность связи», а использование ECC при подписании кода может обеспечить те же самые преимущества высокого уровня безопасности в сочетании с высокой производительностью и низким энергопотреблением. В этой ситуации предлагаются следующие рекомендации по длине ключа для подписи кода IoT, где безопасность имеет значение:

– минимум 224-bit ECC для сертификатов конечных объектов с предпочтительным 256-bit и 384bit;

– минимум 521-bit ECC для корневых сертификатов, поскольку, как правило, ожидается, что подписанный код будет использоваться годами или даже десятилетиями после подписания, а подписи должны быть достаточно сильными, чтобы оставаться надежными в течение столь длительного времени [6, 7].

Рассмотрим безопасное и эффективное управление IoT. Мы знаем, что реверс-инжиниринг устройств рано или поздно будет проведен, уязвимости будут обнаружены, а для устройств необходимо будет предоставлять обновления OTA. Конечно, механизмы обновления OTA добавляют сложность архитектуре устройства IoT, поэтому многие инженеры стараются избегать их на свой страх и риск [8]. К счастью, хороший механизм OTA может использоваться для многих целей, не только для исправлений программного обеспечения и функциональных обновлений, но также:

1. Обновления конфигурации
2. Управления телеметрией безопасности для аналитики защищенности
3. Управления телеметрией для контроля правильности функционирования устройства
4. Диагностики и восстановления
5. Управления учетными данными доступа к сети (NAC)
6. Управления правами/привилегиями и множества других задач.

Конечно, все вышеперечисленное должно исполняться безопасно и надежно, здесь потребуется наиболее тщательный подход к подписанию кода и организации передачи файлов. Необходимо использовать существующие стандарты управления окружением software и firmware на каждом устройстве, включая конфигурацию, так как многие производители, в частности, Open Mobile Alliance (OMA), поддерживают такие стандарты. Некоторые из решений масштабируются для управления миллиардами устройств [9, 10].

Контроль взаимодействия в сети. Сегодня бесчисленные технологии и системы IoT представляют из себя не более чем «интернета вещей». Однако поскольку все больше систем должны будут связываться друг с другом, все важнее становится знать, «чему доверять». Сертификаты устройств могут содержать информацию о происхождении и типе устройства. Тем не менее на вопросы о том, нужно ли доверять этому устройству, в конечном итоге должны будут отвечать другие службы, например, основанные на репутации, или «Справочник вещей» (Directory of Things) [11]. Такой каталог способен не только отслеживать информацию о безопасности для каждого устройства и систем IoT, но еще отслеживать и управлять привилегиями и полномочиями, которыми устройства и системы наделяют друг друга. Фактически каждый из нас оказывается окруженным все большим количеством устройств IoT, а такие справочники могут помочь разобраться с устройствами с интересующими функциями в интересующих областях. Модель справочника делает возможным быстрый поиск удаленного устройства через каталог и, может быть, будет содействовать ускорению принятия решения об использовании данных с чужого устройства. Даже если пользователь никогда не видел устройство раньше, информация об устройстве, включая его возможности и репутацию, могут быть указаны в таком каталоге. Если предположить, что устройство захочет узнать, может ли оно доверять пользователю, то «Справочника вещей», возможно, будет недостаточно, и в этом случае скорее потребуется «Справочник всего», который будет включать устройства, системы и пользователей. Конечно, у многих людей нет умных чайников или умных холодильников, но это все временно, так как технологии развиваются стремительным ростом [12]. Но все же, у многих из нас уже есть автомобиль, который получает информацию для навигатора через интернет, фитнес-браслеты, Smart TV или проигрыватели Blu-ray, которые транслируют видео через интернет, а еще мы используем банкоматы и вендинговые аппараты. Наше взаимодействие с IoT на самом деле чаще, чем мы замечаем. В этой ситуации возможно захочется иметь свой собственный «Справочник вещей». Защищая устройства и связь,

управляя программными обновлениями и выполняя аналитику безопасности для стратегической защиты от угроз, становится понятно, что все эти меры абсолютно необходимы для защиты IoT. Концепция каталогов «чему доверять» весьма перспективна, но не является сегодня ни основополагающей технологией, ни ключевым ингредиентом в «контроле взаимодействий в сети» для большинства участников. Поэтому будем использовать эту перспективную концепцию каталогов только для того, чтобы дать предварительный обзор стоящих перед многими компаниями вызовов, и приводим пример, как можно справиться со сложными масштабными задачами.

Некоторые компании уже столкнулись с подобного рода проблемами, поскольку они несут ответственность за защиту более чем миллиарда устройств. Для них это «будущее» уже наступило, и они не одиноки [13, 15].

Можно сделать вывод, что сегодня уже очевидно, что реализовать все возможности, которые может предоставить пользователям концепция IoT без решения проблем с безопасностью и конфиденциальностью будет сложно. Указанные выше способы защиты IoT, конечно же, не являются исчерпывающими, над решением проблемы работают множество групп, компаний и энтузиастов. Но прежде всего высокий уровень безопасности устройств «Интернета вещей» должен быть основной задачей их производителей. Надежная защита должна изначально входить как часть функций изделия и стать новым конкурентным преимуществом, как для производителей, так и поставщиков комплексных IoT-решений.

В данной статье была предложена простая и эффективная эталонная архитектура защиты «Интернета вещей», которую легко развернуть и масштабировать с помощью: снижения воздействия вредоносного кода, который гарантирует, что весь код криптографически подписан и авторизирован для устройства, неподписанный код не разрешен для запуска; защиты устройств, которое гарантирует симметричное шифрование и сертификат x.509; защищена связь посредством взаимной проверки подлинности и шифрования. Применяются проверенные временем центры сертификации и модели доверия, которые уже защищают более миллиарда IoT-устройств. Используются новые алгоритмы ECC для обеспечения высокого уровня безопасности в устройствах IoT с ограниченными вычислительными ресурсами; связь между устройством и интернетом, должна быть защищена современными протоколами шифрования (TSL 1.3); ослабления вредоносного воздействия с помощью хостовой защиты и усиления эффективности минимизации рисков от всех остальных угроз с помощью аналитики безопасности; веб – приложения управления устройством, которое должно быть включено device identity registry (реестр удостоверений устройств) police -based authorization of security keys (авторизация ключей безопасности); обнаружения уязвимостей и угроз можно снизить риск их реализации с помощью эффективного, надежного и защищенного динамического управления системой.

Необходимо помнить, что успешное обеспечение безопасности систем начинается с моделирования рисков. Без понимания, как злоумышленники могут скомпрометировать систему, маловероятно надежно защитить любую IT-систему.

Литература

1. Маслова М. А., Кималидинов Э. Л. IOT (Интернет Вещей) : Материалы Студенческой Науч.-Техн. Конф., Г. Севастополь, 2018 / Севастополь. Гос. Ун-Т; Науч. Ред. А. Н. Дегтярев., Севастополь, 2018, с. 8-11.

2. Соколов М.Н., Смолянинова К.А., Якушева Н.А. Проблемы Безопасности Интернет Вещей: Обзор // Вопросы Кибербезопасности: Журнал, 2015, № 5(13), с. 34.

3. Алексей Лукацкий. Криптография в "Интернете Вещей" // www.slideshare.net, сайт, 2016.

4. Сети http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html, http://stfw.ru/page.php?id=19016/.

5. Laurence Cruz. Интернет Вещей и Информационная Безопасность // www.cisco.com.

6. Зеленин Д. В., Логинов Е. Л. Новая Парадигма Управления Экономикой: Переход к "Умным Сетям" Различного Управленческого Назначения // Экономические Науки, 2010, Т. 70, №. 9, с. 156-161.

7. Интернет Протокол IPv6 http://ru.wikipedia.org/wiki/IPv.

8. Tsvetkov V. Ya. Information interaction// European Researcher. Series A, 2013, № 11-1 (62), pp. 2573-2577.

9. Майечак Интернет. Майечак, Беате, М.: Интерэксперт, 2002, с. 345.

10. Эштон К. That "Internet of Things" Thing // RFID Journal: Электронный Журнал, 2009.

11. International Telecommunication Union, Overview of the Internet of Things, Recommendation ITU-T Y.2060, June 2012. Nordrum, Amy (18 Aug 2016).»Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated». IEEE.

12. Грингард, Сэмюэл Интернет Вещей. Будущее уже Здесь / Сэмюэл Грингард, М.: Альпина Паблишер, 2016, 188 с.

13. Грингард, Сэмюэл Интернет вещей: Будущее уже здесь / Сэмюэл Грингард. - М.: Альпина Диджитал, 2015. - 261 с.

14. Зараменских Е. П. Интернет Вещей. Исследования И Область Применения / Е.П. Зараменских, И.Е. Артемьев, М., ИНФРА, М, 2016, 188 с.

15. Дмитрий Подкопаев. Как Работают OTA-Обновления. //xakep.ru./.

Refereces

1. Maslova M. A._ Kimalidinov E. L. The Problems of Information Security .Materials of Student Science-Technical Conference. Sevastopol, 2018, pp. 8-11.

2. Sokolov M.N., Smolyaninova K.A., Yakusheva N.A. Problemy-Bezopasnosti Internet Seshchej Obzor Vopros Kiberbezopasnosti, Zhurnal, 2015, № 5(13), pp.34.

3. Aleksej Lukackij Kriptografiya v Internete Veshchej www.Slideshare.net, Sajt , 2016.

4. Seti http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html, http://stfw.ru/page.php?id=19016/.

5. Laurence Cruz. InternetVeshchej i Information Security, www.cisco.com.

6. Zelenin D.V, Loginov E L. Novaya Paradigma Upravleniya Ehkonomikoj Perekhod k Umnym Setyam Razlichnogo Upravlencheskogo Naznacheniya Ehkonomicheskie Nauki, 2010, T. 70, №. 9, pp. 156-161.

7. Internet Protokol IPv6 http://ru.wikipedia.org/wiki/IPv.

8. Tsvetkov V. Ya. Information interaction// European Researcher. Series A, 2013, № 11-1 (62), pp. 2573-2577.

9. Majechak Internet/ Majechak, Beate,M: Interehkspert, 2002, pp. 345.

10. Ehshton K. That "Internet of Things" Thing // RFID Journal, Ehlektronnyj Zhurnal, 2009.

11. International Telecommunication Union, Overview of the Internet of Things, Recommendation ITU-T Y.2060, June 2012. Nordrum, Amy (18 Aug 2016).»Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated». IEEE.

12. Gringard Sehmyuehl. Internet Veshchej. Budushchee Uzhe Zdes Seh-myuehl Gringard, M., Alpina Pablisher, 2016, pp. 188.

13. Gringard Sehmyuehl. Internet Veshchej. Budushchee Uzhe Zdes Seh-myuehl Gringard¬M.: Alpina Pablisher, 2015, pp. 261.

14. Zaramenskih E.P. Internet Veshchej. Issledovaniya i Oblast Primeneniya/ E.P. Zaramenskih, I.E. Artemev, M., Infra, M, 2016, pp. 188.

15. Dmitrij Podkopaev kak Rabotayut OTA-Obnovleniya, //xakep.ru./.

МАСЛОВА Мария Александровна, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности, ФГАОУ ВО «Севастопольский государственный университет», Россия, 299053, г. Севастополь, ул. Университетская, 33. . E-mail: mashechka¬81@mail.ru

MASLOVA Maria, senior lecturer, Department of Information security, Institute of radio electronics and information security, Sevastopol State University, Russia, 299053, Sevastopol, Universitetskaya str., 33. E-mail: mashechka-81@mail.ru

УДК 681.322 Вестник УрФО № 3(29) / 2018, с. 43–49

Хализев В. Н., Фёдоров С. Ю., Жданова Н. В. DOI: 10.14529/SECUR180307

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕОРИИ ИГР И ПРИМЕНЕНИЯ КВАЛИМЕТРИЧЕСКОЙ ОЦЕНКИ КАЧЕСТВА

Проблема оптимизации выбора при принятии решений присутствует во всех сферах жизни и деятельности современного человека. Люди принимают решения каждый день, независимо от времени и места нахождения. Многие из решений кажутся нам незначительными, а за некоторые человек, группа, целое предприятие или даже государство несет большую ответственность, в том числе и материальную. В статье рассмотрена математическая модель, позволяющая из предложенных на рынке компонентов оборудования, на основе анализа требований и сравнительного анализа, проведённого на основе квалиметрической оценки качеств выбрать оптимальное решение для синтеза интегрированной системы безопасности.

Ключевые слова: *математическая модель, синтез, анализ требований, интегрированная система безопасности.*

MATHEMATICAL MODEL OF SYNTHESIS OF INTEGRATED SECURITY SYSTEM BASED ON THE THEORY OF GAMES AND APPLICATION OF QUALIMETRIC QUALITY ASSESSMENT

The problem of optimization of choice when making decisions is present in all spheres of life and activity of a modern person. People make decisions every day, regardless of time and location. Many of the decisions seem insignificant to us, and for some people, a group, a whole enterprise or even a state bears a great responsibility, including material ones. The article discusses a mathematical model that allows the equipment components offered on the market to select the optimal solution for the synthesis of an integrated security system based on requirements analysis and comparative analysis based on a qualimetric quality assessment.

Keywords: *mathematical model, synthesis, requirements analysis, integrated security system.*

При проектировании интегрированных систем безопасности, на проектировщике лежит большая ответственность за выбор набор элементов. Принимаемое решение, очевидно, должно быть наилучшим из представленных альтернатив, однако рассмотреть все аспекты и детали, которые могут влиять на выбор в принятии решения практически невозможно. Естественно, есть исключения, и можно произвести расчеты и сравнения параметров вручную, но затраты и усилия для обработки такого количества информации будут огромными. Между тем, неоптимальность принимаемых решений ведет к значительным потерям времени, возможностей и ресурсов.

В наши дни на предприятиях и объектах в целях повышения технической оснащенности стали широко применяться интегрированные системы безопасности (ИСБ). Интегрированная система безопасности представляет собой аппаратно-программный комплекс технических средств, обладающих технической, информационной, программной и эксплуатационной совместимостью. Использование таких систем позволяет решать на новом качественном уровне задачи по обеспечению безопасности объектов, повышать эффективность действий службы безопасности.

Как правило, ИСБ включают в себя совместно функционирующие подсистемы охранной, тревожной, пожарной сигнализации и пожарной автоматики, телевизионную систему наблюдения (ТСН), системы контроля и управления доступом, систему защиты автоматизированных рабочих мест сотрудника службы безопасности, а также ряд дополнительных подсистем, обеспечивающих защиту от различных видов угроз. В состав ИСБ могут входить как изделия разных производителей, так и комплексы систем физической защиты объектов одной торговой марки. Все подсистемы, входящие в состав ИСБ имеют разнообразные количественные и качественные характеристики и параметры. К качественным характеристики можно отнести адаптируемость подсистемы под различные условия эксплуатации. Количественные параметры более разнообразны, к ним можно отнести

напряжение питания, тип и размеры зоны обнаружения, чувствительность, вероятность обнаружения, время наработки на ложное срабатывание и прочие. Так в результате анализа средств обнаружения по физическому принципу действия можно выделить множество видов и типов элементов.

Перед проектировщиком возникает проблема выбора элементов для построения ИСБ для конкретного объекта, что является трудной задачей в связи с большим количеством фирм-производителей, появившимся разнообразием систем и их комплектующих, а также индивидуальными особенностями объектов и запрашиваемого заказчиком решения. Перед специалистом возникает задача формирования такого набора средств защиты, который будет удовлетворять всем запрашиваемым условиям, требованиям и пожеланием заказчика.

В соответствии с ГОСТ Р 22.1.12, ГОСТ Р 50775 и ГОСТ Р 50776 в состав комплексной системы безопасности (КСБ) должны входить следующие технические подсистемы: 1) дежурно-диспетчерская; 2)производственно-технологического контроля; 3) охранной и тревожной сигнализации; 4) пожарной сигнализации; 5) контроля и управления доступом; 6) теле/видеонаблюдения и контроля; 7) досмотра и поиска; 8)пожарной автоматики; 9) связи с объектом; 10) защиты информации; 11)инженерно-технических средств физической защиты; 12) инженерного обеспечения объекта (электроосвещения и электропитания; газоснабжения; водоснабжения; канализации; поддержания микроклимата). [1, 2, 3]

Все эти подсистемы могут входить в состав ИСБ, но не все они обязательны при проектировании. Изучая требования заказчика и уже имеющиеся на объекте элементы КСБ, специалист по защите информации должен анализировать необходимость включения какой-либо из подсистем, а также и включения дополнительных подсистем с новыми качествами. Также необходимо учитывать пожелания заказчика при приобретении оборудования и осуществлении связанных с установкой и эксплуатацией материальных затрат. Не имеет смысла приобретать заведомо дорогостоящие компоненты ИСБ, если их стоимость превышает максимальный суммарный ущерб, наносимый объекту. Таким образом, в случае постановки задачи заказчиком, не предусматривающей проектирования конкретной подсистемы, а подразумевающей создание комплекса подсистем, входящих в состав интегрированной системы безопасности, необходимо начать проектирование с этапа выбора набора подсистем физической защиты, необходимых и достаточных для минимизации ущерба. Эта проблема находит свое решение в математическом методе изучения оптимальных стратегий, а именно теории игр.

Теория игр - это математические методы, изучающие поиск оптимальных стратегий в различных ситуациях. Для поиска наиболее оптимальной стратегии или нескольких альтернативных стратегий защиты информации можно провести математическую игру двух противоборствующих сторон, одной из которых является система защиты информации (компьютерной и (или) физической безопасности) на объекте, а другая подразумевающая возможные действия злоумышленника. Так как цель создания системы безопасности – это определение оптимальной стратегии злоумышленника и его действий, то можно считать, что преступник увлечен желанием нанести как можно больший ущерб этой разрабатываемой системе безопасности. [4]

Из предположения следует, что выигрыш нарушителя будет равен проигрышу «защитника», таким образом можно получить матрицу для антагонистической игры двух противоборствующих сторон с нулевой суммой. В качестве стратегий злоумышленника примем строки матрицы x_i, где $i=1,...,n$, а в качестве стратегий администратора безопасности обозначим столбцы y_j, где $j=1,...,m$. К стратегиям нарушителя отнесем различные виды действий, наносящих ущерб системе безопасности, а к стратегиям «защитника» отнесем применением им различных компонентов и подсистем интегрированных систем безопасности.

Для проведения игры необходимо знать результаты игры А при каждой паре стратегий x_i и y_j. Обозначим a_{ij} - причинённый преступником материальный ущерб, p_{ij} - вероятность нанесения ущерба при x_i. В качестве a_{ij} можно учитывать годовые материальные потери предприятия при реализации определенного типа угроз. Следует учитывать, что использование систем безопасности требует дополнительного финансирования (стоимость оборудования и его годового обслуживания), поэтому это тоже необходимо учесть при расчетах. Таким образом, необходимо построить такую стратегию y_i, при которой

сведутся к минимуму средние потери: $\sum_{i-1}^{n} a_{ij} p(x_i)$.

Для выбора оптимального набора компонентов интегрированной системы безопасности в математической игре в качестве стратегий необходимо использовать различные сочетания из угроз и методов защиты. Предположим, 1-й игрок (злоумышленник) выбирает свою стратегию *i*. В наихудшем случае он получит выигрыш min aij. Предвидя это, 1-й игрок должен выбрать свою стратегию i0 таким образом, чтобы сделать этот выигрыш лучшим:

$$\min_j a_{i_0 j} = \max_i \min_j a_{ij} \qquad (1)$$

В этом случае 2-й игрок «защитник» должен выбрать такую свою стратегию j0 чтобы получить минимальный ущерб:

$$\min_i a_{ij_0} = \min_j \max_i a_{ij} . \qquad (2)$$

Выигрыш 1-го игрока должен лежать между правыми частями формул, он называется значением игры и равен элементу a_{i0j0}. Действия «защитника» будут верными в том случае, если максимальный суммарный ущерб, нанесенный злоумышленником, будет сведен к минимуму.

Итак, ранее определили, что первый этап проектирования ИСБ состоит в определении входящих в систему подсистем. Для этого необходимо разложить математическую игру, где на стороне «защитника» будут различные компоненты и подсистемы, входящие в состав интегрированной системы безопасности, а на противоположной стороне – требования заказчика. В данном случае выполнение требования заказчика выражается, как «перекрывание» его определенной подсистемой и будет считаться наиболее благоприятным исходом. По итогу разложения игры выбирается комплекс, состоящий из выполняющих требования подсистем, достаточных для построения оптимальной интегрированной системы безопасности.

Следующий этап состоит в «наполнении» каждой подсистемы элементами. Для определения моделей оборудования и ПО раскладывается новая игра, в которой на стороне «защитника» уже будут элементы подсистем безопасности, а на стороне нарушителя – угрозы, возможные на исследуемом объекте, функции и требования, возложенные на подсистему.

На данном этапе возникает проблема расчета ущерба от реализации этих угроз. То есть, максимальный ущерб – это общее количество ресурсов, которые может потерять предприятие в случае реализации угроз нарушителем. Следовательно, при противодействии какой-то определенной угрозе или набору угроз с помощью компонентов и подсистем безопасности ИСБ, величина максимального ущерба будет уменьшаться. Но не стоит забывать, что практически все элементы системы, их установка и ежегодное обслуживание тоже несут потери ресурсов.

Таким образом, суммарный максимальный ущерб будет рассчитываться, как сумма максимального ущерба с учетом применения интегрированной системы безопасности и ресурсов, вложенных в эту систему. Ресурсы, вложенные в ИСБ, – это стоимость оборудования, стоимость его обслуживания (установка, ремонт, замена и т.д.), при необходимости, заработная плата персонала, рассчитанные за годовой период. Сумма максимального ущерба - это ежегодные потери из-за угроз, выраженные в денежном эквиваленте.

Далее предлагается рассчитать, во сколько раз уменьшится максимальный ущерб, в случае применения интегрированной системы безопасности. Для определения степени влияния того или иного продукта на величину максимального ущерба в расчеты можно ввести такой элемент, как «коэффициент влияния», который будет вычисляться на каждый компонент, программу или комплекс оборудования в отдельности, с помощью методов квалиметрической оценки качества продукции.

Термин «квалиметрия» впервые был предложен группой советских учёных еще в 1968 году. Азгальдов Г. Г., Гличев А. В. и другие научные работники предложили единую методику количественной оценки качества различных объектов и процессов. Квалиметрия - это наука о методах формирования количественных представлений о качестве, иными словами, это оценка качества, значимости и эффективности применения продукции. В настоящее время данная научная дисциплина широко используется при определении показателей качества для потребителей, оценке качества закупаемой продукции с целью анализа рынка, совершенствовании технологического процесса производства на основе потребительских требований, ведении количественных показателей качества объектов на основе учета перспектив научно-технического прогресса, различных требова-

ний и международных стандартов. Основная задача квалиметрии - это разработка методик оценки конкретного объекта или процесса, числом, характеризующим степень его соответствия предъявляемым требованиям. [5]

Оценивание объектов с помощью методов квалиметрии происходит поэтапно. На начальном этапе имеется определенный набор компонентов и подсистем интегрированной системы безопасности, которые имеют схожие характеристики и единую целевую направленность. Далее необходимо произвести оценку каждого элемента по различным критериям и определить число, характеризующее степень его соответствия предъявляемым требованиям и ожиданиям. После того, как произведен выбор оптимального компонента ИСБ на основе теории игр, необходимо с помощью квалиметрического расчета определить коэффициент влияния на максимальный суммарный ущерб (стоимость применения оборудования + максимальный ущерб от реализации угроз), наносимый предприятию до применения системы безопасности. Далее, используя полученные для каждого компонента коэффициенты влияния на максимальный суммарный ущерб, производится расчет, при котором определяется оптимальный набор компонентов и подсистем ИСБ, то есть максимальный суммарный ущерб при использовании которого будет сведен к минимуму. Таким образом, конечным этапом оценки продукта является принятие решения: «использовать» - «не использовать».

Так же следует отметить, что оптимальный набор средств защиты информации не является статичным, он может изменяться при изменении списка угроз и изменении показаний максимального ущерба. Данный вывод связан с тем, что стоимость оборудования будет различаться и может существенно влиять на величину полученного максимального суммарного ущерба. Эту зависимость мы можем наблюдать с помощью формул:

$$МСУ = МУ + СО \quad (3)$$

$$МСУ^* = МУ * К_в + СО \quad (4)$$

где МСУ – максимальный суммарный ущерб

МУ – максимальный ущерб

СО – стоимость оборудования

$К_в$ – коэффициент влияния

$МСУ^*$ - полученный максимальный суммарный ущерб

Любое набор компонентов и подсистем ИСБ можно охарактеризовать множеством различных показателей. Для расчета коэффициента влияния необходимо построить дерево общих свойств. Пример такого дерева представлен на рисунке 1:

Рис. 1. Начальные уровни дерева общих свойств

Для каждой функциональной группы компонентов и подсистем ИСБ строится свое индивидуальное дерево общих свойств, в котором выделяют только те свойства, которые влияют на качество обеспечения безопасности по своей функциональной направленности.

На следующем этапе проводится анализ, то есть количественная оценка качества на основе формирования определяющих показателей. Суть этого этапа состоит в определении весомостей показателей, получении необходимого количества определяющих показателей, используемых на последующих стадиях расчетов. Существуют десятки способов определения коэффициентов весомости. Один из самых популярных – это способ вспомогательной процентной шкалы. Такой способ является эффективным, так как для его реализации необходимо составить опрос экспертов по определенным критериям.

Для начала, составитель анкеты формирует дерево общих свойств для каждого ком-

понента и подсистемы ИСБ. Для одной функциональной группы компонентов, подсистем или программного обеспечения составляются одинаковые анкеты, так как смысл оптимизации состоит в выборе одного элемента из всей функциональной группы (например, к одной функциональной группе можно отнести объемные извещатели). Далее названия всех ветвей дерева, не имеющих последующего разветвления, записываются в анкету. Это критерии качества. Анкета отдается эксперту, которому необходимо определить оценки в баллах для каждого критерия качества продукта. В первой графе эксперт определяет степень важности критерия для продукта данной функциональной группы, во второй графе – оценку продукта по данному критерию. В данном случае экспертами выступают люди, непосредственно связанные с областью применения или активно применяющие оцениваемые продукты. Для точности расчета необходимо опросить как минимум 12 экспертов.

На следующем шаге складываются баллы первой графы оценивания и переводятся степень важности каждого критерия в проценты, затем в доли. Сумма степеней важности критериев в процентах равна 100%, в долях – 1, соответственно. Степень важности критерия (в долях) умножаем на оценку критерия и складываем с остальными показателями, получаем, в данном случае, суммарный коэффициент весомости Квес равный значению от 1 до 10. Чем больше коэффициент Квес, тем лучше элемент выполняет свои функциональные задачи.

Далее следует перевести $К_{вес}$ в доли и рассчитать коэффициент влияния:

$$К_{в} = 1 - К_{вес} \quad (5)$$

Формула 5 представлена таким образом потому, что коэффициент влияния, фактически, показывает во сколько раз, увеличится максимальный ущерб при применении данного продукта. Полученные коэффициенты влияния для конкретной модели устройства усредняются, так как анкетирование производится среди множества экспертов. Далее полученный результат подставляются в формулу 4 и рассчитывается величина максимального суммарного ущерба. Значения МСУ* сравниваются у всех продуктов одной функциональной группы. Выбирается компонент и подсистема интегрированной системы безопасности с наименьшим значением данного показателя. Исходя из положений теории игр, использование именно этого компонента (одного средства или подсистемы) будет наиболее оптимальным.

Также следует учитывать, что большое расхождение в баллах говорит о межэкспертной несогласованности. Сравнение производится отдельно по каждой ветви дерева. Уровень согласованности в зависимости от ответственности задачи устанавливают в размере ±5% для более ответственных задач и ±10% для менее ответственных задач. Если расхождения в оценках экспертов укладываются в этот интервал, то их считают согласованными. В случае, если оценки экспертов являются несогласованными, то их просят пересмотреть свои исходные оценки, анкетирование проводится повторно.

Таким образом, в настоящей статье предлагается решение проблем, возникающих при разработке проектов интегрированной системы безопасности. Методика позволяет на основе анализа требований, предъявляемых к обеспечению безопасности объекта, и индивидуальных предпочтений заказчика выбирать оптимальный набор оборудования и программного обеспечения для синтеза интегрированной системы безопасности из различных компонентов и подсистем, предложенных на рынке.

Литература

1. ГОСТ Р 22.1.12-2005 Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. - Режим доступа: http://docs.cntd.ru/document/1200039543. Дата обращения: 09.03.2018.

2. ГОСТ Р 50775 Системы тревожной сигнализации. - Режим доступа: http://www.arseng.ru/pdf/gost_r_50775-95.pdf. (Дата обращения: 09.03.2018)

3. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) Системы тревожной сигнализации. - Режим доступа: http://docs.cntd.ru/document/1200005308. (Дата обращения: 09.03.2018)

4. Гуц А.К, Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие – Издательство Омского государственного университета, 2013. – 160 с.

5. Газарян Н.В. Квалиметрия и экспертиза качества продукции и услуг: методические указания к

практическим занятиям. КубГТУ, каф. Стандартизации, сертификации и аналитического контроля. – Краснодар, 2015. – 33 с.

Refereces

1. GOST R 22.1.12-2005 Bezopasnost' v chrezvychaynykh situatsiyakh. Strukturirovannaya sistema monitoringa i upravleniya inzhenernymi sistemami zdaniy i sooruzheniy. - Rezhim dostupa: http://docs.cntd.ru/document/1200039543. Data obrashcheniya: 09.03.2018.

2. GOST R 50775 Sistemy trevozhnoy signalizatsii. - Rezhim dostupa: http://www.arseng.ru/pdf/gost_r_50775-95.pdf. (Data obrashcheniya: 09.03.2018).

3. GOST R 50776-95 (MEK 60839-1-4:1989) Sistemy trevozhnoy signalizatsii. - Rezhim dostupa: http://docs.cntd.ru/document/1200005308. (Data obrashcheniya: 09.03.2018).

4. Guts A.K, Vakhniy T.V. Teoriya igr i zashchita komp'yuternykh sistem: uchebnoye posobiye – Izdatel'stvo Omskogo gosudarstvennogo universiteta, 2013. – 160 s.

5. Gazaryan N.V. Kvalimetriya i ekspertiza kachestva produktsii i uslug: metodicheskiye ukazaniya k prakticheskim zanyatiyam. KubGTU, kaf. Standartizatsii, sertifikatsii i analiticheskogo kontrolya. – Krasnodar, 2015. – 33 s.

ХАЛИЗЕВ Вячеслав Николаевич, кандидат технических наук, профессор кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: ha53@mail.ru.

ФЕДОРОВ Сергей Юрьевич, старший преподаватель кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: iitib@rambler.ru.

ЖДАНОВА Наталья Владимировна, студентка кафедры компьютерных технологий и информационной безопасности, Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: natalia.zhdanova.kras@mail.ru

VYACHESLAV Nikolaevich Halizev, Candidate of Technical Sciences, Professor of the Department of Computer Technologies and Information Security of the Institute of Computer Systems and Information Security of FSBEI HE "Kuban State Technological University", 350072, Krasnodar, st. Moskovskaya, 2. E-mail: ha53@mail.ru.

SERGEY Yuryevich Fedorov, Senior Lecturer, Department of Computer Technologies and Information Security, Institute of Computer Systems and Information Security, FSBEI HE "Kuban State Technological University", Russia, 350072, Krasnodar, st. Moskovskaya, 2. E-mail: iitib@rambler.ru.

NATALYA Zhdanova, Student, Department of Computer Technologies and Information Security, Institute of Computer Systems and Information Security, FSBEI HE "Kuban State Technological University", Russia, 350072, Krasnodar, st. Moskovskaya, 2. E-mail: natalia.zhdanova.kras@mail.ru.

УДК 681.322 Вестник УрФО № 3(29) / 2018, с. 50–54

Карташевский В. Г., Крыжановский А. В. DOI: 10.14529/SECUR180308

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализируются возможности наиболее распространённых стандартов в области менеджмента инцидентов информационной безопасности. Анализируется методика выявления инцидентов на основе операционных и технических процедур с точки зрения управления бизнес - процессами и технической перспективы. Оцениваются возможности основных этапов (шагов): сбор информации об уязвимостях, проверка информации и оценка риска, выбор метода распространения информации. Рассмотрены возможные инциденты информационной безопасности и разработана соответствующая классификация. Сформулированы требования к техническим средствам и системам выявления инцидентов информационной безопасности.

Ключевые слова: *инциденты информационной безопасности, классификация инцидентов информационной безопасности, обнаружение инцидентов информационной безопасности и управление ими, международные и национальные стандарты менеджмента инцидентов информационной безопасности.*

Kartashevskiy V. G., Kryzhanovsky A. V.

ANALYSIS OF METHODS AND MEANS OF DETECTING INFORMATION SECURITY INCIDENTS

We analyze here the possibilities of the most common standards in the field of management of information security incident. We also analyze the methodology of incident detection based on operational and technical procedures from the point of view of business process management and technical perspective. The possibilities of the main stages (steps) are evaluated: collection of information about vulnerabilities, verification of information and risk assessment, choice of the method of information dissemination. Possible incidents of information security are considered and the corresponding classification is developed. We formulate requirements to technical means and systems of detection of information security incidents.

Keywords: *information security incidents, classification of information security incidents, detection and management of information security incidents, international and national standards of management of information security incident.*

Под инцидентами информационной безопасности (ИБ) понимаются различные происшествия, приводящие к нарушениям безопасности компании. Эти нарушения могут привести к серьёзным последствиям, поэтому сотрудники безопасности фирмы должны подготовиться к своевременному противодействию возникающим угрозам. Кроме того, специалистам, обеспечивающим, ИБ необходимо фиксировать все произошедшие на предприятии случаи нарушений безопасности для дальнейшего их анализа. Для лучшей организации процедур выявления угроз специалист должен скомпоновать обнаруженные им случаи нарушения защиты в строго выделенные группы. Данные базовые действия регламентированы соответствующими нормативными документами, поэтому каждый высококвалифицированный специалист должен строго следовать принятой политике безопасности, чтобы организовать комплекс мер по обнаружению и управлению инцидентами ИБ [1,2].

ренцировать обязанности должностных лиц в области менеджмента инцидентов ИБ, в результате риск возникновения инцидентов ИБ на предприятии значительно уменьшается [3].

В качестве примера стандарта, регламентирующего процедуры менеджмента инцидентов ИБ, рассмотрим стандарт ENISA «CSIRT Setting up Guide in Russian». Этот европейский регламентирующий документ «Пошаговое руководство по созданию CSIRT» детально описывает процесс создания Computer Security and Incident Response Team (CSIRT — группа реагирования на инциденты компьютерной безопасности) с точки зрения управления бизнес - процессами, а также технической перспективы [4].

Методика выявления инцидентов на основе операционных и технических процедур иллюстрируется на рис. 1.

Процесс обработки информации состоит из трёх основных этапов (шагов).

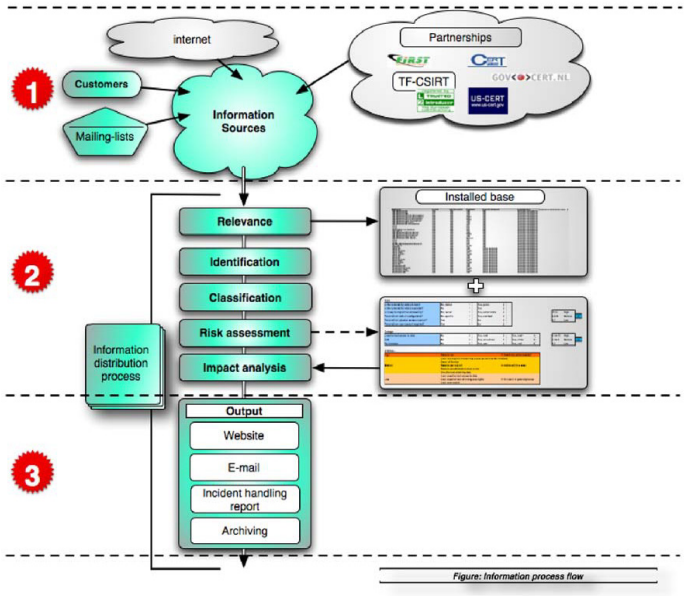


Рис.1. Процесс обработки информации

В области менеджмента инцидентов ИБ, в основном, применяются три национальных стандарта: российский (ГОСТ), европейский (ENISA-European Network and Security Information Agency -европейское агентство сетевой и информационной безопасности) и американский (NIST-National Institute of Standarts and Technology - национальный институт стандартов и технологий). Рекомендации этих стандартов помогают разграничить полномочия сотрудников компании и диффе-

Шаг 1 — сбор информации об уязвимостях.

Обычно существует два основных типа источников информации, которые предоставляют исходную информацию для сервисов:

– информация об уязвимости IT-системы;

– отчёты об инцидентах.

Шаг 2 — проверка информации и оценка риска.

Этот шаг приведёт к анализу последствий

специфической уязвимости на IT-инфраструктуру клиента. Основные критерии анализа — идентификация, актуальность и классификация.

Шаг 3 —выбор метода распространения информации.

CSIRT может выбрать один из нескольких методов распространения, в зависимости от пожеланий клиентов и корпоративной коммуникационной стратегии: веб-сайт, электронная почта, отчёты, архивирование и исследования.

Инцидентами информационной безопасности, представленными на рис. 2, являются: утрата услуг и сбой оборудования, системные сбои или перегрузки, ошибки пользователей, несоблюдение политики или рекомендаций по ИБ, нарушение физических мер защиты, неконтролируемые изменения систем, сбои программного обеспечения и отказы технических средств, нарушение правил доступа [5].

Инциденты информационной безопасности можно классифицировать по ряду признаков, изображённых на рис. 3 [6].

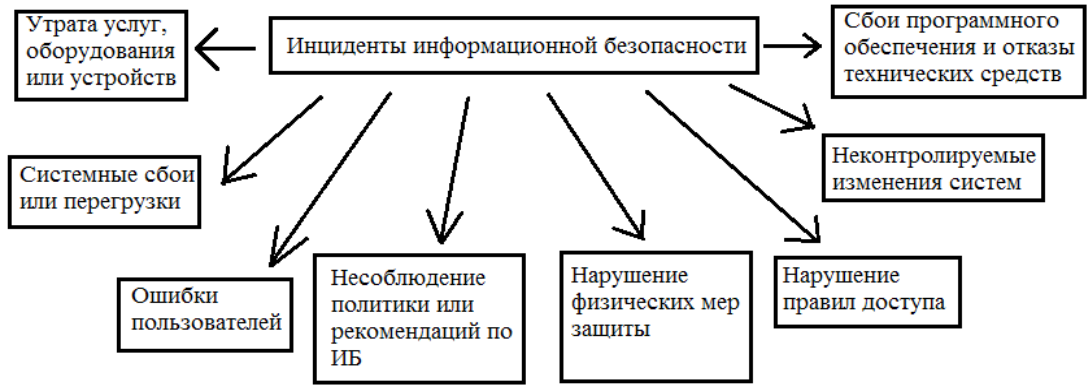


Рис. 2. Инциденты информационной безопасности

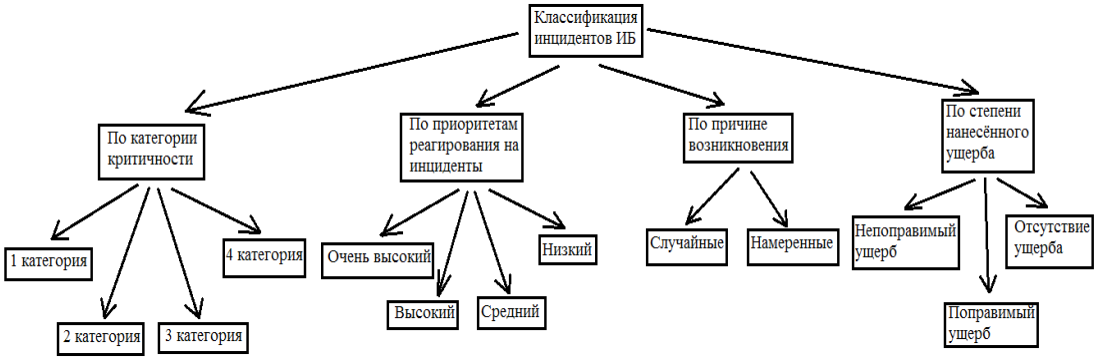


Рис. 3. Классификация инцидентов ИБ

1. По категории критичности:

1 категория: инцидент может привести к значительным негативным последствиям (ущербу) для информационных активов или репутации организации;

2 категория: инцидент может привести к негативным последствиям (ущербу) для информационных активов или репутации организации;

3 категория: инцидент может привести к незначительным негативным последствиям (ущербу) для информационных активов или репутации банка;

4 категория: инцидент не может привести к негативным последствиям (ущербу) для информационных активов или репутации.

2. По приоритетам реагирования на инциденты:

– очень высокий: соответствует 1-й категории критичности, время реагирования не более 1 часа;

– высокий: соответствует 2-й категории критичности, время реагирования не более 4 часов;

– средний: соответствует 3-й категории критичности, время реагирования не более 8 часов;

– низкий: соответствует 4-й категории критичности, время реагирования не определено.

3. По причине возникновения: случайные; преднамеренные.

4.По степени нанесенного ущерба: непо-

правимый ущерб; поправимый ущерб; отсутствие ущерба.

В качестве основных целей структурированного, хорошо спланированного менеджмента инцидентов ИБ ГОСТ 18044-2007 выделяет следующие цели [7,8]:

– обнаружение и эффективная обработка событий ИБ, выделение из их числа инцидентов ИБ;

– оценка и разрешение идентифицированных инцидентов ИБ наиболее оптимальным способом;

– минимизация негативных воздействий инцидентов ИБ соответствующими защитными мерами;

– извлечение уроков из инцидентов ИБ с целью их предотвращения в будущем, улучшения общей система менеджмента инцидентов ИБ (СМИИБ).

Литература

1. ГОСТ Р ИСО/МЭК 20000-2-2012.Издания. Международная стандартная нумерация книг. – М.: Изд-во стандартов, 2011. Часть 2 – 35 с.

2. ГОСТ Р ИСО/МЭК 27002-2013.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2014. – 104 с.

3. ГОСТ Р ИСО/МЭК 27037-2014.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2014. – 47 с.

4. СТО БР ИББС-1.3-2016.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2016. – 49 с.

5. Карташевский В.Г., Крыжановский А.В., Раков А.С. Особенности реализации в ПГУТИ ФГОС ВПО специальности 10.05.02 с учётом специфики Самарской области и отраслевой направленности вуза. Материалы XIX пленума УМО по образованию в области информационной безопасности. Научно-практический журнал «Информационное противодействие угрозам терроризма» № 25, том 2, Таганрог, 2015.-с.122-128.

6. Крыжановский А.В., Кухарев С.Н., Афанасьев В.Н. Реализация лабораторного практикума дисциплины «Информационная безопасность телекоммуникационных систем» специальности 10.05.02. Материалы XIX пленума УМО по образованию в области информационной безопасности. Научно-практический журнал «Информационное противодействие угрозам терроризма» № 25, том 1, Таганрог, 2015.- с.224-234.

7. Карташевский В.Г., Крыжановский А.В., Раков А.С., Алексеев А.П.,

8. Борисенков А.В. О подготовке специалистов в области информационной безопасности в ПГУТИ. Материалы XX юбилейного пленума федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки10.00.00 «Информационная безопасность», 23-28 ноября 2016: Москва- с.79-85.

9. Крыжановский А.В., Кухарев С.Н., Афанасьев В.Н. Применение бюджетных решений при обучении технической защите информации. Материалы XXI пленума ФУМО: труды Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности». - Самара: Изд-во Инсома-пресс, 2017. -с.111-118.

References

1. GOST R ISO/MEK 20000-2-2012.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M.: Izd-vo standartov, 2011. Chast' 2 – 35 s.

2. GOST R ISO/MEK 27002-2013.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M. : Izd-vo standartov, 2014. – 104 s.

3. GOST R ISO/MEK 27037-2014.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M. : Izd-vo standartov, 2014. – 47 s.

4. STO BR IBBS-1.3-2016.Izdaniya. Mezhdunarodnaya standartnaya nu-meratsiya knig. – M. : Izd-vo standartov, 2016. – 49 s.

5. Kartashevskiy V.G., Kryzhanovskiy A.V., Rakov A.S. Osobennosti realizatsii v PGUTI FGOS VPO spetsial'nosti 10.05.02 s uchotom spetsifiki Samarskoy oblasti i otraslevoy napravlennosti vuza. Materialy XIX plenuma UMO po obrazovaniyu v oblasti informatsionnoy bezopasnosti. Nauchno-prakticheskiy zhurnal «Informatsionnoye protivodeystviye ugrozam terrorizma» № 25, tom 2, Taganrog, 2015.-s.122-128.

6. Kryzhanovskiy A.V., Kukharev S.N., Afanas'yev V.N. Realizatsiya laboratornogo praktikuma distsipliny «Informatsionnaya bezopasnost' telekommunikatsionnykh sistem» spetsial'nosti 10.05.02. Materialy XIX plenuma UMO po obrazovaniyu v oblasti informatsionnoy bezopasnosti. Nauchno-prakticheskiy zhurnal «Informatsionnoye protivodeystviye ugrozam terrorizma» № 25, tom 1, Taganrog, 2015.- s.224-234.

7. Kartashevskiy V.G., Kryzhanovskiy A.V., Rakov A.S., Alekseyev A.P.,

8. Borisenkov A.V. O podgotovke spetsialistov v oblasti informatsionnoy bezopasnosti v PGUTI. Materialy XX yubileynogo plenuma federal'nogo uchebno-metodicheskogo ob"yedineniya v sisteme vysshego obrazovaniya po ukrupnennoy gruppe spetsial'nostey i napravleniy podgotovki10.00.00 «Informatsionnaya bezopasnost'», 23-28 noyabrya 2016: Moskva- s.79-85.

9. Kryzhanovskiy A.V., Kukharev S.N., Afanas'yev V.N. Primeneniye byudzhetnykh resheniy pri obuchenii tekhnicheskoy zashchite informatsii. Materialy XXI plenuma FUMO: trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii «Aktual'nyye problemy obespecheniya informatsionnoy bezopasnosti». - Samara: Izd-vo Insoma-press, 2017. -s.111-118.

КАРТАШЕВСКИЙ Вячеслав Григорьевич, доктор технических наук, профессор, заведующий кафедрой Информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». Россия, 443010, Самара, Льва Толстого, д.23. E-mail: kartash@psati.ru

КРЫЖАНОВСКИЙ Анатолий Владиславович, кандидат технических наук, доцент кафедры Информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». Россия, 443010, Самара, Льва Толстого, д.23. E-mail: kryzan@mail.ru

KARTASHEVSKIY Viacheslav, Doctor of Engineering Science, Professor, Head of the department of information security of the «Povolzhskiy State University of Telecommunications and Informatics», 23, L.Tolstoy str., Russia, 443010, E-mail: kartash@psati.ru

KRYZHANOVSKY Anatoly, Candidate of Engineering Science, Docent of the department of information security of the «Povolzhskiy State University of Telecommunications and Informatics», 23, L.Tolstoy str., Russia, 443010, E-mail: kryzan@mail.ru

УДК 378.046.4

Вестник УрФО № 3(29) / 2018, с. 55–61

Ветров И. А., Котенков С. М.

DOI: 10.14529/SECUR180309

НЕКОТОРЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА РФ» В КАЛИНИНГРАДСКОЙ ОБЛАСТИ НА БАЗЕ КАЛИНИНГРАДСКОГО ГОСУДАРСТВЕННОГО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ЦЕНТРА ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ (КГ НИЦ)

Статья посвящена особенностям реализации программы «Цифровая экономика РФ» в обособленном регионе Российской Федерации. Рассматриваются вопросы организации комплексной системы подготовки, переподготовки и аттестации кадров в области защиты информации, составляющей государственную, банковскую и коммерческую тайну в региональном учебно-научном центре информационной безопасности (РУНЦ ИБ) на базе Калининградского государственного научно-исследовательского центра информационной и технической безопасности (КГ НИЦ). Излагаются особенности реализации образовательных программ профессиональной переподготовки и повышения квалификации в Калининградской области.

Ключевые слова: *информационная безопасность, подготовка специалистов, инновационные технологии образовательного процесса, методы обучения, знания, умения, навыки.*

SOME QUESTIONS OF IMPLEMENTATION OF THE "DIGITAL ECONOMY OF RUSSIA" IN THE KALININGRAD REGION ON THE BASIS OF KALININGRAD STATE RESEARCH CENTER OF INFORMATION AND TECHNICAL SAFETY (KG NITS)

The article is devoted to the peculiarities of the program" Digital economy of the Russian Federation " in a separate region of the Russian Federation. The article deals with the organization of a comprehensive system of training, retraining and certification of personnel in the field of protection of information constituting state, banking and trade secrets in the regional training and research center for information security (RUNC is) on the basis of the Kaliningrad state research center for information and technical security (CG SIC). The features of realization of educational programs of professional retraining and advanced training in the Kaliningrad region are stated.

Keywords: *information security, training of specialists, innovative technologies of educational process, teaching methods, knowledge, skills.*

Экспертный прогноз потребности в специалистах по информационным технологиям в Калининградской области позволяет сделать вывод, что по мере вхождения региона в европейские интеграционные процессы и с учётом тенденций экономического развития области, спрос на этих специалистов будет устойчиво повышаться.

Учитывая особое геополитическое положение Калининградской области, как анклавной территории, полностью отделенной от остальной территории страны иностранными государствами и международными морскими водами, совершенно очевидна необходимость организации в регионе научно-обоснованной **государственной системы подготовки (переподготовки) и повышения квалификации кадров в области защиты информации.**

В настоящее время в Российской Федерации разработана целостная законодательная база, позволяющая решить указанные задачи, и базирующаяся на требованиях Доктрины информационной безопасности Российской Федерации, утверждённой Указом Президента РФ от 5 декабря 2016 г. N 646 [1], решений Межведомственной комиссии Совета Безопасности РФ по информационной безопасности и Межведомственной комиссии по защите государственной тайны, а также положений Федерального закона от 29.07.2017 N 216-ФЗ «Об инновационных научно-технологических центрах и о внесении изменений в отдельные законодательные акты Российской Федерации», программы «Цифровая экономика Российской Федерации» [2].

Таким образом, для реализации проектов по проведению научных исследований и профессиональной переподготовки специали-

стов региона в области информационной безопасности, защиты информационного пространства региона Правительством Калининградской области, как учредителем, было принято решение о корректировке формата работы Государственного автономного учреждения Калининградской области «Калининградский государственный научно — исследовательский центр информационной и технической безопасности» (далее КГ НИЦ).

По сути, на базе существующего КГ НИЦ создано новое учреждение с конкретизированными функциями и новой командой, перед которым Правительством Калининградской области поставлены достаточно серьёзные задачи в области информационной безопасности региона.

К основным задачам относятся следующие:

– проведение прикладных научных исследований в регионе по проблемам обеспечения информационной безопасности;

– создания информационных систем, комплексных систем и средств безопасности, анализа их влияния на различные аспекты региональной безопасности;

– осуществление экспертно-аналитической деятельности и консалтинга;

– проведение мониторинга развития и обеспечения безопасности информационных систем региона с целью выработки научных рекомендаций по их технической защите;

– создание учебно - научной и исследовательской, а в перспективе производственной базы в области информационной безопасности;

– создание комплексной системы повышения квалификации и переподготовки кадров в области защиты информации, составляющей государственную, банковскую и коммерческую тайну;

– аттестация объектов информатизации, средств и систем на соответствие требованиям по защите информации;

– проведение специальных проверок и исследований на ПЭМИН технических средств защиты информации;

– выполнение научно – исследовательских и инновационных работ (далее – НИИР) и экспертиз в интересах государственных и коммерческих структур по различным направлениям в области ИБ.

Таким образом, в соответствии с региональными особенностями, актуализированными потребностями и нормативными документами, от КГ НИЦ потребовалось работать в новых условиях, отвечающих современным реалиям. Для чего, в первую очередь, были пересмотрены подходы в работе по следующим направлениям:

• организация научно-исследовательской работы КГ НИЦ;

• повышение квалификации и переподготовки кадров по линии информационной безопасности в регионе;

• реализация программы интеграции в повседневную деятельность государственных и муниципальных органов Калининградской области задач информационной безопасности.

В частности, одним из этапов решения указанных задач стало создание в КГ НИЦ Научного совета, в состав которого, помимо сотрудников Центра, вошли учёные и преподаватели ВУЗов Калининграда и Санкт-Петербурга (КГТУ, БФУ, КПИ ФСБ России, ВМИ, ГУАП), ведущих подготовку специалистов по информационной безопасности, представители потенциальных работодателей региона, Правительства Калининградской области и наших партнёров со стороны коммерческих структур. Такой состав Научного совета КГ НИЦ позволил рассмотреть вопрос о совершенно новом подходе к реализации некоторых вопросов программы «Цифровая экономика РФ» таких как подготовка кадров и образование в области информационной безопасности.

Если ранее, существовало противоречие между работодателем и учебным заведением по требованиям к специалистам по информационной безопасности - каждый формировал свой взгляд и, зачастую, не мог найти «общий язык», то теперь для реализации программы совместной подготовки специалистов появилась площадка (КГ НИЦ), где эти вопросы будут обсуждаться за круглым столом и вырабатываться совместные компромиссные решения, что несомненно в будущем даст свои результаты. Это не говорит о том, что КГ НИЦ берёт на себя право вмешиваться в учебный процесс ВУЗов или регулировать требования тех или иных работодателей к выпускникам, но некоторые вопросы, для общего государственного дела по подготовке специалистов по ИБ, решить может. И самый главный вопрос, который рассмотрен на Научном совете - это т.н. вопрос «движения от работодателя к ВУЗу».

Что предлагается:

1. Формирование единой информационной образовательной среды в области ИБ для образовательных учреждений Калининградской области. Заключение договоров о научно-техническом сотрудничестве между работодателем и ВУЗом инициативно идёт от работодателя. КГ НИЦ уже подготовлены договора о сотрудничестве с учебными заведениями Калининграда, некоторые уже находятся на рассмотрении администраций ВУЗов.

2. КГ НИЦ на своей территории планирует создание учебной, научной и исследовательской (в перспективе и производственной) базы для научных исследований студентов ВУЗов и молодых учёных в целях подготовки молодых специалистов и специалистов высшей профессиональной квалификации в области информационной безопасности

3. Работа со своими сотрудниками - соискателями учёных степеней. Таких на данный момент в КГ НИЦ 5 человек. Предоставление им соответствующих условий и приоритетов, то, что не всегда может дать высшее учебное заведение, к которым они прикреплены.

4. Сотрудники Центра будут принимать участие в формировании для студентов тем научных работ, тем выпускных квалификационных работ и участие в работе государственных аттестационных комиссий.

5. Предоставление мест практик для студентов ВУЗов, и не только на базе КГ НИЦ, но и на площадках партнёров КГ НИЦ и, необязательно, с оформлением для студентов соответствующего допуска. Есть открытые проекты, в том числе и международные, в которых могут принимать участие студенты и аспиранты ВУЗов.

6. Проведение специальных мероприятий по защите интеллектуальной собственности и авторских прав ученых-исследователей и разработчиков, как основы укрепления прикладной науки и выхода на рынок высокотехнологической продукции.

7. Участие в разработке, формировании и реализации научно-технических и образовательных программ в области информационной безопасности органов государственной власти и местного самоуправления, государственных и критически важных структур и организаций независимо от их ведомственной принадлежности, координация их деятельности на обеспечении защиты информации по приоритетным направлениям науки и техники.

8. Активизация работы в научной и научно-исследовательской деятельности. Заключение научно-исследовательских работ, ОКР, участие в научных проектах и грантах. Организация на плановой основе конференций, научно-методических советов, научных семинаров и др.

9. Внедрение новых информационных технологий в образовательный процесс и оценка их эффективности, в частности, продолжение реализации проекта по разработке программных тренажёров и обучающих программ (ОП) изучения и отработки навыков эксплуатации технических средств защиты информации. Проект разработан с целью методического обеспечения дистанционного и самостоятельного обучения специалистов в области информационной безопасности и позволит изучать ТСЗИ без существенных материальных затрат на их приобретение.

10. Создание в КГ НИЦ комплексной системы подготовки, переподготовки и аттестации кадров в области защиты информации, составляющей государственную, банковскую и коммерческую тайну. Уже, по согласованию с Наблюдательным Советом КГ НИЦ, в составе Центра создан региональный учебно-научный центр информационной безопасности (РУНЦ ИБ), который уже активно начал работу по повышению квалификации работников государственной службы Правительства и муниципальных образований Калининградской области.

Объективная потребность по созданию регионального учебного научного центра в области информационной безопасности (РУНЦ ИБ) в Калининградской регионе, который взял бы на себя решение задачи формирования единого учебного, научного и производственного комплекса, обеспечивающего подготовку кадров, проведение научных исследований, развитие инноваций и повышение качества подготовки специалистов по защите информации сформировалась по следующим причинам.

Несмотря на наличие в регионе высших и средних учебных заведений, ведущих обучение по направлению подготовки «Информационная безопасность», данные образовательные учреждения не осуществляют профессиональную переподготовку и повышение квалификации для специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, орга-

нах местного самоуправления, и подведомственным им организациях, а также предприятиях оборонно-промышленного комплекса и других государственных и коммерческих структур, расположенных на территории Калининградской области.

Данный факт обусловлен слабой материально-технической базой ВУЗов региона и недостаточным уровнем их финансирования.

Ввиду вышеизложенного следует особо отметить, что профессиональная переподготовка и повышение квалификации специалистов в области информационной безопасности в Калининградском регионе фактически не проводится, что существенно осложняет деятельность учреждений и предприятий, в которых циркулирует информация ограниченного доступа. Данная проблема решается руководством этих предприятий путём направления своих специалистов по защите информации в профильные учебные центры, расположенные в других регионах РФ. В частности, учебный центр «ЦБИ» (г. Королёв, Московской области), центр повышения квалификации «ГНИИИ ПТЗИ» (г. Воронеж), учебный центр «Информзащита» (г. Москва), учебный центр «МАСКОМ» (г. Москва), учебный центр «Гамма» (г. Москва), учебный центр «Инфо-ТеКС» (г. Москва) и др.

Следует также отметить, что указанное выше обучение предполагает существенные финансовые затраты, что в условиях усугубляющегося кризиса в экономике страны становится тяжёлой нагрузкой для бюджета предприятий, вынужденных, в итоге, идти на различные непопулярные решения, либо отказываться от подобных программ обучения, нарушая закон и подвергая риску безопасность своих информационных ресурсов. Например, затраты на повышение квалификации одного специалиста по защите информации в центре повышения квалификации «ГНИИИ ПТЗИ» (г. Воронеж) по программе «Техническая защита конфиденциальной информации» в объёме 72 часа с учётом расходов на проезд и проживание в среднем составляет около 100 тыс. рублей. Для многих учреждений и предприятий региона данная сумма является крайне высокой.

С учётом сложившихся условий некоторые учебные центры предлагают образовательные услуги по профессиональной переподготовке и повышению квалификации методом дистанционного обучения. Однако, данный вид обучения при всех своих на первый взгляд преимуществах объективно проигрывает традиционному методу, предполагающему живое и непосредственное общение с преподавателем, а также дающему возможность выйти за рамки программы, что в условиях дистанционного общения в принципе невозможно. Помимо этого, следует также сказать, что большинство учебных центров ориентировано на специалистов, имеющих базовую подготовку в области информационной безопасности (или смежную с ней специальность по автоматизированным системам управления). И работающих, как правило, в отделах или службах по технической защите информации. Это требует использования нетрадиционных форм и методов обучения, ориентации образовательного процесса не на теорию, а на практику. Сегодня слушателей, обучающихся на курсах повышения квалификации, интересуют практические вопросы по обеспечению безопасности информации. Кроме того, курсы должны знакомить слушателей с новыми решениями в области информационной безопасности, которые регулярно собираются, анализируются и предлагаются вниманию слушателей профессорско-преподавательским составом, ведущим непрерывное взаимодействие и обмен информацией со специалистами, имеющими практическими навыками в области разработки и внедрения технологий защиты информации.

Основными целями создания РУНЦ ИБ КГ НИЦ явились:

Обеспечение актуальных потребностей рынка труда региона в высококвалифицированных специалистах по защите информации.

Повышение качества и доступности программ профессиональной переподготовки и повышения квалификации специалистов по защите информации и должностных лиц ответственных за организацию защиты информации, прежде всего для органов государственной власти, органов местного самоуправления и организаций с государственным участием, а также для различных групп потребителей и заказчиков кадров.

Организация совместной работы с ВУЗами, с государственными и коммерческими структурами региона по координации деятельности в учебном и учебно-методическом обеспечении решения проблем информационной безопасности.

Оказания информационных, аналитиче-

ских, консалтинговых, дилерских и других услуг по проблемам информационной безопасности, распространение передового опыта в регионе в сфере информатизации образования.

Задачи, которые будет решать РУНЦ ИБ КГ НИЦ:

1. Создание на региональном уровне комплексной системы по подготовке, повышению квалификации, переподготовке и аттестации кадров для органов государственной власти, органов местного самоуправления и организаций с государственным участием в области информатизации и информационной безопасности;

2. Формирование и совершенствование в регионе межведомственной учебно-методической и технологической баз, включая ВУЗы Калининградской области в интересах повышения качества подготовки, профессиональной переподготовки и повышения квалификации кадров в области информационной безопасности.

3. Участие в разработке, формировании и реализации учебно - методических и научно-технических программ органов государственной власти, местного самоуправления, предприятий и организаций с различной формой собственности.

4. Расширение учебно-методических и общественных связей между образованием, прикладной наукой и промышленностью.

5. Исследование и разработка правовых основ информатизациии обеспечения информационной безопасности, борьбы с преступлениями в электронно-цифровой сфере.

6. Организация работ по оказанию информационно-аналитических, информационно-справочных и инженерных услуг государственным, общественным и другим организациям в области обеспечения информационной безопасности систем, проведение консультаций юридических и физических лиц по проблемам, связанным с разработкой и функционированием региональных информационных систем в условиях внешних и внутренних дестабилизирующих факторов.

В октябре 2018 года РУНЦ ИБ приступает к реализации пилотного проекта - проведение курсов повышения квалификации для специалистов по защите информации органов государственной власти, местного самоуправления и подведомственным им организациях, а также системообразующих предприятий региона (до 72 часов).

Для успешного осуществления данного проекта определена категория слушателей:

• руководители отделов защиты информации;

• администраторы безопасности сети;

• начальники служб безопасности;

• руководители отделов автоматизации;

• специалисты, аналитики в области информационных технологий.

Разработаны учебные программы повышения квалификации:

1. «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»;

2. «Программно-аппаратные средства защиты персональных данных»;

3. «Методы и средства защиты распределенных систем обработки информации».

В целях повышения качества обучения и удобства для слушателей нами планируется применение гибкой системы обучения, которая подразумевает:

– комплектование групп по 15 - 25 человек;

– проведение занятий на базе КГ НИЦ в удобное для слушателей время;

– проведение занятий высококвалифицированными специалистами (многие имеют ученые степени и звания), обладающими практическими навыками в области разработки и внедрения технологий защиты информации, а также опытом преподавательской работы в ВУЗах г. Калининграда;

– разделение процесса обучения на нормативно-базовые, теоретические и практические занятия;

– проведение индивидуальных и групповых тренировочных занятий;

– использование оборудованных аудиторий, оснащенных профессиональной техникой классов;

– адаптацию программы курсов под конкретные требования заказчика;

– решение вопросов и консультации по проблемам слушателей путем привлечения опытных инженеров и специалистов КГ НИЦ и его партнёров;

– возможность проведения курсов на территории заказчика;

– применение различных форм и методов дистанционного обучения;

– использование инновационных разработок в образовательном процессе, а именно использование программных тренажёров, обучающих программ (ОП) и электронных

учебных пособий технических средств контроля защищённости объектов информатизации от утечки информации по техническим каналам и оценки эффективности применяемых технических средств защиты информации.

Реализация вышеизложенного проекта позволит Калининградской области осуществить:

Решение государственной задачи по централизованной подготовке специалистов по защите информации для Калининградского региона.

Устранение в кратчайший срок отставания в базовом образовании по направлению информационной безопасности среди сотрудников государственных и муниципальных органов региона, а также предприятий, организаций и учреждений, отнесённых к субъектам критических информационных инфраструктур.

Возможность организации оперативного обучения по линии ИБ в случае организационно-штатных мероприятий.

Решения проблемы по созданию системы подготовки кадров для себя и партнёров.

Возможность оперативной оценки ситуации в регионе по линии ИБ и выработки научно-обоснованных мер по устранению возникающих угроз.

Литература

1. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

2. Распоряжение Правительства Российской Федерации от 28.07.2017 г. № 1632-р. "Программа "Цифровая экономика Российской Федерации".

References

1. The decree of the President of the Russian Federation of 05.12.2016 N 646 "on approval of the Doctrine of information security of the Russian Federation".

2. Order of the Government of the Russian Federation dated 28.07.2017 № 1632-p. "Program" Digital economy of the Russian Federation".

УДК 004.04 Вестник УрФО № 3(29) / 2018, с. 62–66

Ожиганова М. И., Белов Е. Б.

DOI: 10.14529/SECUR180310

О ФОРМИРОВАНИИ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У ДЕТЕЙ И ШКОЛЬНИКОВ В ДОШКОЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ И ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕПОДХОДЫ

Целью данной работы было показать необходимость формирования культуры информационной безопасности у детей и школьников в дошкольных образовательных и общеобразовательных организациях.В данной работе предложены организационно-методические подходыдля создания системы государственного регулирования социализации детей в новом информационном социальном поле. Приведена схема, позволяющая реализовать формирование сквозной (приращиваемой) компетенции культуры информационной безопасности. Предлагаемая схема позволит обхватить максимальное количество детей и школьников, и гарантирует соответствие материалов, поставленным задачам, поскольку формирование системы знаний будет осуществляться специалистами, профессионально работающими в сфере образования по информационной безопасности.

Ключевые слова: *информационная безопасность, система знаний, культура информационной безопасности, образовательные методики.*

Ozhiganova M. I., Belov E. B.

ABOUT FORMING THE CULTURE OF INFORMATION SECURITY IN CHILDREN AND SCHOOLBOYS IN PRESCHOOL EDUCATIONAL AND SCHOOL ORGANIZATIONS. ORGANIZATIONAL-METHODICAL APPROACHES

The purpose of this work was to show the necessity of forming a culture of information security in children and schoolchildren in pre-school educational and general educational organizations. In this paper, organizational and methodological approaches are proposed for creating a system of state regulation of the socialization of children in a new information social field. The scheme allowing to realize formation of the through (incremental) competence of the culture of information security is given.The proposed scheme will allow to encompass the maximum number of children and schoolchildren, and guarantees the compliance of the materials with the assigned tasks, since the formation of a knowledge system will be carried out by professionals who work in the field of information security education.

Keywords: *information security, knowledge system, information security culture, educational methods.*

Конкурентоспособность страны, ее национальный суверенитет, экономический рост и качество жизни граждан в значительной степени зависят от уровня развития производственных отношений общества. Современные условия вводят в экономику страны принципиально новые виды производительных сил: электронно-вычислительная и компьютерная техника, информационные и коммуникационные технологии, технологические инновации, направленные на развитие информационного общества и формирование национальной цифровой экономики.[1,2] Этот тезис нашел подтверждение в «Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» и в программе «Цифровая экономика Российской Федерации». Успех нашей страны зависит от уровня информационной грамотности общества, на повышение которого направлена работа образовательных учреждений с самого раннего возраста. Знакомство детей с компьютером происходит в достаточно раннем возрасте. Немногим ранее в детском саду компьютер, соединяясь с различными направлениями образовательных процессов, использовался для обновления форм и методов работы с детьми, т.е. являлся средством преобразования предметно-развивающей среды ребенка. А сегодня дошкольные образовательные учреждения реализуют учебные программы по информатике для детей от 4-х лет.

Если мы рассматриваем общество через производственные отношения, то термин «цифровое общество» вполне актуален. Прогресс производственных сил всегда лежит через ломку существующих экономических отношений. А значит, новые производительные силы привнесут в общественные результаты не только позитивные изменения, но будут выступать и как источник вредного воздей-

ствия на человека и общество. [3] Следовательно, вместе с компетенциями в области информационных технологий в нашу жизнь приходит и необходимость соблюдения культуры информационной безопасности.

Одним из направлений обеспечения информационной безопасности в области науки, технологий и образования, согласно Доктрине информационной безопасности РФ, является обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности. [4] Отдельное внимание необходимо уделить подрастающему поколению. Стремительное развитие информационных технологий заставило современное поколение детей и подростков столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях гиперинформационного общества.Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно-телекоммуникационной сетью «Интернет», которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы. Главным образом это происходит в тех случаях, когда родители (законные представители) в семье отстраняются от своих обязанностей по воспитанию и развитию детей и перекладывают их на внешних игроков.[5]

Новое общество, которое не будет способствовать духовному становлению молодёжи, а следовательно, своему преображению, обречено. Старшее поколение во все времена, отставая от перемен, внушая правила своего времени в форме стереотипов и назиданий, вызывает отторжение своего жизненного опыта молодежью.[6]Сейчас эта проблема стоит особенно остро, т.к. зачастую уже школьники разбираются в современных информационных технологиях лучше своих родителей. Молодое поколение формирует свою ценностную систему, которая, во-первых, их сразу отделяет от старшего поколения и возможности их влияния своим опытом; во-вторых, открывает перспективы личностного роста. А значит, в помощь семье необходимо выстроить систему государственного регулирования социализации детей, прививая им культуру информационной безопасности.

Рассматривая определение культуры как комплекса знаний, верований, искусств, законов, морали, обычаев и других способностей и привычек, обретённых человеком как членом общества, можно, проведя параллели, охарактеризовать культуру информационной безопасности как поведенческий комплекс, основанный на знании особенностей коммуникации в информационной среде и нравственно-этических норм современного общества. Лаконичность определения требует раскрытия основных блоков. Особенности коммуникации в информационной среде представлены рисками деструктивных информационных воздействий и правилами защиты от них. По сути, это основы информационной безопасности, а нравственно-этические нормы определяют поведение, способствующее эффективной коммуникации, продуктивной совместной деятельности, с возможностью защитить свой личный мир.[7] Как отметил Патриарх Кирилл, только в душе человека могут быть выстроены нравственные рубежи, защищающие от той информации, что несет ему современный мир.[8]

Каким образом максимально быстро и эффективно донести знания по информационной безопасности до населения? Самый широкий обхват молодежи, безусловно, даст система образования: дошкольная подготовка, школьная и последующие уровни. Целесообразно во все программы по информатике ввести компоненты культуры информационной безопасности. Но такиеобразовательные программы ещё не разработаны в полном объеме, а формировать у учащихся элементарные представления из области Информационной безопасности нужно уже сейчас. В такой ситуации особую значимость приобретают усилия профессионалов высшего образования по подготовке качественного, адаптированного под особенности возрастных групп, контента. И активность волонтеров в донесении этого контента до адресата. Таким образом, мы определяем два смежных вида деятельности:

– нормативно-педагогическая (деятельность воспитателя, учителя, преподавателя);

– общественно-просветительская (общественное движение, центром которого становятся кафедры Информационной безопасности).

Эта схема позволит обхватить максимальное количество детей и школьников, и гарантирует соответствие материалов, поставлен-

ным задачам, поскольку формирование системы знаний будет осуществляться специалистами, профессионально работающими в сфере образования по информационной безопасности.

Базовые компетенции необходимо определить для, минимум, 4-х групп:

1. Дошкольный уровень;
2. Младшая школа;
3. Средняя школа;
4. Старшая школа и студенты техникумов и колледжей.

Первоочередной задачей становится разработка содержания учебных программ для всех уровней, с обеспечением их преемственности, исходя из потребностей общества и возможностей обучающихся. Безусловно, при разработке программ для разных учебных уровней, необходимо учитывать особенности возрастного развития психики, тип ведущей деятельности, физические особенности контингента. Это требование определяет и форму, и содержание контента, и образовательные технологии.

Цель всех этих действий – сформировать систему знаний культуры информационной безопасности, позволяющую начать освоение базовых моментов (положений) в старшем дошкольном возрасте и развивать соответствующие компетенции на каждом последующем уровне обучения.

Формирование сквозной (приращиваемой) компетенции культуры информационной безопасности, позволит выпускнику школы уверенно ориентироваться в информационном обществе, получение знаний в области цифровых технологий станет осознанным и внутренне мотивированным процессом. В конечном итоге это даст молодому человеку возможность занять эффективную деятельностную позицию в экосистеме цифровой экономики России.

Литература

1. Http://www.consultant.ru/document/cons_doc_LAW_216363/ Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

2. Http://www.consultant.ru/document/cons_doc_LAW_221756/Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»».

3. К. В. Островитянов Д. Т. Шепилов Л. А. Леонтьев И. Д. Лаптев И. И. Кузьминов Л. М. Гатовский. Политическая экономия. Учебник. М.: Государственное издательство политической литературы, 1954.

4. http://www.consultant.ru/document/cons_doc_LAW_208191/ Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

5. http://www.consultant.ru/document/cons_doc_LAW_190009/ Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей».

6. А. Д. Костюков. Конфликт поколений. // Чтения молодых ученых. Материалы международной научно-практической конференции . Сер. «Научный вестник» 2015. С. 25-30.

7. А.А.Малюк. Глобальная культура кибербезопасности. М.: Горячая линия – Телеком, 2018.

8. https://pravoslavie.ru/56460.html Рубежи истории - рубежи России.

Refereces

1. Http://www.consultant.ru/document/cons_doc_LAW_216363/ Ukaz Prezidenta RF ot 09.05.2017 N 203 "O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017 - 2030 gody".

2. Http://www.consultant.ru/document/cons_doc_LAW_221756/Rasporyazheniye Pravitel'stva RF ot 28.07.2017 N 1632-r «Ob utverzhdenii programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii"».

3. K. V. Ostrovityanov D. T. Shepilov L. A. Leont'yev I. D. Laptev I. I. Kuz'minov L. M. Gatovskiy. Politicheskaya ekonomiya. Uchebnik. M.: Gosudarstvennoye izdatel'stvo politicheskoy literatury, 1954.

4. http://www.consultant.ru/document/cons_doc_LAW_208191/ Ukaz Prezidenta RF ot 05.12.2016 N 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii".

5. http://www.consultant.ru/document/cons_doc_LAW_190009/ Rasporyazheniye Pravitel'stva RF ot 02.12.2015 N 2471-r «Ob utverzhdenii Kontseptsii informatsionnoy bezopasnosti detey».

6. A. D. Kostyukov. Konflikt pokoleniy. // Chteniya molodykh uchenykh. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii . Ser. «Nauchnyy vestnik» 2015. S. 25-30.

7. A.A.Malyuk. Global'naya kul'tura kiberbezopasnosti. M.: Goryachaya liniya – Telekom, 2018.

8. https://pravoslavie.ru/56460.html Rubezhi istorii - rubezhi Rossii.

ОЖИГАНОВА Марина Ивановна, доцент кафедры «Информационная безопасность», Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет». 299053, г. Севастополь, ул. Университетская, д. 33. E-mail: vip.tapki@list.ru

БЕЛОВ Евгений Борисович, заместитель председателя Совета УМО вузов России в области информационной безопасности. Учебно-методическое объединение по образованию в области информационной безопасности, г. Москва. E-mail: umoib@yandex.ru

OZHIGANOVA Marina, docent of the department "Information security", Federal state autonomous educational institution of higher education "Sevastopol state university". 299053, Sevastopol, ul. Universitetskaya, 33.

BELOV Evgeniy, Deputy Chairman of the Council of the UMO of Russian Higher Education Institutions in the Field of Information Security. Educational-methodical association on education in the field of information security, Moscow. E-mail: umoib@yandex.ru

УДК 004.946, 008.2 Вестник УрФО № 3(29) / 2018, с. 67–73

Максимова Е. А., Молодцова И. А., Бердник М. В. DOI: 10.14529/SECUR180311

ИНФОРМАЦИОННАЯ ГИГИЕНА КАК ФАКТОР ПРЕДОТВРАЩЕНИЯ ПОСЛЕДСТВИЙ Z-ЦИФРОВИЗАЦИИ

Реализация программы «Цифровая экономика Российской Федерации» предусматривает наращивание темпов цифровизации без сопровождения комплекса мероприятий, связанных с мониторингом влияния информационных процессов на жизнь и здоровье людей. Для предотвращения негативных последствий в переходном периоде в первую очередь на z-поколение, с целью предупреждения отрицательного воздействия и оптимизации благоприятного влияния информации на психическое, физическое и социальное благополучие, профилактики заболеваний, связанных с информацией, оздоровления окружающей информационной среды, предлагается введение информационной (цифровой) гигиены, как элемента цифровой культуры личности.

В новых условиях необходима оценка индивидуальных рисков воздействия разных видов информации и прогнозирование их последствий для z-поколения с последующей разработкой необходимых программ и документов. Поэтому, предлагается рассматривать «информационную гигиену» как систему мер сопровождения индивидуума при формировании, реализации и развитии ключевых компетенций цифровой экономики.

Ключевые слова: *цифровизация, z-поколение, информационная (цифровая) гигиена, цифровая экономика, программа развития.*

Maksimova E. A., Molodtsova I. A., Berdnic M. V.

INFORMATIONAL HYGIENE AS PREVENTION FACTOR OF DIGITALIZATION Z-GENERATION

The implementation of the program "Digital Economy of the Russian Federation" provides for increasing the pace of digitalization without the accompaniment of a complex of activities related to monitoring the impact of information processes on the life and health of people. To prevent negative consequences during the transition period, primarily the z-generation, in order to prevent negative impact and optimize the beneficial effect of information on mental, physical and social welfare, prevent diseases related to information, and improve the environment, an information (digital) hygiene, as an element of digital personality culture.

In the new conditions, it is necessary to assess the individual risks of exposure to different types of information and to predict their consequences for the z-generation, and then to develop the necessary programs and documents. Therefore, it is suggested to consider "information hygiene" as a system of measures to accompany an individual in the formation, implementation and development of key competences of the digital economy.

Keywords: *digitalization, z-generation, information (digital) hygiene, digital economy, development program.*

В настоящее время, в России реализуется программа «Цифровая экономика Российской Федерации» [1] (далее – Программа), определяющая цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики. Для управления Программой определены базовые направления, в том числе - информационная безопасность. В утвержденном плане мероприятий по направлению «Информационная безопасность» по итогам заседания Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 18 декабря 2017 года, по Программе обозначено «Формирование культуры информационной безопасности у детей и школьников дошкольных образовательных и общеобразовательных организаций». Следует отметить, что в каждом субъекте РФ по результатам реализации этих мероприятий должно быть охвачено не менее 30% детей и подростков в возрасте от 6 до 16 лет.

Законодательством РФ защита детей от информации, причиняющей вред их здоровью и (или) развитию регламентирована рядом ФЗ, в том числе [2-5]. Кроме того, в качестве одного из основных направлений обеспечения ИБ в области образования, науки и технологий определено: обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности [6].

В утвержденном по итогам заседания Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 9 февраля 2018 года плане мероприятий по направлению «Кадры и образование» Программы особое внимание уделено вопросам цифрового контента, программного обеспечения и требований к цифровой образовательной среде граждан с ограниченными возможностями здоровья (ОВЗ) и инвалидностью при участии компаний цифровой экономики. Однако, на наш взгляд, наращивание темпов цифровизации должно сопровождаться комплексом мероприятий, связанных с мониторингом их влияния на жизнь и здоровье людей. При этом необходимо создание новых норм, правила и методик работы.

Кроме того, считаем, что в рамках реализации Программы показатели целей устойчивого развития должны быть детализированы с учетом возрастного критерия, что подтверждается выполненной нами оценкой демографической ситуации (таблица 1).

В реальной жизни временные границы между поколениями могут варьироваться исходя из географического, политического и экономического положения региона. Для данного анализа возрастные группы выбраны в соответствии с концепцией цифровых поколений Н. Хоува и В. Штраусса [7, 9].

В условиях современных психологических нагрузок, с более активным использованием цифровых технологий, которое будет возрастать при переходе к цифровой экономике, на фоне увеличения числа факторов риска нарушений здоровья, появился новый фактор риска – информационный. Международной классификацией болезней (МКБ-10) определены нозологические формы, имеющие этиологическую связь с влиянием информации. На фоне роста традиционных заболеваний возникли новые информационно-зависимые синдромы - компьютерный; аддикции (патологические зависимости от телевидения, социальных сетей); депрессии, формируемые социальными сетями; интернет-зависимые психозы; мании – сенсорные, связанные с интернетом, лудомания (зависимость от компьютерных игр), фобии (номофобия - боязнь остаться без связи). По данным ВОЗ новые «информационные» заболевания должны быть внесены в Международную классификацию болезней 11 пересмотра (МКБ-11) в 2018 году. Например, интернет-зависимость, цифровая паранойя и т.д. Особую опасность представляют интернет-зависимые суициды.

По данным ВОЗ, за последние 30 лет значительно возросло число суицидов среди детского населения. В мире средний показатель составляет 7 случаев на 100 тыс. населения. В России с начала 1990-х годов коэффициент самоубийств среди подростков (поколение Y и Z) почти удвоился. Наибольшее

Таблица 1

Динамика численности населения РФ по поколениям и возрастным группам за 1926-2018гг

70 и более	65-69	60-64		50-59	45-49	40-44	35-39	30-34	25-29	20-24	15-19		10-14	5-9	0-4	в том числе в возрасте, лет:	Всего дети 0--19 лет	Все население		
2212	1721	2430		2787	3790	4348	5171	5420	7324	2024	10947		10994	9420	14114		45475	92681	молчаливое поколение 1923–1943	1926
2426	2079	2775		3332	4268	5315	7240	8820	10454	8732	9495		14158	11735	13806		49194	108377		1939
4303	2664	3590		4751	7167	6177	6423	11103	10591	8744	8975		8501	12415	13353		43244	117534	«беби-бумеры» 1943-1963	1959
5806	4181	5510		6874	6698	10925	9327	11708	7102	11522	12291		13202	11975	9326		46794	129941	поколение X 1964–1984	1970
8200	5492	5065		5596	9376	10485	8399	8016	11902	9706	12385		9512	9707	10523		42127	137410		1979
9646	4510	8360		8399	7955	7663	11684	12863	12557	12995	9968		10592	11360	12032		43952	147022	поколение «миллениума» 1983-2003	1989

Динамика численности населения РФ по поколениям и возрастным группам за 1926-2018гг

12469	6345	7983		5347	11606	12546	10216	9836	10613	9755	12801		10406	6941	6399		36547	145167	поколение Z 2001-2020	2002
12325	7021	6387		6466	11891	12155	9665	10030	10797	11466	12544		9314	6762	6660		35280	144134		2004
12242	7567	5213		7737	11906	11641	9416	10228	10879	118870	12212		8604	6583	6916		34315	143801		2005
12358	7699	4458		8724	12070	10925	9427	10316	11054	12081	11852		7940	6511	7066		33369	143236		2006
12605	7572	4408		9164	12084	10325	9485	10466	11130	112298	11244		7458	6503	7234		32439	142863		2007
13111	6687	5014		9501	11929	9800	9705	10537	11358	2457	10485		7056	6638	7433		31612	142748		2008
13554	5565	5916		9755	11634	9409	9885	10696	11667	12389	9650		6891	6783	7671		30995	142737		2009
14210	4002	7832		10022	10672	9241	10172	10980	11982	12169	8389		6610	7091	7968		30058	142857		2010
14219	3913	7982		10063	10561	9251	10211	11016	12012	12122	8237		6601	7117	8051		30006	142865		2011
14380	3896	8380		10215	10023	9340	10380	11116	12328	11599	7631		6567	7261	8380		29839	143056		2012
14099	4453	8690		10382	9545	9563	10459	11346	12556	10849	7152		6689	7441	8687		29969	143347		2013
13587	5269	8949		10634	9187	9750	10614	11660	12522	9971	6956		6823	7662	8899		30340	143667		2014
13377	6428	9260		10873	9140	10122	10884	12092	12620	9293	6829		7126	8004	9262		31221	146267		2015
13086	7263	9445		11093	9193	10220	11098	12219	12412	8445	6731		7254	8218	9512		31715	146545		2016
13230	7637	9610		11155	9280	10381	11194	12537	11879	7828	6690		7408	8558	9582		32238	146804		2017
13506	7937	9783		9372	9499	10453	11425	12766	11120	7336	6816		7598	8873	9347		32634	146880		2018

значение этого показателя отмечалось в 2002 году, с 2005 года - 19 - 20 случаев на 100 тыс. человек. По информации Следственного комитета России число детских суицидов (поколение Z) возросло за пять месяцев 2015 года на 28%, в 2016 году - на 57%.

Сегодня, для детей и подростков реальным является мир виртуальный, с соответствующими последствиями в реальном мире [8]. У современных подростков и молодежи отмечается подмена ведущей деятельности учебной и трудовой, на игровую, которая характерна для дошкольников и младших школьников. Результаты многочисленных исследований подтвердили, что самоубийства среди подростков в ряде случаев обусловлены их общением в Интернете (например играми «Синий кит», «Тихий дом» и др.). Поэтому необходимо разрабатывать инновационные подходы, позволяющие использовать современные возможности социальных сетей и других средств коммуникации при общении между поколениями.

В этой связи считаем актуальным развитие нового направления - информационная (цифровая) гигиена. Целью данного направления видим как «предупреждение отрицательного воздействия и оптимизация благоприятного влияния информации на психическое, физическое и социальное благополучие отдельного человека, социальных групп, и населения в целом, профилактика заболеваний населения, связанных с информацией, оздоровление окружающей информационной среды».

Под информационной гигиеной в данном случае мы понимаем элемент цифровой культуры личности. Предлагаем рассматривать «информационную гигиену» как систему мер сопровождения индивидуума при формировании, реализации и развитии ключевых компетенций цифровой экономики.

Цифровая гигиена, на наш взгляд, должна предусматривать:

1) изучение характеристик и закономерностей информационных носителей, процессов и потоков; восприятия, переработки, хранения и производства новой информации; зависимости индивидуального и общественного здоровья от информации;

2) определение гигиенических нормативов информации, информационной среды, информационных сетей и процессов;

3) разработку санитарных мероприятий по организации информационных сетей и процессов, гигиенически обоснованного производства, распространения, потребления, хранения, воспроизведения информации;

4) оптимизацию информационно-интеллектуальной деятельности в том числе в эргатических системах «человек - машина - информационная среда», в рамках системы формирования ключевых компетенций цифровой экономики;

5) обоснование гигиенического информационного поведения.

Информационная гигиена должна представлять собой специальный междисциплинарный раздел науки, взаимосвязанный с гигиеной, физиологией, биологией, биохимией, математикой, физикой, информатикой, психологией, информационной безопасностью, конфликтологией и другими науками.

К объектам информационной гигиены необходимо отнести человека, социальные группы, население в целом; информацию, информационную среду, закономерности информационных процессов; сигналы-носители информации, процессы, базы данных, технологии; санитарную статистику, информационно-зависимые здоровье, заболеваемость, смертность населения; социальные группы и население в целом; профилактические мероприятия по оздоровлению окружающей информационной среды. В этой связи, среди факторов риска нарушений здоровья можно выделить такие группы факторов цифровой среды, как контентные, коммуникационные, технические, зональные, психо-эмоциональные.

Следует обозначить некоторые принципы информационной гигиены: комплексность, целенаправленность, социально-политическая активность, научность, доступность, целостность, системность, качественно-количественного подхода при анализе полученных данных, последовательность, непрерывность защиты, простота применения защитных методов и средств, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты, обоснованность доступа, персональная ответственность и другие.

Таким образом, развитие цифровой экономики в России предполагает становление цифровой гигиены для создания полноценной системы формирования ключевых компетенций цифровой экономики, профилактики негативного влияния информационной

нагрузки от разных источников на здоровье населения. Необходимы расчет индивидуальных рисков воздействия разных видов информации и прогнозирование их последствий для здоровья подрастающего поколения с последующей разработкой программ профилактической и оздоровительной работы, что требует изменений в общеметодологические оценки, гигиенические регламентации, технологии управления санитарно - эпидемиологическим благополучием населения, особенно детского. Для этого Россия располагает научным потенциалом и современными технологиями в сфере информационной безопасности, гигиены, охраны и укрепления здоровья детей, подростков и молодежи.

Литература

1. Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс]: Распоряжение от 28 июля 2017 г. №1632. URL: http://government.ru/docs/28653/ (дата обращения: 10.09.2018).

2. Конституция Российской Федерации [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 16.09.2018).

3. «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]: Федеральный закон N 139-ФЗ от 29 декабря 2010 года. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102144583/ (дата обращения: 16.09.2018).

4. «О государственном языке Российской Федерации» [Электронный ресурс]: Федеральный закон N 53-ФЗ от 1 июня 2005 года. URL: http://www.consultant.ru/document/cons_doc_LAW_53749/ (дата обращения: 16.09.2018).

5. «О связи» [Электронный ресурс]: Федеральный закон № 126-ФЗ от 7 июля 2003 года (с изменениями на 3 августа 2018 года). URL: http://docs.cntd.ru/document/901867280/ (дата обращения: 16.09.2018).

6. Доктрина информационной безопасности в Российской Федерации [Электронный ресурс]: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ 4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения 10.09.2018).

7. Максимова, О.А. «Цифровое» поколение: стиль жизни и конструирование идентичности в виртуальном пространстве / О.А. Максимова // Вестник Челябинского государственного университета. - 2013. - № 22 (313). - Вып.81. - С. 6-10.

8. Максимова, Е.А., Евдокимова, Е А. Технологии недопущения распространения угрозы информации, приводящей к негативным последствиям / Е.А. Максимова, Е.А. Евдокимова // Вестник ВолГУ. - Сер. 10, Иннов. деят. - 2017. - №2 (25). - С.16-21.

9. Ожиганова, Е.М. Теория поколений Н. Хоува и В. Штрауса Возможности практического применения / Е.М. Ожиганова // Бизнес-образование в экономике знаний. - 2015. - №1. - С. 94-97.

References

1. Ob utverzhdenii programmy «Tsifrovaya ekonomika Rossiyskoy Federatsii» [Elektronnyy resurs]: Rasporyazheniye ot 28 iyulya 2017 g. №1632. URL: http://government.ru/docs/28653/ (data obrashcheniya: 10.09.2018).

2. Konstitutsiya Rossiyskoy Federatsii [Elektronnyy resurs] // SPS «Konsul'tantPlyus». URL: http://www.consultant.ru/ (data obrashcheniya: 16.09.2018).

3. «O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorov'yu i razvitiyu» [Elektronnyy resurs]: Federal'nyy zakon N 139-FZ ot 29 dekabrya 2010 goda. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102144583/ (data obrashcheniya: 16.09.2018).

4. «O gosudarstvennom yazyke Rossiyskoy Federatsii» [Elektronnyy resurs]: Federal'nyy zakon N 53-FZ ot 1 iyunya 2005 goda. URL: http://www.consultant.ru/document/cons_doc_LAW_53749/ (data obrashcheniya: 16.09.2018).

5. «O svyazi» [Elektronnyy resurs]: Federal'nyy zakon № 126-FZ ot 7 iyulya 2003 goda (s izmeneniyami na 3 avgusta 2018 goda). URL: http://docs.cntd.ru/document/901867280/ (data obrashcheniya: 16.09.2018).

6. Doktrina informatsionnoy bezopasnosti v Rossiyskoy Federatsii [Elektronnyy resurs]: Ukaz Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № 646. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ 4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (data obrashcheniya 10.09.2018).

7. Maksimova, O.A. «Tsifrovoye» pokoleniye: stil' zhizni i konstruirovaniye identichnosti v virtual'nom

prostranstve / O.A. Maksimova // Vestnik Chelyabinskogo gosudarstvennogo universiteta. - 2013. - № 22 (313). - Vyp.81. - S. 6-10.

8. Maksimova, Ye.A., Yevdokimova, Ye A. Tekhnologii nedopushcheniya rasprostraneniya ugrozy informatsii, privodyashchey k negativnym posledstviyam / Ye.A. Maksimova, Ye.A. Yevdokimova // Vestnik VolGU. - Ser. 10, Innov. deyat. - 2017. - №2 (25). - S.16-21.

9. Ozhiganova, Ye.M. Teoriya pokoleniy N. Khouva i V. Shtrausa Vozmozhnosti prakticheskogo primeneniya / Ye.M. Ozhiganova // Biznes-obrazovaniye v ekonomike znaniy. - 2015. - №1. - S. 94-97.

МАКСИМОВА Е. А., ФГАОУ ВО «Волгоградский государственный университет», г. Волгоград, проспект Университетский, д.100, E-mail: maksimova@volsu.ru, E-mail: infsec@volsu.ru

МОЛОДЦОВА И. А., кандидат медицинских наук, магистрант кафедры информационной безопасности ФГАОУ ВО «Волгоградский государственный университет». Россия, 400062, г. Волгоград, проспект Университетский, д 100. E-mail: infsec@volsu.ru

БЕРДНИК М. В., Кубанский государственный технологический университет (КубГТУ). 350072, Россия, Краснодарский край, Краснодар, ул. Московская, д. 2. E-mail: marviktr@mail.ru

MAKSIMOVA E. A., Volgograd State University prospectus Universitetsky, 100, 400062 Volgograd, Russian Federation. E-mail: maksimova@volsu.ru, E-mail: infsec@volsu.ru

MOLODTSOVA I. A., candidate of medical Sciences, student of information security Department FSAEI HE «Volgograd State University», Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation, E-mail: infsec@volsu.ru

BERDNIC M. V., Kuban State Technological University (KubGTU). 350072, Russia, Krasnodar Region, Krasnodar, ul. Moscow, 2. E-mail: marviktr@mail.ru

УДК 681.518 Вестник УрФО № 3(29) / 2018, с. 74–78

Московченко В. М., Шилина А. Н.

DOI: 10.14529/SECUR180312

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ РАСЧЕТА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССАХ

В работе приведено описание последовательности решения задач управления обеспечением безопасности автоматизированной системы управления производственными и технологическими процессами, разработаны предложения по совершенствованиюметодики оценки эффективности качества управления системой обеспечения безопасности.

Ключевые слова: *информационная безопасность, автоматизированные системы управления производственными и технологическими процессами, эффективность управления, система обеспечения безопасности.*

IMPROVEMENT OF THE METHOD OF CALCULATION OF INDICATORS OF EFFICIENCY OF MANAGEMENT OF THE SECURITY SYSTEM OF AUTOMATED CONTROL SYSTEMS IN TECHNOLOGICAL PROCESSES

The paper describes the sequence of solving the problems of managing the security of the automated control system for production and technological processes, developed proposals to improve the methodology for assessing the effectiveness of quality management system security.

Keywords: *Information security, automated control systems for production and technological processes, management effectiveness, security management system.*

Основными целями создания и внедрения автоматизированных систем управления (АСУ) являются: повышение качества (эффективности) управления путем упорядочения и ускорения информационных процессов; оптимизация и ускорение оперативно-технических расчетов; научное обоснование принимаемых решений; освобождение должностных лиц от нетворческой (рутинной) работы.

Совокупность технических, программных средств и системы организационных мероприятий реализует информационную технологию, которая предназначена для автоматизации информационных процессов в профессиональной деятельности иопределяется ролью и местом в системе управления, спецификой решаемых задач и уровнем в иерархии управления.

Автоматизированные системы управления в производственных и технологических процессах (АСУ ТП) — это комплекс программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях (автоматизация производства) [1].

Особую роль АСУ играют в автоматизации технологических процессов вкритических информационных инфраструктурах (КИИ), т.е. объектах критической информационной инфраструктуры, а так же сетях электросвязи, используемых для организации и функционирования таких объектов [2].

Широкое применение АСУ в производственных и технологических процессах на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природы различного назначения ставит вопрос об обеспечении защиты информации, требования к которой закреплены приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 [2]. Решением этой задачи становится вопрос создания и использования АСУ для обеспечения безопасности производственных и технологических процессов, а так же о проведении оценки их эффективности.

С этой точки зрения, несмотря на отличия задач решаемых АСУ различного назначения, звена управления, структурной топологии, используемых аппаратно-программных средств, методическая основа оценки эффективности должна быть унифицированной. Данную методику следует рассматривать с позиции верифицированности оценки эф-

фективности решения конечных задач стоящих перед системой обеспечения безопасности (СОБ) в целом.

Совокупность свойств СОБ определяется выбранным и обоснованныммножествомпоказателей качества ,определяющих успешность решения стоящих перед СОБ задач[3]:

$$\sum_{q}^{1} n_q \in \boldsymbol{Z}, \quad (1)$$

*где q= 1,2,…,**Z**.*

При этом, значения всех показателей качества СОБ «закрепляются» в ее созданном варианте

$$n_q = n_q(\boldsymbol{X}), q = 1, 2, \ldots, \boldsymbol{Z}, \quad (2)$$

где ***X*** – множество реализованных характеристик защищаемого объекта и его СОБ (топология, инженерно-технические средства, алгоритмы работы, численность и квалификация персонала и т.п.).

Отличие показателя эффективности обеспечения безопасности АСУ ТП от остальных показателей качества будет заключаться в следующем:

1) содержание (вид) показателя эффективности АСУ ТП зависит от конкретной решаемой системой $з_{ij}$-й задачи по обеспечению защиты *i*-го объекта АСУ от *j*-гонегативного воздействия, а его величина определяется степенью достижения цели решения этой задачи;

2) численное значение показателя эффективности АСУ ТП $W^{АСУ}$ зависит отчисленного значения функционала показателей её качества, т.е.

$$W^{АСУ} = \sum_{q}^{1} n_{\boldsymbol{Z}}^{АСУ} = W^{АСУ}(з_{ij}, n_q^{АСУ} \in \boldsymbol{Z}^{АСУ}, q = 1, 2, \ldots, \boldsymbol{Z}^{АСУ} - 1) \quad (3)$$

Из выражения (3) следует, что показатели эффективности должны формироваться применительно к конкретной задаче, решаемой СОБ, и определяться степенью достижения цели функционирования АСУ ТП.

Величина $W_{ij}^{АСУ}$ показателя эффективности АСУ ТП применительно к конкретной задаче $з_{ij}$, решаемой СОБ, вместе с остальными значениями показателей качества АСУ соответствует определенной величине $W_{ij}^{СОБ}$ показателя эффективности этой системы в целом:

$$\leftrightarrow W^{СОБ}{}_{ij} W^{АСУ}(з_{ij}, n_q^{АСУ} \in \boldsymbol{Z}^{АСУ}, q = 1, 2, \ldots, \boldsymbol{Z}^{АСУ} - 1) \quad (4)$$

В описании показателя эффективности АСУ обозначим через ***P*** - множество задач $з_{ij}$ решаемых органов управления СОБ с применением АСУ.

Предположим, что для каждой задачи $з_{ij} \in \boldsymbol{P}$ управления по противодействию (*j*= 1, 2, …, *J*) негативному воздействию на i-й (*i* = 1, 2,…, *I*) объект безопасности (ОБ) в СОБ определено смысловое и формальное содержание показателя эффективности ее решения. В качестве показателя могут выступать:

– абсолютная величина снижения вероятности угрозы $в_j$ негативного воздействия на *i*-й ОБ (с использованием, например, информационной системы анализа и оценки окружающей обстановки);

– степень защищенности *i*-й ОБ от *j*-го негативного воздействия (с использованием, например, АСУ управления силами и средствами СОБ);

– степень защищенности *i*-го ОБ от получения недопустимого ущерба *l*-го вида при реализации *j*-го негативного воздействия (с использованием, например, системы подготовки принятия решений и оперативного реагирования на чрезвычайные ситуации);

– время t_l, затраченное на сбор, анализ, обработку и доведение информации до соответствующих должностных лиц или населения (с использованием, например, системы сигнализации и оповещения).

Обозначим через W_{ij}^{+} и W_{ij}^{-} соответственно значения показателя $W_{ij}^{СОБ}$ при использовании в СОБ исследуемой (предлагаемой к разработке) и существующей АСУ ТП (или при ее отсутствии). Тогда применительно к решению $з_{ij}$-й задачи показатель эффективности $W_{ij}^{АСУ}$ исследуемой (предлагаемой к разработке) АСУ ТП может быть охарактеризован величинами:

– абсолютное приращение показателя эффективности СОБ:

$$W_{ij}^{АСУ} = W_{ij}^{+} - W_{ij}^{-} \quad (5)$$

– относительного приращения этого показателя:

$$W_{ij}^{АСУ}(W_{ij}^{+} - W_{ij}^{-})/W_{ij}^{-} \quad (6)$$

Положительное или отрицательное значение показателей и в зависимости от содержания определяет, является ли указанное приращение следствием увеличения или уменьшения эффективности решения -й задачи при использовании АСУ.

Выбор и обоснование конкретного состава имитационной системы моделирования требует глубокого анализа задач управления, выделения их основных сторон и связей и представляет собой сложную задачу, трудность которой зависит от степени изученности исследуемого процесса управления, полноты и достоверности информации о нем.

Символическое описание процесса решения управляющим органом (УО) задач противодействия негативного воздействия представлено на рис. 1.

Показатели качества АСУ:

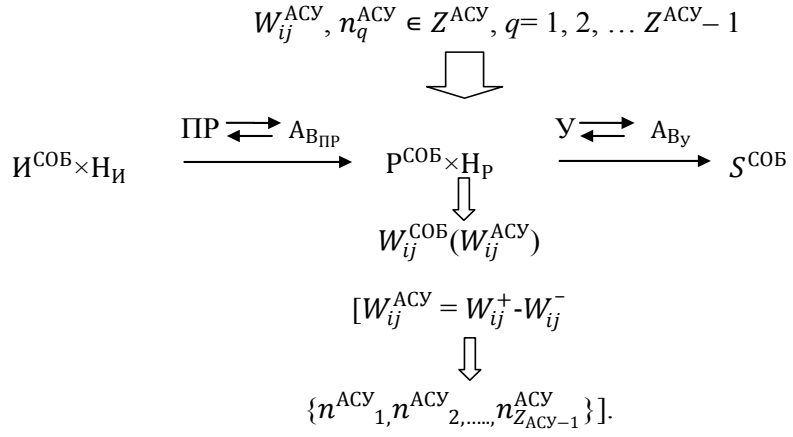


Рис.1 Символическое описание процесса решения задач управления обеспечением безопасности АСУ ТП.

Рассмотрим более подробно структуру предлагаемого процесса решения управляющим органом (УО) задач противодействия негативным воздействиям.

Принятие решения задач управления обеспечением безопасности будет зависеть от $И^{СОБ}$ – множестваинформации, поступающей в УО в результате оценки обстановки на каждом этапе управления, при множестве неопределенностей $H_и$ на каждом этапе управления; $P^{СОБ}$ – множества решений, принимаемых и реализуемых персоналом УО в результате оценки обстановки (анализа информации $И^{СОБ}$), при множестве неопределенностей, сопровождающих рассматриваемый процесс управления $H_р$; а так же от $S^{СОБ}$ – множества состояний СОБ в результате доведения решений $P^{СОБ}$ до исполнителей и реализации управляющих воздействий.

Основанием для принятия решения станут механизмы (рабочие алгоритмы) УО процесса подготовки, обоснования и принятия решений $P^{СОБ}$-$ПР$ и процессы реализации управляющих воздействий, являющиеся элементами общего алгоритма СОБ противодействия негативному воздействия – У.

Определим под негативным воздействием преднамеренное или непреднамеренное, организованное или случайное действие людей, событие или явление различной природы и характера, являющееся причиной негативных последствий для объекта безопасности в виде ущерба определенного вида и масштаба [3].

Негативные воздействия на процессы принятия решения $B_{ПР}$ и управления $B_у$ будут учтены алгоритмами АСУ $A_{B_{ПР}}$ и $A_{B_У}$ соответственно.

Практическая реализация моделив рамках рассмотренной имитационной системы моделирования и использование зависимостей (5), (6) позволяют ответить на вопросы:

– какой является величина показателя эффективности АСУ $W_{ij}^{АСУ}$ при решении $з_{ij}$-й задачи управления при принятых в управляющем органе механизмах (рабочих алгоритмах) ее решения и алгоритмах негативных воздействий $A_{Впр}$ и $A_{Ву}$ на этот орган;

– какой вектор $\{n_1^{АСУ}, n_2^{АСУ}, \ldots, n_{QАСУ-1}^{АСУ}\}$ количественных значений показателей качества АСУ соответствует оцененному значению $W_{ij}^{АСУ}$ показателя эффективности АСУ и показателю $W_{ij}^{СОБ}$ эффективности СОБ в целом.

Представленная в работе модель позволяетсформировать исходные данные и произвести оценку эффективности функционирования АСУ ТП при решении управляющим органом задач обеспечения безопасности в условиях прогнозируемых негативных воздействий.

Литература

1. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных систе-

мах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природы».

2. Федеральный закон от 26 июлю 2017 г. № 187-ФЗ «О безопасности информационной инфраструктуры Российской Федерации».

3. Научно-методические основы обеспечения безопасности защищаемых объектов. – М-: Горячая линия – Телеком, 2016. – 322 с.

References

1. Prikaz Federal'noy sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. № 31 «Ob utverzhdenii Trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a tak zhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirody».

2. Federal'nyy zakon ot 26 iyulyu 2017 g. № 187-FZ «O bezopasnosti informatsionnoy infrastruktury Rossiyskoy Federatsii».

3. Nauchno-metodicheskiye osnovy obespecheniya bezopasnosti zashchishchayemykh ob"yektov. – M-: Goryachaya liniya – Telekom, 2016. – 322 s.

МОСКОВЧЕНКО Валерий Михайлович, доктор экономических наук, профессор, профессор кафедры «Информационная безопасность» Южно-Российского государственного политехнического университета (НПИ) имени М.И.Платова. Россия, 346428, Ростовская область, г. Новочеркасск, улица Просвещения, 132, E-mail: fvo.urgpu.npi@yandex.ru

ШИЛИНА Анна Николаевна, кандидат технических наук, доцент учебного военного центра Южно-Российского государственного политехнического университета (НПИ) имени М.И. Платова. Россия, 346428, Ростовская область, г. Новочеркасск, улица Просвещения, 132, E-mail: anna_shilina@pochta.ru

MOSKOVCHENKO Valery, doctor of Economicssciences, Professor Professor of the Department of Information Security of the South-Russian State Polytechnic University (NPI) named after M. Platov. Russia, 346428, Rostov Region, g. Novocherkassk, street of Enlightenment, 132. E-mail: fvo.urgpu.npi@yandex.ru

SHILINA Anna, candidate of technical Sciences, associate Professor at the military training center South-Russian state Polytechnic University (NPI) named after M. I. Platov. Russia, 346428, Rostov Region, g. Novocherkassk, street of Enlightenment, 132. E-mail: anna_shilina@pochta.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта или заключение от экспертной комиссии.

Библиографические ссылки

Цитируемая в статье литература приводится в виде списка в конце текста. В тексте в квадратных скобках дается ссылка на порядковый номер списка (ГОСТ Р 7.0.5.-2008). Полный текст ГОСТа размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии Авторские примечания (не являющиеся используемой литературой или ссылкой на источник) размещаются в постраничных сносках.

Ниже приводятся образцы оформления сносок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 3(29) / 2018

Дата выхода в свет 30.06.2018. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 6,65. Тираж 100 экз. Заказ 360/427.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 3(29) / 2018

Date of publication of the 30.06.2018. Format 70×108 1/16. Screen printing.
Conventional printed sheet 6,65. Circulation – 100 issues. Order 360/427. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080