ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(30) / 2018

УЧРЕДИТЕЛИ

ФГБОУ ВПО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

ГЛАВНЫЙ РЕДАКТОР

ШЕСТАКОВ А. Л.,
д. т. н., профессор, ректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ОТВЕТСТВЕННЫЙ РЕДАКТОР

РАДИОНОВ А. А.,
д. т. н., профессор, проректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ШРЕЙБЕР А. Е.

КОРРЕКТОР

ФЁДОРОВ В. С.

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+

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА

ЧУВАРДИН О. П., руководитель Управления Федеральной службы по техническому и экспортному контролю России по Уральскому федеральному округу

РЕДАКЦИОННЫЙ СОВЕТ:

БАРАНКОВА И. И.,
д. т. н., профессор, зав. кафедрой «Информатика и информационная безопасность» ФГБОУ ВО «Магнитогорский государственный технический университет им. Г. И. Носова (г. Магнитогорск);

ВАСИЛЬЕВ В. И.,
д. т. н., профессор, профессор кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет» (г. Уфа);

ВОЙТОВИЧ Н. И.,
д. т. н., профессор, зав. кафедрой «Конструирование и производство радиоаппаратуры» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)»(г. Челябинск);

ГАЙДАМАКИН Н. А.,
д. т. н., профессор, начальник ФГКОУ ВО «Институт Федеральной службы безопасности Российской Федерации» (г. Екатеринбург);

ДИК Д. И.,
к. т. н., доцент кафедры «Безопасность информационных и автоматизированных систем» ФГБОУ ВО «Курганский государственный университет» (г. Курган);

ЗАХАРОВ А. А.,
д.т.н., профессор, зав. базовой кафедрой «Безопасность информационных технологий умного города» ФГАОУ ВО «Тюменский государственный университет» (г. Тюмень);

ЗЫРЯНОВА Т. Ю.,
к. т. н., доцент, зав. кафедрой «Информационные технологии и защита информации» ФГБОУ ВО «Уральский государственный университе путей сообщения» (г. Екатеринбург);

МЕЛЬНИКОВ А. В.,
д. т. н., профессор, директор АУ «Югорский научно-исследовательский институт информационных технологий» (г. Ханты-Мансийск);

ПОРШНЕВ С. В.,
д. т. н., профессор, директор Учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий — РТФ ФГАОУ ВО «УрФУ им. Первого Президента России Б. Н. Ельцина» (г. Екатеринбург);

СОКОЛОВ А. Н.
(зам. отв. редактора), к. т. н., доцент, зав. кафедрой «Защита информации» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)» (г. Челябинск);

ХОРЕВ А. А.,
д. т. н., профессор, зав. кафедрой «Информационная безопасность» Национального исследовательского университета «Московский институт электронной техники» (г. Москва, г. Зеленоград);

ШАБУНИН С. Н.,
д.т.н., профессор, профессор департамента «Радиоэлектроника и связь» Института радиоэлектроники и информационных технологий - РТФ ФГАОУ ВО «УрФУ им. Первого Президента России Б.Н. Ельцина» (г. Екатеринбург).

Journal of the Ural Federal District
Information security

ISSN 2225-5435

№ 4(30) / 2018

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHIEF EDITOR

SHESTAKOV A. L.,
doctor of Technical Sciences, Professor, Rector South Ural State University, (Chelyabinsk)

MANAGING EDITOR

RADIONOV A. A.,
Doctor of Technical Sciences, Professor, Vice-Rector South Ural State University, (Chelyabinsk

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

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+

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P., Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

EDITORIAL COUNCIL:

BARANKOVA I. I.,
Doctor of Technical Sciences, Professor, Head of Department «Informatics and Information Security» of the Federal State Educational Establishment of Higher Education «Magnitogorsk State Technical University named after. G.I. Nosova (Magnitogorsk city);

VASILYEV V. I.,
Doctor of Technical Sciences, Professor, Professor of the Department «Computer Science and Information Protection» FGBOU VO «Ufa State Aviation Technical University» (Ufa city);

VOITOVICH N. I.,
Doctor of economic sciences, professor, head. Department of «Design and production of radio equipment» FGAOU VO «South Ural State University (National Research University)» (Chelyabinsk city);

GAYDAMAKIN N. A.,
Doctor of Technical Sciences, Professor, Head of FGKOU VO «Institute of the Federal Security Service of the Russian Federation» (Yekaterinburg city);

DIK D. I.,
associate professor «Security of information and automated systems» of the FGBOU VO «Kurgan State University» (Kurgan city);

ZAHAROV A. A.,
Doctor of Technical Sciences, Professor, Head, basic. Department of «Security information technologies smart city» FSAEI of HE «Tyumen State University» (Tyumen city);

ZYRYANOVA T. Y.,
Cand. Tech. Sc., associate professor, head. Department of Information Technologies and Information Protection «FGBOU VO» Ural State University ways of communication» (Yekaterinburg city);

MELNIKOV A. V.,
Doctor of Technical Sciences, Professor, Director Ugra Research Institute of Information Technologies (Khanty-Mansiysk city);

PORSHNEV S. V.,
Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» Institute of Radio-electronics and Information Technology - RTF FGAOU VU «UrFU named after. The First President of Russia Boris N. Yeltsin» (Yekaterinburg city);

SOKOLOV A. N.,
(Deputy Editorial Editors), Cand. Tech. Sc., Associate Professor, Head. Department of Information Security of the Federal State Optical Institute of South Ural State University (National Research University) (Chelyabinsk city);

HOREV A. A.,
Doctor of Technical Sciences, Professor, Head of Department. Department of «Information Security» National Research University «Moscow Institute of Electronic Technology» (Moscow, the city of Zelenograd);

SHABUNIN S. N.,
Doctor of Technical Sciences, Professor, Professor Department of Radio Electronics and Communications, Institute Radio Electronics and Information Technology - RTF FSAEI of HE «UrFU them. First President of Russia B.N. Yeltsin» (Yekaterinburg city).

В НОМЕРЕ

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

СИДОРКИНА И. Г., КУБАШЕВА Е. С., СОЛОВЬЕВ М. Г., ГАЛАНИНА Н. А.
Подход к реализации алгоритмов работы с цифровым водяным знаком в аудиофайлах для систем защиты информации 5

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

БУХАРЕВ Д.А., ВАГИН С.В., СОКОЛОВ А.Н.
Защита устройств Интернета вещей от Mirai-подобных вирусных программ-червей 11

ЧАСТИКОВА В.А., ЖЕРЛИЦЫН С.А., ВОЛЯ Я.И.
Нейросетевой метод идентификации личности по неформализованной семантической характеристике 20

МЕТОДЫ АНАЛИЗА ДАННЫХ

БОНДАКОВА О.С., ЗЯЗИН В.П.
О первичной оценке вероятности возникновения коллизии для уменьшенного варианта хэш-функции «Стрибог» 27

КЛЯУС Т.К., ГАТЧИН Ю.А.
Определение вероятности реализации атак на информационную систему с помощью деревьев событий 31

МАКСИМОВА Е.А., БАРАНОВ В.В., ЗЯЗИН В.П.
Модель оценки рисков при расследовании компьютерных преступлений 38

МИНАЕВ В. А., КОРОЛЕВ И. Д., САБАНОВ А. Г.
Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия 43

ХАЛИЗЕВ В.Н., УГРЮМОВ Д.В.
Системная интеграция программно-аппаратных компонент защиты 50

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

УТОРОВ О.Р.
Проблемы правоприменения отношений в сфере обращения служебной тайны 60

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

ВАСИЛЬЕВ В. И. , КИРИЛЛОВА А. Д. , КУХАРЕВ С. Н.
Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) 66

ШАБУРОВ А.С., ДВОЙНИШНИКОВ Н.Э., ШЛЫКОВ А.И.
Особенности реализации требований по категорированию объектов критической информационной инфраструктуры 75

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ 83

IN THIS ISSUE

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

SIDORKINA I. G., KUBASHEVA E. S., SOLOVIEV M. G., GALANINA N. A.
Approach to realizing working algorithms with digital water sign in audio files for information security systems 5

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

BUKHAREV D.A., VAGIN S.V., SOKOLOV A.N.
Internet of things devices protection from Mirai-like worm-viruses 11

CHASTIKOVA V.AZHERLITSYN., S.A., VOLYA Y.I.
Neural network method of identification by unformalized semantic characteristics 20

METHODS OF DATA ANALYSIS

BONDAKOVA O.S., ZIAZIN V.P.
About the primary estimation of the probability of the collision for a reduced variant of the «Stribog» hash-function 27

KLYAUS T. K., GATCHIN YU.A.
Probability evaluation of attacks on information system using event tree analysis 31

MAKSIMOVA E.A., BARANOV V.V., ZIAZIN V.P.
The model of risk assessment in the investigation of computer crimes. 38

MINAEV V.A., KOROLEV I.D., SABANOV A.G.
Risk assessment identification and authentication of electronic interaction subjects 43

HALIZEV V.N., UGRIUMOV D.V.
System integration of hardware-software protection component 50

ORGANIZATIONAL, TECHNICAL AND LEGAL PROTECTION OF INFORMATION

UTOROV O.R.
Problems law enforcement relations in the sphere of circulation official secret. 60

TOPICAL PROBLEMS OF CYBERSECURITY

VASILYEV V. I. , KIRILLOVA A. D. , KUKHAREV S. N.
Cybersecurity of apcs: modern trends and approaches (current state, perspectives) 66

SHABUROV A.S., DVOINISHNIKOV N.E., SHLYKOV A.I.
Features of the implementation of the requirements for the categorization of critical information infrastructure objects 75

REQUIREMENTS TO THE ARTICLESTO BE PUBLISHED IN MAGAZINE 83

УДК 003.26.09 + 004.056 Вестник УрФО № 4(30) / 2018, с. 5–10

Сидоркина И. Г., Кубашева Е. С., Соловьев М. Г., Галанина Н. А.

DOI: 10.14529/secur180401

ПОДХОД К РЕАЛИЗАЦИИ АЛГОРИТМОВ РАБОТЫ С ЦИФРОВЫМ ВОДЯНЫМ ЗНАКОМ В АУДИОФАЙЛАХ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Методы стеганографии получили активное развитие только в последние годы. Одно из направлений стеганографии – встраивание цифровых водяных знаков (ЦВЗ) в контейнеры, представляющие собой файлы разнородных данных. ЦВЗ – это информация, которая внедряется в файл, с целью контроля правомерного использования информационного объекта. ЦВЗ бывают видимые и скрытые. Видимые ЦВЗ легко обнаружить и удалить. Невидимые ЦВЗ встраиваются в компьютерный файл, не меняя основной функциональности файла. Актуальность вопроса применения ЦВЗ связана с необходимостью обеспечения безопасности и достоверности информации, которой владеет пользователь. Предложенные алгоритмы реализации ЦВЗ в аудиофайле демонстрируют обеспечение эффективной защиты прав автора.

Ключевые слова: *стеганография, цифровой водяной знак, файловый контейнер, формат данных, аудиофайл, преобразование Фурье, автокорреляционная функция (АКФ), АКФ кепстра, алгоритм встраивания ЦВЗ, алгоритм извлечения ЦВЗ.*

Sidorkina I.G., Kubasheva E.S., Soloviev M.G., Galanina N.A.

APPROACH TO REALIZING WORKING ALGORITHMS WITH DIGITAL WATER SIGN IN AUDIO FILES FOR INFORMATION SECURITY SYSTEMS

The methods of steganography have been actively developed only in recent years. One of the directions of steganography is the embedding of digital watermarks (DWs) into containers, which are files of heterogeneous data. CEH is information that is embedded in a file, in order to control the legitimate use of the information object. CEHs are visible and hidden. Visible CEHs are easy to detect and remove. Invisible CEHs are built into the computer file without changing the main functionality of the file. The relevance of the application of CEH is related to the need to ensure the security and reliability of information that the user owns. The proposed algorithms for implementing the CEH in the audio file demonstrate the effective protection of the author's rights.

Keywords: *steganography, digital watermark, file container, data format, audio file, Fourier transform, autocorrelation function (ACF), AKF cepstrum, embedding algorithm, CEV extraction algorithm.*

Для эффективного применения технологий ЦВЗ [1], необходимо обеспечить аудио и визуальную незаметность сообщений, сохранить исходное качество исходного контейнера и, одновременно, обеспечить высокую достоверность извлечения сообщения с учетом возможных непреднамеренных и преднамеренных воздействий в канале передачи информации.

Так как информация представляет собой передаваемое знание, то приведем пример абстрактной модели канала скрытной передачи информации (Рис. 1). Имеется отправитель, получатель и противник, который хочет завладеть этой информацией. Но противником может быть не один человек, а группа, и они могут ставить себе различные цели: например, уничтожение скрытой информации, обнаружение факта передачи, подделка или искажение информации, навязывание ложной. Поэтому для различных случаев методы противодействия различаются. Например, это попытки скрыть факт передачи информации, попытки в открытом канале связи создать трудности для перехвата. И таких вариантов много, и на каждом этапе решается задача обеспечения надежности [2].

Цифровое изображение представляет собой матрицу пикселей. Изменение младшего бита LSB изображения обычно не заметно для глаза человека, поэтому его можно использовать для встраивания информации. Таким образом, графические файлы позволяют передавать большое количество данных. Так для картинки 1024x768 можно в закрытом виде передать 294912 байт, используя метод наименее значимого бита – LSB.

Реализация методов цифровой стеганографии включает в себя следующую последовательность:

1) встраивание ЦВЗ(watermarking);
2) встраивание заголовков;
3) встраивание номеров идентификации;
4) встраивание информации для скрытой передачи.

Выделим следующие два принципа компьютерной стеганографии: файлы, не требующие особой аутентичности (например, медиафайлы), могут видоизменяться до определенной степени без потери функциональности и человеческие органы неспособны идентично различать изменения в таких данных.

ЦВЗ — это специальная метка, идентифи-

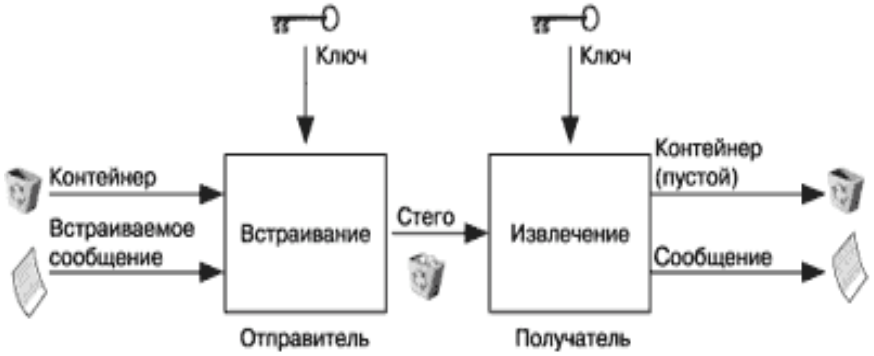

Рис. 1. Обобщенная модель стегосистемы

цированная и внедренная для защиты авторских прав мультимедийных файлов. Как правило, они (метки) встроены в цифровые данные, с целью иметь возможность контролировать файлы. Но, как известно, система защиты информации должна выполнять свои функции даже при полной информативности злоумышленника о структуре и алгоритмах ее функционирования [3]. Невидимые ЦВЗ внедряются в цифровые объекты таким образом, чтобы пользователю было крайне сложно выявить добавленную метку. Например, если ЦВЗ внести на графическое изображение, то мы можем изменить яркость определенных точек, тем самым при просмотре рисунка человек может не заметить следов искусственного изменения.

1) человек, использующий мультимедийный файл, визуально не должен заметить встроенную метку;

2) возможность для автора обнаружить несанкционированное использование файла;

3) невозможность удаления метки сторонними лицами, не имеющими на то право;

4) устойчивость к изменениям файла носителя.

Атаки, предназначенные для систем ЦВЗ [4], можно классифицировать, например, следующим образом:

1) Атаки, которые служат для удаления ЦВЗ или его порчи. В задачу таких атак не входит извлечение стегосообщения. В качестве

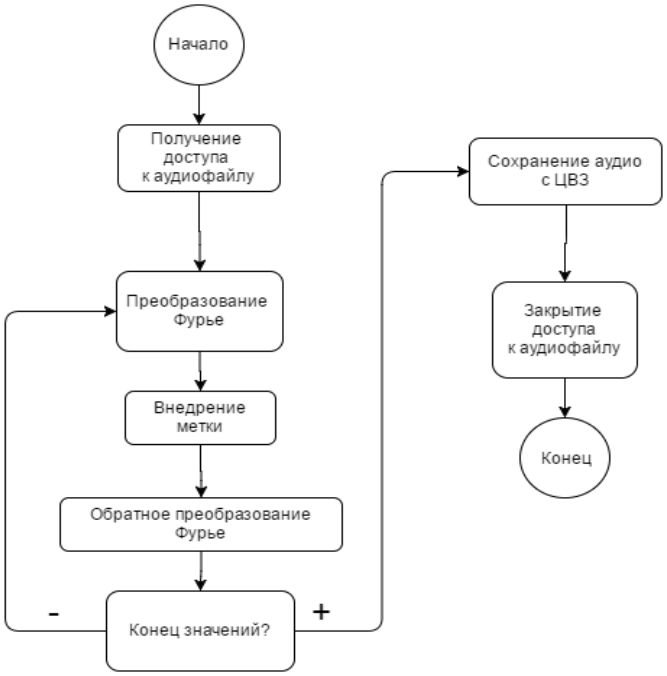

Рис. 2. Общая схема внедрения ЦВЗ

ЦВЗ должны отвечать ряду требований, таких как:

примера можно привести линейную фильтрацию, добавление шума;

2) атаки, направленные на извлечение цифровой метки. Например, статистическое усреднение;

3) атаки, предназначенные для затруднения извлечения ЦВЗ. В данном случае, как правило, происходит искажение самого контейнера. Сюда относятся различные сдвиги, повороты, то есть приемы, связанные с масштабированием;

4) атаки, главная задача которых состоит в создании ложных ЦВЗ.

Это один из вариантов классификации, в других источниках атаки могут классифицироваться по другим параметрам.

Продемонстрируем схемы внедрения ЦВЗ (Рис.2) и извлечения ЦВЗ (Рис.3) в аудиофайл.

Аудио файл представляет собой последовательность бит, в которых представлен частотный спектр звука. Для получения доступа к этим числовым данным, а также возможность воспроизводить аудио использована библиотека OpenAl, которая содержит в себе необходимые функции для работы с аудио.

Далее внедряем данные в аудио файл. После того, как получили значения частотного спектра звука, формируем их для дальнейшего внедрения с помощью преобразования Фурье. Само внедрение происходит методом Хола-Тиркеля [5], после чего мы сохраняем наш аудио файл с внедренным ЦВЗ.

Для встраивания и извлечения цифрового водяного знака на основе предложенных схем в аудио файл разработаны и исследуются следующие алгоритмы.

Алгоритм встраивания.

1) переводится встраиваемое сообщение в двоичный код;

2) определяется вместительность контейнера и размер встраиваемого сообщения. В случае если сообщение не помещается в контейнер, завершить выполнение с ошибкой;

3) в зависимости от частоты дискретизации, осуществляется разделение контейнера на равные части, для того, чтобы обеспечить пропускаемую способность 16 бит в секунду;

4) рассматривается первая часть контейнера;

5) создается эхо-сигнал путем смещения оригинального сигнала на значение задержки соответствующее текущему биту;

6) уменьшается амплитуда эхо-сигнала. Так же требуется создать спадающий и возрастающий фронты в конце и начале эхо-сигнала соответственно для предотвращения появления резких переходов;

7) наложение эхо-сигнала на оригинальный сигнал.

Алгоритм извлечения.

1) перевести проверяемое сообщение в двоичный код;

2) сверить вместительность контейнера и

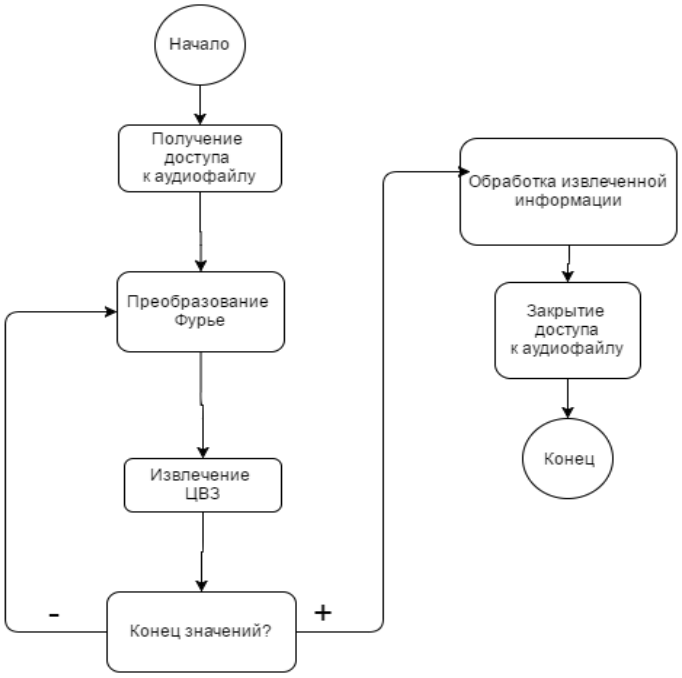

Рис. 3. Общая схема извлечения ЦВЗ

размер проверяемого сообщения. В случае если сообщение не помещается в контейнер, завершить выполнение с ошибкой.

В зависимости от частоты дискретизации, разделить контейнер на равные части, для того, чтобы обеспечить пропускаемую способность 16 бит в секунду.

1) Берем первую часть контейнера;

2) Посчитать АКФ кепстра для текущего фрагмента контейнера;

3) Сравнить значения АКФ кепстра соответствующие времени равному значению смещения эхо-сигналов. Если значение на уровне смещения равного «1» больше, чем «0», то встраивался бит 1;

4) Сравнить полученный бит с соответствующим битом проверяемого сообщения;

5) При условии, что все биты совпали (возможен вариант проверять процент совпадения, т.к. метод эхо-сигналов обладает не 100% вероятностью правильного извлечения бит), делаем вывод о том, что аудио файл защищен.

Алгоритмы по области встраивания относятся к частотным, они достаточно сложны в плане вычислений и затрачиваемых ресурсов. Большинство известных алгоритмов создания ЦВЗ [6,7] имеет общий недостаток, а именно все алгоритмы встраивания информации в объекты образуют конечное множество вариантов, вследствие чего они могут быть идентифицированы и вскрыты. Необходимо отметить, что большинство алгоритмов зависимы от формата, трудоемкости вычисления. Кроме того, например, для извлечения ЦВЗ в некоторых случаях необходимо иметь исходный немаркированный файл.

Таким образом, предложенное решение не требует создания дополнительных сигналов, вследствие чего не нужно сравнивать объем контейнера и сообщение, чтобы записать информацию, и что, следовательно, более эффективно.

Литература

1. Грибунин В.Г. Цифровая стеганография // СПб.: Солон-Пресс, 2002. — 272 С.

2. Рябко Б.Я. Основы современной криптографии и стеганографии. / Б.Я. Рябко, А.Н. Фионов – М.: Горячая линия – Телеком, 2010. – 232 С.

3. Kerckhoffs, La Cryptographie Militare. Journal des sciences militaires, pp:5-83, Jan. 1883, pp:161-191, Feb. 1883.

4. Charbon E., Torunoglu I.H. On Intellectual Property Protection. In proceedings of Custom Integrated Circuits Conference, 2000, pp. 517-523.

5. New Matrices with Good Auto and Cross-Correlation - A. TIRKEL and T. HALL - IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.9 SEPTEMBER 2006.

6. А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов. ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В ГРАФИЧЕСКИХ ФАЙЛАХ. / Научно-технический вестник информационных технологий, механики и оптики,

7. 2013, № 1 (83), С. 152-156.

8. 7. Сидоркина И.Г. Метод аутентификации по биометрическим параметрам// Изд.: «Южный федеральный университет» в г. Таганроге (Таганрог) Информационное противодействие угрозам терроризма. 2015. № 24. С. 202-205.

References

1. Gribunin V.G. Tsifrovaya steganografiya // SPb.: Solon-Press, 2002. — 272 S.

2. Ryabko B.YA. Osnovy sovremennoy kriptografii i steganografii. / B.YA. Ryabko, A.N. Fionov – M.: Goryachaya liniya – Telekom, 2010. – 232 S.

3. Kerckhoffs, La Cryptographie Militare. Journal des sciences militaires, pp:5-83, Jan. 1883, pp:161-191, Feb. 1883.

4. Charbon E., Torunoglu I.H. On Intellectual Property Protection. In proceedings of Custom Integrated Circuits Conference, 2000, pp. 517-523.

5. New Matrices with Good Auto and Cross-Correlation - A. TIRKEL and T. HALL - IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.9 SEPTEMBER 2006.

6. A.G. Korobeynikov, S.S. Kuvshinov, S.YU. Blinov, A.V. Leyman, I.M. Kutuzov. TSIFROVYYe VODYANYYe ZNAKI V GRAFICHESKIKH FAYLAKH. / Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki,

7. 2013, № 1 (83), S. 152-156.

8. 7. Sidorkina I.G. Metod autentifikatsii po biometricheskim parametram// Izd.: "Yuzhnyy federal'nyy universitet" v g. Taganroge (Taganrog) Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. № 24. S. 202-205.

СИДОРКИНА Ирина Геннадьевна, доктор технических наук, профессор, декан Факультета информатики и вычислительной техники ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Республика Марий Эл, г. Йошкар-Ола, пл. Ленина, дом 3. E-mail: igs592000@mail.ru

КУБАШЕВА Елена Сергеевна, кандидат технических наук, доцент кафедры ИВС ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Республика Марий Эл, г. Йошкар-Ола, пл. Ленина, д. 3. E-mail: e.kubasheva@mail.ru

СОЛОВЬЕВ Максим Геннадьевич, студент кафедры Информационной безопасности ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Марий Эл, г. Йошкар-Ола, пл. Ленина, д. 3. E-mail: fivt@volgatech.net

ГАЛАНИНА Наталия Андреевна, доктор технических наук., профессор, г.Чебоксары ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова». 428010, Чувашская Республика г. Чебоксары, Московский просп., 15. E-mail: galaninacheb@mail.ru

SIDORKINA Irina, Doctor of Technical Sciences, Professor, Dean of the Faculty of Informatics and Computer Engineering of Volga State University of Technology. 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: igs592000@mail.ru

KUBASHEVA Helena, Candidate of Technical Sciences, Associate Professor of the Department of IVS FSBEI HE "Volga State University of Technology". 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: e.kubasheva@mail.ru

SOLOVIEV Maksim, student of the Department of Information Security FSBEI of HE "Volga State University of Technology". 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: fivt@volgatech.net

GALANINA Nataliya, Doctor of Technical Sciences., Professor, Cheboksary FSBEI of HE "I. Chuvash State University". Ulyanova. 428010, Chuvash Republic, Cheboksary, Moskovsky Prospect, 15. E-mail: galaninacheb@mail.ru

УДК 004.738.5 Вестник УрФО № 4(30) / 2018, с. 11–19

Бухарев Д. А., Вагин С. В., Соколов А. Н.

DOI: 10.14529/secur180402

ЗАЩИТА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ ОТ MIRAI-ПОДОБНЫХ ВИРУСНЫХ ПРОГРАММ-ЧЕРВЕЙ

В работе проанализированы вредоносное программное обеспечение (ПО) ботнета Mirai и его модификации. Приведена история развития ботнета Mirai с момента первого обнаружения в августе 2016 года. Выделены основные составные части ботнета: бот, загрузчик, сервер управления и контроля, сервер отчетов. Описан процесс заражения вирусной программой-червем Mirai от перебора паролей на заражаемом устройстве до получения команды на начало DDoS атаки на целевой сервер. Рассмотрены отличительные следы вирусной программы-червя в трафике сети (шаблоны пакетов и коммуникации с серверами ботнета), которые позволяют определить наличие зараженного устройства в сети. Описаны модификации Mirai, использующие как открытый исходный код ботнета, так и только основные методики заражения и контроля ботов. Исследованы уязвимости устройств Интернета вещей (IoT) перед вирусной программой-червем Mirai и ее модификациями, сформулированы методы их обнаружения и защиты *устройств IoT.*

Ключевые слова: *DDoS атака, ботнет, вирусная программа-червь, Интернет вещей (IoT).*

Bukharev D. A., Vagin S. V., Sokolov A. N.

INTERNET OF THINGS DEVICES PROTECTION FROM MIRAI-LIKE WORM-VIRUSES

The paper analyzes the malicious software of the Mirai botnet and its modifications. The history of Mirai development since the first discovery in August 2016 is considered, the main components of the botnet are highlighted: bot, loader, command and control server, report server. The process of infection with worm-virus Mirai from brute force passwords on the device to receive a command to start a DDoS attack on the target server. The distinctive traces of the worm-virus in the network traffic (patterns of packets and communication with botnet servers), which allow to determine the presence of an infected device in the network, are considered. The article describes the modifications of Mirai, using both open source botnet and only the basic methods of infection and control of bots. Vulnerabilities of Internet of things (IoT) devices to the Mirai and Mirai-like worm-viruses are investigated, methods of its detection and protection of IoT devices are formulated.

Keywords: *DDoS attack, botnet, worm-virus, Internet of things (IoT).*

Развитие технологий Интернета вещей (Internet of Things, IoT) привело к появлению новых возможностей злоумышленников по реализации кибератак. Устройства IoT постоянно подключены к сети Интернет и имеют множество уязвимостей, которые позволяют злоумышленникам проводить атаки типа «Распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS).

Последними примерами таких атак являются атаки ботнета (вирусной программы-червя) Mirai. Впервые этот ботнет был идентифицирован группой исследователей в области информационной безопасности MalwareMustDie в августе 2016 года [1]. Mirai (с яп. «будущее»), его множественные вариации и имитаторы послужили двигателем для реализации одних из самых крупных DDoS-атак в истории: в сентябре 2016 года веб-сайт консультанта по информационной безопасности Брайана Кребса был подвержен DDoS-атаке, трафик которой в пике составил около 620 Гб/с, что сделало ее одной из самых крупных DDoS-атак [2]. Приблизительно в то же время была произведена еще более крупная атака с помощью ботнета Mirai с трафиком в пике 1,1 Тб/с, нацеленная на поставщика облачных услуг OVH [3].

Через некоторое время после публикации в открытом доступе исходного кода Mirai его создателем [4], злоумышленники стали предлагать в аренду ботнеты на 400 тыс. одновременно зараженных устройств. Наиболее заметная по последствиям атака, которая привела к массовым проблемам доступа пользователей к популярным ресурсам, таким как Amazon, PayPal, GitHub, Twitter и др. [5], осуществлена в октябре 2016 года и была нацелена на известный DNS-провайдер Dyn.

Устройства Интернета вещей оказались наиболее уязвимым звеном в современных компьютерных сетях. Заражение вирусной программой-червем Mirai начинается с таких устройств как веб-камеры, цифровые видеорегистраторы и маршрутизаторы, работающие с использованием набора UNIX-утилит для встраиваемых операционных систем BusyBox. После этого вирусная программа-червь заражает другие незащищенные IoT устройства путем подбора стандартных логина и пароля администратора из небольшого словаря.

В настоящее время вариации Mirai генерируются ежедневно. Поскольку базовые механизмы безопасности в устройствах Интернета вещей, как правило, не реализованы, вполне очевидно, что различные вариации Mirai продолжат наносить ущерб сетевой инфраструктуре, используя методы вторжения, подобные оригинальной версии Mirai [6].

В большинстве случаев Mirai приводит к DDoS-атаке, направленной на целевой список серверов путем своего внедрения в слабозащищенные IoT устройства. Можно выделить пять основных причин, которые делают устройства Интернета вещей приоритетной целью злоумышленников:

1. Работа устройств 24/7. В отличие от стационарных персональных компьютеров (ПК) и ноутбуков, от устройств IoT требуется бесперебойное круглосуточное функционирование.

2. Слабая защита устройств IoT. Приоритетной задачей большинства производителей, как правило, является обладание долей рынка устройств IoT, а не создание их защитных механизмов.

3. Недостаточная поддержка устройств IoT. Многие устройства IoT устанавливаются по принципу «включил и забыл», после чего пользователи и администраторы сети забывают об их обслуживании.

4. Генерация значительного объема трафика. Современные устройства IoT являются достаточно производительными устройствами, чтобы генерировать объемы трафика при DDoS атаке, сравнимые с объемами генерации трафика обычными современными ПК.

5. Неинтерактивный пользовательский интерфейс устройств IoT. Устройства IoT не требуют частого внимания пользователя, поэтому заражение, как правило, проходит незамеченным. Из-за недостаточных возможностей конфигурации устройства IoT пользователю тяжело исправить ситуацию при обнаружении заражения.

Коммуникация и организация ботнета Mirai

Ботнет Mirai состоит из четырех основных частей. Бот является вредоносной программой, которая заражает устройства [7]. Ее двойное предназначение заключается в распространении заражения на незащищенные устройства и атаке целевого сервера при получении соответствующей команды от лица, контролирующего бота, или ботмастера (лицо, контролирующее весь ботнет). Сервер управления и контроля (command and control, C&C) предоставляет ботмастеру интерфейс централизованного управления для проверки состояния ботнета и проведения

целевых DDoS-атак. Обычно вся коммуникация с другими частями сети происходит через анонимную сеть Tor. Сервер-загрузчик (loader) обеспечивает распространение вредоносной программы-червя, нацеливаясь на другие аппаратные платформы (18 платформ, включая ARM, x86, MIPS) путем прямой коммуникации с новыми жертвами. Сервер отчетов, к которому, как правило, обращаются инфицированные устройства, наполняет базу данных деталями о всех устройствах в ботнете.

В момент, когда вредоносное ПО Mirai пытается получить доступ к новым устройствам IoT, проверяются произвольные публичные IP-адреса на портах протокола TCP 23 или 2323. При этом некоторые адреса государственных служб, компаний General Electric и Hewlett-Packard исключены из проверяемого списка, предположительно для того, чтобы не привлекать внимание государственных органов. На рис. 1 показаны ключевые шаги организации и коммуникации ботнета Mirai.

ристики скомпрометированного устройства через другой порт TCP.

Шаг 3. Посредством сервера управления и контроля ботмастер регулярно проверяет наличие новых потенциальных жертв для заражения, а также текущий статус ботнета, посылая запрос серверу отчетов, обычно через анонимную сеть Tor.

Шаг 4. После определения потенциально уязвимых устройств ботмастер подает серверу-загрузчику команду на заражение с указанием всей необходимой информации: IP-адрес, аппаратную архитектуру, операционную систему и т.д.

Шаг 5. Сервер-загрузчик удаленно входит в целевую систему, загружает и запускает бинарную версию вредоносной программы при помощи утилиты Wget или по протоколу TFTP. После заражения вирусная программа-червь пытается защитить устройство от других вредоносных программ путем закрытия возможностей удаленного подключения к устройству, таких как Telnet или SSH. Зараженное

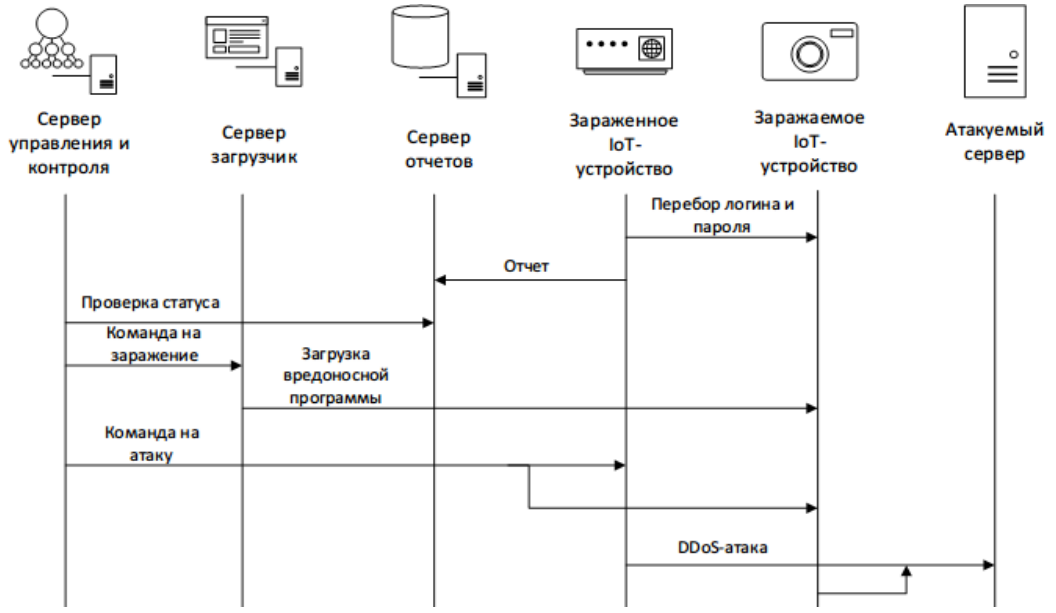

Рис.1. Ключевые шаги организации и коммуникации ботнета Mirai

Рассмотрим процедуру заражения и атаки пошагово.

Шаг 1. Бот пытается получить контроль над слабозащищенными IoT устройствами путем перебора логина и пароля. Словарь для перебора прописан в программном коде Mirai и содержит 62 стандартные пары пользователь:пароль.

Шаг 2. После успешного подбора и запуска удаленной командной оболочки бот передает серверу отчетов различные характе-

устройство начинает связываться с сервером управления и контроля для получения инструкций для атаки. Это происходит путем разрешения доменного имени cnc.changeme.com (в оригинальной версии Mirai), которое прописано в программном коде вирусной программы-червя, не используя статический IP-адрес. Таким образом, ботмастер имеет возможность по своему желанию изменять IP-адрес сервера управления и контроля с течением времени, не прибегая к изменению

бинарного файла вредоносной программы на зараженных устройствах.

Шаг 6. Ботмастер указывает всем ботам в сети атаковать определенный сервер путем выполнения простой команды на сервере контроля и управления с указанием типа DDoS атаки, ее длительности, списка IP-адресов ботов и целевых серверов.

Шаг 7. Боты после получения приказа атакуют сервер одним из 10 возможных типов DDoS атак, включая DDoS атаки TCP SYN-флуд, HTTP-флуд и DDoS атаку, использующую протокол GRE.

Модификации Mirai

Появление в открытом доступе исходного кода Mirai не только не привело к быстрому появлению механизмов защиты от него, но и позволило создать новые модификации Mirai. Через два месяца после публикации исходного кода Mirai количество ботов в сети увеличилось с 213 тыс. до 493 тыс. [1]. Модификации Mirai используют те же уязвимости устройств IoT, что и оригинальная версия ботнета Mirai.

Как правило, заражения Mirai проходят через порты TCP 23 и 2323. Модификации Mirai, обнаруженные в ноябре 2016 года, используют для заражения другие порты TCP, например, порт 7547, который используется интернет-провайдерами для удаленного управления широкополосными маршрутизаторами клиентов. Одна из таких модификаций привела к отключению от сети около миллиона пользователей Deutsche Telekom [8]. В феврале 2017 года очередная модификация Mirai запустила 54-часовую DDoS атаку на сайт колледжа в США [9]. В марте 2017 года появилась новая модификация с функцией добычи криптовалюты Bitcoin. Учитывая малые вычислительные мощности устройств IoT, злоумышленники не получили от очередной модификации значительных выгод [10].

Очередной модификацией вредоносного ПО Mirai стал ботнет Persirai [11], открытый в апреле 2017 года исследователями компании Trend Micro и названный из-за своего, предположительно, иранского происхождения (Persian Mirai). Механизм работы Persirai предполагает получение доступа к веб-камерам определенного производителя через порт TCP 81. Если доступ удается, вирусная программа-червь пытается проникнуть в маршрутизатор, к которому подключено само устройство через уязвимости набора протоколов UPnP. После этого на маршрутизатор загружается вредоносный бинарный файл, который удаляется после запуска. Для доступа к устройствам Persirai использует не простой перебор паролей, а задокументированные уязвимости первого дня для получения файла с паролем. Это становится возможным, поскольку пользователи, как правило, не обновляют программное обеспечение устройств IoT в процессе эксплуатации.

В сети все чаще появляются новые ботнеты, использующие все те же базовые принципы заражения устройств, но более продуманные механизмы сокрытия и распространения.

Ботнет IoT, написанный на языке программирования Lua, был обнаружен группой MalwareMustDie в конце августа 2016 года [12]. Большинством устройств, вошедших в ботнет, были модемы с процессорами архитектуры ARM и операционными системами Linux. Вредоносная программа использует шифрованное соединение с сервером контроля и управления и особый список правил фаервола iptables для защиты зараженных устройств.

Ботнет Hajime, обнаруженный в октябре 2016 года специалистами компании Rapidity Networks [13], использует метод заражения, схожий с Mirai. Однако механизм сокрытия ботнета Hajime предполагает вместо централизованной архитектуры использование децентрализованных механизмов связи при помощи протоколов BitTorrent DHT (для поиска пиров) и µTP (для передачи данных). Каждое сообщение, отправляемое отдельным ботом, шифруется и подписывается ассиметричным протоколом RC4. При этом своими действиями вирусная программа-червь закрывает все порты доступа к устройству IoT, которые используются Mirai-подобными ботнетами.

Другой ботнет, основанный на работе с набором утилит BusyBox – BrickerBot был обнаружен группой исследователей Radware в апреле 2017 года [14]. Путем получения удаленного доступа по SSH, используя стандартные пары логин-пароль, вредоносная программа производит атаку типа «Постоянный отказ в обслуживании» (PDoS) путем перезаписи системной прошивки, удаления всех файлов во встроенной памяти и реконфигурации параметров сетевого подключения.

Методы защиты от вредоносного ПО Mirai

В отличие от другого вредоносного ПО, Mirai не пытается избежать обнаружения. Во всех стадиях заражения, вирусная программа-

червь оставляет следы, которые можно обнаружить даже при простом анализе трафика в сети. Трафик в сети с устройством, зараженным Mirai, может включать в себя:

• последовательную проверку данных для входа по определенному порту;

• отсылку отчетов, имеющих различимый шаблон;

• скачивание бинарного кода определенного типа;

• обмен keep-alive сообщениями;

• получение команд от удаленного сервера на атаку, которые имеют определенную структуру;

• генерацию трафика с очень малым числом произвольных компонентов.

Таким образом, зараженное устройство можно определить по четко различимому шаблону, который формируется типами сообщений, размерами пакетов и последовательностью отправки.

При первоначальном заражении Mirai производит перебор логинов и паролей из встроенного в программный код словаря, который содержит 62 стандартных и самых популярных пар. Поэтому для защиты от заражения Mirai рекомендуется предпринять следующие действия:

1. Разработчикам устройств IoT необходимо:

• предоставить пользователю возможность изменения логина и пароля для входа в устройство при первоначальной настройке;

• предоставить пользователю возможность генерации нового логина и пароля с использованием криптографически стойких генераторов псевдослучайных чисел;

• реализовать технологию проверки подлинности исполняемого кода с целью исключения возможности выполнения вредоносного неподписанного кода вирусной программой-червем на устройстве [15].

2. Пользователям и администраторам сети с устройствами IoT необходимо:

• изменить стандартный логин и пароль для входа при первоначальной настройке устройства IoT;

• запретить доступ к IoT устройству из внешней сети, если в этом нет необходимости;

• все устройства IoT объединить в отдельную подсеть путем физического разделения сети или с использованием VLAN.

Реализация предложенных рекомендаций позволит закрыть возможности проникновения вирусной программы-червя Mirai и его вариаций в устройства IoT и внутреннюю сеть.

Для обнаружения возможности заражения устройств Интернета вещей, находящихся во внутренней сети, можно воспользоваться бесплатным ресурсом Mirai Vulnerability Scanner [16], которое осуществляет проверку на предмет наличия уязвимых устройств и уведомляет пользователя, если таковые устройства были найдены. При наличии уязвимых устройств следует воспользоваться предложенными ранее методами устранения уязвимостей и реализовывать новые проверки до тех пор, пока сканер не сообщит об отсутствии уязвимых устройств.

Для обнаружения уже зараженных устройств во внутренней сети можно воспользоваться бесплатной утилитой для диагностики сети Wireshark [17] и специальными аппаратными перехватчиками трафика (network TAP), устанавливаемыми внутри сети. Wireshark позволяет «прослушивать» трафик в сети в реальном времени, либо считать уже заготовленные pcap-файлы с записанным трафиком. В утилите Wireshark необходимо отфильтровать ранее записанный трафик и оставить только те пакеты, которые отправляются устройствами Интернета вещей. Для этого следует использовать фильтр «ip.dest == X.X.X.X», где X.X.X.X – IP-адрес проверяемого устройства.

После фильтрации трафика необходимо его проанализировать. Проверяемое устройство IoT можно считать зараженным, если оно в течение 10-15 минут отправляет пакеты на различные IP-адреса сети Интернет или внутренней сети, которые содержат:

• запросы на авторизацию по telnet, SSH, http;

• DNS-запросы по доменному имени cnc.changeme.com, так как это доменное имя принадлежит серверу управления и контроля Mirai.

При обнаружении зараженного устройства следует провести сброс устройства к заводским настройкам и установить на нем новые логин и пароль для входа [18].

На рис. 2 представлена общая схема алгоритма обнаружения и устранения угроз заражения устройств Интернета вещей вирусной программой-червем Mirai и его модификациями.

Выводы

Ущерб, причиненный атаками ботнета

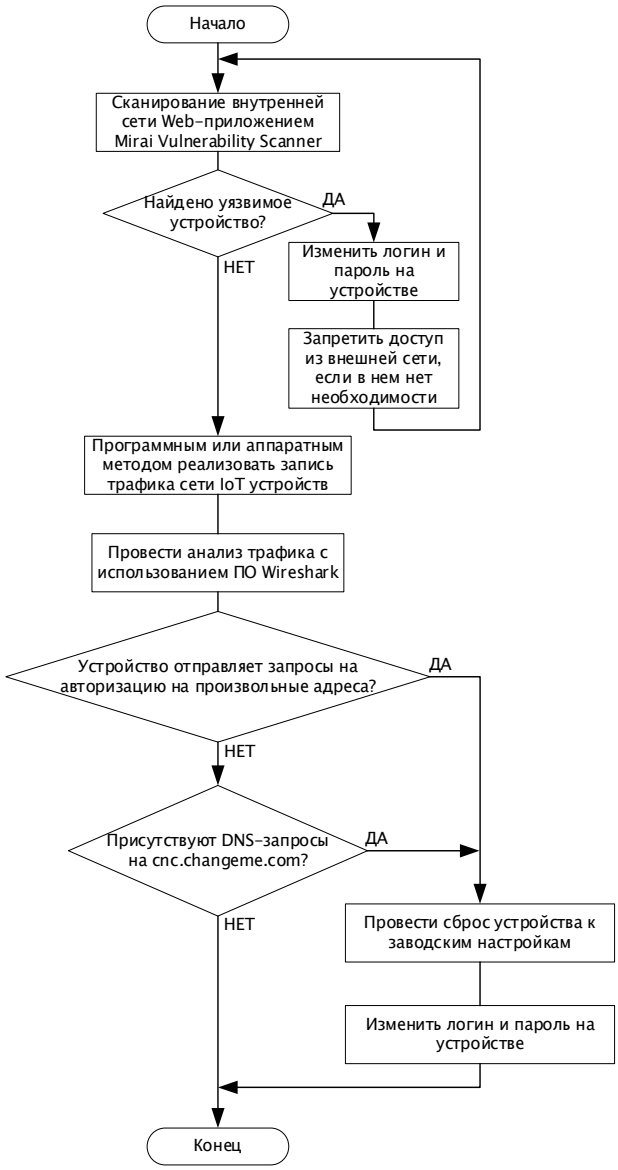

Рис. 2. Схема алгоритма обнаружения и устранения угроз заражения устройств Интернета вещей вирусной программой-червем Mirai и его модификациями.

Mirai, его модификациями и подражателями указывает на уязвимости, которыми обладают устройства Интернета вещей. Самые обычные подходы к получению несанкционированного доступа к таким устройствам позволяют злоумышленникам объединять устройства в большие группы, которые могут использоваться для DDoS атак. В работе описана структура и характеристики ботнета Mirai и его модификаций, приведены причины, которые делают устройства Интернета вещей приоритетной целью для атак злоумышленников. К этим причинам относятся:

• слабая защита устройств IoT;

• недостаточная поддержка со стороны производителя;

• малые возможности пользовательской конфигурации устройств IoT;

• большой вычислительный потенциал большого числа IoT устройств, объединенных в одну сеть.

Для реализации противодействия атакам на IoT устройства рассмотрен типовой процесс их заражения и предложены рекомендации по защите от ботнета Mirai и его модификаций как для разработчиков устройств Интернета вещей, так и для конечных пользователей и администраторов сетей.

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

Литература

1. Блог «MalwareMustDie» [Электронный ресурс]. – Режим доступа: http://blog.malwaremustdie.org/2016/08 /mmd-0054-2016-pnscan-elf-worm -that.html, свободный (дата обращения: 13.10.2018).

2. Блог «KrebsonSecurity» [Электронный ресурс]. – Режим доступа: https://krebsonsecurity.com /2016/09/krebsonsecurity-hit -with-record-ddos, свободный (дата обращения: 13.10.2018).

3. Сайт компании ArsTechnica [Электронный ресурс]. – Режим доступа: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/, свободный (дата обращения: 13.10.2018).

4. Исходный код вирусной программы-червя Mirai [Электронный ресурс]. – Режим доступа: https://github.com/jgamblin/Mirai-Source-Code, свободный (дата обращения: 13.10.2018).

5. Британский новостной сайт «The Register» [Электронный ресурс]. – Режим доступа: https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/, свободный (дата обращения: 15.10.2018).

6. Tuptuk N., Hailes S. Security of smart manufacturing systems // Journal of Manufacturing Systems. – 2018. – № 47. – С. 93–106.

7. Багай Д.И. Угроза Интернету вещей: ботнет Mirai // Современные технологии: актуальные вопросы, достижения и инновации: сборник статей XIV Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2018. – С. 69–72.

8. Блог «KrebsonSecurity» [Электронный ресурс]. – Режим доступа: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/, свободный (дата обращения: 15.10.2018).

9. Сайт веб-сервиса мониторинга и защиты от DDoS атак Imperva Incapsula [Электронный ресурс]. – Режим доступа: https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html, свободный (дата обращения: 15.10.2018).

10. Сайт компании SecurityIntelligence [Электронный ресурс]. – Режим доступа: https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/, свободный (дата обращения: 16.10.2018).

11. Блог компании SecurityIntelligence [Электронный ресурс]. – Режим доступа: https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/, свободный (дата обращения: 16.10.2018).

12. Блог «MalwareMustDie» [Электронный ресурс]. – Режим доступа: http://blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html, свободный (дата обращения: 19.10.2018).

13. Статья S. Edwards and I. Profetis, 16 Окт. 2016; [Электронный ресурс]. – Режим доступа: http://security.rapiditynetworks.com/publications /2016-10-16/hajime.pdf, свободный (дата обращения: 19.10.2018).

14. Сайт группы исследователей Radware [Электронный ресурс]. – Режим доступа: https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/, свободный (дата обращения: 19.10.2018).

15. Маслова М.А. Принципы безопасности интернета вещей // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(29). – С. 38–42.

16. Mirai Vulnerability Scanner [Электронный ресурс]. – Режим доступа: https://www.incapsula.com/mirai-scanner/, свободный (дата обращения: 17.11.2018)

17. Утилита Wireshark [Электронный ресурс]. – Режим доступа: https://www.wireshark.org/, свободный (дата обращения: 17.11.2018)

18. Коновалова С.В., Миронов А.Н. Вопросы информационной безопасности Интернета Вещей // ИТ-Стандарт. – 2016. – № 9. – С. 37–39.

References

1. Blog «MalwareMustDie» [Elektronnyy resurs]. – Rezhim dostupa: http://blog.malwaremustdie.org/2016/08 /mmd-0054-2016-pnscan-elf-worm -that.html, svobodnyy (data obrashcheniya: 13.10.2018).

2. Blog «KrebsonSecurity» [Elektronnyy resurs]. – Rezhim dostupa: https://krebsonsecurity.com /2016/09/krebsonsecurity-hit -with-record-ddos, svobodnyy (data obrashcheniya: 13.10.2018).

3. Sayt kompanii ArsTechnica [Elektronnyy resurs]. – Rezhim dostupa: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/, svobodnyy (data obrashcheniya: 13.10.2018).

4. Iskhodnyy kod virusnoy programmy-chervya Mirai [Elektronnyy resurs]. – Rezhim dostupa: https://github.com/jgamblin/Mirai-Source-Code, svobodnyy (data obrashcheniya: 13.10.2018).

5. Britanskiy novostnoy sayt «The Register» [Elektronnyy resurs]. – Rezhim dostupa: https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/, svobodnyy (data obrashcheniya: 15.10.2018).

6. Tuptuk N., Hailes S. Security of smart manufacturing systems // Journal of Manufacturing Systems. – 2018. – № 47. – С. 93–106.

7. Bagay D.I. Ugroza Internetu veshchey: botnet Mirai // Sovremennyye tekhnologii: aktual'nyye voprosy, dostizheniya i innovatsii: sbornik statey XIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – Penza: MTSNS «Nauka i Prosveshcheniye». – 2018. – S. 69–72.

8. Blog «KrebsonSecurity» [Elektronnyy resurs]. – Rezhim dostupa: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/, svobodnyy (data obrashcheniya: 15.10.2018).

9. Sayt veb-servisa monitoringa i zashchity ot DDoS atak Imperva Incapsula [Elektronnyy resurs]. – Rezhim dostupa: https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html, svobodnyy (data obrashcheniya: 15.10.2018).

10. Sayt kompanii SecurityIntelligence [Elektronnyy resurs]. – Rezhim dostupa: https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/, svobodnyy (data obrashcheniya: 16.10.2018).

11. Blog kompanii SecurityIntelligence [Elektronnyy resurs]. – Rezhim dostupa: https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/, svobodnyy (data obrashcheniya: 16.10.2018).

12. Blog «MalwareMustDie» [Elektronnyy resurs]. – Rezhim dostupa: http://blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html, svobodnyy (data obrashcheniya: 19.10.2018).

13. Stat'ya S. Edwards and I. Profetis, 16 Okt. 2016; [Elektronnyy resurs]. – Rezhim dostupa: http://security.rapiditynetworks.com/publications /2016-10-16/hajime.pdf, svobodnyy (data obrashcheniya: 19.10.2018).

14. Sayt gruppy issledovateley Radware [Elektronnyy resurs]. – Rezhim dostupa: https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/, svobodnyy (data obrashcheniya: 19.10.2018).

15. Maslova M.A. Printsipy bezopasnosti interneta veshchey // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2018. – № 3(29). – S. 38–42.

16. Mirai Vulnerability Scanner [Elektronnyy resurs]. – Rezhim dostupa: https://www.incapsula.com/mirai-scanner/, svobodnyy (data obrashcheniya: 17.11.2018)

17. Utilita Wireshark [Elektronnyy resurs]. – Rezhim dostupa: https://www.wireshark.org/, svobodnyy (data obrashcheniya: 17.11.2018)

18. Konovalova S.V., Mironov A.N. Voprosy informatsionnoy bezopasnosti Interneta Veshchey // IT-Standart. – 2016. – № 9. – S. 37–39.

БУХАРЕВ Дмитрий Александрович, магистрант кафедры вычислительной математики и высокопроизводительных вычислений высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: needleinspace@gmail.com

ВАГИН Сергей Владиславович, магистрант института спорта, туризма и сервиса ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: vaginserg.96@mail.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

BUKHAREV Dmitrii, student of the Department of computational mathematics and high-performance computing of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: needleinspace@gmail.com

VAGIN Sergey, student of the Institute of sport, tourism and service FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: vaginserg.96@mail.ru

SOKOLOV Alexander, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

УДК 004.8 + 004.438 Вестник УрФО № 4(30) / 2018, с. 20–26

Частикова В. А., Жерлицын С. А., Воля Я. И.

DOI: 10.14529/secur180403

НЕЙРОСЕТЕВОЙ МЕТОД ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО НЕФОРМАЛИЗОВАННОЙ СЕМАНТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ

В данной статье описаны основные алгоритмические блоки, различные сочетания которых позволяют решать ряд практически значимых задач, как, например, генерация изображений, описаний к изображениям или идентификацию личности. Основными технологиями, используемыми в этих блоках, являются: свёрточная нейронная сеть, развёртывающая сеть, рекуррентная нейросеть с долгой краткосрочной памятью, генеративно-состязательные нейронные сети и нейросетевой инструмент преобразования слов в вектора word2vec. Описана модификация, позволяющая преобразовать развёртывающую сеть в самостоятельный дискретный компонент без введения дополнительных функциональных зависимостей. Для каждого пункта приведено краткое описание и способ применения для решения поставленной задачи. Описана база данных, разработанная для организации процессов обучения и эксплуатации нейросетей, способ составления выборки для настройки нейронных сетей. Приведен алгоритм поиска человека по словесному описанию с применением описанных средств.

Ключевые слова: *рекуррентная нейронная сеть, развертывающая нейронная сеть, свёрточная нейронная сеть, генеративно-состязательная нейронная сеть, word2vec, машинное обучение.*

Chastikova V. A., Zherlitsyn S.A., Volya Y.I.

NEURAL NETWORK METHOD OF IDENTIFICATION BY UNFORMALIZED SEMANTIC CHARACTERISTICS

The article describes the main algorithmic blocks, the various combinations of which allow to solve practically important tasks, such as the generation of images, descriptions for images or identification of a person. The main technologies used in these blocks are: a convolutional neural network, a deconvolutional network, a recurrent neural network with a long short-term

memory, generative-competitive neural networks and a neural network word conversion tool into word2vec vectors. The described modification allows transform the deconvolutional network into the independent discrete component without introducing additional functional dependencies. For each item, a brief description and method of application for solving the task is given. There is a describing of the database developed for the organization of the processes of training and operation of neural networks, a method of drawing a sample for tuning neural network. The algorithm of the person search by the verbal description with the application of the described means is given.

Keywords: *recurrent neural network, deconvolutional neural network, convolutional neural network, generative-competitive neural network, word2vec, machine learning.*

Связка технологии идентификации и аутентификации широко применяется в настоящее время. Их сочетание позволяет регистрировать активность участников информационного обмена, поставлять услуги определенному клиенту и совершать прочие действия, требующие подтверждения личности со стороны субъекта или объекта. Однако даже идентификация, отвечающая за установление, но не приводящая к подтверждению личности, является важнейшей задачей во многих областях деятельности человека. Примерами тому является деятельность сыскных служб, поиск знакомых людей через сеть Интернет и даже первый этап авторизации.

Формализации подвергаются два наиболее естественных и близких человеку идентификатора: изображение и свободная речь. Конечно, в общем случае, технология позволяет использовать и другие описательные параметры, но в целях повышения наглядности принципов работы модели выбраны именно названные выше характеристики.

Под изображением понимается фотоснимок человека, в идеальном случае, фото лица в анфас. Для интерпретирования сложных массивов, коим и является изображение, существует технология, неоднократно доказывавшая свою эффективность, – свёрточная нейронная сеть.

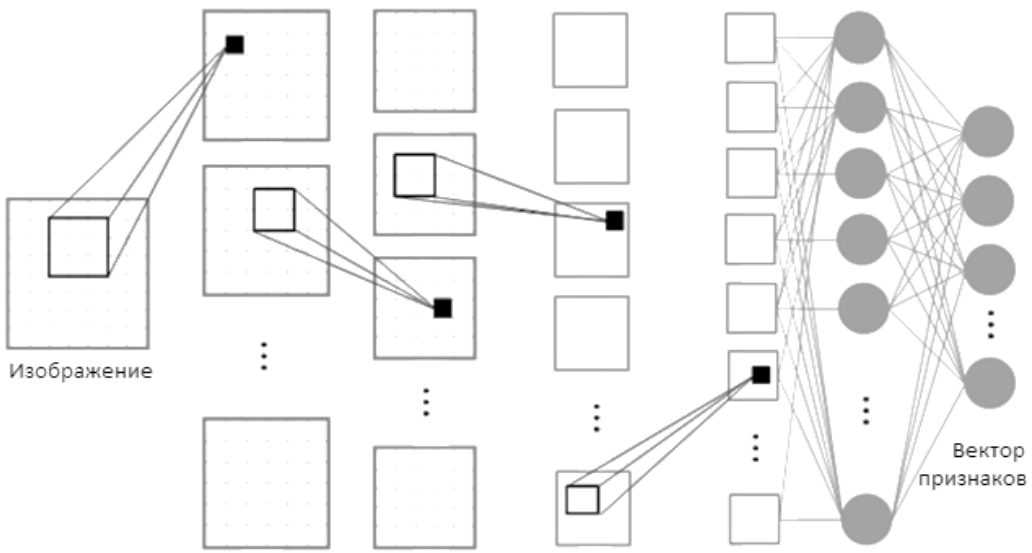

Рис. 1. Принцип работы свёрточной нейронной сети

Постановка задачи

Именно такие задачи решаются разработанными в ходе данного исследования алгоритмами. На базе стека нейросетевых технологий решается задача автоматизации приведения к единому, машинно-интерпретируемому и способному подвергаться операциям сортировки, сравнения и прочей обработки виду.

Свёрточная нейронная сеть

Принцип её работы заключается в постепенной конкретизации признаков, замеченных на изображении. С каждым слоем она переходит к набору всё более и более сложных признаков, составляя их карты, каждое значение в которых своей координатой обозначает область, где отслеживаемый признак находился, а значение – степень присутствия

рассматриваемого признака в соответствующей области [1, 2]. Таким образом, при последовательном просчёте достаточного количества слоев вплоть до уплотнения каждой из карт признаков до одного единственного значения становится возможным определение степени наличия заданных признаков во внешности человека [3]. Более подробно принцип работы показан на рисунке 1.

При достаточном количестве построенных признаков можно с той или иной степенью уверенности по образованному вектору чисел определить, какому человеку присущ рассматриваемый набор качеств. Следует отметить, что отображаемые качества, их интерпретация и отношение к конкретным чертам внешности выбираются алгоритмом самостоятельно в процессе обучения и результат является трудноинтерпретируемым для человека.

Развёртывающая нейронная сеть

Главными условиями для идентификации по такому параметру как внешность является полнота и однозначность описания [4]. В данном проекте она достигается в процессе обучения за счёт расширения свёрточной сети дополнительным модулем – так называемой развёртывающей сетью. По своему функционалу она выполняет действия, обратные свёртке. То есть в контексте поставленной задачи она восстанавливает изображение из вектора признаков и располагается следующим модулем за свёрточной сетью, принимая на свой вход её выход. Обучение данного каскада необходимо проводить исключительно в комплексе, так как именно композиция данных модулей гарантирует полноту и однозначность описания. Данный вывод обоснован тем фактом, что обученный модуль развёртывания дискретен, и на фиксированный входной сигнал реагирует однозначным выходом, а если при этом выход совпадает с изображением на входе свёрточной сети, что и достигается в процессе обучения, то вектор признаков достаточно полно описывает внешность продемонстрированной модели человека.

Свёрточная сеть состоит из нескольких чередующихся и повторяющихся блоков: слой свёртки, слой субдискретизации, или pooling, и полносвязные слои на выходе сети. Однако если первый и третий из них имеют обратные функции без фактора неопределенности, то субдискретизацию можно обратить, лишь имея данные об уже проделанном ранее прямом преобразовании, как это показано на рисунке 2, или внося некоторую дополнительную функциональную или вероятностную зависимость.

Рис. 2. Механизм субдискретизации

Во избежание нарушения дискретности данного элемента системы, а также его автономности и свободы применения в качестве независимого блока этот тип слоёв исключен из состава развёртывающей сети.

Обучение и генеративно-состязательные нейронные сети

При прямом обучении развёртывающей сети генерации изображений производится минимизация фитнесс-функции - суммы квадратов отклонений каждого пикселя выхода от оригинального изображения. При таком подходе возникает довольно распространённая проблема размытости результата, так как полученная функция имеет большой локальный экстремум в состоянии сети, приводящем к усреднению значений соседних пикселей.

Решением данной проблемы является технология генеративно-состязательной нейронной сети [5]. Её суть заключается в наличии двух конкурирующих элементов. Первый из них называют генератором, а второй дискриминатором. Генератор обучается созданию изображений, созданные им изображения подаются на вход дискриминатора, который обучается определению, искусственное изображение ему предоставлено или оригинальное. В случае угадывания дискриминато-

ром факта сгенерированности изображения в фитнесс-функцию, по которой обучается генератор, вносятся штрафные очки, которые должны быть минимизированы. Таким образом, генератор обучается более натурально подделывать изображения, а дискриминатор – более чётко определять, настоящие ему предъявлены данные или нет.

В поставленной задаче генератор имеет особенность: он состоит из композиции свёрточной и развёртывающей сетей. Соответственно, поправки, вносимые дискриминатором и влияющие на чувствительность системы к более мелким деталям, отражаются на обучении обоих блоков, что сказывается и на промежуточном для них векторе признаков.

Нейронные сети с долгой краткосрочной памятью

С помощью описанных выше средств реализуется механизм формирования векторного представления изображения лица человека. Каждому портрету сопоставляется точка многомерного пространства, однако целью работы является разработка механизма автоматического приведения неформализованного словесного описания к общему виду аналогично тому, как это было проделано с изображениями. Для этого необходим механизм экстрагирования семантического значения из анализируемых сообщений. С учётом поставленного условия отсутствия формализации исходная длина описания является неизвестной.

Для анализа временных рядов, в которых не определены по времени и продолжительности важные события, используются нейронные сети с долгой краткосрочной памятью (LSTM-сети) [6].

Особенность архитектуры LSTM-сети заключается в наличии рекуррентного модуля, способного запоминать и передавать зависимости на большое количество итераций, без размытия и потери важной информации. Это достигается за счёт контроля потоков информации на входах и на выходах памяти рекуррентного модуля. Регулирование осуществляется за счёт частичного пропускания в память новой важной информации, выделенной остальной частью сети и удаления неактуальной. Веса сети, отвечающие за обработку информации и регулирование её потоков, настраиваются в процессе обучения.

Таким образом, получая на входе семантическую характеристику, сеть обучается сопоставлять ей соответствующий вектор описания внешности соответствующего изображения. В этом и заключается основа механизма экстракции полезной семантической нагрузки из описания.

Анализ семантики естественных языков

Однако для того, чтобы передать на вход нейросети словесное описание, его всё же необходимо подвергнуть приведению к понятному для вычислителя виду. LSTM-сеть обладает константным количеством входов и способна принимать последовательности векторов заданной длины. Существует несколько методов преобразования человеческой речи в заданный вид. Наиболее очевидным, но вместе с тем и крайне неэффективным является побуквенное представление слов, так как отдельная буква несет в себе лишь фонетическую и грамматическую, но не семантическую нагрузку. При потоковом выявлении зависимости между названными сущностями нейросеть превращается в крайне громоздкий и неэффективный механизм в силу многообразия сочетаний букв, значений слов и непредсказуемости контекста.

Чтобы перейти на более высокий уровень абстракции, процедура оцифровки и нормализации текста перекладывается на технологию word2vec, предоставляющую возможность отобразить слова на векторное пространство заданной длины. В данном проекте именно из этих векторов и строится входная последовательность для LSTM-сети.

Word2vec - инструмент анализа семантики естественных языков, представляющий собой технологию, которая основана на дистрибутивной семантике и векторном представлении слов [7]. В основу алгоритма заложена нейронная сеть, анализирующая большие текстовые блоки и делающая из них выводы о смысловой близости встречающихся слов. Таким образом, расстояние в многомерном пространстве между векторами пропорционально смысловой близости соответствующих этим векторам слов, что позволяет использовать технологию в качестве подготовительного этапа для семантического анализа.

Как промежуточный итог исследования с помощью применения указанных технологий, их композиция образует инструмент для генерации изображения по словесному описанию. Итоговый механизм состоит из следующих блоков из числа обученных сетей и механизмов, описание которых приведено ранее:

1. Словесное описание поступает на вход преобразователя word2vec.

2. Преобразованные в последовательность векторов слова передаются на вход LSTM-сети. На выходе сеть генерирует вектор признаков внешности.

3. Вектор признаков внешности поступает на вход развёртывающей сети, которая генерирует изображение описанного человека.

Генерация описания

Выше были рассмотрены алгоритмические блоки, способные выполнять различные функции при определенных их конфигурациях. Аналогично генерации изображения по описанию осуществляется и обратная задача: используется уже обученная свёрточная сеть, генерирующая вектор характеристик внешности. Далее данный вектор посылается на вход новой LSTM-сети, обученной из вектора характеристик генерировать семантическое описание в виде последовательности многомерных точек пространства word2vec.

Обучающая выборка

Для обучения полученной модели собрана выборка, состоящая из пар фотография-описание. Для повышения скорости и оптимизации процесса обучения все фотографии приведены к одной форме и размеру, а также обесцвечены. Благодаря такой процедуре происходит не только стандартизация входа свёрточной сети, но и оптимизация её обучения, массив входных данных сокращается в 3 раза, так как остается вместо трёх каналов, каждый из которых отвечает за свой цвет, только один. При таком обучении на выходе развёртывающей сети, разумеется, будет происходить генерация также чёрно-белых портретов.

Для описания было принято решение задать ограничение на минимальное количество символов в целях повышения информативности и семантической нагрузки. Более для данного параметра нет никаких ограничений: словесное описание внешности человека на соответствующем изображении. В силу особенностей алгоритмов анализа описания и обучения других сетей при недостаточном описании каких-либо характеристик внешности они будут усредняться относительно степени их присутствия у обладателей описанных черт.

Организация хранения данных

Для сбора, хранения и обработки обучающей выборки и результатов работы моделей была разработана база данных. Все собранные и сгенерированные изображения и портреты снабжаются соответствующими метками и связями и записываются в базу. Реляционная схема базы данных приведена на рисунке 3. В ней хранятся не только обучающие материалы нейросетей, но и промежуточные результаты вычислений, например, вектора признаков, а также их вариации для разных опытных образцов нейронных сетей и, непосредственно, сами нейронные сети.

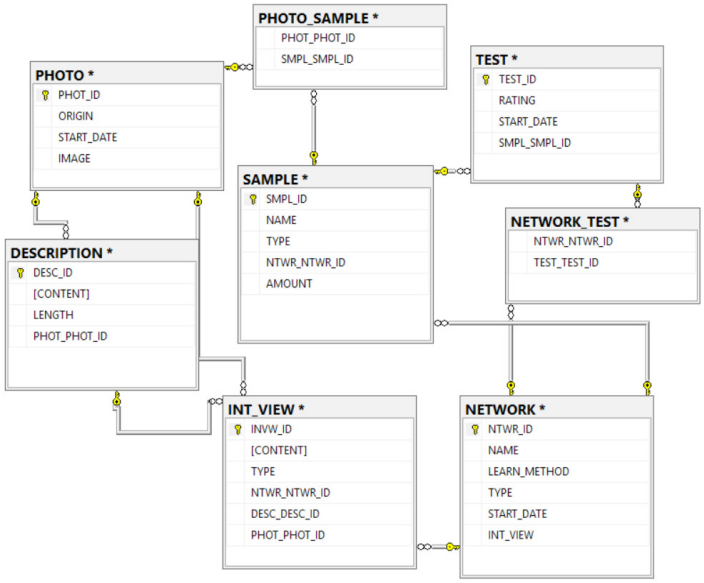

Рис. 3. Реляционная схема базы данных для обучения моделей

Система поиска по описанию

Благодаря стеку разработанных приемов

семантического и графического анализа появляется возможность осуществления гибкого поиска людей, причем не только по фотографии, но и по словесному неформализованному описанию внешности. Данный результат достигается за счёт возможности преобразования текста во внутренне представление, по которому в созданной базе данных можно найти фотографии людей с максимально близкими векторами значений. Преимуществом данного метода является то, что вектор характеристик внешности можно предрассчитывать с помощью первой из упомянутых в работе сетей – свёрточной нейронной сети. Принцип работы системы поиска представлен на рисунке 4.

Выводы

Таким образом, благодаря применению разработанных методик применения нейросетевых алгоритмов становится возможной процедура поиска, определения и идентификации личности по неформализованной семантической характеристике, выраженной в виде словесного описания внешности.

В ходе исследований разработана база данных, упрощающих взаимодействие описанных блоков, предложены новые способы и направления их применения.

Также описана методика решения нескольких других прикладных задач, как, например, генерация изображения человека по его описанию и получение семантической характеристики внешности по фотографии.

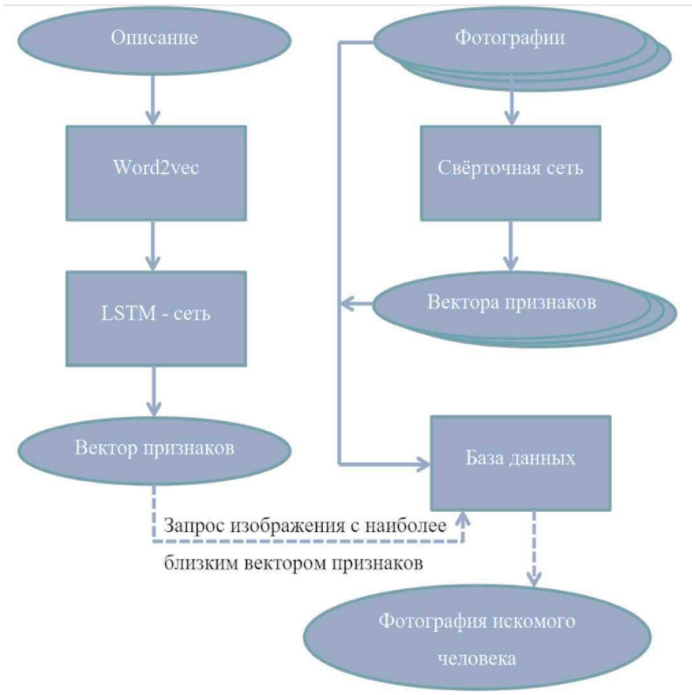

Рис. 4. Схема работы системы поиска

Литература

1. Le Cun Y., Bengio Y. Convolutional networks for images, speech, and time series. The handbook of brain theory and neural networks, 1995. T. 3361. №. 10. P. 1995.

2. Частикова В.А., Жерлицын С.А., Воля Я.И. Нейросетевой подход к решению задачи построения фоторобота по словесному описанию // Известия ВолгГТУ, 2018. №8.

3. Хайкин С. Нейронные сети. Полный курс 2-е изд. Пер. с англ. - М.: Издательский дом «Вильямс», 2006.

4. Частикова В.А., Малыхина М.П., Жерлицын С.А., Воля Я.И. Сравнительный анализ некоторых алгоритмов роевого интеллекта при обнаружении сетевых атак нейросетевыми методами // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2017. № 129. С. 106-115.

5. Hochreiter S., Schmidhuber J. Long short-term memory. Neural computation, 1997. Vol. 9, no. 8. Pp. 1735-1780.

6. Goodfellow, Ian J.; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron & Bengio, Yoshua (2014), "Generative Adversarial Networks" URL: https://arxiv.org/pdf/1406.2661.pdf (дата обращения: 18.09.2018).

7. Word2Vec. How does it work URL: https://code.google.com/archive/p/word2vec/ (дата обращения: 18.09.2018).

References

1. LeCun Y., Bengio Y. Convolutional networks for images, speech, and time series. The handbook of brain theory and neural networks, 1995. T. 3361. №. 10. P. 1995.

2. Chastikova V.A., Zherlicyn S.A., Volja Ja.I. Nejrosetevoj podhod k resheniju zadachi postroenija fotorobota po slovesnomu opisaniju // Izvestija VolgGTU, 2018. №8

3. Hajkin S. Nejronnye seti. Polnyj kurs 2-e izd. Per. s angl. M.: Izdatel'skij dom "Vil'jams", 2006.

4. Chastikova V.A., Malyhina M.P., Zherlicyn S.A., Volja Ja.I. Sravnitel'nyj analiz nekotoryh algoritmov roevogo intellekta pri obnaruzhenii setevyh atak nejrosetevymi metodami // Politematicheskij setevojj elektronnyj nauchnyj zhurnal Kubanskogogo sudarstvennogo agrarnogo universiteta, 2017. № 129. S. 106-115.

5. Hochreiter S., Schmidhuber J. Long short-term memory. Neural computation, 1997. Vol. 9, no. 8. Pp. 1735-1780.

6. Goodfellow, Ian J.; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron & Bengio, Yoshua (2014), "Generative Adversarial Networks" URL: https://arxiv.org/pdf/1406.2661.pdf (data obrashhenija: 18.09.2018).

7. Word2Vec. How does it work URL: https://code.google.com/archive/p/word2vec/ (data obrashhenija: 18.09.2018).

ЧАСТИКОВА Вера Аркадьевна, кандидат технических наук, доцент, доцент кафедры компьютерных технологий и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет». Россия, 350072, г. Краснодар, улица Московская, 2. E-mail: chastikova_va@mail.ru

ЖЕРЛИЦЫН Сергей Анатольевич, студент кафедры компьютерных технологий и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет». Россия, 350072, г. Краснодар, улица Московская, 2. E-mail: kpytooooo@gmail.com

ВОЛЯ Яна Игоревна, студент кафедры компьютерных технологий и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет». Россия, 350072, г. Краснодар, улица Московская, 2. E-mail: volya_y@mail.ru

CHASTIKOVA Vera, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Technologies and Information Security at the Kuban State Technological University. Russia, 350072, Krasnodar Krai, Krasnodar, Moskovskaya street, 2. E-mail: chastikova_va@mail.ru

ZHERLITSYN Sergey, student of the Department of Computer Technologies and Information Security of the Kuban State Technological University. Russia, 350072, Krasnodar, Moskovskaya street, 2. E-mail: kpytooooo@gmail.com

VOLYA Yana, student of the Department of Computer Technologies and Information Security of the Kuban State Technological University. Russia, 350072, Krasnodar, Moskovskaya street, 2. E-mail: volya_y@mail.ru

УДК 519.719.2 + 004.056 Вестник УрФО № 4(30) / 2018, с. 27–30

Бондакова О. С., Зязин В. П.

DOI: 10.14529/secur180404

О ПЕРВИЧНОЙ ОЦЕНКЕ ВЕРОЯТНОСТИ ВОЗНИКНОВЕНИЯ КОЛЛИЗИИ ДЛЯ УМЕНЬШЕННОГО ВАРИАНТА ХЭШ-ФУНКЦИИ «СТРИБОГ»

В статье обоснована актуальность исследований в направлении синтеза lightweight криптосхем, с целью их использования в технологиях IIoT и IoT. И необходимость проведения криптографического анализа таких «облегченных» криптопримитивов.

Ключевые слова: *уменьшенная хэш-функция «Стрибог», разностный криптоанализ хэш-функций, криптография в IIoT.*

Bondakova O. S., Ziazin V. P.

ABOUT THE PRIMARY ESTIMATION OF THE PROBABILITY OF THE COLLISION FOR A REDUCED VARIANT OF THE "STRIBOG" HASH-FUNCTION

The article proves the relevance of research in the direction of synthesis of lightweight cryptocircuits, with the aim of using them in IIoT and IoT technologies. And the need for cryptographic analysis of such "lightweight" cryptoprimitives.

Keywords: *reduced hash function "Stribog", difference cryptanalysis of hash functions, cryptography in IIoT.*

На XXIII международной научно-практической конференции «Комплексная защита информации» была представлена хэш-функция с размером хэш-кода 64 бит [1], в качестве возможного механизма защиты информации, в краткосрочном периоде времени. Малый размер блока позволяет сделать реализацию хэш-функции быстрой и не требующей больших ресурсов, что является её преимуществом для применения в устройствах IIoT. Однако определение оптимального количества раундов в ней является важной

задачей как со стороны криптографических качеств функции, так и её быстродействия. Эта задача требует проведение исследования стойкости хэш-функции к различным атакам

Одной из важных характеристик криптографической хэш-функции, является низкая вероятность возникновения коллизии. С учетом, предполагаемой области применения исследуемой хэш-функции, наибольший интерес вызывают коллизии возникающий для сообщений отличающихся в определенных позициях. На основании этого было принято решение о получении первичной оценки стойкости хэш-функции [1] по средствам применения к ней разностного метода криптографического анализа.

Кратко опишем основные особенности анализируемого примитива. Хэш-функция, описанная в [1], основана на модифицированной МД-конструкции [1], общий вид которой можно представить в виде рисунка 1.

Где h_1 – значение, получаемое применением одношаговой функции сжатия h к блоку сообщения m_1, N_1 – количество захэшированных до этого бит, Σ – результат сложения всех захэшированных блоков сообщения в кольце $Z_{2^{64}}$. Одношаговая функция сжатия h построена по схеме Миягучи-Пренеля:

$$h(m_i) = E(m_i, h_i \oplus N_i) \oplus m_i \oplus h_i.$$

Где $E(m_i, h_i \oplus N_i)$ - алгоритм блочного шифрования (внутренний блочный шифр). В качестве внутреннего блочного шифра используется XSPL-шифр.

Известно, что стойкость к коллизиям МД-конструкции и её модификаций, зависит от стойкости к коллизиям, используемой в них одношаговой функции сжатия. Поэтому представляется возможность, сведения анализа свойств функции к исследованию свойств внутреннего блочного шифра.

Разностный метод криптографического анализа является одним из классических методов криптоанализа блочных шифров [2]. Основные подходы и принципы, которого, были также описаны в работе [3]. Для нахождения коллизии для функции сжатия, необходимо построить дифференциальный путь, у которого разность открытых текстов равна разности, соответсвующих им, шифртекстов. Пример такого дифференциального пути для открытых текстов, различающихся только в первом полубайте, приведен на рис.2.

Посредством вычислительного эксперимента, были построены все возможные виды дифференциальных путей для размера блока равного 64 битам. Здесь и далее под видом дифференциального пути подразумевается расположение активных полубайт в разностях, входящих в него.

Для этого использовались характеристики параметров хэш-функции, приведенные в [1]. Из [1] известно, что при умножении вектора из 4-х полубайт на матрицу в линейном преобразовании, суммарный вес (количество активных полубайт) входного и результирующего векторов не должен быть меньше 5. Поэтому при построении всех видов дифференциальных путей после применения преобразования L рассматривались вектора всех весов, в которые могли перейти исходные вектора. Из полученных векторов составлялись все возможные комбинации, которые и образовывают блоки на выходе линейного преобразования L. Пример дифференциального пути на 4 раунда представлен на рисунке 2.

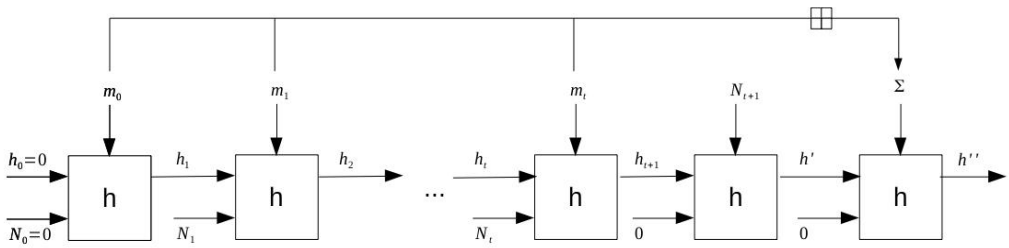

Рис. 1. Общая структура исследуемой хэш-функции

Для оценки вероятности каждого вида дифференциального пути, было вычислено $P=(\rho_\pi)^k$, где - количество активных S-боксов, входящих в путь. Также известно [1], что $\rho_\pi = \frac{1}{4}$ есть максимально возможная вероятность перехода одного полубайта разности в некоторый другой для выбранной подстановки. Пара сообщений, удовлетворяющая дифференциальному пути может быть найден, если вероятность пути $P < \frac{1}{2^n}$, в случае исследуемой функции n=64.

Поскольку для любого дифференциального пути можно вычислить его вероятность, будем считать эту вероятность вероятностью возникновения коллизия для сообщений, отличающихся в соответствующих позициях.

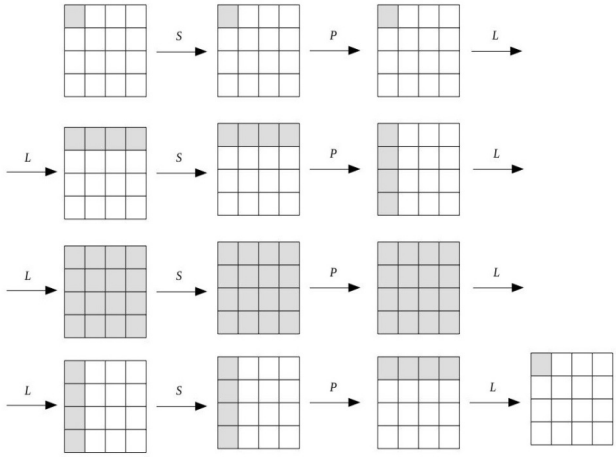

Рис. 2. Пример дифференциального пути на 4 раунда

Полученные в результате вычислительного эксперимента данные представлены в таблице 1. Каждый вид дифференциального пути охарактеризуем тремя параметрами:

1) количество активных полубайт в разности открытых текстов.

2) количество раундов, на которые «протянут» путь.

3) вероятность пути.

В соответствии со значениями этих параметров все виды дифференциальных путей разбиты на группы. Первый столбец таблицы содержит все возможные значения первого параметра от 1 до 16. В каждой строке содержится информация по всем видам путей имеющих соответственное значение первого параметра. Каждый из остальных столбцов отвечает возможным значениям второго параметра. В ячейках записаны значения вероятностей для наиболее крупных групп путей с соответствующими первым и вторым параметрами. В скобках указаны их примерные доли среди видов путей с таким же значением первого параметра.

Жирным шрифтом выделены значения вероятностей для групп путей, имеющих самую большую долю среди других групп с таким же значением первого параметра.

На основании данных таблицы можно сделать вывод, что подход синтеза хэш-функции в [1], позволяет с большой долей вероятности достичь хороших криптографических качеств примитива, имеющего размер хэш-кода 64 бит. Поскольку основная большая часть дифференциальных путей имеют оценку сверху вероятности , или достаточно близкую к ней.

Невозможно построить дифференциальные пути более на 4 раунда, в не зависимости от конкретных значений параметров преобразований, если выполнены требования к параметрам преобразований [1].

В дальнейшем планируется продолжить вычислительные эксперименты и убедится, что при фиксации параметров преобразовании хэш-функции, коллизий не возникает, либо они имеют вероятность близкую к $\frac{1}{2^{64}}$.

Количество активных полубайт в разности открытых текстов	**1 раунд**	**2 раунд**	**3 раунд**	**4 раунд**
1	–	–	–	**2-50 (100%)**
2	–	–	–	**2-62 (77%)**
3	–	–	2^{-46}	**2-62 (83%)**
4	–	2^{-40}	2^{-52}	**2-62 (76%)**
5	–	–	2^{-52}	**2-62 (62%)**
6	–	2^{-42}	**2^{-60} (36%)**	2^{-62}
7	2^{-16}	2^{-42}	**2^{-60} (38%)**	2^{-62}
8	2^{-18}	2^{-44}	**2^{-60} (39%)**	2^{-62}
9	2^{-20}	2^{-44}	**2^{-62} (66%)**	2^{-62}
10	2^{-22}	2^{-44}	**2^{-62} (89%)**	2^{-62}
11	2^{-24}	2^{-46}	**2^{-62} (96%)**	2^{-62}
12	2^{-24}	2^{-46}	**2^{-60} (34%)**	2^{-62}
13	2^{-26}	2^{-46}	**2^{-62} (39%)**	2^{-62}
14	2^{-28}	2^{-48}	**2^{-62} (49%)**	2^{-62}
15	2^{-30}	2^{-48}	**2^{-62} (65%)**	2^{-62}
16	2^{-32}	2^{-50}	**2^{-62} (88%)**	2^{-60}

Литература

1. Бондакова О. С. «Уменьшенный вариант хэш-функции «Стрибог» и его свойства» - XXIII научно-практическая конференция «Комплексная защита информации» // https://kzi.su/

2. BihamE., ShamirA. Differential Cryptanalysis of DES-ike Cryptosystems (Extended Abstract). Lect. Note. Comp. Sci,. 1991.

3. Kiryukhin V., "Exact Maximum Expected Differential and Linear Probability for 2-round Kuznyechik", 7th Workshop on Current Trends in Cryptology (CTCrypt 2018) ,May 28-30, 2018.

References

1. Bondakova O. S. «Umen'shennyj variant hehsh-funkcii «Stribog» i ego svojstva» - XXIII nauchno-prakticheskaya konferenciya «Kompleksnaya zashchita informacii» // https://kzi.su/

2. BihamE., ShamirA. Differential Cryptanalysis of DES-ike Cryptosystems (Extended Abstract). Lect. Note. Comp. Sci,. 1991.

3. Kiryukhin V., "Exact Maximum Expected Differential and Linear Probability for 2-round Kuznyechik", 7th Workshop on Current Trends in Cryptology (CTCrypt 2018) ,May 28-30, 2018.

БОНДАКОВА Ольга Сергеевна, студент кафедры Информационной безопасности Института кибернетики ФГБОУ ВО «МИРЭА – Российский технологический университет». Россия, 119454 г. Москва, проспект Вернадского, дом 78. E-mail: o.bondakova@mail.ru

ЗЯЗИН Валентин Петрович, профессор кафедры информационной безопасности, Института Кибернетики ФГБОУ ВО «МИРЭА – Российский технологический университет». 119454, г. Москва, проспект Вернадского, 78. E-mail: zval47@yandex.ru

BONDAKOVA Olga, student of the Information Security Department of the Institute of Cybernetics, FSBEI of HE "MIREA - Russian Technological University". Russia, 119454, Moscow, Vernadskogo Avenue, Building 78. E-mail: o.bondakova@mail.ru

ZIAZIN Valentin, professor at Information Security department of Cybernetics Institute Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University". 119454, Moscow, Vernadskogo Avenue, Building 78. E-mail: zval47@yandex.ru

УДК 004.056 + 003.26 Вестник УрФО № 4(30) / 2018, с. 31–37

Кляус Т. К., Гатчин Ю. А.

DOI: 10.14529/secur180405

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ С ПОМОЩЬЮ ДЕРЕВЬЕВ СОБЫТИЙ

В статье рассматриваются графические подходы к анализу возможных сценариев реализации угроз в информационных системах, основанные на использовании направленных ациклических графов. Рассматриваются особенности применения деревьев атак в качестве инструмента оценки безопасности информационной системы. Предлагается подход для определения вероятностей реализации атак на информационную систему на основе метода анализа деревьев событий. Для иллюстрации предлагаемого подхода на основе данных каталога общих шаблонов атак CAPEC построена блок-схема алгоритма прогнозирования вероятностей реализации атак на идентификаторы сеанса и ресурсов.

Ключевые слова: *информационная безопасность, атака, деревья атак, деревья событий, оценка рисков безопасности*

Klyaus T. K., Gatchin Yu. A.

PROBABILITY EVALUATION OF ATTACKS ON INFORMATION SYSTEM USING EVENT TREE ANALYSIS

The article deals with graphical approaches to analysis of possible information systems threats realization scenarios based on the use of directed acyclic graphs. The features of attack trees usage as a tool for information systems security assessment are considered. An approach for determining the likelihood of attacks realization based on the event tree analysis is proposed. To illustrate the proposed approach, a block scheme for predicting the likelihood of attacks on session and resource IDs based on the catalog of common attack patterns (CAPEC) is built.

Keywords: *information security, attack, attack trees, event trees, information security risk assessment.*

Вследствие постоянного усложнения архитектуры информационных систем (ИС), роста числа уязвимостей в используемом программном обеспечении (ПО), улучшения технических возможностей потенциальных нарушителей, на предприятиях и в организациях возникает необходимость в разработке модели угроз (атак), необходимой для после-

дующего определения перечня мер и средств защиты информации. Как правило, проблема выбора средств защиты информации (СЗИ) представляет собой оптимизационную задачу выбора при заданных ограничениях минимизации стоимости при требуемой эффективности мер защиты или максимизации эффективности мер защиты при ограничении на стоимость средств [1].

При разработке модели угроз наибольший интерес для специалистов по информационной безопасности представляют угрозы, обусловленные действиями субъекта (антропогенные угрозы), поскольку вероятности возникновения угроз, источниками которых являются технические средства, могут быть рассчитаны с помощью методов теории надежности, а вероятности стихийных бедствий и природных катастроф могут быть определены на основе статистических данных или рассчитаны на этапах проектирования, строительства и эксплуатации объектов (помещений). В настоящее время широкое распространение получили графические подходы к представлению и анализу сценариев реализации угроз, основанные на использовании направленных ациклических графов. Графические подходы обладают рядом преимуществ: они наглядны, позволяют представить атаки (угрозы, уязвимости) в иерархическом виде, позволяют производить качественный и количественный анализ, для некоторых подходов существует программное обеспечение для проведения расчетов. Наиболее подробное описание графических подходов, основанных на использовании направленных ациклических графов, приведено в исследовании [2]. Авторы данной статьи группируют рассматриваемые ими формализмы, опираясь на два основных критерия:

— Моделирует ли рассматриваемый подход атаки и (или) защитные меры;

— Является ли подход статическим (временной аспект не учитывается) или последовательностным (временной аспект влияет на рассматриваемые действия).

Классификация подходов к моделированию атак, предложенная в статье [2], представлена на рис. 1.

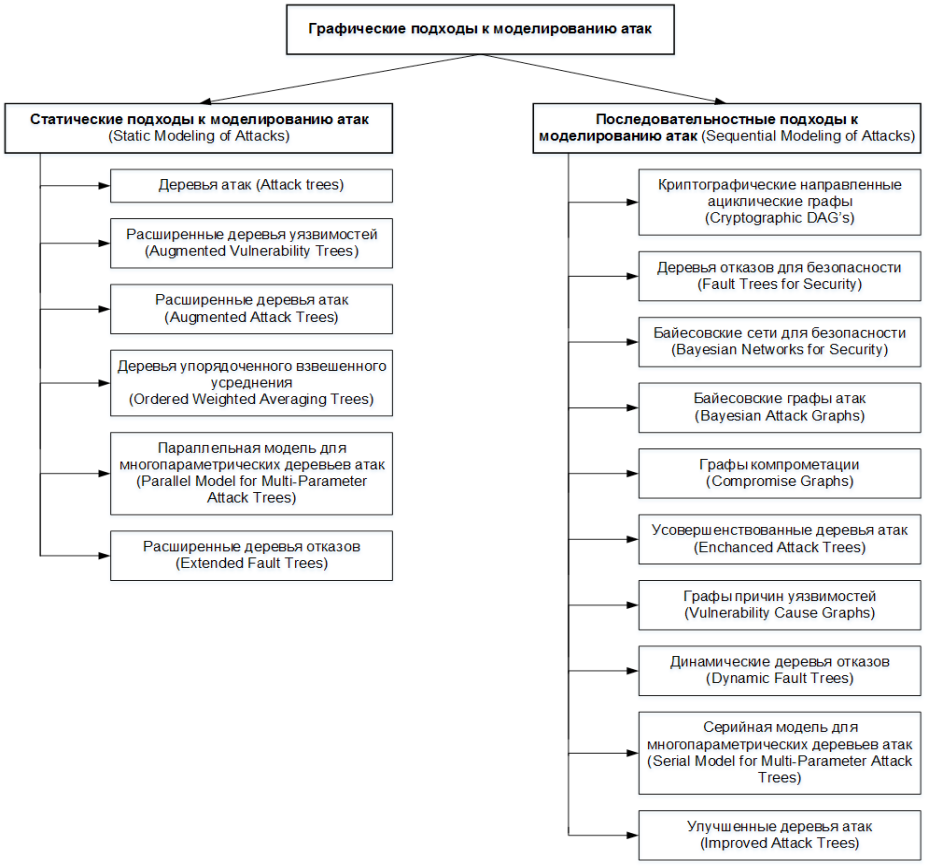

Рис. 1. Классификация графических подходов к моделированию атак [2]

Наиболее популярным подходом к анализу возможных способов реализации угроз и представления их в структурированном

виде являются деревья атак. Понятие деревьев атак было популяризировано Б. Шнайером [3] в качестве инструмента для оценки безопасности систем. Прототипом деревьев атак являются деревья отказов, применяющиеся в теории надежности и служащие для графического описания комбинаций событий, приводящих к отказу системы [4].

Дерево атак представляет собой связный граф, не содержащий циклов и кратных ребер. Вершина дерева (корневой узел) обозначает конечную цель атакующей стороны. Вершины, соединенные ребрами с корнем дерева, представляют собой действия атакующей стороны, которые она предпринимает для достижения поставленной цели. Конечная вершина, из которой не выходит ни одного нового ребра, называется листовым узлом и представляет собой действие атакующей стороны или защитную меру, которая не может быть разложена на составляющие. Вершины, не являющиеся листовыми узлами или корнем, называются узлами ветвления. Узлы ветвления представляют собой промежуточные состояния или подцели атакующего и обозначаются как узлы «И» (конъюнктивные узлы) или узлы «ИЛИ» (дизъюнктивные узлы). Для того, чтобы была достигнута цель узла «И», все исходящие из него вершины должны быть истинными – должно выполняться каждое действие злоумышленника из всей совокупности дочерних элементов узла ветвления. Истинное состояние узла «ИЛИ» достигается в случае, если хотя бы один из его дочерних элементов принимает истинное значение.

В настоящее время исследования деревьев атак фокусируются на улучшении эффективности формализма [5], а также на основе совместного использования деревьев атак с другими формализмами – сетями Байеса [6], сетями Петри [7], деревьями отказов [8] и методом вариантов злоупотребления (misuse cases) [9].

Широкое применение деревьев атак объясняется возможностью их использования как для качественного, так и для количественного анализа рисков. С помощью метода восходящего анализа (присвоения значений атрибутов листовым узлам и дальнейшего расчета значения для корневого узла) могут быть найдены такие атрибуты, как: затраты на проведение атаки, ее трудность и вероятность успешного проведения, наличие специальных навыков и оборудования у атакующей стороны и т.д. Области значений атрибутов могут варьироваться в зависимости от их содержания: это могут быть булевы значения, значения номинальной шкалы, действительные числа, а также дискретные или непрерывные распределения вероятностей [10]. Одним из наиболее часто рассчитываемых с помощью деревьев атак атрибутов является вероятность успешной реализации атаки [8, 11], поскольку определение ее значения необходимо для оценки рисков информационной безопасности.

В данной работе предлагается противоположный подход для расчета значений вероятностей атак на ИС, а именно, выполнение анализа дерева атак с корневого узла, поскольку данный подход также базируется на хорошо проработанной методической основе. За основу взят метод анализа деревьев событий (ETA – Event Tree Analysis), рекомендованный ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» [12] и представляющий собой графический метод представления взаимоисключающих последовательностей событий, следующих за появлением исходного события. Данный метод применяется как для качественной, так и для количественной оценки рисков. Количественная оценка рисков, в отличии от качественной, предполагает использование точных численных значений для ряда параметров, необходимых для расчета рисков безопасности (вероятности или прогнозируемого числа инцидентов, следствием которых может быть нанесение ущерба активам организации, величины ущерба, частоты возникновения угроз и т.д.). Качественная оценка рисков основывается на описании сценариев угроз, для анализа которых применяется фиксированная шкала значений (например, «низкий», «средний», «высокий»).

Каждая ветвь дерева событий представляет собой вероятность того, что все события на этом пути произойдут, поэтому вероятность результата вычисляют как произведение отдельных условных вероятностей и вероятности начального события при условии независимости событий.

К основному преимуществу метода ETA относят возможность анализа сценариев развития событий после возникновения начального события. Недостатком является то, что реализация каждого последующего события обусловлена сочетанием событий, произошедших в предыдущих точках ветвления схемы дерева событий, что вызывает необходи-

мость рассматривать все взаимосвязи по возможным путям развития событий [12].

Для реализации в данной статье метода ETA представим дерево атак на ПО (рис. 2), корневым узлом которого является нарушение конфиденциальности информации, контроля доступа и авторизации путем реализации атак на идентификаторы сеанса и ресурсов. Данный пример дерева атаки был построен на основе данных каталога общих шаблонов атак CAPEC (Common Attack Pattern Enumeration and Classification), созданного Министерством внутренней безопасности США в рамках стратегической инициативы Software Assurance (SwA) Управления кибербезопасности и коммуникаций (CS&C) [13]. Каталог шаблонов атак CAPEC и список недостатков программного обеспечения CWE (Common Weakness Enumeration) поддерживаются MITRE Corporation [14].

Вероятность атаки с использованием доверенных учетных данных примем равной 1,0. Условные вероятности в узлах ветвления определяют вероятность наступления указанного события на основе критерия «да» или «нет», при этом сумма вероятностей, определяющих оба события, принимается равной 1,0. Условная вероятность листовых событий определяется произведением вероятностей, определенных в предшествующих узлах ветвления. Полученные значения дают оценку расчетного прогноза условных вероятностей атак с использованием доверенных учетных данных, которые может предпринять атакующая сторона. Сумма условных вероятностей, соответствующих атакам, указанным в листовых узлах, также равна 1,0.

Значения вероятностей событий для прогнозирования вероятностей атак присваиваются на основании имеющихся данных о недостатках и уязвимостях, которыми обладает рассматриваемое ПО и которыми может воспользоваться атакующая сторона. Данная оценка вероятности зависит от точности экспертных оценок вероятностей наступления

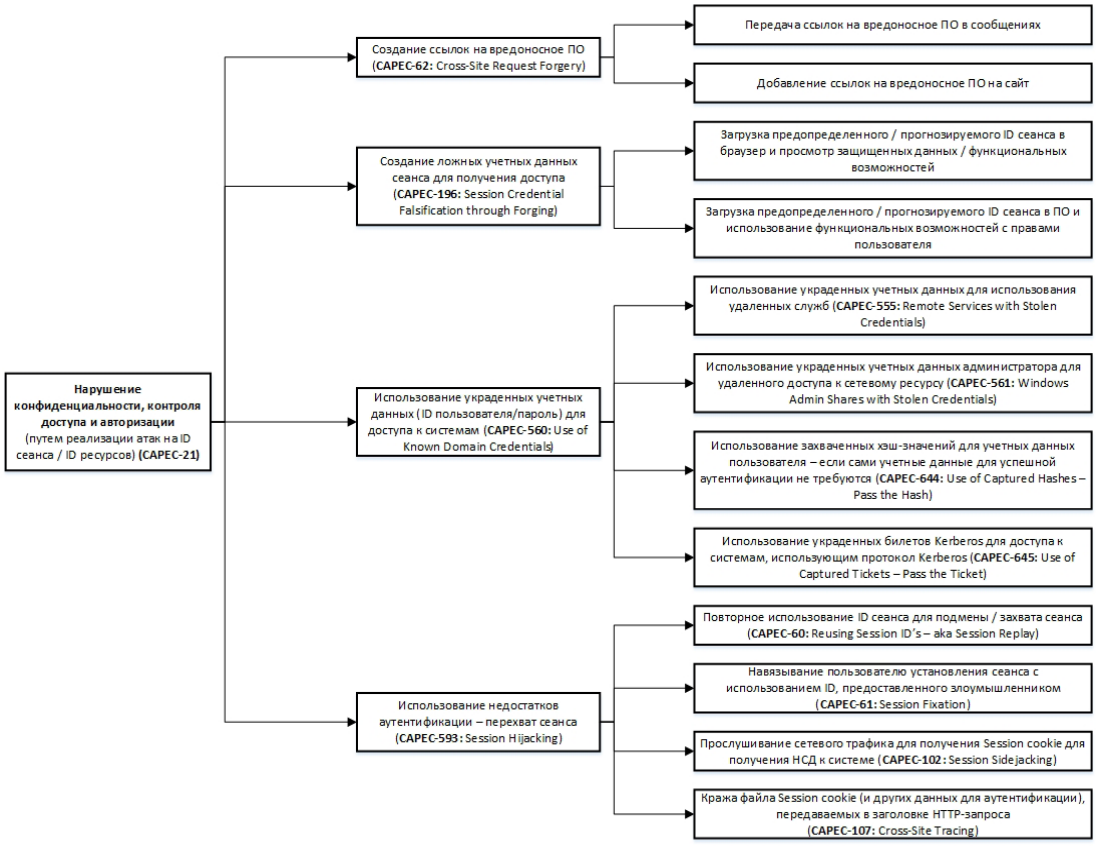

Рис. 2. Дерево атак на идентификаторы сеанса и ресурсов, построенное на основе каталога общих шаблонов атак CAPEC

Представим построенное дерево виде блок-схемы, в которой корневой узел располагается в левом верхнем углу. Узлы ветвления и листовые узлы изображаются в виде ромбов и прямоугольников, соответственно (рис. 3).

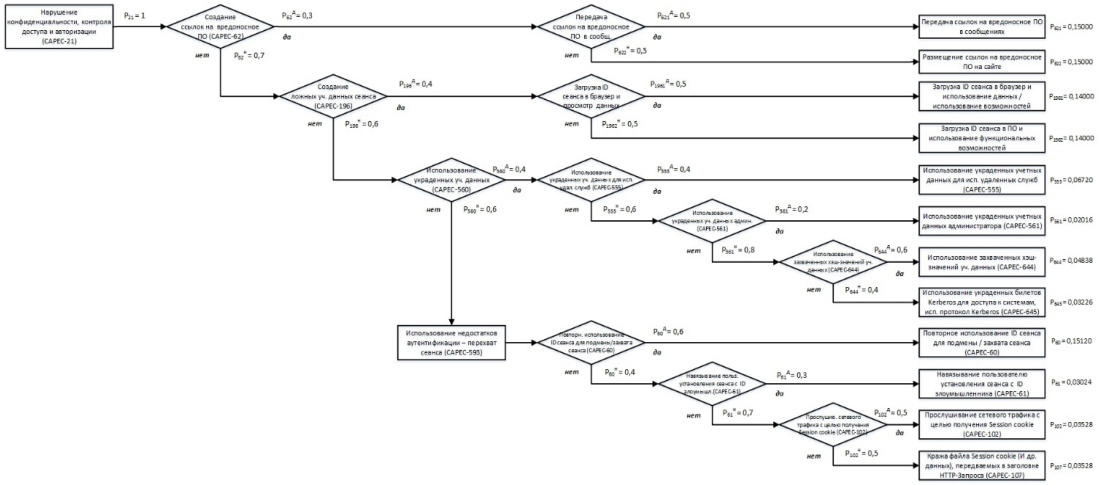

Рис. 3. Блок-схема алгоритма прогнозирования вероятности атак на идентификаторы сеанса и ресурсов с целью нарушения конфиденциальности информации, контроля доступа и авторизации с присвоенными и рассчитанными значениями вероятностей атак

событий в узлах ветвления. Для иллюстрации предлагаемого в настоящей работе подхода на рис. 3 приведен пример расчета вероятностей атак, основанных на использовании доверенных учетных данных. Для присвоения значений вероятностей атак был проанализирован ряд параметров, указанных в каталоге общих шаблонов атак CAPEC: вероятность реализации атаки, степень серьезности последствий реализации атаки, уровень требуемых навыков злоумышленника и количество соответствующих недостатков программного обеспечения CWE.

В настоящее время наблюдается широкое применение графических подходов к моделированию атак и защитных мер – они используются для анализа состояния информационной безопасности в системах SCADA, системах голосования, мобильной связи, для анализа удаленных и социотехнических атак [2]. Наиболее распространенным графическим подходом к моделированию атак являются деревья атак, представляющие собой модель, с помощью которой легко представляются схемы последовательных действий, при этом используется классический алгоритмический аппарат [15]. Существует тенденция интеграции деревьев атак с другими формализмами. В настоящей работе предлагается подход к определению вероятности реализации атак на основе метода анализа деревьев событий – в данном случае для расчета вероятностей используется нисходящий, а не восходящий подход, применяемый при анализе деревьев атак. Данный подход позволяет выполнять количественный и качественный анализ возможных атак на ИС, в дальнейшем полученные с его помощью результаты могут использоваться в расчетах при оценке рисков безопасности ИС. Однако необходимо отметить, что для выполнения корректного количественного анализа деревьев событий существует проблема поиска статистических данных об атаках.

Литература

1. Хализев В.Н., Кузьмин Д.И. Методика выбора оптимального набора средств программно-аппаратной защиты информации // Физико-математические науки и информационные технологии: проблемы и тенденции развития: сб. ст. по матер. VIII междунар. науч.-практ. конф. – 2012. – № 8. – С. 102-107.

2. Kordy B., Pietre-Cambacedes L., Schweitzer P. DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees // Computer Science Review. – 2014. – Vol. 13-14. – P. 1-38.

3. Schneier B. Attack trees // Dr. Dobb's Journal of software tools. – 1999. – № 24(12). – P. 21-29.

4. Кляус Т.К., Гатчин Ю.А. Применение графического представления атак в моделировании угроз безопасности информации // Научно-технический вестник Поволжья. – 2017. – № 3. – С. 108-110.

5. Gadyatskaya O., Trujillo-Rasua R. New Directions in Attack Tree Research: Catching up with Industrial Needs // GraMSec 2017: 4th International Workshop on Graphical Models for Security. – 2017. – P. 115-126.

6. Gribaudo M., Iacono M., Marrone S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees // Electronic Notes in Theoretical Computer Science. – 2015. – Vol. 310. – P. 91-111.

7. Dalton G.C., Mills R.F., Colombi J.M., Raines R.A. Analyzing Attack Trees using Generalized Stochastic Petri Nets // Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY. – 2006. – P. 116-123.

8. Fovino I.N., Masera M., De Cian A. Integrating cyber attacks within fault trees // Reliability Engineering & System Safety. – 2009. – Vol. 94(9). – P. 1394–1402.

9. Tondel I. A., Jensen J., Rostad L. Combining Misuse Cases with Attack Trees and Security Activity Models // 2010 International Conference on Availability, Reliability and Security. – 2010. – P. 438-445.

10. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees // International journal of secure software engineering. – 2012. – Vol. 3(2). – P. 1-35.

11. Edge K.S., Dalton D.C., Raines R.A., Mills R.F. Using attack and protection trees to analyze threats and defenses to homeland security // MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications. – 2006. – P. 953-959.

12. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска // Москва: Стандартинформ. – 2012.

13. CAPEC – Common Attack Pattern Enumeration and Classification // A community resource for identifying and understanding attacks. URL: https://capec.mitre.org/ (дата обращения: 03.10.2018)

14. MITRE // The MITRE Corporation. URL: https://www.mitre.org/ (дата обращения: 03.10.2018)

15. Кляус Т. К., Наумов А. Д., Гатчин Ю. А., Бондаренко И. Б. Сравнительное исследование применимости деревьев атак-контрмер и метода куста событий для оценки безопасности информационных систем // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 2(28). – С. 36-42.

References

1. Halizev V.N., Kuz'min D.I. Metodika vybora optimal'nogo nabora sredstv programmno-apparatnoj zashchity informacii. Fiziko-matematicheskie nauki i informacionnye tekhnologii: problemy i tendencii razvitiya: sb. st. po mater. VIII mezhdunar. nauch.-prakt. konf., 2012, no. 8, pp. 102-107.

2. Kordy B., Pietre-Cambacedes L., Schweitzer P. DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees. Computer Science Review, 2014, Vol. 13-14, pp. 1-38.

3. Schneier B. Attack trees. Dr. Dobb's Journal of software tools, 1999, no. 24(12), pp. 21-29.

4. Klyaus T.K., Gatchin Ju.A. The Use of Attacks Graphical Representation for Threat Modeling [Primenenie graficheskogo predstavlenija atak v modelirovanii ugroz bezopasnosti informacii]. Nauchno-tehnicheskij vestnik povolzh'ja [Scientific and Technical Bulletin of the Volga Region], 2017, no. 3, pp. 108-110.

5. Gadyatskaya O., Trujillo-Rasua R. New Directions in Attack Tree Research: Catching up with Industrial Needs. GraMSec 2017: 4th International Workshop on Graphical Models for Security, 2017, pp. 115-126.

6. Gribaudo M., Iacono M., Marrone S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. Electronic Notes in Theoretical Computer Science, 2015, Vol. 310, pp. 91-111.

7. Dalton G.C., Mills R.F., Colombi J.M., Raines R.A. Analyzing Attack Trees using Generalized Stochastic Petri Nets. Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2006, pp. 116-123.

8. Fovino I.N., Masera M., De Cian A. Integrating cyber attacks within fault trees. Reliability Engineering & System Safety, 2009, Vol. 94(9), pp. 1394–1402.

9. Tondel I. A., Jensen J., Rostad L. Combining Misuse Cases with Attack Trees and Security Activity Models. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 438-445.

10. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees. International journal of secure software engineering, 2012, Vol. 3(2), pp. 1-35.

11. Edge K.S., Dalton D.C., Raines R.A., Mills R.F. Using attack and protection trees to analyze threats and defenses to homeland security. MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications, 2006, pp. 953-959.

12. GOST R ISO/IEC 31010-2011. Risk management. Risk assessment techniques. Moscow, Standartinform, 2012.

13. CAPEC – Common Attack Pattern Enumeration and Classification. A community resource for identifying and understanding attacks. Available at: https://capec.mitre.org/

14. The MITRE Corporation. Available at: https://www.mitre.org/

15. Klyaus T. K., Naumov A. D., Gatchin Yu. A., Bondarenko I. B. A Comparative Study of Attack-Defense Trees and Event Bush Method Applicability for Information Systems Security Assessment [Sravnitel'noe issledovanie primenimosti derev'ev atak-kontrmer i metoda kusta sobytij dlya ocenki bezopasnosti

informacionnyh sistem]. Vestnik UrFO. bezopasnost' v informacionnoj sfere [UrFR Newsletter. Information Security], 2018, no. 2(28), pp. 36-42.

КЛЯУС Татьяна Константиновна, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: t_klyaus@corp.ifmo.ru

ГАТЧИН Юрий Арменакович, доктор технических наук, профессор кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: gatchin@mail.ifmo.ru

KLYAUS Tatiana, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: t_klyaus@corp.ifmo.ru

GATCHIN Yurii, doctor of technical sciences, professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: E-mail: gatchin@mail.ifmo.ru

УДК 004.021 + 343.143 Вестник УрФО № 4(30) / 2018, с. 38–42

Максимова Е. А., Баранов В. В., Зязин В. П.

DOI: 10.14529/secur180406

МОДЕЛЬ ОЦЕНКИ РИСКОВ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Количество компьютерных преступлений постоянно возрастает. В это же время показатели расследования их остаются на низком уровне и отражают низкую степень профессионализма сотрудников правоохранительных органов. В ходе расследования данного вида преступлений не исключена ситуация «эксперт-возможный злоумышленник». Следовательно, необходима соответствующая оценка рисков.

Предлагается для обсуждения разработанная модель «эксперт-возможный злоумышленник». Элементы модели: набор возможных мотивов, соответствующий набор личностных характеристик, соотношение между возможными угрозами и мотивами потенциального злоумышленника–эксперта. Стоимость возможного ущерба от совершенного компьютерного преступления в количественной оценке рисков обоснована с точки зрения законодательства. В том случае, когда оценочная величина риска больше допустимой, то предлагается принять решение о возможности участия эксперта в работе. Если вариант привлечения иного специалиста не возможен, то в ходе следственных мероприятий предлагается использовать программу видеозахвата.

Предложенная модель оценки рисков позволит автоматизировать процесс работы с компьютерными преступлениями на этапе расследования и повысить уровень их раскрываемости.

Ключевые слова: *риск, компьютерное преступление, расследование, мотив, угроза, архитектура, модель.*

Maksimova E. A., Baranov V. V., Ziazin V. P.

THE MODEL OF RISK ASSESSMENT IN THE INVESTIGATION OF COMPUTER CRIMES

The number of computer crimes is constantly growing. At the same time, their investigation indicators remain low and reflect the low degree of professionalism of law enforcement officers. During the investigation of this type of crime, the situation is not excluded: "an expert-possible attacker". Therefore, an appropriate risk assessment is necessary.

The developed model "expert-possible attacker" is proposed for discussion. Elements of the model: a set of possible motives, a corresponding set of personal characteristics, the relationship between possible threats and motivations of a potential attacker-expert. The cost of possible damage from a committed computer crime in the quantitative assessment of risks is justified from the point of view of legislation.

In the event that the estimated value of the risk is more than acceptable, it is proposed to

decide on the possibility of the expert's participation in the work. If the option of engaging another specialist is not possible, then during the investigation activities it is proposed to use the video capture program.

The proposed model of risk assessment will allow to automate the process of working with computer crimes during the investigation phase and to raise their level of disclosure.

Keywords: *risk, computer crime, investigation, motive, threat, architecture, model.*

В последнее время количество компьютерных преступлений (КП) постоянно увеличивается. Так, согласно данных Главного информационно-аналитического центра Министерства внутренних дел РФ, количество их за последние 10 лет увеличилось в 22,3 раза и ежегодно продолжает увеличиваться, в среднем, в 3,5 раза. Кроме того, ежегодный размер материального ущерба от КП - 613,7 млн. рублей; средний ущерб потерпевшего от 1 КП - 1,7 млн. рублей. В это же время расследуется около 49% преступлений; обвинительные приговоры выносятся в 25,5% случаев от общего числа возбужденных уголовных дел; средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43,5% и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению указанных преступных посягательств.

Сегодня при работе с КП применяются стандартные алгоритмы действий, не учитывающие специфик данного вида деяний [2-5]. Это является одной из причин роста киберпреступности и низким показателем их раскрытия. Таким образом, необходим новый подход к работе, эффективность которого, в том числе определяется оценкой рисков.

Сравнительный анализ методов и этапов работы с КП показал существенное отличие в работе с данного вида деянием. На этапе расследования КП привлекаются эксперты. Высококвалифицированных специалистов, способных провести экспертизу в данном направлении не достаточно. Таким образом, не исключена ситуация «эксперт-возможный злоумышленник». Следовательно, необходима оценка рисков, связанных с данной ситуацией.

В разработанной модели «эксперт-возможный злоумышленник» (рисунок 1) выделен набор возможных мотивов [1]:

М1 – Причинение имущественного ущерба путем мошенничества или иным преступным путем.

М2 – Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.

М3 – Получение конкурентных преимуществ.

М4 – Причинение имущественного ущер-

Рис. 1. Схема работы с экспертами при расследовании компьютерных преступлений

ба путем обмана или злоупотребления доверием

М5 – Непреднамеренные, неосторожные или неквалифицированные действия

М6 – Любопытство или желание самореализации (подтверждение статуса).

М7 – Месть за ранее совершенные действия.

М8 – Идеологические или политические мотивы.

Каждый из представленных мотивов соответствует набору личностных характеристик (таблица 1).

Так как в УК за совершенное компьютерное преступление предусмотрен либо штраф, либо срок отбывания наказания, то можно рассмотреть в качестве оценочного эквивалента - стоимость возможного ущерба от совершенного компьютерного преступления.

При этом, для оценки срок-эквивалента, так как отсутствует точная денежная оценка, то можно ввести показатель Е – одна условная денежная единица, соответствующая одному году лишения свободы и оценить стоимость возможного ущерба по каждому виду компьютерного преступления.

Таблица 1

Соответствие возможных мотивов показателям характеристик личности

Показатели характеристики личности	Мотивы
Уровень тревожности (U1)	М3, М5
Уровень упорства (U2)	М3, М6, М7
Уровень агрессию(U3)	М1, М6, М7,М4,М5
Уровень обидчивость(U4)	М1, М6, М7,М5
Уровень жадности (U5)	М1, М6, М8
Уровень алчности (U6)	М2, М8, М3
Уровень самооценки (U7)	М3, М2, М6, М7

В свою очередь, можно составить соотношение между возможными угрозами и мотивами потенциального злоумышленника –эксперта. К примеру, для угроз: «уничтожение данных», «изменение системы», «модификация данных» представлено следующее соответствие (рисунок 2), где количественные показатели: «0; 0,3; 0,6; 0,9» - мотивационная оценка в шкале «0,1».

Тогда, оценка стоимости возможного ущерба от совершенного компьютерного преступления рассчитывается по формуле:

$$C = S + Y \cdot E$$

где S- штраф за совершенное компьютерное преступление,

Y- срок отбывания наказания за совершенное компьютерное преступление,

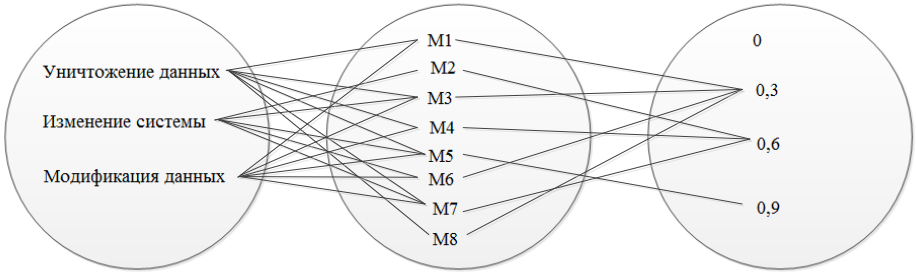

Рис. 2. Соотношение «угрозы при расследовании КП – мотивы эксперта-потенциального злоумышленника»

Обобщенная оценка риска определяется по формуле:

$$|\mathrm{Risk}| = \frac{1}{n} \cdot \sum_{i=1}^{n} Risk_i;$$

где i – номер пройденного модуля,

n - количество пройденных модулей,

$Risk_i$ - риск наличия i-го мотива

$$Risk_i = p_i \cdot \mathrm{C},$$

С – стоимость возможного ущерба от совершенного компьютерного преступления.

Е – одна условная денежная единица, соответствующая одному году лишения свободы.

В том случае, когда оценочная величина риска больше допустимой, то должно быть принято решение о возможности участия эксперта в работе. Если вариант привлечения иного специалиста не возможен, то в ходе следственных мероприятий предлагается использовать программу видеозахвата.

На рисунке 3 представлена архитектура модели оценки рисков при расследовании компьютерных преступлений.

Для каждого из модулей представлен модуль расчета результата.

Из данных модулей формируется общий

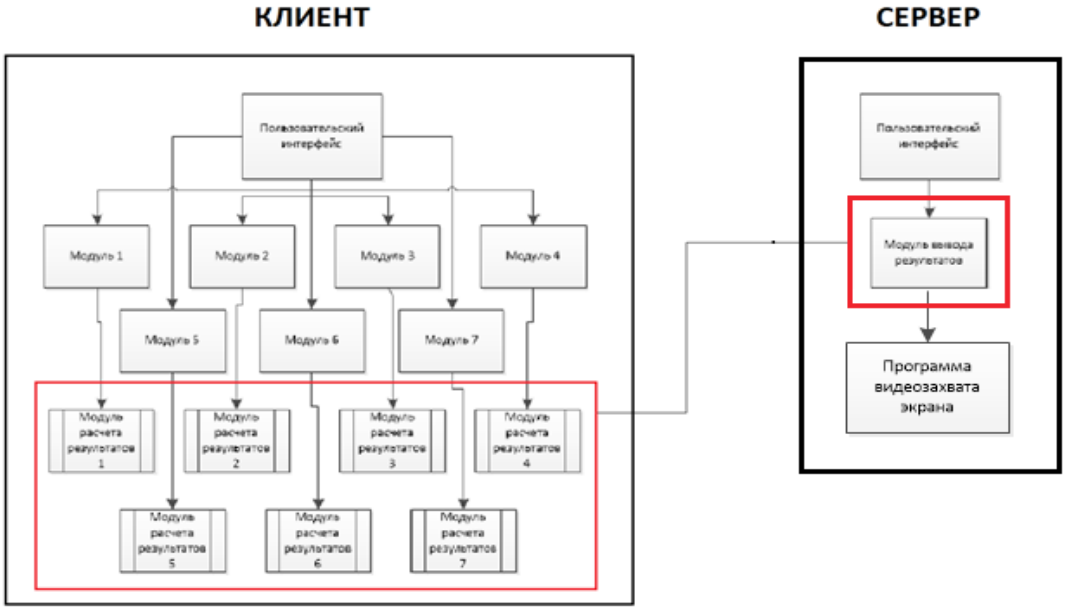

Рис. 3. Архитектура модели оценки рисков при раскрытии компьютерных преступлений

Архитектура модели представлена управляющим модулем, который содержит:

для КЛИЕНТА:

— Модуль 1. Тест на определение уровня тревожности

— Модуль 2. Тест «Упорство» (Методика е.П.Ильина, е.К.Фещенко)

— Модуль 3. Тест агрессивности (опросник л. Г. Почебут)

— Модуль 4. Тест на обидчивость

— Модуль 5. Тест на алчность

— Модуль 6. Тест на жадность

— Модуль 7. Тест на самооценку личности. Методика Будасси.

отчет по пройденным тестам и вывод результата на сервер;

для СЕРВЕРА:

— Модуль вывода результатов, и уровня риска (в соответствии с пройденными тестами)

— Программа видеозахвата экрана.

Предложенная модель позволит автоматизировать процесс работы с компьютерными преступлениями на этапе расследования и повысить уровень их раскрываемости.

Литература

1. Максимова Е.А.

2. Ляхова О. О. Классификация следственных версий // Молодой ученый. — 2018. — №7. — С. 137-138. — URL https://moluch.ru/archive/193/48373/ (дата обращения: 16.09.2018)

3. Коровин Н. К. Криминалистика: учебное пособие/ НГТУ 2014. — 308 С.

4. Никифоров В. Г. Процессуальный и криминалистический аспекты производства судебного следствия: монография/ ЮНИТИ-ДАНА: Закон и право, 2010. — 144 С.

5. Шаталов А.С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики/ Право. Журнал Высшей школы экономики. 2017. №2. — С. 155-172

References

1. Maksimova E.A.

2. Lyahova O. O. Klassifikaciya sledstvennyh versij // Molodoj uchenyj. — 2018. — №7. — S. 137-138. — URL https://moluch.ru/archive/193/48373/ (data obrashcheniya: 16.09.2018)

3. Korovin N. K. Kriminalistika: uchebnoe posobie/ NGTU 2014. — 308 S.

4. Nikiforov V. G. Processual'nyj i kriminalisticheskij aspekty proizvodstva sudebnogo sledstviya: monografiya/ YUNITI-DANA: Zakon i pravo, 2010. — 144 S.

5. SHatalov A.S. Algoritmizaciya i programmirovanie rassledovaniya prestuplenij v sisteme kriminalisticheskoj metodiki/ Pravo. ZHurnal Vysshej shkoly ehkonomiki. 2017. №2. — S. 155-172

МАКСИМОВА Елена Александровна, кандидат технических наук, доцент, заведующий кафедрой информационной безопасности ФГАОУ ВО «Волгоградский государственный университет». Россия, 400062, г. Волгоград, проспект Университетский, д. 100. E-mail: maksimova@volsu.ru

БАРАНОВ Владимир Витальевич, кандидат военных наук, доцент, заведующий кафедрой информационной безопасности Южно-Российского государственного политехнического университета имени М.И. Платова, 346428, Ростовская обл., г. Новочеркасск, ул. Просвещения, 132. E-mail: baranov.vv.2015@yandex.ru

ЗЯЗИН Валентин Петрович, профессор кафедры информационной безопасности Института кибернетики, ФГБОУ ВО «МИРЭА - Российский технологический университет», 119454 г. Москва, проспект Вернадского, дом 78. E-mail: zval47@yandex.ru

MAKSIMOVA Elena, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Security, Volgograd State University. Russia, 400062, Volgograd, Universitetsky Avenue, 100. E-mail: maksimova@volsu.ru

BARANOV Vladimir, Candidate of Military Sciences, Associate Professor, Head of the Department of Information Security of the South-Russian State Polytechnic University named after M.I. Platov. 346428, Rostov region, Novocherkassk, str. Enlightenment, 132. E-mail: baranov.vv.2015@yandex.ru

ZIAZIN Valentin, Professor, Department of Information Security, Institute of Cybernetics, FSBEI HE "MIREA - Russian Technological University". 119454, Moscow, Vernadskogo Avenue, 78. E-mail: zval47@yandex.ru

УДК 004.089 + 004.056 Вестник УрФО № 4(30) / 2018, с. 43–49

Минаев В. А., Королев И. Д., Сабанов А. Г.

DOI: 10.14529/secur180407

ОЦЕНКА РИСКОВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ СУБЪЕКТОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

В статье рассматриваются факторы снижения наблюдающегося сегодня резкого обострения информационного противоборства и ослабления информационной безопасности. В качестве основного фактора определяется эффективное управление доступом в информационные системы, включающее идентификацию и аутентификацию пользователей. Обращается внимание на снижение рисков и формирование доверия взаимодействующих субъектов и объектов доступа за счет научно обоснованных в нормативно-правовой базе и методических рекомендациях методах, механизмах и средствах идентификации и аутентификации. Показана необходимость создания многоуровневой методики аутентификации. Описываются её основные принципы, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты. Особое внимание при этом уделяется управлению рисками в облачных сервисах. Приводится наглядный графический пример оценки рисков.

Ключевые слова: *Оценка, риск, идентификация, аутентификация, электронное взаимодействие, информационная безопасность, управление рисками.*

Minaev V. A., Korolev I. D., Sabanov A. G.

RISK ASSESSMENT IDENTIFICATION AND AUTHENTICATION OF ELECTRONIC INTERACTION SUBJECTS

The article considers the factors of reducing the sharp aggravation of information confrontation and weakening of information security observed today. The main factor is the effective management of access to information systems, including the identification and authentication of users. Attention is drawn to the reduction of risks and the formation of subjects and objects interacting trust access due to the methods, mechanisms and means of identification and authentication scientifically grounded in the legal framework and methodological recommenda-

tions. The necessity of creating a multi-level authentication method is shown. Its basic principles based on the formation of the information security concept, threat and intruder models, application of organizational and technical protection measures are described. Particular attention is paid to risk management in cloud services. An illustrative graphical example of a risk assessment is considered.

Keywords: *Assessment, risk, identification, authentication, electronic interaction, information security, risk management.*

Введение

В условиях резкого обострения информационного противоборства (ИП) в государственной, социально-экономической и гражданской сферах, непрерывного роста кибератак на информационные системы (ИС) различного назначения, практически любая среда информационного обмена априори может быть рассмотрена в качестве потенциально подверженной возможным нападениям. Значительное влияние на снижение факторов такого обострения имеет эффективное управление доступом пользователей в ИС, в качестве основных этапов включающее идентификацию (ИД) и аутентификацию (АУ) субъектов и объектов доступа.

Процессы аутентификации особенно востребованы в случае недоверия к подлинности предъявленных идентификаторов взаимодействующих сторон, например, при удалённом доступе и/или использовании недоверенной среды информационного обмена.

Существуют и риски того, что в среде современных многозадачных информационных систем вычислительный процесс, реализующийся в интересах злоумышленника, может имитировать функционирование легальных субъектов и объектов доступа, как параллельно с ними, так и автономно.

Для снижения указанных рисков и формирования определённого уровня доверия в подлинности взаимодействующих сторон (субъектов и объектов доступа) необходимо применять научно обоснованные, закреплённые в нормативно-правовой базе и методических рекомендациях методы, механизмы и средства ИД и АУ в составе систем управления доступом к ИС.

Еще одна актуальная задача связана с быстро увеличивающимся числом зарегистрированных субъектов доступа, насчитывающих сотни тысяч, а нередко – десятки миллионов пользователей. Это вызывает необходимость научного поиска достаточного числа надежных идентификаторов для достижения заданного уровня достоверности ИД и разработки шкалы доверия к результатам АУ для ИС. Многообразие реализаций схем информационного обмена, методов АУ в отсутствии чётких требований нормативной базы также нуждается во введении определённых уровней доверия к результатам аутентификации сторон электронного взаимодействия.

Значительный вклад в решение проблем идентификации и аутентификации содержится в работах [1-5], в которых разработаны концептуальные основы защиты информации (ЗИ), обоснованы принципы обеспечения информационной безопасности (ИБ) и построения систем защиты информации (СЗИ), рассмотрены теоретические аспекты и методология организации ЗИ, развита теория функциональной надежности (ФН), основы теории функциональной устойчивости, а также сформулированы направления построения моделей угроз и нарушителей безопасности информации.

Методические подходы к оценке рисков идентификации и аутентификации

Сравнительный анализ международных и российских стандартов, зарубежной и отечественной нормативной базы по вопросам регулирования процессов аутентификации, научных исследований по вопросам анализа рисков, надежности и безопасности применительно к процессам АУ показал, что за рубежом нормативная и научно-методическая база по вопросам их регулирования существенно опережает отечественную. Терминология в данной области также нуждается в существенном совершенствовании. Так, из 66 международных стандартов по идентификации и аутентификации в нашей стране имеется только один аналог – стандарт 1998 года (ГОСТ 9594-8 [6]).

Таким образом, вопросы идентификации и аутентификации и особенно разработки их математических моделей нуждаются в расширении исследований, системном изложении функций основных участников, процессов, а также способов построения систем ИД и АУ с учетом требований функциональной

надёжности и безопасности передаваемой и обрабатываемой в них информации. Также нуждаются в развитии требования ИБ к проектированию и построению систем удалённой аутентификации, к безопасности и надёжности выполнения идентификации и аутентификации в корпоративных (закрытых) ИС и современных ИС общего пользования, особенно при переходе к облачным вычислениям.

Исследования [7, 8] показали, что анализ рисков аутентификации в конкретно взятой ИС может проводиться в соответствии с традиционным подходом, основанном на оценке вероятности реализации угроз и величины ущерба (тяжести последствий от их реализации). Однако при этом можно получить лишь грубые оценки, а для более глубокого и точного анализа существует необходимость разработки многоуровневой методики оценки рисков, учитывающей специфику последовательно организованных процессов, составляющих процедуру аутентификации.

чительными. На рис. 1 представлена схема оценки рисков, учитывающая специфику процессов ИД и АУ.

При разработке требований к аутентификации в качестве основного метода анализа взята оценка рисков. За основу критериев оценки выбрано обеспечение трех взаимосвязанных компонент – конфиденциальности, доступности и целостности персональной информации при организации доступа с применением аутентификации.

Основными задачами являлись описание рассматриваемой системы, выработка целей и критериев идентификации и анализа рисков.

Затем был выбран перечень известных методов исследования рисков для рассматриваемой системы. Учитывая, что аутентификация является сложным процессом, в который включены персонал, аппаратное и программное обеспечение нескольких систем, сначала оценены высокоуровневые риски с помощью качественных методов.

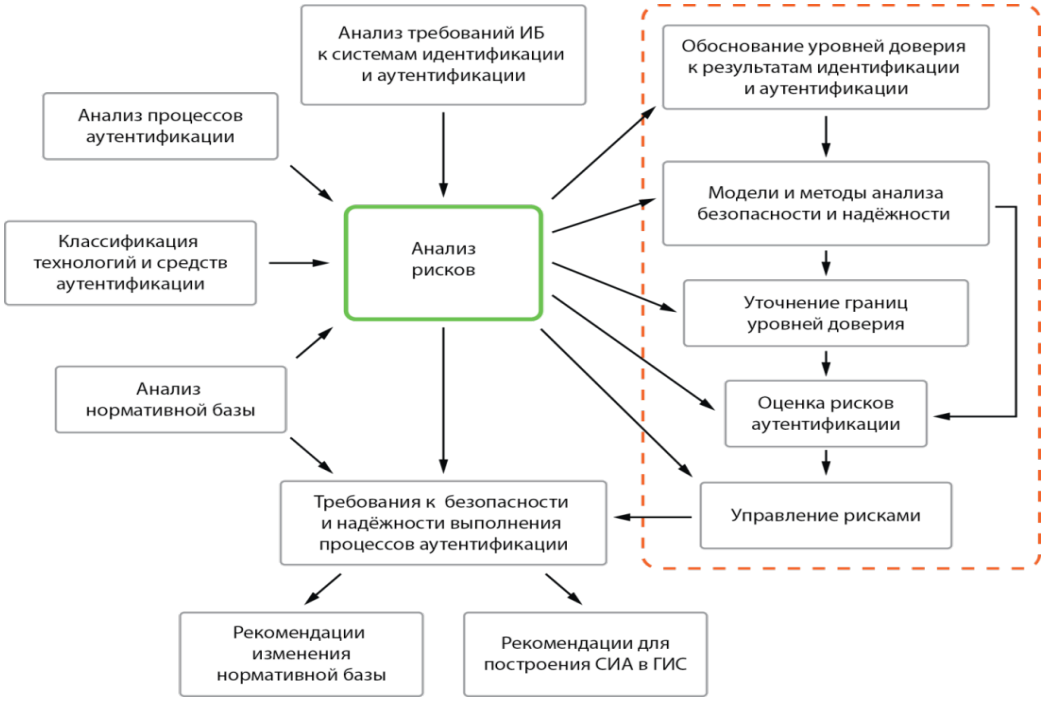

Рис. 1. Блок-схема методики оценки рисков ИД и АУ

Методика связана с исследованием рисков на различных уровнях детализации: сначала рассматриваются риски всей системы ИД и АУ, затем отдельные процедуры, составляющие процесс АУ, следующими уровнями детализации являются отдельные её элементы, для которых значения рисков и тяжести последствий их реализации могут быть зна-

Потом для проведения детализированного анализа рисков применительно к развитым ИС при наличии ценных информационных активов применены количественные оценки рисков. Кроме того, при необходимости осуществлялся дополнительный анализ процесса аутентификации с помощью построения дерева событий, дерева неисправностей и вида отка-

зов. Далее выявленные уязвимости соотнесены с соответствующими угрозами и имеющимися статистическими данными по инцидентам и механизмам контроля для оценки потенциального ущерба от реализации рисков.

Пример расчета рисков удаленной аутентификации

Результаты предложенной методики проиллюстрированы на конкретном примере, представленном в таблице 1. При этом учитывалось, что процедуры первого блока процесса (с 1.1 по 1.6 в таблице 1) являются разовыми, а процедуры 2.1 – 4.1 – многократными. Уязвимости с высокой вероятностью реализации (р = 0,9 ÷ 1) обозначены буквой В, со средней вероятностью (р ≈ 0,5) – буквой С, с низкой вероятностью (р ≤ 0,1) – буквой Н. Аналогично для оценки наиболее вероятных угроз принято обозначение В, для средней вероятности реализации угроз – С, для низкой – Н.

Выявлено, что наиболее уязвимыми являются процедуры проверки идентификаторов, предъявленных центру регистрации (ЦР), процедуры хранения и предъявления аутентификатора.

$$R = \sum_{i=1}^{M} R_i = \sum_{i=1}^{M} p(U_i) \cdot L(U_i), \quad (1)$$

где U_i – i-ое опасное событие; $p(U_i)$ – вероятность наступления i-го опасного события; $L(U_i)$– ущерб от наступления i-го опасного события; M – количество опасных событий.

Проранжируем вероятные опасные события (ВОС), используя значение вероятности появления опасного события в год – p_i и относительного значения риска R_i (таблица 2). Условием нормировки является

$$\overline{R} = \frac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} L(U_i)} = 1 \quad (2)$$

Результаты ранжирования представлены на рисунке 2 в виде пронумерованных кружков, обозначающих номер события в таблице 2 в плоскости переменных $\{R_i,\ lgp_i\}$.

Из анализа рисунка 2 следует, что, например, для снижения ВОС 2 (фишинг – подмена сайта, на который пользователю необходимо предоставить доступ) достаточно перейти с парольной аутентификации на технологию защищенного доступа с использованием TLS (Transport Secure Socket Layer) с двусторонней взаимной аутентификацией на основе применения цифровых SSL-сертификатов на стороне сервера и клиента.

Таблица 1

Оценки уязвимостей и угроз процедур удаленной аутентификации

Блоки	Процесс	Уязвимости	Угрозы
1	**Регистрация**	С	С
1.1	Субъект ***предъявляет*** свои идентификаторы	Н	С
1.2	ЦР ***проверяет*** предъявленные субъектом идентификаторы	С	В
1.3	ЦР ***создает*** учетную запись субъекта	Н	Н
1.4	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	Н	С
1.5	ЦР ***делегирует*** права доступа субъекта к другим ИС	Н	Н
1.6	ЦР ***выдает*** секрет и ЭУ на руки субъекту	Н	Н
2	**Подтверждение подлинности**	С	С
2.1	Субъект ***хранит*** секрет и ЭУ	С	В
2.2	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	С	С
3	**Валидация**	Н	Н
3.1	ДС ***проверяет*** цепочку сертификатов, срок и область действия ЭУ	Н	С
4	**Принятие решения**	Н	Н
4.1	ДС ***принимает решение*** о результате аутентификации	Н	Н

Предложенный подход использован авторами для оценки риска в системах управления доступом в различных ИС, начиная от локальных корпоративных систем и завершая доступом к сервисам публичного облака.

Интегральная оценка рисков проведена на основе экспертного метода, используя соотношение:

Это приведет к снижению вероятности подмены сайта приблизительно на два порядка (с 10^{-4} до 10^{-6}). Еще примерно на два порядка можно снизить вероятность фишинговой атаки за счет применения технологии хранения закрытого ключа и клиентского

Таблица 2

Пример ранжирования рисков аутентификации

ВОС	Описание опасного события	p_i	R_i
1	Воздействие вредоносного ПО	10^{-3}	0,122
2	Фишинг	10^{-4}	0,141
3	Риск добровольной передачи носителя (ключа и АУ)	10^{-4}	0,110
4	Ошибки или целенаправленные действия при смене АУ	10^{-4}	0,096
5	Использование уязвимостей системы АУ	10^{-4}	0,088
6	Ошибки валидации	10^{-5}	0,120
7	Spoofing (подмена) доверенной стороны	10^{-5}	0,089
8	Помощь инсайдера	10^{-5}	0,084
9	Регистрация злоумышленника под видом легального пользователя	10^{-6}	0,137

сертификата в устройстве класса SSCD (Secure Signature Creation Design – устройство генерации ключей электронной подписи). Итоговое снижение ВОС в год за счет указанных мер может снизиться до 10^{-6} и даже ниже.

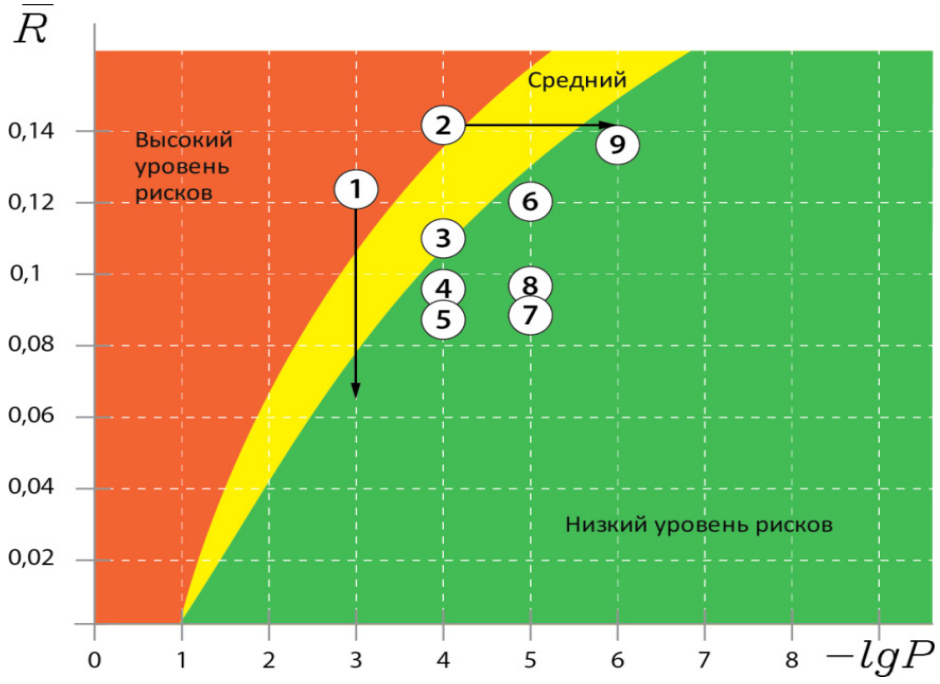

Рис. 2. Поле управления рисками для системы ИД и АУ

В то же время снижение рисков в рассмотренных примерах может проводиться в отношении не только частоты реализации ВОС, но и размера риска, используя в качестве механизмов снижения рисков традиционные способы обеспечения доступности, целостности и конфиденциальности информации, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты. При этом риски будут снижаться в вертикальном направлении до определенного уровня.

Соответствующими способами можно снизить риски за счет внедрения СЗИ (ВОС 1 – установка антивирусного программного обеспечения; ВОС 3 – переход на смарт-карты с технологией Match-on-Card; ВОС 8 – внедрение СЗИ в систему АУ).

При достижении приемлемых уровней рисков по частоте (в горизонтальном направ-

лении) и размеру (в вертикальном направлении) процесс управления рисками можно считать выполненным.

Если приемлемых уровней для остаточных рисков достичь не удается, необходимо подключать такие механизмы управления рисками, как уклонение от риска (ликвидация причин и/или последствий риска), ограничение (нейтрализация) риска (например, путем реализации контрмер, уменьшающих воздействие угроз безопасности), перенос риска на стороннюю организацию (страхование рисков).

К достоинствам данного метода анализа рисков аутентификации можно отнести его наглядность. Недостатком же его является необходимость в большом объеме предварительной работы по выявлению ВОС, зачастую в условиях отсутствия фактического материала в виде статистических данных или результатов мониторинга за достаточно продолжительный период времени. В таких случаях, согласно ГОСТ Р ИСО/МЭК 13335-1-2006, рекомендуется воспользоваться методом экспертных оценок.

Выводы

1. В условиях резкого обострения информационного противоборства и ослабления информационной безопасности вследствие роста кибератак различного характера, значительное влияние на снижение факторов такого обострения имеет эффективное управление доступом в информационные системы, в качестве основных этапов включающее идентификацию и аутентификацию пользователей.

2. Для снижения рисков и формирования определённого уровня доверия в подлинности взаимодействующих сторон (субъектов и объектов доступа) необходимо применять научно обоснованные, закреплённые в нормативно-правовой базе и методических рекомендациях методы, механизмы и средства ИД и АУ в составе систем управления доступом к ИС.

3. Для глубокого и точного анализа рисков аутентификации необходима разработка многоуровневой методики их оценки, учитывающей специфику последовательно организованных процессов, составляющих процедуру аутентификации. За основу критериев оценки следует выбирать обеспечение трех взаимосвязанных компонент – конфиденциальности, доступности и целостности информации при организации доступа с применением аутентификации.

4. Снижение рисков должно проводиться не только в отношении частоты реализации опасных событий, но и размера риска, используя в качестве механизмов снижения рисков традиционные способы, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты [9]. Особое внимание при этом должно уделяться управлению рисками в облачных сервисах [10].

Литература

1. Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие. / Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. М.: Горячая линия-Телеком, 2012. – 552 С.

2. Баушев С. В., Аристархов И. В., Кузьмин А. С., Сабанов А. Г. и др. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику. СПб.: "БХВ-Петербург", 2016. – 304 С.

3. Сабанов А.Г. Основные процессы аутентификации // Вопросы защиты информации. 2012. №3. – С. 54-57.

4. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь. 2013. №4. – С. 27-32.

5. Смит Р. Э. Аутентификация: от паролей до открытых ключей. М.: «Вильямс», 2002. – 432 С.

6. "Информационная технология. Взаимосвязь открытых систем. Основы аутентификации". Справочник. Часть 8. Государственный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 9594-8-98.

7. Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь. 2012. №8. С. 40-44.

8. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь. 2013. №4. – С. 27-32.

9. Фисун А.П., Касилов А.Г., Фисенко В. Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р. А., Джевага К.А., Кожухов С. А. Развитие методологических основ информатики и информационной безопасности систем. Депонированная рукопись. Орловский государственный университет. Номер 1165-В2004. ВИНИТИ. Дата депонирования 07.07.2004. – 253 С.

10. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013. №2-1. – С. 45-51.

References

1. Afanas'ev A. A., Veden'ev L. T., Voroncov A. A. i dr. Autentifikaciya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informacionnym resursam. Uchebnoe posobie. / Pod red. A. A. SHelupanova, S. L. Gruzdeva, YU. S. Nahaeva. M.: Goryachaya liniya-Telekom, 2012. – 552 S.

2. Baushev S.V., Aristarhov I.V., Kuz'min A. S., Sabanov A. G. i dr. Udostoveryayushchie avtomatizirovannye informacionnye sistemy i sredstva. Vvedenie v teoriyu i praktiku. SPb.: "BHV-Peterburg", 2016. – 304 S.

3. Sabanov A.G. Osnovnye processy autentifikacii // Voprosy zashchity informacii. 2012. №3. – S. 54-57.

4. Sabanov A.G. Ob ocenke riskov udalennoj autentifikacii // EHlektrosvyaz'. 2013. №4. – S. 27-32.

5. Smit R. EH. Autentifikaciya: ot parolej do otkrytyh klyuchej. M.: «Vil'yams», 2002. – 432 S.

6. "Informacionnaya tekhnologiya. Vzaimosvyaz' otkrytyh sistem. Osnovy autentifikacii". Spravochnik. CHast' 8. Gosudarstvennyj standart Rossijskoj Federacii GOST R ISO/MEHK 9594-8-98.

7. Sabanov A.G. Autentifikaciya kak chast' edinogo prostranstva doveriya // EHlektrosvyaz'. 2012. №8. S. 40-44.

8. Sabanov A.G. Ob ocenke riskov udalennoj autentifikacii // EHlektrosvyaz'. 2013. №4. – C. 27-32.

9. Fisun A.P., Kasilov A.G., Fisenko V. E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R. A., Dzhevaga K.A., Kozhuhov S. A. Razvitie metodologicheskih osnov informatiki i informacionnoj bezopasnosti sistem. Deponirovannaya rukopis'. Orlovskij gosudarstvennyj universitet. Nomer 1165-B2004. VINITI. Data deponirovaniya 07.07.2004. – 253 S.

10. Sabanov A.G. Osobennosti autentifikacii pri dostupe k oblachnym servisam // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo. 2013. №2-1. – S. 45-51.

МИНАЕВ Владимир Александрович, доктор технических наук, профессор, профессор Московского государственного технического университета им. Н.Э. Баумана. Россия, 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1. E-mail: m1va@yandex.ru

КОРОЛЕВ Игорь Дмитриевич, доктор технических наук, профессор, профессор Краснодарского высшего военного училища имени генерала армии С. М. Штеменко. Россия, 350063, г. Краснодар, ул. Красина, 4. E-mail: pi_korolev@mail.ru

САБАНОВ Алексей Геннадьевич, кандидат технических наук, доцент, доцент Московского государственного технического университета им. Н.Э. Баумана. Россия, 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1. E-mail: aladdin@aladdin-rd.ru

MINAEV Vladimir, Doctor of Technical Sciences, Professor, Professor of Moscow State Technical University. N.E. Bauman. Russia, 105005, Moscow, 2 nd Baumanskaya Str., 5, bld. 1. E-mail: m1va@yandex.ru

KOROLEV Igor, Doctor of Technical Sciences, Professor, Professor of the Krasnodar Higher Military School named after Army General S. M. Shtemenko. Russia, 350063, Krasnodar, ul. Krasin, 4. E-mail: pi_korolev@mail.ru

SABANOV Alexey, Candidate of Technical Sciences, Associate Professor, Associate Professor of Moscow State Technical University. N.E. Bauman. Russia, 105005, Moscow, 2 nd Baumanskaya Str., 5, bld. 1. E-mail: aladdin@aladdin-rd.ru

УДК 004.056 Вестник УрФО № 4(30) / 2018, с. 50–59

Хализев В. Н. Угрюмов Д. В.,

DOI: 10.14529/secur180408

СИСТЕМНАЯ ИНТЕГРАЦИЯ ПРОГРАММНО-АППАРАТНЫХ КОМПОНЕНТ ЗАЩИТЫ

В статье приведены исследования по оптимизации принятия решений в процессе системной интеграции компонент защиты, использующие сочетание подхода получения тупиковых альтернатив с построением серии множественных решений в виде задачи о наименьшем покрытии набора функциональных требований и выработки показателя предпочтительности ранжирования по модифицированному целевому методу.

Ключевые слова: *системная интеграция, критерии выбора средств защиты, принятие решений.*

Halizev V. N., Ugriumov D. V.

SYSTEM INTEGRATION OF HARDWARE-SOFTWARE PROTECTION COMPONENT

The article presents a study on decision-making process optimization system integration component of protection using a combination of approaches to get dead-end alternatives with the construction of a series of multiple solutions in the form of lesser coverage a set of functional requirements and develop a preference ranking indicator modified target method.

Keywords: *decision-making, criteria for selection of remedies, minimum coverage.*

Задача определения набора программно-аппаратных средств (компонент) защиты во многих теоретических работах неоднократно формулировалась в виде задачи оптимального выбора при заданных ограничениях, например в [1], как задача первого или второго вида. Первая – это минимизация затрат при требуемой эффективности мер защиты и второго вида – максимизация эффективности мер защиты при ограничении на суммарную стоимость затрат.

Нормативными документами ФСТЭК определен несколько иной порядок построения эффективной защиты – через управление рисками: выявление всех возможных угроз безопасности информации, оценка их вероятности реализации и ущерба (риска), актуальности угроз, определения класса защищенности АС, (либо требуемого уровня защищенности для ИСПДн, категории для КИИ) и выработка по этим данным минимального набора защитных мер, соответствующих введенному классу защищенности (уровню защиты), то есть новый вид задачи из [1] – как задачи покрытия множества угроз (или функциональных требований (ФТ)) множеством мер и способов защиты. Что соответствует созданию профиля функциональных требований защиты – в терминах ГОСТ Р ИСО\МЭК 15408. В этом случае задача количественного

определения эффективности или оптимизации стоимости выбранных мер и средств защиты не ставится. При этом отсутствие строгой методики обоснования выбора конкретных мер и способов защиты и реализующих их средств защиты информации (СрЗИ) может привести к неоптимальности, а иногда даже к несостоятельности выбранного набора компонентов системы защиты.

Процесс анализа и выбора программно-аппаратных компонент достаточно сложен и продолжителен, зависит от большого количества влияющих факторов, глубины знаний специалистов. Поэтому возможно появление ошибок в силу различных причин, которые могут привести к выбору не лучшего варианта, что может затем сказаться на бюджете и безопасности. Поэтому задача формализованного выбора оптимального состава комплекта СрЗИ является актуальной.

Решать задачу можно применив систему поддержки принятия решения, базирующуюся на комплексе новых математических моделей многокритериальной оптимизации.

В [6] предлагается оптимизацию выбора СрЗИ проводить по критерию «предпочтительности выбора», вычисляемого как суммарный показатель экспертных оценок обязательных (по функциональным требованиям РД ФСТЭК и ФСБ) и дополнительных показателей, взвешенных коэффициентами важности, по каждому виду СрЗИ в отдельности - защиты от НСД, межсетевым экранам (МЭ), антивирусным средствам (АВС) (по одному средству каждого вида). Эта модель не решает проблемы выбора комплекта СрЗИ когда имеются средства, покрывающие ФТ из разных видов подсистем (известны средства с функциями МЭ, СОВ и АВС одновременно и всеми их сочетаниями), а также внутри одного вида СрЗИ – защиты от НСД, когда одни средства покрывают все ФТ, другие – частично, а некоторые элементы с одним - двумя ФТ (например, е-токен как электронный ключ, Шипка как электронный ключ и средство хранения сертификатов КриптоПРО).

Решить эту задачу можно применив предлагаемую модель системы поддержки и принятия управленческих решений (СППР), базирующуюся на уточнённых моделях многокритериальной оптимизации и методах системного анализа.

Данная модель сочетает принятую парадигму построения системы защиты в виде покрытия набора функциональных требований для класса защищенности АС (уровня защиты ИСПДн) и выработки комплексного показателя защищенности и его оптимизации внутри каждого класса.

Функционирование СППР при построении систем защиты информации с технологической точки зрения можно представить в виде известных в теории системного анализа следующих этапов жизненного цикла принятия решения: целевыявление, выработки (генерации) решений, оценки решений, выбора схемы принятия решения, координация его выполнения.

Общая схема принятия решений представлена на рисунке 1.

Рис. 1. Схема принятия решений

Определим содержание перечисленных этапов принятия решений с точки зрения процесса работы системного интегратора при комплектовании систем защиты информации компонентами и подсистемами.

Более подробно:

Этап 1. Формулировка проблемы - выявление и формулировка проблемной ситуации, формирование цели системы СППР. Является творческим процессом из-за объективной сложности, многомерности и многосвязности проблем управления, неструктуризованном характере многих из них, трудностях измерения переменных, отсутствии априорных сведений о существенных связях между ними [7]. Формулировка цели СППР первого этапа - построение универсальной модели и методики выбора оптимального на-

бора подсистем или компонент интегрированной системы с учетом детальных особенностей сложного комплекса входящих в нее составляющих подсистем.

Этап 2. Формирование подцелей системы управления для определения желаемого состояния по устранению проблемной ситуации. На этом этапе целевыявления формулируются направления выхода из существующей проблемной ситуации, определяется, ***что*** нужно сделать для снятия проблемы. Методологические основы - системный анализ и экспертные методы [7].

На этом этапе формируются подцели: определяются наборы функций подсистем и компонентов системы защиты (мер нейтрализации угроз). их входных и выходных параметров - массивов данных, подлежащих обработке с целью оптимизации в разрабатываемой математической модели.

Обычно функциональные задачи (ФЗ) комплексируемых подсистем информационной инфраструктуры формируются экспертами на разных архитектурных уровнях: конструктивно-технологическом - энергетика, температурный режим, системы доступа и охраны; вычислительном - сервера, рабочие станции, периферия; сетевом – маршрутизаторы, коммутаторы, концентраторы; программно-аппаратной защите информации – управления доступом, антивирусных средств, IDS/IPS-средств, средств анализа защищенности, межсетевого экранирования и т. д.

Выбор уровней декомпозиции определяются специалистами по известным им методам и моделям присущим в каждой конкретной сфере для каждого вида подсистем, то есть экспертными методами.

Для некоторых видов подсистем разработаны стройные иерархически структурированные модели декомпозиции архитектур, для других – композиция-декомпозиция проводится на интуитивном уровне экспертами.

Например, в стандарте ИСО/МЭК 15408 "Общие критерии информационных технологий" содержатся иерархическое описания 6 классов, 15 подклассов, 360 элементов информационных технологий реализующих информационную безопасность в ИТ-системах. Реально системные интеграторы пользуются наборами защитных мер, сформулированных в соответствующих приказах ФСТЭК (№ 21,17,31,239)

Этап 3. Выработка (генерация) решений. На данном этапе вырабатываются альтернативные варианты решений, осуществляется поиск различных путей, способов достижения поставленных целей. Наиболее известными организационными формами генерирования альтернатив являются мозговой штурм, синектика, разработка сценариев, морфологический анализ, деловые игры, когнитивные карты [7].

На третьем этапе специалистами для каждой функциональной задачи формируется блок возможных альтернативных вариантов решения этой задачи с помощью выявленных на рынке для этих целей средств, компонентов или подсистем. Совокупность всех блоков альтернатив по всем ФЗ является той базой экспертных знаний, которая и составляет исходные данные рассматриваемой задачи системного интегрирования компонент. При этом альтернативным решением, подлежащим выбору ЛПР является набор компонент (подсистем) по одному из каждого блока. Собственно этот этап генерации альтернативных наборов компонент, входящих в комплексную интегрированную систему, и является основным источником проблемы обсуждаемой в данной работе вместе с последующим способом оценивания этого набора компонент (а именно наличие существенных нелинейностей при оценивании полезности каждой альтернативы). Ниже рассмотрим это более подробно.

Этап 4. Формирование критериев выбора решений как измерителей степени достижения намеченной цели. Критерием ценности альтернативы служит любой ее признак (параметр), измеренный на качественном либо количественном уровне. Например, объем памяти, скорость или быстродействие, другие параметры качества или эффективности.

На четвертом этапе экспертами для каждой задачи отбираются частные показатели качества (эффективности) решения этой конкретной задачи в виде объективных технических характеристик компонент (подсистем) либо субъективных качественных показателей, определяющих специфические функции этой подсистемы. Выбор их может быть субъективным и зависит от опыта экспертов либо сформулирован в качестве отдельной задачи для каждого типа подсистем. Из частных могут быть построены обобщенные показатели качества для комплексной интегрированной системы по известным либо вновь разрабатываемым моделям и алгоритмам. Вопрос о выборе обобщенных показателей качества и эф-

фективности (безопасность, надежность, эргономичность, устойчивость,…) и особенности их объединения как правило представляют собой отдельные научные задачи для каждого типа показателей и в данной работе не рассматриваются. (Например, показатели надежности и их способы объединения для последовательного или параллельного в смысле надежности объединения компонентов, показатели информационной безопасности – через приемлемые урони риска по каждой угрозе – по ИСО МЭК 27005). Однако во многих случаях наряду с обобщенными показателями для всей системы, при предъявлении требований эксперты выставляют именно частные показатели (конкретные ТТХ подсистем), по которым ЛПР более привычно и легко сравнивать альтернативные варианты при их отборе.

Каждому показателю (технической характеристике) ЛПР устанавливает соответствующий критерий путем наложения ограничений либо формирования предпочтения – «чем больше (меньше), тем лучше», либо более сложные – близость к константе, вхождению в диапазон, нелинейные предпочтения и т. д. Субъективный характер выбора частных критериев проявляется в разных методологиях принятия решений в виде процедур назначения экспертами коэффициентов важности для критериев (например, известная технология парных сравнений в методе анализа иерархий – МАИ [8]).

Этап 5. Оценка возможных решений. При решении задач принятия решений по многим критериям (векторных задач оптимизации) возникают трудности определения наилучшего с точки зрения ЛПР компромиссного решения из множества допустимых решений, в том числе и по отдельным локальным критериям. К этим приёмам относят согласование и нормализацию критериев, учет приоритета критериев. Нормализация критериев связана с возможностью соизмерения в различных единицах и масштабах измерения. После нормализации все критерии приводят к единому масштабу – приведение их к диапазону [0,1] и согласование – направленость в одну сторону – меньшее предпочтение – значение 0, большее - 1.

Этап 6. Выбор схемы и алгоритма принятия решения. На данном этапе необходимо осуществить выбор решения по определенной схеме или алгоритму, наилучшему с точки зрения некоторого суперкритерия, некоторого принципа оптимальности.

В задачах принятия решений в условиях определенности поиск оптимальных решений достаточно формализован. Используемые методы оптимизации математического программирования, вариационного исчисления, эвристические, организованного поиска и другие, в настоящее время получили широкое распространение [8]. Применимы методы компромиссных решений следующие: уступки; свертывания критериев в один (например, алгоритм линейной свертки - взвешенной суммы, критерий Вальда, Сэвджа, Гурвица, Ходжа-Лемана); выделения главного критерия; целевой метод (опорной или идеальной точки).

Если требуется определить единственное наилучшее решение, то необходимо множество всех допустимых решений сузить до множества Парето (множество недоминируемых решений, компромиссное множество), а далее на этом множестве искать решение на основе некоторой принятой ЛПР схемы поиска компромисса. Наиболее распространенными принципами компромиссных решений являются следующие: равномерности (равенства); уступки; свертывания критериев в один (например, взвешенной суммы); выделения главного критерия; задания целевой точки (опорной или идеальной) [8]. В случае если количественно оценить отдельную альтернативу (решение) по одному либо по множеству критериев затруднительно или невозможно, можно попытаться описать выбор на языке бинарных отношений. Выбор на языке бинарных отношений распространен достаточно широко, в частности при решении таких многокритериальных задач, как задачи о назначениях, о рюкзаке, в методе «ЭЛЕКТРА» и др. [9].

Системная интеграция — это разработка комплексных решений по автоматизации технологических и бизнес-процессов предприятия с целью максимально эффективного управления технологическим процессом, производством, организацией в целом. Решение данной проблемы в настоящее время видится путем разработки научно-методического аппарата поддержки принятия решения лицом (ЛПР), выполняющим системную интеграцию с применением модели оптимизации многоальтернативного выбора.

Задача выбора оптимальной структуры системы из составляющих ее объектов может быть сформулирована в теоретико-множественной интерпретации как задача о наи-

меньшем покрытии (ЗНП) множества следующим образом [3].

Таблица 1

Структура исходных данных задачи многоальтернативного выбора

Средства ЗИ	Параметр 1	Параметр 2	Параметр 3	Параметр 4	Параметр 5	Параметр 6	Параметр 7	Параметр 8
АВС 1	6	7	8					
АВС 2	2	11	7					
АВС 3	3	6	6					
МЭ 4				8	9	4		
МЭ 5				7	0	9		
МЭ 6				9	6	7		
МЭ 7				9	7	6		
СОВ 8							0	8
СОВ 9							4	4
СОВ 10							4	10
СОВ 11							5	11
UTM 12	3	4	5				6	7
UTM 13				4	5	6	5	6

Пусть определено множество угроз АС (либо мер нейтрализации) $R=\{r_1,r_2,\ldots r_m\}$, и множество компонент СрЗИ (элементов оборудования) $S=\{S_1,S_2,\ldots,S_n\}$, таких, что каждый S_j ассоциирован с подмножеством $R_j \subseteq R$, где $j \in N=\{1,\ldots,n\}$. При этом S_j нейтрализует некоторые угрозы из R_j, либо выполняет функции из R_j с определенным качеством. Совокупность $\{R_j\}$, $j \in J$, $J \subseteq N$ называется покрытием множества R, если $\cup R_j = R$, при $j \in J$. Определим матрицу $A=(a_{ij})$:

$$a_{ij}=\begin{cases} 1, \text{ если элемент ri входит в множество Rj} \\ \text{(требование ri покрыто)} \\ 0, \text{иначе} \end{cases}$$

Задача выбора оптимальной структуры системы защиты из составляющих ее компонент $S=\{S_1,S_2,\ldots,S_n\}$, для реализации покрытия всех угроз (либо набора заданных мер (требований) $R=\{r_1,r_2,\ldots r_m\}$ как задача ЦЛП имеет вид:

$$F_1(x)=\sum_{j=1}^{n}(C_j x_j) \to \min, \quad (1)$$

при условиях:

$$\sum_{j=1}^{n}(a_{ij}x_j) \geq 1, \text{ где } i \in M \quad (2)$$

$$x \in 0,1, \text{ где } j \in N \quad (3)$$

В этом случае задача структурного синтеза сводится к определению экстремального значения целевой функции (1).

Если C_j интерпретировать как стоимость элементов оборудования, то значения целевой функции (1) определят минимальную стоимость оборудования, для построения АС, удовлетворяющей всем заданным требованиям.

Если B_j интерпретировать как эффективность защиты элементов оборудования, то значения целевой функции (4) определят максимальную эффективность набора оборудования, для построения системы, удовлетворяющей всем заданным требованиям, при тех же ограничениях (2) и (3):

$$F_2(x)=\sum_{j=1}^{n}(\hat{A}_j x_j) \to \max \quad (4)$$

Введем в математическую модель (1) данные о технических параметрах решаемых задач R путем добавления матрицы натуральных чисел B. Определим матрицу $B=(b_{ij})$, $i \in M$, $j \in N$:

$$b_{ij}=\begin{cases} b, \text{ если } a_{ij}=1 \text{ и требование } r_i \text{ выполнено объектом j} \\ \text{с качеством b=1..100} \\ 0, \text{ иначе} \end{cases} \quad (5)$$

Если объекты имеют конкретные числовые характеристики, отражающие их количественные или качественные параметры по реализации функции (требования) r_i, то их можно взять в качестве величин b_{ij}, проведя стандартную процедуру нормализации и приведения к единому диапазону[0..1] (1 - лучший показатель, 0 - худший), чтобы их пра-

вомерно было сравнивать как показатели качества. Если таковых характеристик нет, то следует провести экспертную оценку каким либо из известных методов и получить числовую характеристику качественных параметров решения каждым объектом j задачи r_i. Пусть величины b определяются экспертным путем, например по методу Саати, методом парных сравнений и нормализации по каждому требованию r_i.

В общем случае технические параметры r_i имеют разный физический смысл, поэтому для одних i включение в решение объектов j и k требует суммирования показателей b_j и b_k, а для других значения max (b_j , b_k), поэтому сумму в критерии (4) необходимо заменить на нелинейный функционал Ψ: В общем случае функционал Ψ может иметь и более сложный вид.

Вводится вектор $\alpha=\{\alpha_1\alpha_2\ldots\alpha_m\}$, ($\alpha_1+\alpha_2+\ldots+\alpha_m=1$), и целевая функция (4) приобретает вид:

$$F_3(x)=\sum_i^m \alpha_i \Psi_j(b_{ij}x_j)\to \min \qquad (6)$$

Задача выбора оптимальной структуры системы из составляющих ее объектов $S=\{S_1,S_2,\ldots,S_n\}$, для реализации заданных функций (требований) $R=\{r_1,r_2,\ldots r_m\}$ по критерию максимума показателя цена/качество решения всех задач R формулируется заменой в матрице B всех величин b на величины c/b и решения задачи (1), (4), либо (7).

С практической точки зрения интересной задачей является задача определения выбранного состава оборудования минимальной стоимости при заданной степени качества решения задачи r_i (качества решения всех задач R), то есть уровня безопасности b* по требованию i, (уровня безопасности объекта в целом). Эта задача решается как задача ЦЛП вида:

$$F_1(x)=\sum_{j=1}^n (C_j x_j)\to \min \qquad (7)$$

при условиях:

$$\sum_{j=1}^n (B_j x_j)\le b^*, \quad i\in M \qquad (8)$$

$$\sum_{j=1}^n (a_{ij}x_j)\ge 1, \quad i\in M \qquad (9)$$

$$x\in 0,1, \quad j\in N \qquad (10)$$

Обратная задача - при заданной максимальной стоимости C_{max} выбранного состава оборудования обеспечить максимальную степень безопасности объекта, то есть максимальную степень качества решения всех задач из R - решается как задача нелинейного программирования вида:

$$F_3(x)=\sum_i^m \alpha_i \Psi_j(b_{ij}x_j)\to \min, \qquad (11)$$

при ограничениях:

$$\sum_{j=1}^n (C_j x_j)\le c_{\max}, \quad i\in M \qquad (12)$$

$$\sum_{j=1}^n (a_{ij}x_j)\ge 1, \quad i\in M$$
$$x\in 0,1, \quad j\in N \qquad (13)$$

Известна задача многокритериальной дискретной оптимизации МКДО [2], в частности двухкритериальная задача о покрытии множества, в которой требуется найти покрытие одновременно минимизирующее функцию затрат (1) и максимизирующее функцию эффективности, имеющую вид (4).

Путем последовательных итераций методом уступок, меняя поочереди параметры стоимости и эффективности, предлагается строить парето-оптимальный фронт, из которого ЛПР уже может выбрать решение пользуясь экспертными знаниями.

При наличии только одной ФЗ, решаемой каждой подсистемой и, соответственно, выборе одного из n вариантов подсистем из группы альтернатив (блока), поставленная задача решается как классическая задача МКДО.

В более сложном случае - при выборе набора подсистем или компонент интегрированной системы с учетом показателей качества всех входящих в нее составляющих подсистем – искомое решения включает несколько подсистем, каждая из которых решает свою функциональную задачу (набор задач), причем решение должно состоять из набора альтернатив, покрывающих весь набор задач интегрированной системы. С точки зрения МКДО здесь альтернатива, подлежащая оценке и выбору, генерируется из нескольких элементарных подсистем-альтернатив, входящих в разные группы (блоки).

Способов генерации таких наборов может быть несколько в зависимости от исходных данных задачи. Если каждая подсистема решает только одну ФЗ, то при интеграции m ФЗ проблема может быть поставлена как известная блочная задача о ранце - выбора набора m подсистем по одной из каждого блока.

Причем локальный выбор в каждом блоке наилучшего компонента дает глобально

оптимальный выбор интегрированного решения, только если в качестве алгоритма выбора используется линейная свертка. При нелинейных методах свертки (Вальда, Сэвиджа и др.) это не выполняется.

Глобальный поиск оптимума в общем случае требует полного перебора вариантов – по одному из n компонентов в каждом из m блоков и дает $\mathbf{n^m}$ вариантов, что для реальных задач находится на границе возможностей перебора.

Если же каждая подсистема решает не одну, а несколько ФЗ (комплектовании ИТ-систем системно-интегрированными решениями), то при интеграции m ФЗ проблема формулируется как известная НЕблочная задача о ранце, в которой условием генерации решения является покрытие всех ФЗ, т. е. применение известной модели многоальтернативной оптимизации (МАО) профессора Я.Е. Львовича [10], в которой поиск оптимума целевой функции идет одновременно с решением задачи о наименьшем покрытии (ЗНП), и за счет унимодальности целевой функции отыскивается тупиковое покрытие.

Ограничение полного перебора 2^{m*n} вариантов комбинаций в задачах МАО реализуются путем построения только тупиковых покрытий (остальные отсекаются).

Однако модель МАО дает решение задачи о наименьшеи покрытии только для линейных функций либо нелинейных одномодальных целевых функций (с одной точкой экстремума). Наличие неунимодальных функций типа max(min) в целевой функции дает в результате одинаковые значения результирующих весов для большого числа решений – и возможно нетупиковых. Таким образом получение всех тупиковых решений ЗНП для большинства методов оптимизации (Вальда, Сэвиджа, Гурвица, Ходжа-Лемана) никаким из математических алгоритмов поиска экстремума невозможно.

Даже если ограничиться только целевым методом (линейным) решения задачи МКДО от неунимодальности в искомой задаче не удается избавиться по следующим соображениям. При попадании в решение системно-интегрированных компонентов два или более значения показателей должны объединяться по его физическому смыслу и чаще всего по правилу max либо min, то есть также неунимодальной функции. То есть операции для показателей из разных блоков сгенерируют значительное число решений с одинаковыми по весу результатами оценки и даже нетупиковых. Большое количество нетупиковых покрытий в данном случае это не изъян модели МАО или способа поиска оптимума функции (он может быть различный -линейный, градиентный или эвристический), а скорее последствие неунимодальности целевой функции на подготовительном этапе отбора компонентов в решение.

При переходе к 2-х факторному анализу, выделив затраты, можно найти одно тупиковое решение с минимальной стоимостью, но при этом остальные тупиковые покрытия теряются среди всех решений с равным весом целевой функции. Между тем именно тупиковые (пусть и с одинаковым весом) нам интересны с точки зрения системного интегрирования – стоимости их не сильно отличаются, но они минимальны и могут выбираться ЛПР по другим принципам.

Чтобы получить все возможные тупиковые решения необходимо включить этот механизм (определения тупиковых покрытий) в систему генерации альтернатив, который бы заменял его в известной модели МАО.

Таким образом, ставится задача - построить новую модель генерации альтернатив для СППР: сначала генерация тупиковых альтернатив только потом оценка в задаче МКДО. Так мы прорежививаем множество Парето-оптимльных альтернатив до множества строго тупиковых вариантов. (Т.е в какой-то степени разрабатываемая модель может считаться одним из способов сокращения Парето-оптимального множества решений для задачи МАО с нелинейными и неунимодальными целевыми функциями).

Кроме того эта модель генерации альтернатив вызывает следующую подзадачу. С точки зрения задачи системного интегрирования в этой модели теряются некоторые возможные решения, включающие «узкоспециализированные» компоненты. Механизм отсечения тупиковых решений таков, что эти «узкоспециализированные» компоненты доминируются и никогда не будут выбраны при поиске тупиковых решений. Чтобы устранить этот пробел необходимо дополнить механизм генерации альтернатив через поиск покрытий путем введения нового критерия поиска уточненного тупикового решения (Ту-критерия) искусственным внедрением таких доминируемых компонентов в решение.

Алгоритм Ту-критерия основан не на снижении требования к параметру на заданное

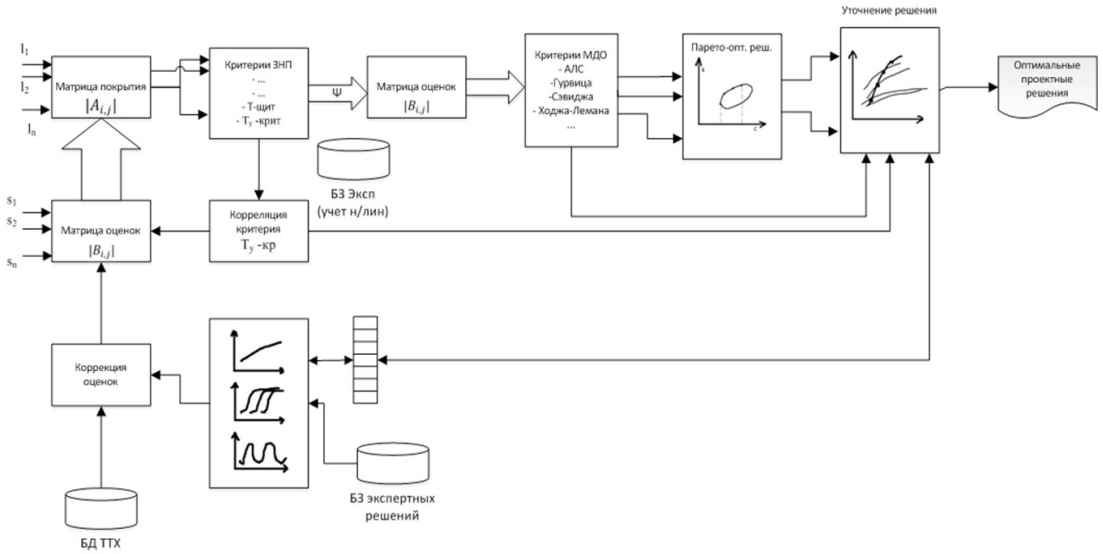

Рис. 2. Структура модели многоальтернативного выбора

число процентов (это известный прием в МКДО), а на видоизменении множества генерируемых альтернатив за счет выявления доминирующей компоненты и модификации ее параметров булева покрытия так, что она перестает доминировать и механизм генерации обязательно выберет эту ранее доминированную компоненту в новое решение. И если его вес на этапе 5 окажется больше, чем другие при том же либо меньшем значении затрат, то эта альтернатива строго лучше. Сравнение возможно, т. к. все величины параметров не изменялись, а корректировалась только матрица булевых покрытий. Даже если затраты оказались большим (не на много, т.к. УСК как правило дешевы), то это увеличение не дает решению выйти за пределы исходного Парето-оптимального фронта и эта альтернатива также «лучше». Т.е. результат применения Ту-критерия зависит от того насколько анализируемый «узкоспециализированный» компонент по этому выбранному параметру лучше, чем доминирующий и соотношения других цен. Конечно, при выборе системно-интегрированных компонентов вручную ЛПР таких тонкостей оценить не может.

В целом методика включает следующую последователностшагов:

1. Оценка коэффициентов важности внутри групп компонентов;

2. Оценка качества отбора результатов различными критериями, выбор наиболее информативных;

3. Оценка коэффициентов важности между группами компонентов;

4. Отбор ПО-решений за счет варьирования коэффициентов важности между группами компонентов, за счет учета нелинейности предпочтения ЛПР конкретного параметра;

5. Уточнение решений за счет нового Ту-критерия, объединяющего в единую модель ЗНП и МДО.

Таким образом, с учетом рассмотренных особенностей задач системной интеграции можно сделать вывод, что методологический подход при решении подобных задач разработан не в должной мере, поэтому возникают сложности с применением традиционных подходов. Таким образом, была обоснована недостаточная эффективность существующих методов в задачах системной интеграции и необходимость дальнейшего совершенствования методик и алгоритмов оптимизации, что позволит повысить качество принимаемых решений. Задача разработки моделей и методов, позволяющих на основе анализа требований, выбирать оптимальный набор параметров для синтеза интегрированной системы защиты из различных имеющихся подсистем и компонент, является актуальной и практически значимой, обеспечивая повышение эффективности принимаемых решений при управлении крупными проектами для анализа и оптимизации выбора программно-аппаратных компонент системы защиты.

Литература

1. Бурушкин А.А., Соловьев С.В., Ступников А.В. Об актуальности разработки методического обеспечения построения комплексных систем защиты информации в системах электронного документооборота при интеграции разноплатформенных программно-технических средств. //Информационное противодействие угрозам терроризма. Научно-практический журнал – 2009. – №13, С. 4–8.

2. Заозерская Л.А., Колоколов А.А. Исследование и решение двухкритериальной задачи о покрытии множества. //Проблемы информатики. – 2009 – №2 .

3. Львович Я.Е., Чернышева Г.Д., Каширина И.Л., Оптимизация проектных решений в САПР на основе эквивалентных преобразований задачи о минимальном покрытии. // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2006 – №1, С. 4.

4. Ногин В.Д. Границы применимости распространенных методов скаляризации при решении задач многокритериального выбора// Методы возмущений в гомологической алгебре и динамика систем: Межвуз. сб. науч. тр. Саранск: Изд-во Мордов. ун-та, 2004, – С. 59-68.

5. Ногин В.Д., Басков О.В. Сужение множества Парето на основе учёта произвольного конечного набора числовой информации об отношении предпочтения // Доклады АН, 2011, т. 438, № 4. – С. 1-4.

6. Прокушева А.П., Прокушев Я.Е. Моделирование и оптимизация выбора средств программно-аппаратной защиты информации с точки зрения экономической и технической целесообразности.// Информация и безопасность – 2012. – №1, С. 55-60.

7. Ехлаков Ю. П. Теоретические основы автоматизированного управления: Учебник. — Томск: Изд-во ТУСУР, 2001.

8. Нейман Дж., Моргенштейн О. Теория игр и экономическое поведение. — М.: Наука, 1970.

9. Ларичев О. И. Теория и методы принятия решений. — М.: Логос, 2002.

10. Львович Я. Е. Многоальтернативная оптимизация: теория и приложения/ Я.Е. Львович.- Воронеж: Кварта, 2006. – 428 С.

References

1. Burushkin A.A., Solov`ev S.V., Stupnikov A.V. Ob aktual`nosti razrabotki metodicheskogo obespecheniya postroeniya kompleksny`x sistem zashhity` informacii v sistemax e`lektronnogo dokumentooborota pri integracii raznoplatformenny`x programmno-texnicheskix sredstv. //Informacionnoe protivo dejstvie ugrozam terrorizma. Nauchno-prakticheskij zhurnal -2009. - №13, S. 4.

2. Zaozerskaya L.A., Kolokolov A.A. Issledovanie i reshenie dvuxkriterial`noj zadachi o pokry`tii mnozhestva. //Problemy` informatiki.- 2009.- №2 [E`lektronny`j resurs]- Rezhim dostupa- URL: problem-info.ru/2009-2/2.pdf, (data obrashheniya: 25.10.2012).

3. L`vovich Ya.E., Cherny`sheva G.D., Kashirina I.L., Voronezhskij gosudarstvenny`j texnicheskij universitet, Voronezhskij gosudarstvenny`j universitet- Optimizaciya proektny`x reshenij v SAPR na osnove e`kvivalentny`x preobrazovanij zadachi o minimal`nom pokry`tii. E`lektronnoe nauchno-texnicheskoe izdanie № FS 77 - 30569. Gosudarstvennaya registraciya №0421100025 [E`lektronny`j resurs]- Rezhim dostupa- URL: http://technomag.edu.ru/index.html, (data obrashheniya: 25.06.2012).

4. Nogin V.D. Granicy primenimosti rasprostranenny`x metodov skalyarizacii pri reshenii zadach mnogokriterial`nogo vy`bora// Metody` vozmushhenij v gomologicheskoj algebre i dinamika sistem: Mezhvuz. sb. nauch. tr. Saransk: Izd-vo Mordov. un-ta, 2004. – S. 59-68.

5. Nogin V.D., Baskov O.V. Suzhenie mnozhestva Pareto na osnove uchyota proizvol`nogo konechnogo nabora chislovoj informacii ob otnoshenii predpochteniya // Doklady` AN, 2011, t. 438, № 4. – S. 1-4.

6. Prokusheva A.P., Prokushev Ya.E. Modelirovanie i optimizaciya vy`bora sredstv programmno-apparatnoj zashhity` informacii s tochki zreniya e`konomicheskoj i texnicheskoj celesoobraznosti.// Informaciya i bezopasnost` -2012.- №1, S. 55-60.

7. Yekhlakov YU. P. Teoreticheskiye osnovy avtomatizirovannogo upravleniya: Uchebnik. — Tomsk: Izd-vo TUSUR, 2001.

8. Neyman Dzh., Morgenshteyn O. Teoriya igr i ekonomicheskoye povedeniye. — M.: Nauka, 1970.

9. Larichev O. I. Teoriya i metody prinyatiya resheniy. — M.: Logos, 2000.

10. L'vovich YA. Ye. Mnogoal'ternativnaya optimizatsiya: teoriya i prilozheniya/ YA.Ye. L'voviya.- Voronezh: Kvarta, 2006. – 428 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

УГРЮМОВ Дмитрий Викторович, аспирант кафедры компьютерных технологий и информационной безопасности, Кубанский государственный технологический университет (КубГТУ), 350072, Россия, Краснодарский край. Краснодар, ул. Московская, д. 2. E-mail: d.ugryumov@mail.ru

HALIZEV Vyacheslav, Candidate of Technical Sciences, Professor, Department of Computer Technologies and Information Security, Institute of Computer Systems and Information Security, FSBEI HE "Kuban State Technological University", Russia, 350072, Krasnodar Krai, Krasnodar, Moskovskaya str, 2. E-mail: ha53@mail.ru

UGRIUMOV Dmitry, Postgraduate Student, Department of Computer Technologies and Information Security, Kuban State Technological University (KubGTU), Krasnodar Region, 350072, Russia, Krasnodar Krai , Krasnodar, Moskovskaya str., 2. E-mail: d.ugryumov@mail.ru

УДК 343.353.12 + 347.961.38 Вестник УрФО № 4(30) / 2018, с. 60–65

Уторов О. Р.

DOI: 10.14529/secur180409

ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ ОТНОШЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ СЛУЖЕБНОЙ ТАЙНЫ

В статье проводится анализ нормативного правового регулирования служебной тайны, выявляются нерегламентированные отношения в данной сфере, и в связи с этим формулируются проблемы правоприменения на практике. Приводятся примеры непоследовательности законодателя в конструировании норм, относящихся к служебной тайне, и высказывается необходимость их унификации принятием федерального закона. Прогнозируются возможные негативные последствия, связанные с субъективным толкованием отнесения конкретных сведений к служебной информации ограниченного распространения.

Ключевые слова: *служебная тайна, служебная информация, информация ограниченного доступа, конфиденциальная информация.*

Utorov O. R.

PROBLEMS LAW ENFORCEMENT RELATIONS IN THE SPHERE OF CIRCULATION OFFICIAL SECRET

The article analyzes the normative legal regulation of official secrecy, reveals the unregulated relations in this sphere and in this regard formulates the problems of law enforcement in practice. Examples of inconsistency of the legislator in the construction of rules relating to official secrecy are given, and the need for their unification by the adoption of Federal law is expressed. Predicts the possible negative consequences associated with the subjective interpretation of the classification of specific information as official information for restricted dissemination.

Keywords: *service secret, service information, limited access information, confidential information.*

Анализ законодательства, регулирующего обращение служебной тайны, позволяет констатировать, что оно представляет собой вместо единой выстроенной системы некий набор положений различных отраслей права, не объединенных ни общим предметом регулирования, ни общим принципом.

Вместе с тем информация, представленная в форме служебной тайны, прослеживается во многих законах и еще больше в ве-

домственных правовых актах. При рассмотрении норм, регламентирующих сбор (получение), использование, передачу, хранение и уничтожение служебной тайны применяются различные ее наименования: служебная тайна, информация ограниченного распространения, служебная информация ограниченного доступа, просто служебная информация и т. п. При этом, необходимо отметить, что само понятие служебной тайны, так и не определено законодательством.

Авторы пояснительной записки к проекту Федерального закона «О служебной тайне» считают, что, несмотря на практически полное отсутствие нормативного регулирования в сфере отнесения сведений к служебной тайне и их защиты, нормы о ней находятся более чем в 40 федеральных законах, в том числе: «Об основах государственной службы Российской Федерации», «О Правительстве Российской Федерации», «Об основах муниципальной службы Российской Федерации», «О защите конкуренции», и в иных. При этом исследователи акцентируют внимание на разнообразии правовых подходов, получивших закрепление в законодательстве [1], и противоречии друг с другом многих нормативных актов [2, с. 18].

Так, в Трудовом кодексе Российской Федерации (ст.ст. 37, 57, 81, 243, 358), Федеральном законе «О защите конкуренции» (ст.ст. 24, 25, 25.6, 26, 45) упоминается охраняемая законом тайна, в том числе служебная; в Федеральных законах «О страховании вкладов физических лиц в банках Российской Федерации» (ст. 31), «О кредитных историях» (ст.ст. 5, 6, 7, 17) прописывается служебная тайна; в Указе Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера» служебная тайна отнесена к сведениям конфиденциального характера; в Федеральном законе «О государственной гражданской службе Российской Федерации» (ст. ст. 17, 18, 24, 37), Федеральном законе «О Центральном банке Российской Федерации (Банке России)» (ст. 90 и 92) и ряде других законов используется термин «служебная информация»; Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» (ст.ст. 6, 9, 18, 20) предусматривает одну из мер безопасности в отношении защищаемого лица – обеспечение конфиденциальности сведений о нем. Эти примеры свидетельствуют о том, что не только терминология, но и содержание института служебной информации не имеет в законодательстве однозначного понимания [1].

Поэтому, на наш взгляд, справедливо отмечает А.А. Антопольский, что в законодательстве для обозначения одного и того же круга объектов используются различные термины (служебная информация, служебная тайна, служебная информация ограниченного распространения и др.). Именно по этой причине трудно построить четкую классификацию служебной тайны и отграничить ее от смежных категорий [3, с. 25].

Вместе с этим, вопрос осуществления управления в государственных органах и регулирование использования служебной тайны можно рассматривать с одной стороны как предупреждение манипулирования информацией или ее утечки, а с другой как ограничение бесконтрольного «засекречивания» информации. Кроме того, бесконтрольное ограничение доступа к информации является весьма серьезным коррупциогенным фактором. Соответственно системное правовое регулирование служебной тайны должно повысить прозрачность деятельности государственных органов и должностных лиц [2, с. 18].

Исследователи указанного направления в защите информации причины изложенных противоречий связывают с историей формирования института служебной тайны, а точнее с его трансформацией на постсоветском пространстве [4]. Чтобы разобраться подробней с проблематикой вопроса обратимся к ее ретроспективе.

Действительно до принятия в 1993 г. Закона Российской Федерации «О государственной тайне» служебная тайна входила в состав сведений, составляющих государственную тайну, а точнее, как отмечает П.Н. Кораблев и Т.М. Занина – в интегрированное понятие государственных секретов, которые по степени их важности подразделялись на государственную и служебную тайны [5, с. 31]. Последняя имела гриф секретности «секретно» и охранялась в режиме государственной тайны.

Волчинская Е. К. дополняя данную мысль, указывает что ограничительная пометка «Для служебного пользования» использовалась для ограничения доступа к иной информации на основе ведомственных инструкций и перечня сведений, определяемого Главлитом. После принятия Закона о государственной тайне часть сведений, составляющих служебную тайну, поглотилась режимом государ-

ственной тайны без выделения особой категории. Другая часть была выведена из режима государственной тайны и стала охраняться в режиме ограниченного доступа [6, с. 71-72].

В этом же году была принята Конституция Российской Федерации, в которой в части 3 статьи 55 определено, что права и свободы человека и гражданина могут быть ограничены только федеральным законом [7]. Соответственно служебная тайна как системная категория практически исчезла из российского законодательства. В этой связи, по мнению А.В. Швецова, а также П.Н. Кораблева и Т.М. Заниной, принятие Закона о государственной тайне, привнеся массу позитивных моментов, повлекло за собой одно существенное негативное последствие – отнесение в соответствии с указанным законом грифа «секретно» для обозначения исключительно сведений, составляющих государственную тайну, де-факто ликвидировало служебную тайну как институт и заодно создало серьезную правовую неопределенность в вопросе квалификации ранее обозначенных им сведений (то есть, подпадают ли они под режим ограничений государственной тайны либо нет) [8, с. 78; 5, с. 31].

Возникшие противоречия и неурегулированность названных общественных отношений обусловили появление в 1994 году во вновь приятном Гражданском кодексе Российской Федерации статьи 139, которая хоть и «вернула» обратно в правовое русло категорию служебной тайны, но ее содержание по-прежнему оставалось очень размыто. Так, в указанной статье было предусмотрено, что информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности [9].

По нашему мнению, следует согласиться с позицией Ю.В. Пономаревой, подчеркнув, что такая формулировка законодателя фактически предусматривала регулирование служебной тайны по аналогии с коммерческой, при этом служебной тайне приписывались свойства «действительной или потенциальной коммерческой ценности», что фактически подрывало всю научную доктрину в области конфиденциальной информации как таковой [2, с. 119]. Действительно наделение коммерческой ценностью в качестве основного признака служебной тайны ставило под сомнение в принципе ее правовое существование в таком виде в органах власти. Тем не менее, указанная норма действовала двенадцать лет, а после ее отмены в 2008 г. служебная тайна так опять и не получила законодательного закрепления.

Таким образом, можно сделать вывод, что использование служебной тайны в качестве конфиденциальной информации и проставление на документе ограничительной пометки «Для служебного пользования» не предусмотрено федеральным законом, а, следовательно, не совсем легитимно.

Однако, как пишет Волчинская Е. К. практика использования грифа «ДСП» для ограничения доступа к некоторой информации сохранилась как в органах власти, так и в организациях. По мнению исследователя, поскольку такая практика не базируется на законе, это создает предпосылки массового нарушения прав физических и юридических лиц на доступ к информации [6, с. 72].

Следует также отметить, что в 1994 г. одновременно с вступлением в силу Гражданского кодекса Российской Федерации было принято «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденное постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 [10], которое хотя бы на уровне подзаконного нормативного правового акта, но закрепило основные вопросы регулирования служебной тайны, определяя ее как служебную информацию ограниченного распространения – несекретную информацию, касающуюся деятельности организаций, ограничения, на распространение которой диктуются служебной необходимостью.

Согласимся с позицией Фатьянова А. А., который считает, что данная дефиниция, скажем прямо, неуклюжая, но суть категории из нее ясна – это сведения, распространение которых ограничивается, исходя из служебной целесообразности, то есть информация, для которой предусмотрен гриф «Для служебного пользования» [11, с. 24].

По мнению же Павлова И. Ю., поскольку критерием отнесения тех или иных сведений к категории служебной информации ограниченного распространения являются не конкретные объективные факторы, а субъективная категория – «служебная необходимость»,

возникает повод для возможности принятия произвольных правоприменительных решений [12, с. с. 35].

Еще одно упоминание служебной тайны, как уже мы обозначали, содержится в Указе Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188, в котором в качестве одного из видов конфиденциальной информации выступают служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна) [13].

Вместе с тем, несмотря на имеющиеся правовое регулирование, регламентация служебной тайны исключительно на подзаконном уровне, на наш взгляд, противоречит:

– концепции ч. 3 ст. 55 Конституции Российской Федерации [7], согласно которой права и свободы человека и гражданина могут быть ограничены только федеральным законом;

– принципу, предусмотренному п. 2 ст. 3 Федерального закона «Об информации, информационных технологиях и защите информации» [14], согласно которому ограничение доступа к информации устанавливается только федеральными законами;

– положению ч. 2 ст. 5 указанного закона, на основании которого информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);

– требованию ч. 4 ст. 9 указанного закона, в соответствии с которым федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Исходя из изложенного, следуя формальной логике, на практике может возникнуть ситуация, при которой сформируется правовая позиция, заключающаяся в том, что если регулирование служебной тайны осуществляется не на уровне федерального закона, как этого требует законодательство, то исполнение таких требований, а тем более связанных с этим ограничений, не является обязательным. Надо отметить, что при таких условиях правоприменителям и судам придется «очень постараться» как-то юридически обосновать законодательный пробел.

Дополнительно стоит подчеркнуть, что при отсутствии единого федерального закона, ответы на поставленные выше вопросы найти крайне сложно по причине отсутствия систематезированности требований подзаконных актов, а так же, как было сказано выше – с их противоречивостью.

Тем не менее, необходимость ограничения доступа к служебной информации органов публичной власти все же объективно существует. И это актуально не только для органов исполнительной власти (хотя для них в большей степени), но и для других ветвей власти, а также для органов местного самоуправления, поскольку везде существует внутрисистемная информация, ограничение в доступе к которой необходимо и оправдано. Однако, как справедливо отмечает А.А. Фатьянов если не сформировать законодательные рамки для чиновников, то могут пострадать права и свободы граждан, прежде всего, право на доступ к информации [11, с. 24].

Таким образом, проблема правоприменения отношений в сфере обращения служебной тайны, в связи с отсутствием законодательного закрепления, очевидна. Указанные проблемы регулирования служебной тайны только на подзаконном уровне, безусловно, свидетельствует о необходимости глубокого анализа названных противоречий и теоретического их осмысления через призму вновь разработанного законопроекта, но с учетом соотносимости и четкой корреляции служебной тайны с другими видами охраняемых законом тайн.

Литература

1. Пояснительная записка к проекту законопроекта «О служебной тайне» при повторном внесении в Государственную Думу Федерального Собрания Российской Федерации 05.04.2006 В.В. Бобыревым, А.Н. Волковым, М.И. Гришанковым, В.В. Дятленко, В.И. Илюхиным, Н.С. Леоновым, В.В. Маргеловым, А.М. Розуваном // http://www.consultant.ru/cons/cgi/online. cgi?req=doc&base=PRJ &n=40148#0956362910113622.

2. Пономарева Ю.В. Актуальные вопросы служебной тайны // Вестник УрФО. Безопасность в информационной сфере. – 2013. – № 4 (10). – С. 17-30.

3. Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управлении: автореф. дис. ... канд. юрид. наук. – М. – 2004. – 29 С.

4. Лукичев К.Е. К вопросу об институте служебной тайны // Журнал «Право и безопасность» – 2009. – № 3 (32). // http://dpr.ru/pravo/pravo_28_15.htm.

5. Кораблев П.Н., Занина Т.М. Особенности правовой защиты служебной тайны // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 31-34.

6. Волчинская Е.К. Проблемы правовой регламентации режима служебной тайны в законодательстве Российской Федерации // Вопросы совершенствования законодательства в сфере обеспечения информационной безопасности. – М.: Издание Государственной Думы. – 2007. – С. 71-79.

7. Конституция Российской Федерации // Собрание законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.

8. Швецов А.В. Защита информации в сфере служебной тайны в деятельности ОВД (Правовой аспект): дис. ... канд. юрид. наук. – Воронеж. – 2005. – 189 С.

9. Гражданский кодекс Российской Федерации // Собрание законодательства Российской Федерации. – 1994. – № 32. – Ст. 3301.

10. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» // Собрание законодательства Российской Федерации. – 2005. – № 30. – Ст. 3165.

11. Фатьянов А.А. Правовой институт служебной тайны: история и современное состояние // Защита информации. Инсайд. – 2005. – № 4. – С. 22–25.

12. Павлов И.Ю. Современные проблемы правового регулирования государственной и служебной тайны в России // Ленинградский юридический журнал. – 2013. – № 1 (31). – С. 29–37.

13. Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188 // Собрание законодательства Российской Федерации. – 1997. – № 10. – Ст. 1127.

14. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собрание законодательства **Российской Федерации**. – 2006. – № 31 (1 ч.). – Ст. 3448.

References

1. Poyasnitel'naya zapiska k proyektu zakonoproyekta «O sluzhebnoy tayne» pri povtornom vnesenii v Gosudarstvennuyu Dumu Federal'nogo Sobraniya Rossiyskoy Federatsii 05.04.2006 V.V. Bobyrevym, A.N. Volkovym, M.I. Grishankovym, V.V. Dyatlenko, V.I. Ilyukhinym, N.S. Leonovym, V.V. Margelovym, A.M. Rozuvanom // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=40148#0956362910113622.

2. Ponomareva YU.V. Aktual'nyye voprosy sluzhebnoy tayny // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2013. – № 4 (10). – S. 17-30.

3. Antopol'skiy A.A. Pravovoye regulirovaniye informatsii ogranichennogo dostupa v sfere gosudarstvennogo upravlenii: avtoref. dis. ... kand. yurid. nauk. – M. – 2004. – 29 S.

4. Lukichev K.Ye. K voprosu ob institute sluzhebnoy tayny // Zhurnal «Pravo i bezopasnost'» – 2009. – № 3 (32). // http://dpr.ru/pravo/pravo_28_15.htm.

5. Korablev P.N., Zanina T.M. Osobennosti pravovoy zashchity sluzhebnoy tayny // Vestnik Voronezhskogo instituta MVD Rossii. – 2008. – № 1. – S. 31-34.

6. Volchinskaya Ye.K. Problemy pravovoy reglamentatsii rezhima sluzhebnoy tayny v zakonodatel'stve Rossiyskoy Federatsii // Voprosy sovershenstvovaniya zakonodatel'stva v sfere obespecheniya informatsionnoy bezopasnosti. – M.: Izdaniye Gosudarstvennoy Dumy. – 2007. – S. 71-79.

7. Konstitutsiya Rossiyskoy Federatsii // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 2014. – № 31. – St. 4398.

8. Shvetsov A.V. Zashchita informatsii v sfere sluzhebnoy tayny v deyatel'nosti OVD (Pravovoy aspekt): dis. ... kand. yurid. nauk. – Voronezh. – 2005. – 189 S.

9. Grazhdanskiy kodeks Rossiyskoy Federatsii // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 1994. – № 32. – St. 3301.

10. Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 3 noyabrya 1994 g. № 1233 «Ob utverzhdenii polozheniya o poryadke obrashcheniya so sluzhebnoy informatsiyey ogranichennogo rasprostraneniya v federal'nykh organakh ispolnitel'noy vlasti» // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 2005. – № 30. – St. 3165.

11. Fat'yanov A.A. Pravovoy institut sluzhebnoy tayny: istoriya i sovremennoye sostoyaniye // Zashchita informatsii. Insayd. – 2005. – № 4. – S. 22-25.

12. Pavlov I.YU. Sovremennyye problemy pravovogo regulirovaniya gosudarstvennoy i sluzhebnoy tayny v Rossii // Leningradskiy yuridicheskiy zhurnal. – 2013. – № 1 (31). – S. 29-37.

13. Ukaz Prezidenta Rossiyskoy Federatsii «Ob utverzhdenii perechnya svedeniy konfidentsial'nogo kharaktera» ot 6 marta 1997 g. № 188 // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 1997. – № 10. – St. 1127.

14. Federal'nyy zakon ot 27 iyulya 2006 g. № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i zashchite informatsii» // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 2006. – № 31 (1 ch.). – St. 3448.

УТОРОВ Олег Равильевич, кандидат педагогических наук, доцент кафедры Защиты информации высшей школы электроники и компьютерных наук ФГАО ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail utorov@mal.ru.

UTOROV Oleg, candidate of pedagogical sciences, docent of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail utorov@mal.ru.

УДК 004.056.5 + 003.26 Вестник УрФО № 4(30) / 2018, с. 66–74

Васильев В. И. , Кириллова А. Д. , Кухарев С. Н.

DOI: 10.14529/secur180410

КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ (СОВРЕМЕННОЕ СОСТОЯНИЕ, ТЕНДЕНЦИИ)[1]

Последние годы характеризуются резким ростом актуальности проблемы обеспечения кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. В данной статье рассматривается общее состояние данной проблемы и пути ее решения. Основное внимание уделяется анализу существующей нормативно-методической и правовой базы обеспечения кибербезопасности критически важных объектов. Дается краткая характеристика основных положений ключевых документов в области кибербезопасности АСУ ТП (NIST SP 800-82, NERC CIP, ISA/IEC 62443, Федеральный закон № 187-ФЗ, Приказы ФСТЭК Рос-сии №№ 31 и 239, ГОСТ Р МЭК 62443).Отмечается активная роль указанных документов в решении практических задач, связанных с обеспечением кибербезопасности.

Ключевые слова: *кибербезопасность, автоматизированная система управления, технологический процесс, стандарт, оценка риска.*

Vasilyev V. I. , Kirillova A. D. , Kukharev S. N.

CYBERSECURITY OF APCS: MODERN TRENDS AND APPROACHES (CURRENT STATE, PERSPECTIVES)

Last years are characterized by sharp increase of urgency of the problem connected with providing the cybersecurity of automated process control systems (APCS) of industrial objects. The given paper investigates a general state of this problem and the ways of its solving. The main attention is paid to analysis of existing normative-methodical and legal base of cybersecurity maintenance of critically important objects. The brief characteristic of main principles

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-48-020095

containing in some key documents in APCS cybersecurity sphere (NIST SP 800-82, NERC CIP, ISA/IEC 62443, Federal Law 187-FZ, FSTEC of Russia Orders No. 31 and 239, GOST R 62443 series) is given. The active role of these documents in solving practical tasks connected with providing cybersecurity is emphasized.

Keywords: *cybersecurity, automated process control systems, technological process, standard, risk assessment.*

Введение

Статистика последних лет подтверждает резкий рост числа хакерских атак на автоматизированные системы управления технологическими процессами (АСУ ТП) крупных и средних промышленных предприятий. Так, по материалам исследований «Лаборатории Касперского» [1] только во втором полугодии 2017 г. около половины (46,8%) компьютеров, используемых в системах промышленной автоматизации в России, хотя бы один раз подвергались компьютерным атакам. В 2017 г. 10,8% всех систем АСУ ТП стали мишенью атак ботнет-агентов. Основными источниками атак ботнет-агентов при этом были Интернет, сменные носители и сообщения электронной почты. В качестве наиболее крупных целевых атак на системы промышленной инфраструктуры в 2017 г. наибольшую известность получили вирус-шифровальщик WannaCry (на него пришлось 13,4% от всех атакованных компьютерных систем технологической инфраструктуры организаций), а также широко нашумевшие атаки Industroyer и Trisis/Triton. Особенностью 2-х последних атак является то, что впервые после вируса Stuxnet атакующим удалось создать собственные реализации промышленных сетевых протоколов и получить возможность напрямую влиять на работу управляющих устройств в составе АСУ ТП.

Общее число уязвимостей, выявленных в различных компонентах АСУ ТП экспертами «Лаборатории Касперского» в 2017 г., составило 322. Наибольшее количество уязвимостей было выявлено в:

– компонентах SCADA-систем (т.е. систем диспетчерского управления и сбора данных);

– сетевых устройствах промышленного назначения;

– программируемых логических контроллерах (ПЛК);

– инженерном программном обеспечении (ПО).

Как отмечается в [1], эксплуатация злоумышленниками указанных уязвимостей может привести к выполнению произвольного кода, несанкционированному управлению промышленным оборудованием, отказу в его работе. При этом значительная часть уязвимостей может эксплуатироваться удаленно без аутентификации, и их эксплуатация не требует от злоумышленника каких-либо специальных знаний и навыков.

Приведенные факты являются безусловным доказательством обострения ситуации, складывающейся вокруг обеспечения безопасности систем промышленной автоматизации. Это особенно касается потенциально опасных производств и объектов критической инфраструктуры в области энергетики, нефтехимии, водоснабжения, транспорта и т.п., реализация атак на которые может привести к серьезным последствиям для жизни и здоровья людей или нанесению ущерба окружающей среде. Сегодня фактически уже общепризнано, что безопасность АСУ ТП не сводится к обеспечению информационной безопасности (ИБ), т.е. обеспечению конфиденциальности собираемой, обрабатываемой и передаваемой информации. Безопасность АСУ ТП должна заключаться прежде всего в обеспечении непрерывности и целостности самого ТП, что составляет содержание нового, бурно развивающегося направления «кибербезопасность» (cybersecurity) АСУ ТП [2-4].

Вместе с тем, хотя на Западе термины «киберпространство», «кибербезопасность» уже давно заняли свое прочное место в профессиональной среде, в России все еще продолжаются споры относительно сути самого понятия «кибербезопасность» и сферы его применения [5-7]. На данный момент в российском законодательстве понятие «киберпространство» и «кибербезопасность» отсутствуют. Вынесенная в начале 2014 г. на обсуждение «Концепция стратегии кибербезопасности Российской Федерации» [8] получила неоднозначные оценки и так и не была принята. В то же время, сегодня наметилось определенное противоречие между отставанием нормативно-правовой базы и многочисленными предложениями на рынке в области обеспечения кибербезопасности АСУ ТП со стороны веду-

щих российских компаний («ДиалогНаука», «ИнфоТеКС», «Лаборатория Касперского», «Информзащита», Positive Technologies, «Ростелеком» и др.). В июле 2018 г. в Москве состоялся Международный конгресс по кибербезопасности, одной из главных целей которого явилась координация усилий и планов совместных действий производителей и специалистов в сфере кибербезопасности.

Учитывая актуальность затронутой проблемы, рассмотрим современное состояние нормативно-правового и методического обеспечения работ в области кибербезопасности АСУ ТП. Для определенности далее будем пользоваться следующим определением кибербезопасности, приведенном на сайте Cisco [9]: **кибербезопасность** – это реализация мер по защите систем, сетей и программных приложений от цифровых атак.

Американские и международные стандарты в области кибербезопасности АСУ ТП

Наиболее известными стандартами, имеющими непосредственное отношение к проблеме кибербезопасности АСУ ТП, являются следующие стандарты, изначально разработанные в США и получившие широкое распространение по всему миру:

1) NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security»;

2) NERC Critical Infrastructure Protection (CIP), Cybersecurity;

3) ANSI/ISA-99 «ISA-99 Security for Industrial Automation and Control Systems»;

4) ISA/IEC 62443 «Industrial Automation and Control Systems Security».

Стандарт NIST SP 800-82 («Рекомендации по обеспечению безопасности промышленных систем автоматизации») разработан Центром компьютерной безопасности (CSRC) Национального института стандартов и технологий (NIST, National Institute of Standards and Technology) в 2011 г. (2-ая редакция – в 2015 г.).

Данный стандарт фактически представляет собой набор практических рекомендаций и методических наработок по комплексному обеспечению безопасности АСУ ТП [10]. Стандарт NIST содержит:

– рекомендации, связанные с построением системы защиты информации;

– упрощенные модели злоумышленника и угроз АСУ ТП;

– перечень типовых угроз и уязвимостей АСУ ТП;

– рекомендации по созданию и внедрению программы обеспечения безопасности АСУ ТП;

– описание архитектуры типовой АСУ ТП и подсистемы безопасности;

– описание традиционных подсистем ИБ (контроля и управления доступом, идентификации и аутентификации, антивирусной защиты и др.).

Семейство отраслевых стандартов NERC-CIP (Critical Infrastructure Protection) – «Защита объектов критической инфраструктуры» – разработаны Северо-Американской корпорацией по обеспечению надежности электросетей (NERC, North American Electric Reliability Corporation) в начале 2000-х гг. Целью применения данных стандартов является обеспечение надежной защиты автоматизированных систем и сетей коммуникации для объектов энергетического сектора от возможных кибератак [10]. В состав данного семейства стандартов входят стандарты NERC CIP-001÷009, в том числе:

– CIP-002-1 Critical Cyber Asset Identification («Идентификация критических киберактивов);

– CIP-005-1 Electronic Security Perimeter («Электронный периметр безопасности»);

– CIP-006-1 Physical Security («Физическая безопасность»);

– CIP-007-1 Systems Security Management («Управление безопасностью систем»).

Как и стандарт NIST SP 800-82, стандарты NERC CIP представляют собой детально проработанные методические руководства по обеспечению кибербезопасности АСУ ТП (в данном случае – объектов в энергетической сфере), которые успешно применяются не только в США, но и во многих странах мира, включая Россию.

Семейство стандартов ANSI/ISA-99 («Безопасность промышленных систем автоматизации и управления») – это комплексная программа обеспечения безопасности АСУ ТП, разработанная комитетом ISA-99 в составе Международного общества автоматизации (ISA, International Society of Automation), отвечающим за разработку стандартов. В 2007 г. стандарт ISA-99 был поддержан Американским национальным институтом стандартов (ANSI, American National Institute of Standards) и был опубликован как ANSI/ISA-99, а в 2010 г. переиздан как ANSI/ISA-62443 [11].

В качестве базовой концепции в этих

стандартах используется подход, основанный на сегментации сети передачи данных предприятия на зоны и связывающие их тракты (пути сообщения). Под зоной при этом понимается объединение логических или физических средств, для которых предъявляются схожие требования по безопасности, например, критичность для ТП. В стандартах не определены конкретные методы или алгоритмы выделения зон и трактов внутри сети передачи данных. Вместо этого предлагается осуществлять такой выбор (с обоснованием соответствующих требований к ним по обеспечению безопасности) исходя из анализа уровня рисков компании. Риск в данном случае заключается не столько в самой возможности реализации кибератаки, сколько в ее последствиях, а уменьшение последствий достигается за счет локализации их в выделенной зоне, максимально изолированной от других сегментов. Обеспечение безопасности зон и каналов осуществляется путем выбора специализированных средств защиты, например, промышленных межсетевых экранов или VPN.

Предложенная в указанных стандартах концепция обеспечения безопасности АСУ ТП на основе сегментации (зонирования) системы получила поддержку Международной электротехнической комиссии (IEC, International Electrotechnical Commission) и в дальнейшем легла в основу разработки стандартов кибербезопасности АСУ ТП нового поколения ISA/IEC 62443.

Серия международных стандартов ISA/IEC 62443 («Безопасность промышленных систем автоматизации и управления») – это совместная перспективная разработка комитетов ISA-99 и IEC, имеющая своей целью обеспечение безопасности, доступности, целостности и конфиденциальности компонентов и систем, входящих в состав промышленных АСУ ТП [13].

Работа над созданием стандартов ведется начиная с 2009 г. Всего предполагается выпуск 13 ключевых стандартов и технических отчетов, разделенных на 4 группы:

1) «Общие положения» (General) – 2 стандарта и 2 технических отчета, определяющие базовые понятия, модели, термины, количественные показатели (метрики) безопасности АСУ ТП;

2) «Политики и процедуры» (Policies and Procedures) – 2 стандарта и 2 технических отчета, устанавливающие общие требования к системе управления защитой АСУ ТП, а также ряд конкретных правил в рамках программы безопасности АСУ ТП;

3) «Системные требования» (System Requirements) – 1 стандарт и 2 технических отчета, описывающие различные технологии обеспечения безопасности АСУ ТП, оценки рисков и контроля уровня защищенности системы;

4) «Требования к компонентам» (Component Requirements) – 2 стандарта, определяющие требования к безопасности на уровне отдельных подсистем и компонентов АСУ ТП (нижний уровень).

В настоящее время часть этих стандартов уже опубликована, другие находятся в процессе разработки и утверждения.

В основе требований, предъявляемых стандартами ISA/IEC 62443 к обеспечению безопасности АСУ ТП, лежит риск-ориентированный подход. В соответствии с этим подходом, проектирование системы управления защитой АСУ ТП предполагает выполнение следующих этапов:

– высокоуровневая (ориентировочная) оценка рисков от воздействия кибератак;

– построение *референсной (reference)* модели АСУ ТП как объекта защиты, описывающей классификацию основных видов деятельности, ТП, АСУ и других активов;

– построение *модели активов* (asset model), описывающей иерархию основных объектов и активов АСУ ТП, их взаимодействие с сетями, ключевыми подразделениями и т.д.;

– построение *референсной модели архитектуры* (reference architecture model), отражающей все основные элементы АСУ ТП, телекоммуникационное оборудование, линии связи и т.п.;

– построение *модели зонирования* (zone and conduit model), разделяющей объект защиты на отдельные зоны;

– детальный *анализ рисков* для каждой выделенной зоны;

– определение *текущего уровня безопасности* для каждой зоны и требований по обеспечению *целевого уровня безопасности* зоны, реализуемых путем выбора соответствующих мер защиты.

Ряд стандартов серии ISA/IEC 62443 сегодня переведены на русский язык и активно используются ведущими российскими компаниями – лидерами рынка систем защиты АСУ ТП.

Нормативно-правовые основы обеспечения кибербезопасности АСУ ТП в России

Одним из базовых нормативно-законодательных актов, определяющих общие требования к безопасности промышленных объектов, является **федеральный закон «О безопасности объектов топливно-энергетического комплекса» от 21 июля 1997 г. № 116-ФЗ** (последняя редакция с изменениями 2018 г.). Этот закон устанавливает организационные и правовые основы в сфере обеспечения безопасности объектов топливно-энергетического комплекса (ТЭК). В соответствии со статьей 11 этого закона, определена необходимость создания на объектах ТЭК системы защиты информации и информационно-телекоммуникационных сетей от неправомерного доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий.

Конкретные требования, предъявляемые к системам защиты АСУ ТП промышленных предприятий, определены **Приказом ФСТЭК России от 14 марта 2014 г. № 31** «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды» [14]. В рамках Приказа рассматривается 3-хуровневая структура АСУ ТП, включающая в себя: уровень ввода-вывода данных (датчики, исполнительные механизмы), уровень автоматического управления (программируемые логические контроллеры, ПЛК) и уровень операторского управления (АРМ, SCADA-серверы, телекоммуникационное оборудование).

В качестве объектов защиты АСУ ТП выделяются:

– критически важная (технологическая) информация, включающая управляющую, контрольно-измерительную информацию и др.;

– программно-технический комплекс, включающий технические средства, ПО и средства защиты информации.

Требования к защите АСУ ТП определяются в зависимости от *класса защищенности* системы, который, в свою очередь, зависит от *уровня значимости (критичности)* обрабатываемой информации. Уровень значимости (критичности) информации определяется степенью возможного ущерба от нарушения ее целостности, доступности или конфиденциальности, в результате которого возможно нарушение штатного режима функционирования АСУ или незаконное вмешательство в процессы функционирования АСУ ТП.

Для каждого класса защищенности в Приказе ФСТЭК № 31 определены базовые наборы мер защиты, в состав которых входят:

1) идентификация и аутентификация;
2) управление доступом;
3) ограничение программной среды;
4) защита машинных носителей информации;
5) регистрация событий безопасности;
6) антивирусная защита;
7) обнаружение вторжений;
8) контроль (анализ) защиты информации;
9) обеспечение целостности;
10) обеспечение доступности;
11) защита среды виртуализации и др.

Выбранные меры защиты рассматриваются отдельно для каждого уровня АСУ ТП с учетом особенностей функционирования каждого из уровней.

Достоинством предложенного в Приказе ФСТЭК № 31 подхода к обеспечению защиты информации, обрабатываемой в АСУ ТП, является комплексное применение организационных и технических мер защиты информации на всех стадиях жизненного цикла АСУ ТП. В то же время, следует заметить, что требования Приказа, хотя и в значительной степени коррелируют с перечисленными выше международными стандартами, также носят рекомендательный (не обязательный) характер. Окончательное решение о выборе класса защищенности и необходимых мер защиты принимает собственник АСУ ТП.

Важную роль в решении проблемы безопасности АСУ ТП крупных промышленных предприятий играет **федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ** [15]. Под объектами критической информационной инфраструктуры (КИИ) здесь понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов РФ, функционирование которых критически важно для экономики государства. В соответствии с данным законом, должно производиться категорирование объектов КИИ, составляется общегосударственный реестр

значимых объектов КИИ, предусмотрено выполнение обязательных требований по обеспечению безопасности значимых объектов КИИ, контролируемых государством.

С целью конкретизации требований, предусмотренных федеральным законом 187-ФЗ, и условий их применения, ФСТЭК России выпустила **Приказ «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 г. № 239** [16]. В этом документе даются рекомендации по обеспечению безопасности значимых объектов на различных стадиях (этапах) их жизненного цикла:

а) установление требований к обеспечению безопасности значимого объекта;

б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;

в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввода его в действие;

г) обеспечение безопасности значимого объекта в ходе его эксплуатации;

д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Перечислен состав базового набора мер по обеспечению безопасности для значимых объектов КИИ различных категорий значимости.

Серия стандартов ГОСТ Р МЭК 62443 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» – издается в России начиная с 2015 г. в рамках политики гармонизации системы национальных стандартов и приведения ее в соответствие с международной системой стандартов в области обеспечения безопасности АСУ ТП. Последнее очень важно для унификации терминологии, понятийной базы и формирования согласованных подходов и взаимодополняющих технических решений в условиях резкого обострения проблемы кибер-безопасности АСУ ТП, проявляющегося в форме глобального нарастания интенсивности кибератак и тяжести их последствий.

В настоящее время в России переведены и приняты следующие стандарты серии 62443:

– ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Терминология, концептуальные положения и модели» (введен 01.01.2016);

– ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2) «Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики» (введен 01.01.2016);

– ГОСТ Р 56498 IEC 62443-3-3-2016 «Требования к системной безопасности и уровни безопасности» (введен 01.04.2017).

Ожидается продолжение выпуска данной серии по мере завершения работы над запланированными версиями стандартов ISA/IEC 62443. Очевидно, что в данном случае специалисты и организации, занимающиеся задачами проектирования, эксплуатации и аудита комплексных систем обеспечения безопасности АСУ ТП, получат в свое распоряжение мощный инструментарий для достижения поставленных перед ними целей. Вместе с тем, необходимо отметить, что «узким местом» указанных выше нормативных документов, регламентирующих вопросы обеспечения кибербезопасности АСУ ТП, является отсутствие формализованных методик детальной оценки рисков кибербезопасности. Как отмечается в ГОСТ Р 56205-2014 IEC/TS 62443-1-1, в настоящее время можно считать более или менее отработанными лишь методики ориентировочной (качественной) оценки рисков, применяемые для качественного сравнения уровней безопасности АСУ ТП. По мере увеличения объема статистических данных и разработки математических моделей риска, угроз и инцидентов безопасности, актуальной становится задача разработки методов и алгоритмов количественной оценки риска, обеспечивающих возможность обоснованного выбора устройств АСУ ТП и необходимых контрмер как в пределах отдельных зон безопасности, так и при обеспечении требуемого уровня кибербезопасности АСУ ТП в целом.

В качестве перспективного способа решения данной задачи можно указать активно ведущиеся в последние годы исследования, связанные с получением количественной оценки рисков (ущерба) на основе технологий интеллектуального анализа данных. Подобные исследования включают в себя такие направления, как:

а) разработку моделей и алгоритмов оценки рисков с использованием нечеткой логики и нейронных сетей [17-19];

б) разработку моделей и алгоритмов оценки рисков с использованием технологий когнитивного моделирования [20, 21];

в) разработку моделей и алгоритмов оценки рисков с использованием динамических байесовских сетей и скрытых марковских моделей [22, 23].

Заключение

Статистика последних лет показывает, что проблема обеспечения защищенности (кибербезопасности) АСУ ТП в условиях резкого нарастания числа и интенсивности кибератак, а также масштабов их последствий становится все более актуальной. Отсюда понятен интерес к разработке национальных и международных стандартов в области защиты АСУ ТП, устанавливающих требования к комплексным системам обеспечения безопасности критически важных объектов и рекомендации по выбору и реализации соответствующих мер защиты. Среди наиболее известных нормативных документов в области кибербезопасности АСУ ТП выделяют стандарты NIST SP 800-82, NERC CIP, ANSI/ISA-99, IEC 62443, а в нашей стране – Федеральный закон № 187-ФЗ, Приказы ФСТЭК России №№ 31 и 239, стандарты ГОСТ Р МЭК 62443. Отличительной чертой указанных документов является использование системного риск-ориентированного подхода к решению задач обеспечения безопасности АСУ ТП на всех этапах жизненного цикла. Особую роль при этом должно сыграть применение технологий интеллектуального анализа данных, позволяющих дать более точную количественную оценку рисков кибербезопасности и, как следствие, обеспечить более обоснованный выбор устройств АСУ ТП и необходимых контрмер для реализации стратегии многоуровневой эшелонированной защиты (defense in depth).

Литература

1. Ландшафт угроз для систем промышленной автоматизации, второе полугодие 2017 [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017 (дата обращения 26.07.2018).

2. Корольков С., Ярушевский Д. Обеспечение безопасности автоматизированных систем управления технологическими процессами/Пресс-Центр «ДиалогНаука» [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/141148 (дата обращения 26.07.2018).

3. Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226 (дата обращения 26.07.2018).

4. Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г. Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2–10.

5. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). – С. 22–27.

6. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибер-безопасности. 2014. № 5 (8). – С. 39–42.

7. Ватрушкин А. А. Правовые основы обеспечения кибер-безопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. № 6 (31).– С. 78–84.

8. Концепция стратегии кибербезопасности Российской Федерации (проект) [Электронный ресурс]. URL: http://www.council.gov.ru/media/files/41d4b3dfbd b25cea8a 73.pdf (дата обращения 26.07.2018).

9. Что такое кибербезопасность? [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (дата обращения 26.07.2018).

10. Обзор стандарта безопасности промышленных систем управления NIST SP 800-82 Rev. 2 [Электронный ресурс]. URL: https://www.ussc.ru/news/id/254 (дата обращения 26.07.2018).

11. Лукацкий А. Применимость стандартов NERC CIP в России / Безопасность инфраструктуры энергоснабжения [Электронный ресурс]. URL: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (дата обращения 26.07.2018).

12. Байрс Э. Использование стандартов ANSI/ISA-99 для обеспечения безопасности системы управления промышленным предприятием // Современные технологии автоматизации. 2014. № 1. – С. 6–15.

13. Ярушевский Д. Обеспечение безопасности АСУ ТП – краткий обзор семейства стандартов IEC 62443 // Information Security/Информационная безопасность. 2014. № 3 [Электронный ресурс]. URL: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443 (дата обращения 26.07.2018).

14. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды / Приказ ФСТЭК России от 14 марта 2014 г. № 31 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.07.2018).

15. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 26.07.2018).

16. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.07.2018).

17. Глушенко С. А., Долженко А. И. Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации // Информационные технологии, Т. 21, № 1, 2015. – С. 68-74.

18. Булдакова Т. И., Миков Д. А. Методика анализа информационных рисков с применением нейро-нечеткой сети // НТИ. Сер. 2. Информационные процессы и системы, № 4, 2015. – С. 13-17.

19. Кириллова А. Д., Васильев В. И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП // Проблемы информационной безопасности / Материалы VII Всеросс. Заочной Интернет-конференции, 20-21 февр. 2018 г. – Ростов-на-Дону: Изд-во ООО «Азов Принт», 2018. – С. 138-142.

20. Васильев В. И., Вульфин А. М., Кудрявцева Р. Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования // Доклады ТУСУР, Т. 20, № 4, г. Томск, 2017. – С. 61-66.

21. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии, Т. 24, № 10, 2018. – С. 657-664.

22. Арустамов С. А., Дайнеко В. Ю. Применение динамической байесовской сети в системах обнаружения вторжений // Научно-технический вестник информационных технологий, механики и оптики, № 3 (79), 2012. – С. 128-133.

23. Козачек А. В. Математическая модель системы распознавания разрушающих программных средств на основе скрытых марковских моделей // Вестник СибГУТИ, № 3, 2012. – С. 29-39.

References

1. Landshaft ugroz dlya sistem promyshlennoy avtomatizatsii, vtoroye polugodiye 2017 [Elektronnyy resurs]. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017 (data obrashcheniya 26.07.2018).

2. Korol'kov S., Yarushevskiy D. Obespecheniye bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami/Press-Tsentr «DialogNauka» [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/141148 (data obrashcheniya 26.07.2018).

3. Yarushevskiy D. Kiberbezopasnost' ASU TP – chto eto i zachem? [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/13226 (data obrashcheniya 26.07.2018).

4. Massel' L. V., Voropay N. I., Senderov S. M., Massel' A. G. Kiberbezopasnost' kak odna iz strategicheskikh ugroz energeticheskoy bezopasnosti Rossii // Voprosy kiberbezopasnosti. 2016. № 4 (17). – S. 2–10.

5. Bezkorovaynyy M. M., Tatuzov A. L. Kiberbezopasnost' – podkhody k opredeleniyu ponyatiya // Voprosy kiberbezopasnosti. 2014. № 1 (2). – S. 22–27.

6. Alpeyev A. S. Terminologiya bezopasnosti: kiberbezopasnost', informatsionnaya bezopasnost' // Voprosy kiber-bezopasnosti. 2014. № 5 (8). – S. 39–42.

7. Vatrushkin A. A. Pravovyye osnovy obespecheniya kiber-bezopasnosti kriticheskoy infrastruktury Rossiyskoy Federatsii // Yevraziyskaya advokatura. 2017. № 6 (31). – S. 78–84.

8. Kontseptsiya strategii kiberbezopasnosti Rossiyskoy Federatsii (proyekt) [Elektronnyy resurs]. URL: http://www.council.gov.ru/media/files/41d4b3dfbd b25cea8a 73.pdf (data obrashcheniya 26.07.2018).

9. Chto takoye kiberbezopasnost'? [Elektronnyy resurs]. URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (data obrashcheniya 26.07.2018).

10. Obzor standarta bezopasnosti promyshlennykh sistem upravleniya NIST SP 800-82 Rev. 2 [Elektronnyy resurs]. URL: https://www.ussc.ru/news/id/254 (data obrashcheniya 26.07.2018). 11. Lukatskiy A. Primenimost' standartov NERC CIP v Rossii / Bezopasnost' infrastruktury energosnabzheniya [Elektronnyy resurs]. URL: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (data obrashcheniya 26.07.2018).

12. Bayrs E. Ispol'zovaniye standartov ANSI/ISA-99 dlya obespecheniya bezopasnosti sistemy upravleniya promyshlennym predpriyatiyem // Sovremennyye tekhnologii avtomatizatsii. 2014. № 1. – S. 6–15.

13. Yarushevskiy D. Obespecheniye bezopasnosti ASU TP – kratkiy obzor semeystva standartov IEC 62443 // Information Security/Informatsionnaya bezopasnost'. 2014. № 3 [Elektronnyy resurs]. URL: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443 (data obrashcheniya 26.07.2018).

14. 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 takzhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i okruzhayushchey sredy / Prikaz FSTEK Rossii ot 14 marta 2014 g. № 31 [Elektronnyy resurs]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (data obrashcheniya 26.07.2018).

15. Federal'nyy zakon № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» ot 26.07.2017 [Elektronnyy resurs]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (data obrashcheniya 26.07.2018).

16. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii / Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 [Elektronnyy resurs]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (data obrashcheniya 26.07.2018).

17. Glushenko S. A., Dolzhenko A. I. Sistema podderzhki prinyatiya resheniy nechetkogo modelirovaniya riskov informatsionnoy bezopasnosti organizatsii // Informatsionnyye tekhnologii, T. 21, № 1, 2015. – S. 68-74.

18. Buldakova T. I., Mikov D. A. Metodika analiza informatsionnykh riskov s primeneniyem neyronechetkoy seti // NTI. Ser. 2. Informatsionnyye protsessy i sistemy, № 4, 2015. – S. 13-17.

19. Kirillova A. D., Vasil'yev V. I. Primeneniye nechetkoy neyronnoy seti dlya otsenki riskov informatsionnoy bezopasnosti ASU TP // Problemy informatsionnoy bezopasnosti / Materialy VII Vseross. Zaochnoy Internet-konferentsii, 20-21 fevr. 2018 g. – Rostov-na-Donu: Izd-vo OOO «Azov Print», 2018. – S. 138-142.

20. Vasil'yev V. I., Vul'fin A. M., Kudryavtseva R. T. Analiz i upravleniye riskami informatsionnoy bezopasnosti s ispol'zovaniyem tekhnologiy kognitivnogo modelirovaniya // Doklady TUSUR, T. 20, № 4, g. Tomsk, 2017. – S. 61-66.

21. Vasil'yev V. I., Vul'fin A. M., Guzairov M. B., Kirillova A. D. Interval'noye otsenivaniye informatsionnykh riskov s pomoshch'yu nechetkikh serykh kognitivnykh kart // Informatsionnyye tekhnologii, T. 24, № 10, 2018. – S. 657-664.

22. Arustamov S. A., Dayneko V. YU. Primeneniye dinamicheskoy bayyesovskoy seti v sistemakh obnaruzheniya vtorzheniy // Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki, № 3 (79), 2012. – S. 128-133.

23. Kozachek A. V. Matematicheskaya model' sistemy raspoznavaniya razrushayushchikh programmnykh sredstv na osnove skrytykh markovskikh modeley // Vestnik SibGUTI, № 3, 2012. – S. 29-39.

ВАСИЛЬЕВ Владимир Иванович, доктор технических наук, профессор кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vasilyev@ugatu.ac.ru.

КИРИЛЛОВА Анастасия Дмитриевна, магистр, программист кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kirillova.andm@gmail.com

КУХАРЕВ Сергей Николаевич, аспирант кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kuharev.sn@zaorczi.ru

VASILYEV Vladimir, Dr. Sc. (Eng.), Professor of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: vasilyev@ugatu.ac.ru.

KIRILLOVA Anastasiya, M. Sc., programmer of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kirillova.andm@gmail.com

KUKHAREV Sergey, post-graduate of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kuharev.sn@zaorczi.ru

УДК 004.056.5 Вестник УрФО № 4(30) / 2018, с. 75–82

Шабуров А. С., Двойнишников Н. Э., Шлыков А. И. DOI: 10.14529/secur180411

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье анализируется последовательность выполнения требований законодательства в области категорирования объектов критической информационной инфраструктуры. На основе рекомендаций сформированы алгоритмы, для каждого этапа выполнения требований. Данные алгоритмы позволяют систематизировать информацию, предоставленную в нормативноправовых актах, а также раскрывают особенности реализации установленных требований. Детально рассмотрены этапы формирования комиссии по категорированию, формирования перечня объектов критической информационной инфраструктуры, а также отдельные этапы категорирования объектов.

Ключевые слова: *критическая информационная инфраструктура, объект критической информационной инфраструктуры, категорирование объектов, защита информации, компьютерная атака.*

Shaburov A. S., Dvoinishnikov N. E., Shlykov A. I.

FEATURES OF THE IMPLEMENTATION OF THE REQUIREMENTS FOR THE CATEGORIZATION OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

The article analyzes the sequence of the requirements of the legislation. The article analyzes the sequence on the implementation of the requirements of legislation in the field of critical information infrastructure of the Russian Federation in terms of categorization of critical information infrastructure objects. Based on the recommendations, algorithms were formed, for each

stage of meeting the requirements separately. These algorithms allow you to systematize the information provided in regulatory legal acts, facilitates its assimilation, and also describes the subtleties of the implementation of the established requirements. The stages of the formation of a commission for categorization, the formation of a list of objects of critical information infrastructure, as well as the actual stage of categorization of objects are considered in detail.

Keywords: *critical information infrastructure, critical information infrastructure facility, categorization of objects, information security, computer attack.*

В современных условиях деятельность по обеспечению безопасности объектов критической информационной инфраструктуры приобретает особую актуальность. В 2018 г. вступил в силу закон «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – 187-ФЗ), открыв новый нормативно определенный перечень требований в сфере информационной безопасности.

В целом, отрасль критической информационной инфраструктуры Российской Федерации (далее – КИИ) концептуально направлена на сферы социально-экономической деятельности, отнесенные к приоритетам устойчивого социально-экономического развития Российской Федерации, а именно: повышение качества жизни российских граждан, экономический рост, наука, технологии, образование здравоохранение и культура, экология и рациональное природопользование[2].

На данный момент проблема реализации требований 187-ФЗ является наиболее широко обсуждаемой кругах специалистов по информационной безопасности в России. Причина столь пристального внимания к данной проблеме состоит, как в отсутствии практического опыта реализации нормативных требований, так и в недостаточной проработанности изданных нормативных документов. Примером может служить неоднозначность определения категории объекта КИИ, в соответствии с «Перечнем показателей критериев значимости объектов критической инфраструктуры Российской Федерации и их значений» [3]. Проблема заключается в том, что показатель 2 и 3 категории объекта КИИ не может быть определен корректно, исходя из определенных границ их значений (рис. 1).

Показатель	Значение показателя		
	III категория	II категория	I категория
9. Возникновение ущерба бюджетам Российской Федерации, оцениваемого:			
а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1

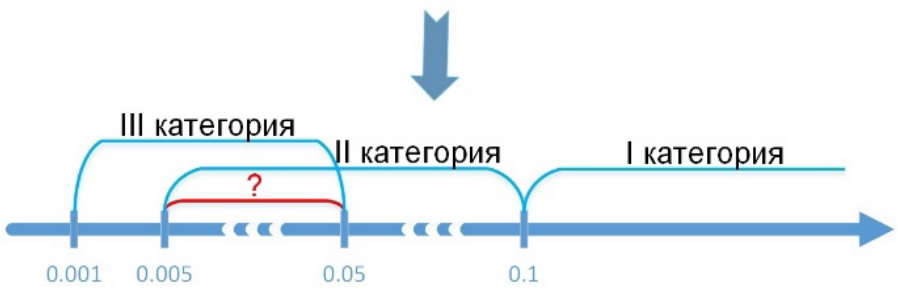

Рис. 1. Неоднозначность толкования категории объекта КИИ

В данной статье, рассматривается лишь часть требований по обеспечению безопасности КИИ, касающуюся категорирования объектов КИИ (далее - Категорирование). Подобный анализ направлен не только на облегчение понимания тонкостей реализации требований нормативных документов, но и на предотвращение ошибок, провоцируемых неоднозначностью толкования отдельных требований. Дальнейшую деятельность целесообразно представить в виде последовательности этапов.

Этап 1. Составление перечня объектов КИИ, подлежащих категорированию. Представляется целесообразным начать работу именно с данного этапа, вопреки поряд-

ку, предлагаемому в [3]. Это обосновано тем, что в комиссию по категорированию (далее - Комиссия) следует включать исключительно тех специалистов, которые в высшей степени осведомлены в особенностях работы объектов КИИ, непосредственно связаны с созданием или обслуживанием объектов КИИ. В противном случае этап категорирования объектов КИИ может сильно затянуться. Практика показывает, что безошибочно определить состав комиссии по категорированию практически невозможно.

В целях исключения возможных ошибок в работе Комиссии по категорированию КИИ, в состав комиссии целесообразно включить уполномоченного в вопросах, касающихся IT-инфраструктуры Организации (чаще всего это главный системный администратор или начальник IT-отдела). Председателя Комиссии необходимо уполномочить в формировании состава Комиссии, а сотрудников организации – в безотлагательной консультативной помощи председателю Комиссии. Формировать Комиссию следует исключительно в процессе составления перечня объектов КИИ, подлежащих категорированию (далее – Перечень объектов), в целях безошибочного определения уровня осведомленности сотрудников.

Чтобы понять процесс составления Перечня объектов КИИ более детально, рассмотрим несколько наиболее характерных вариантов подобных ситуаций:

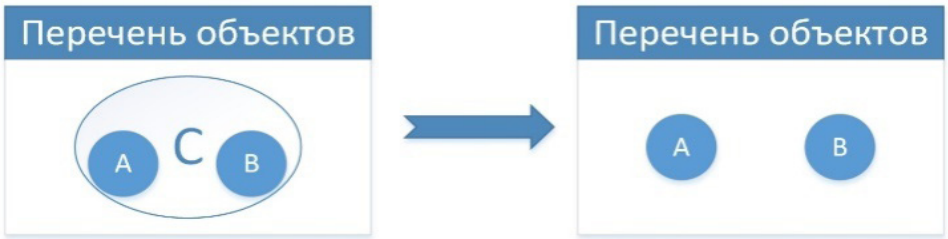

Рис. 2. Сегментирование объектов КИИ

Вариант 1: субъекту КИИ (далее – Организация) характерна высокая степень интеграции вычислительных систем, сетей и средств автоматизации. В данном случае количество объектов КИИ крайне велико, что может спровоцировать ошибки при их перечислении и оставлении Перечня объектов.

Составление Перечня объектов начинается с составления перечня всех процессов, производимых организацией. Для составления данного перечня необходимо обратиться к ОКВЭД, ЕГРЮЛ и уставу организации, лицензиям, которыми обладает организация, а также всем направлениям видов деятельности организации, перечисленных в уставе. После данной процедуры из Перечня исключаются все повторяющиеся процессы.

После составления перечня всех процессов, производимых организацией, выделяются процессы, которые являются критическими. Основное свойство критического процесса заключается в необходимости его выполнения и определяется исходя из последствий его нарушения.

Завершающим шагом на данном этапе является определение процессов, реализуемых за счет информационных систем, информационно-телекоммуникационных сетей и (или) автоматизированных систем управления, принадлежащих Организации. Данные объекты КИИ следует включить в Перечень объектов.

Вариант 2: Организации не характерна высокая степень интеграции вычислительных систем, сетей и средств автоматизации, т. е. количество объектов КИИ не велико.

В данном случае совокупное количество объектов КИИ не должно превышать 10 шт. Тогда можно с легкостью определить, какой объект КИИ отвечает за критический процесс и внести его в Перечень объектов.

Составляя Перечень объектов, стоит учитывать, что распределенный объект КИИ возможно сегментировать (рис. 2). Таким образом, распределенный объект КИИ **C**, включающий в свой состав объекты **A** и **B**, может быть сегментирован на объекты КИИ **A** и **B**, в случае чего в Перечень объектов будут вписаны только объекты **A** и **B**. Для этого должны выполняться следующие требования:

1. Объект **A** должен быть обособлен программноаппаратно, и, при исключении из объекта **C** этой части, функционирование объекта **B** будет продолжаться планомерно. Иначе говоря, выделяемый объект КИИ должен функционировать автономно.

2. Критические процессы, обеспечивае-

мые выделяемым объектом **А**, не взаимосвязаны с критическими процессами, обеспечиваемыми объектом **В**.

Обобщенный алгоритм формирования состава Перечня объектов КИИ представлен на рис. 3

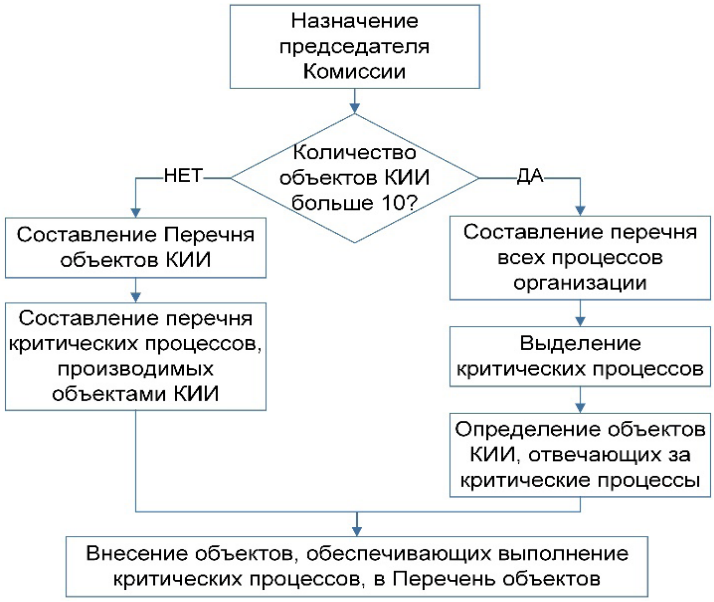

Рис. 3. Алгоритм формирования состава Перечня объектов КИИ

Этап 2. Формирование комиссии по категорированию и заполнение формы перечня объектов КИИ, подлежащих категорированию. По итогу формирования Перечня объектов у председателя Комиссии формируется представление о необходимом составе Комиссии. Ограничения по количественному составу сотрудников, составляющих Комиссию, нет. В то же время, следует минимизировать их количество, с точки зрения экономии временных и человеческих ресурсов. Состав Комиссии формируется исходя из компетентности ее членов в вопросах основных функций и состава программно-аппаратных устройств объектов КИИ, подлежащих категорированию, а также на основании эксплуатационной документации объекта КИИ (приказа на ввод в эксплуатацию, технического задания на разработку и др.).

Рис. 4. Алгоритм формирования Перечня объектов КИИ

В состав Комиссии запрещено включать сотрудников, не связанных с обеспечением безопасности организации, а также не связанных с осуществлением видов деятельности в области информационных технологий. Исключением является руководитель Организации.

В случае, если Организация является подведомственной, то решение включить в состав Комиссии представителя головной организации, уполномоченного в согласовании Перечня объектов с подведомственными организациями, позволит избавиться от необходимости согласовывать Перечень объектов КИИ, что может потребовать дополнительного времени.

Результатом выполнения первых двух этапов по составлению Перечня объектов и работы Комиссии, является формирование информации по составу объектов КИИ [4]. Целесообразно представить ее в табличном варианте (рис.5).

№ п/п	Наименование объекта	Тип объекта	Сфера деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество представителя, его телефон, адрес электронной почты

Рис. 5. Форма представления информации по составу КИИ

Этап 3. Категорирование объектов КИИ. Данный этап гораздо более объемный и трудоемкий по сравнению с этапом составления Перечня. В соответствии с требованиями законодательства на Категорирование отводится один год с момента утверждения Перечня объектов. Результатом его выполнения является Акт категорирования объектов КИИ (далее – Акт категорирования), подписанный членами Комиссии и утвержденный руководителем, и заполненная форма [5].

В Акте категорирования должны содержаться следующие сведения:

1. Сведения об объекте КИИ.

2. Результаты анализа угроз безопасности информации объекта КИИ.

3. Реализованные меры по обеспечению безопасности объекта КИИ.

4. Сведения о присвоенной объекту КИИ категории значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

5. Сведения о необходимых мерах по обеспечению безопасности [6].

Акт категорирования не имеет стандартной формы, хранится как документ внутреннего пользования и может запрашиваться регулятором во время проверки. Акт категорирования объектов КИИ утверждается руководителем Организации.

Форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости должна быть утверждена руководителем Организации и отправлена в управление ФСТЭК России в течение десяти дней с момента утверждения Акта категорирования. Данная форма нацелена на комплексное описание объекта КИИ и должна содержать:

1. Сведения об объекте КИИ.

2. Сведения о субъекте КИИ.

3. Сведения о взаимодействии объекта КИИ и сетей электросвязи.

4. Сведения о лице, эксплуатирующем объект КИИ.

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ.

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ.

7. Возможные последствия в случае возникновения компьютерных инцидентов.

8. Категория значимости, которая присвоена объекту КИИ.

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ.

При этом, наиболее существенными для обеспечения информационной безопасности КИИ являются п. 6-9 [7].

Пункт 6 требует формирования модели угроз безопасности информации и модели нарушителя в отношении рассматриваемого объекта КИИ. При их формировании нужно руководствоваться такими документами, как «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» и «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры».

Пункт 7 требует рассмотрения и анализа всех возможных негативных социальных, политических, экономических, экологических последствий и последствий для обороны страны, к которым привело прекращение выполнения критического процесса, за обеспечение которого отвечает рассматриваемый объект КИИ. Для этого требуется проанализировать все показатели критериев значимости объектов КИИ и их значений, к которым приведет прекращение и(или) нарушение работы рассматриваемого объекта КИИ.

Качественная оценка, в первую очередь необходимо:

– проанализировать уязвимости объектов КИИ и характерных инцидентов, связанных с последствиями компьютерных атак на компоненты объектов КИИ;

– рассмотреть потенциальные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации. Если таковые действия невозможны, то это необходимо обосновать;

– провести оценку угроз безопасности информации, в соответствии с перечнем показателей критериев значимости тяжестью возможных последствий, в случае возникновения компьютерных инцидентов на объектах КИИ.

Пункт 8 требует расчета значений тех показателей критериев значимости, которые были выбраны ранее. Расчет производится из соображений о том, что наступили худшие обстоятельства из всех возможных, но в рамках разумного. Иначе говоря, следует найти такую конфигурацию происходящих/не происходящих критических процессов, при которой последствия будут максимально пагубными. При этом, унифицированного метода расчета не предлагается. Руководствоваться при расчете необходимо логикой и здравым смыслом, а значения показателей критериев значимости объекта КИИ напрямую определяют категорию его значимости.

Сначала категория значимости определяется в соответствии с каждым полученным значением показателя критерия значимости в отдельности. Затем из всех полученных критериев выбирается самое высокое значение категории значимости объекта КИИ. Если объект не является значимым (ни одно из значений показателей критериев значимости не достигло даже показателя третьей категории значимости), то категория ему не присваивается.

Пункт 9 требует перечислить все реализованные меры, направленные на обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой категорируемым объектом КИИ. С целью экономии времени будет гораздо более выгодным решением сначала заполнить форму из [5], после чего просто включить сведения из нее в Акт категорирования.

Таким образом, реализация требований по категорированию объектов КИИ и последующая их защита является сложным процессом, включающим комплекс различных задач, требующим итерационного подхода и коллегиальности в принятии решений на каждом из этапов. Пути решения наиболее часто возникающих вопросов являются универсальными, с одной стороны, с другой, - требуют учета характерных особенностей объекта критической инфраструктуры. Качественная реализация требований по категорированию объектов КИИ является основой для обеспечения их информационной безопасности в условиях актуальных угроз безопасности информации.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26.07.2017. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ № 683 от 31.12.2015. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

3. Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ № 127 от 08.02.2018. [Электронный ресурс]: Доступ из справ.правовой системы «КонсультантПлюс».

4. О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации: Информационное сообщение № 240/22/2339 от 04.05.2018. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: Приказ ФСТЭК России № 236 от 22.12.2017. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России № 239 от 25.12.2017 (ред. от 09.08.2018). [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

7. Борисов С.В. КИИ. Категорирование объектов, часть 1 // SecurityLab.ru: [электронный ресурс] URL: https://www.securitylab.ru/blog/personal/sborisov/344035.php (дата обращения: 24 октября 2018г.).

References

1. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon № 187-FZ ot 26.07.2017. [The law of the Russian Federation # 187-FL from 26.07.2017 "On the Security of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed 2 July 2018)

2. O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii: Ukaz Prezidenta Rossiyskoy Federatsii № 683 ot 31.12.2015. [Presidential Decree # 683 from 31.12.2015 "On the National Security Strategy of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_191669/ (accessed 17 July 2018).

3. Ob utverzhdenii pravil kategorirovaniya ob'yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley pokazateley znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy: Postanovleniye Pravitel'stva Rossiyskoy Federatsii № 127 ot 08.02.2018 [Resolution of the Government of the Russian Federation # 127 from 08.02.2018 "On the approval of the rules for categorizing the objects of the critical information infrastructure of the Russian Federation, as well as the list of indicators of the significance indicators of the objects of the critical information infrastructure of the Russian Federation and their values"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_290595/6fd5c84bc2921316798d46fcf3d736b5f223b3c3/ (accessed 2 July 2018).

4. O metodicheskikh dokumentakh po voprosam obespecheniya bezopasnosti informatsii v klyuchevykh sistemakh informatsionnoy infrastruktury Rossiyskoy Federatsii: Informatsionnoye soobshcheniye № 240/22/2339 ot 04.05.2018. [FSTEC Information Communication # 240/22/2339 from 04.05.2018 "On methodological documents on ensuring information security in key information infrastructure systems of the Russian Federation"]. Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie-fstek-rossii-ot-4-maya-2018-g-n-240-22-2339 (accessed 13 July 2018).

5. Ob utverzhdenii formy napravleniya svedeniy o rezul'tatakh prisvoyeniya ob"yektu kriticheskoy informatsionnoy infrastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobkhodimosti prisvoyeniya yemu odnoy iz takikh kategoriy: Prikaz FSTEK Rossii № 236 ot 22.12.2017. [FSTEC Order # 236 from 22.12.2017 "On the approval of the form for sending information on the results of assigning a critical information infrastructure to an object of one of the significance categories or about the absence of the need to assign one of such categories to the object"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_295855/c2b49c620b4a6d35245ddbc52c2bb621252443cb/ (accessed 13 July 2018).

6. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz FSTEK Rossii № 239 ot 25.12.2017. [FSTEC Order # 239 from 25.12.2017 "On the Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_294287/ (accessed at 27 June 2018).

7. Borisov S.V. KII. Kategorirovaniye obyektov, chast 1 [Borisov S.V. KII. Categorization of objects, part 1]. Available at: https://www.securitylab.ru/blog/personal/sborisov/344035.php (accessed at 24 October 2018).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики. Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: shans@at.pstu.ru

ДВОЙНИШНИКОВ Николай Эдуардович, студент кафедры автоматики и телемеханики Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: rerfrerf00@gmail.com

ШЛЫКОВ Алексей Игоревич, студент кафедры автоматики и телемеханики Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: thekingofthedas@gmail.com

SHABUROV Andrey, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. Email: shans@at.pstu.ru

DVOINISHNIKOV Nikolai, student of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: rerfrerf00@gmail.com

SHLYKOV Alexey, student of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: thekingofthedas@gmail.com

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.**

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.

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

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 № 4(30) / 2018

Дата выхода в свет 28.12.2018. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 7,35. Тираж 100 экз. Заказ 4/9.
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. 4(30) / 2018

Date of publication of the 28.12.2018. Format 70×108 1/16. Screen printing.
Conventional printed sheet 7,35. Circulation – 100 issues. Order 4/9. Open price.

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