ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(25) / 2017

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

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА

ЧУВАРДИН О. П., руководитель Управления ФСТЭК России по УрФО

РЕДАКЦИОННЫЙ СОВЕТ:

БАРАНКОВА И. И.,
д. т. н., профессор, зав. каф. информатики и информационной безопасности МГТУ им. Г. И. Носова (г. Магнитогорск);

ГАЙДАМАКИН Н. А.,
д. т. н., профессор, начальник Института ФСБ России (г. Екатеринбург);

ДИК Д. И.,
к. т. н., доцент кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета (г. Курган);

ЗАХАРОВ А. А.,
д. т. н., профессор, зав. кафедрой информационной безопасности ТюмГУ (г. Тюмень);

ЗЫРЯНОВА Т. Ю.,
к. т. н., доцент, зав. кафедрой информационных технологий и защиты информации УрГУПС (г. Екатеринбург);

ЗЮЛЯРКИНА Н. Д.,
д. ф.-м. н., профессор кафедры защиты информации ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск);

МЕЛЬНИКОВ А. В.,
д. т. н., профессор, директор Югорского научно-исследовательского института информационных технологий (г. Ханты-Мансийск);

СОКОЛОВ А. Н.
(зам. отв. редактора), к. т. н., доцент, зав. кафедрой защиты информации ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск);

ТРЯСКИН Е. А.,
начальник специального управления ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ХОРЕВ А. А.,
д. т. н., профессор, зав. кафедрой информационной безопасности НИУ МИЭТ (г. Москва, г. Зеленоград);

АСЛАНОВ Р. М.,
к.ю.н., преподаватель кафедры конституционного права БГУ, Азербайджанская Республика (г. Баку);

ЕФРЕМОВ А. А.,
к. ю. н., доцент, в. н. с. (ЦТГУ) ИПЭИ РАНХиГС, доцент кафедры международного и европейского права ФГБОУ ВО «ВГУ» (г. Воронеж);

КИРЕЕВ В. В.,
д.ю.н., доцент, директор Института права ФГБОУ ВО «ЧелГУ» (г. Челябинск);

КУЗНЕЦОВ П. У.,
д. ю. н., профессор, зав. каф. информационного права УрГЮУ (г. Екатеринбург);

ЛЕБЕДЕВ В. А.,
д. ю. н., профессор, профессор кафедры конституционного и муниципального права МГЮА (Университет им. О. Е. Кутафина) (г. Москва);

МЕЛИКОВ У. А.,
к. ю. н., нач. отдела гражданского, семейного и предпринимательского законодательства Национального центра законодательства при Президенте Республики Таджикистан (г. Душанбе);

МИНБАЛЕЕВ А. В.
(зам. отв. редактора), д. ю. н., профессор кафедры теории государства и права, конституционного и административного права, зам. директора юридического института ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск);

ПОЛЯКОВА Т. А.,
д. ю. н., профессор, зав. сектором информационного права ИГП РАН (г. Москва)

16+

ISSN 2225-5435

UrFR Newslette
INFORMATION SECURITY
№ 3(25) / 2017

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., director of the Office of Russian FSTEC UFD

EDITORIAL COUNCIL:

BARANKOVA I. I.,
Doctor of Technical Sciences, Professor, Head. cafes. Informatics and Information Security Bauman (Magnitogorsk);

GAYDAMAKIN N. A.,
Doctor of Technical Sciences, Professor, Head. of the Institute of Advanced Training of employees of FSB of Russia (Ekaterinburg);

DIK D. I.,
to. Sci. Sciences, Head of the Department. BliAS KSU (Kurgan);

ZAHAROV A. A.,
., Doctor of Technical Sciences, Prof., Head. cafes. Information Security TSU (Tyumen);

ZYRYANOVA T. Y.,
Cand, associate professor, Head. of Department «Information Technology and Information Security» of the Ural State University of Railway Transport (Ekaterinburg);

ZYULYARKINA N. D.,
professor of department «Security of information systems» South Ural State University, (Chelyabinsk);

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

SOKOLOV A. N.,
a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", (Chelyabinsk);

TRYASKIN E. A.,
head of the special control SUSU (Chelyabinsk)

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

ASLANOV R. M.,
candidate of jurisprudence, lecturer constitutional law of BSU,The Republic of Azerbaijan (Baku city);

YEFREMOV A. A.,
Candidate of Law, Associate Professor, Senior Researcher of the Center for Public Administration Technologies in RANEPA Institute of Applied Economic Research, (Voronezh);

KIREEV V. V.,
Doctor of Law, Associate Professor, Director Institute of Law FGBOU VO Chelyabinsk State University (Chelyabinsk);

KUZNETSOV P. W.,
Doctor of Law, Professor, Head of Information Law department Ural State Law Universit (Ekaterinburg);

LEBEDEV V. A.,
Doctor of Legal Science, Professor, Honored Scientist of Russian Federation, Honored Lawyer of Russian Federation, Professor of Constitutional and Municipal Law Department of Moscow State Law Academy named after O. E. Kutafin (Moscow);

MELIKOV W. A.,
to. Th. n., beginning. department of civil, family and business law of the National Centre for Legislation under the President of the Republic of Tajikistan (Dushanbe);

MINBALEEV A. V.
Doctor of Law, Professor department of Theory of state and law, constitutional and administrative law of the South Ural State University (national research university) (Chelyabinsk);

POLYAKOVA T. A.,
Doctor of Law, Professor, head of the information law sector IGP RAS (Moscow)

В НОМЕРЕ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

ШАБУРОВ А. С., ЖУРИЛОВА Е. Е.
Об особенностях интеграции DLP-решений в корпоративные информационные системы 5

БУХАРЕВ Д. А., ВАГИН С. В., СОКОЛОВ А.Н.
Обнаружение вредоносного мобильного кода на основе эвристического анализа PDF-файлов 12

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АСЯЕВ Г. Д., РАГОЗИН А. Н.
Определение минимального набора входных данных для корректной аутентификации по клавиатурному почерку с использованием нейронной сети 19

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

ЗАХАРОВ А. А., РИМША А. С., ХАРЧЕНКО А. М., ЗУЛЬКАРНЕЕВ И. Р.
Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия 24

БАРИНОВ А.Е., СКУРЛАЕВ С.В., СОКОЛОВ А.Н.
Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами 34

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

МИНБАЛЕЕВ А. В.
Развитие правового регулирования информационного общества в России: стратегия и основные направления совершенствования законодательства 43

МЕЛИКОВ У. А.
Правовые аспекты рекламы в интернете 50

ПРАКТИЧЕСКИЙ АСПЕКТ

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ 56

ОБРАЗЕЦ ЭКСПЕРТНОГО ЗАКЛЮЧЕНИЯ 59

COMPUTER SECURITY

SHABUROV A. S., ZHURILOVA E. E.
About features of integration DLP-solutions in corporate information systems 5

BUKHAREV D. A., VAGIN S.V., SOKOLOV A.N.
Detection of malicious mobile code based on heuristic analysis of PDF files 12

MATHEMATICAL METHODS IN INFORMATION SECURITY

ASYAEV G. D., RAGOZIN A. N.
Determination of the minimum set of input data for correct key-based authentication using a neural network 19

ACTUAL PROBLEMS OF CYBERSECURITY

ZAKHAROV A. A., RIMSHA A. S., KHARCHENKO A. M., ZULKARNEEV I. R.
Analysis of Information Security of Automated Control Systems for Technical Processes of a Gas Producing Enterprise 24

BARINOV A.E., SKURLAEV S.V., SOKOLOV A.N.
Method for risk assessment caused by vulnerabilities in ICS software 34

LEGAL REGULATION OF INFORMATION SECURITY

MINBALEEV A. V.
The development of the legal regulation of the information society in Russia: the strategy and the main directions for improving legislation 43

MELIKOV U. A.
Legal aspects of advertising on the internet 50

THE PRACTICAL ASPECT

REQUIREMENTS TO THE ARTICLESTO BE PUBLISHED IN MAGAZINE 56

SAMPLE OF THE EXPERT OPINION 59

УДК 004.056.5 Вестник УрФО № 3(25) / 2017, с. 5–11

Шабуров А. С., Журилова Е. Е.

ОБ ОСОБЕННОСТЯХ ИНТЕГРАЦИИ DLP-РЕШЕНИЙ В КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

В статье рассматриваются проблемы внедрения комплексных систем защиты информации, обусловленные интеграцией различных подсистем безопасности. Анализируется опыт внедрения и эффективность DLP-решений. Приводится модель реализации вариантов решений по внедрению СЗИ. Ставится задача выбора конкретного решения на основе особенностей информационных систем. Приводятся требования, предъявляемые к данным системам, на основе принципов их организации. Сопоставляются особенности корпоративных систем и функциональные возможности DLP-решений. Представлена типовая модель взаимодействия подсистем защиты информации в корпоративной информационной системе. Приводятся аналитические выражения для оценки эффективности внедрения DLP - решений в корпоративные информационные системы.

Ключевые слова: *система защиты информации, DLP-система, синергичность, канал утечки информации, безопасность корпоративных систем, эффективность защиты информации.*

Shaburov A. S., Zhurilova E. E.

ABOUT FEATURES OF INTEGRATION DLP-SOLUTIONS IN CORPORATE INFORMATION SYSTEMS

In this article consider the problems of implementing complex information security systems, due to the integration of various security subsystems. It is analyzed the experience of implementation and efficiency of DLP-solutions. Also, it's given a model of realizing solutions for implementing in ISS. The task is to choose a specific solution based on characteristics of information systems. The requirements for these systems are presented on the basis of the principles of their organization. The features of corporate systems and the functionality of DLP solutions are compared. It is presented a typical model of interaction of information protection subsystems in the corporate information system. Also, there are presented the analytical expressions for evaluat-

ing the effectiveness of implementing DLP-solutions in corporate information systems.

Keywords: *information security system, DLP-system, synergism, data leak channel, security of corporate systems, efficiency of information security.*

В условиях совершенствования информационных технологий, внедрения перспективных проектов, обеспечивающих переход на цифровую экономику, приобретает особое значение проблема информационной безопасности корпоративных систем (КС). Современное обеспечение безопасности информации основано на внедрении эффективных комплексных системных решений. Как правило, комплексная система защиты информации представляет собой множество разнородных компонентов взаимосвязанных и взаимодействующих между собой, обладающих свойствами целостности, синергичности и иерархичности. Это не противоречит традиционному толкованию термина «система защиты информации» (СЗИ), которое предполагает комплексное внедрение совокупности органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованной и функционирующей по правилам и нормам, установленным соответствующими документами в области защиты информации[1]. С другой стороны, традиционное понимание системы защиты не должно противоречить современным инновационным решениям в области обеспечения информационной безопасности, во многом зависящим от интеграции в архитектуру конкретной информационной системы.

Как правило, произвольная информационная система включает множество подсистем, в том числе и СЗИ, в свою очередь, также детализируемую на множество интегрированных и взаимосвязанных компонентов. Традиционно, комплексное функционирование СЗИ обеспечивается подсистемами технических средств охраны (ТСО) управления доступом, антивирусной защиты, криптографической защиты информации и рядом других подсистем. В последние годы также получили распространение SIEM-системы, DLP-системы, а так же аналогичные, достаточно дорогостоящие, но эффективные инструменты защиты. Подобное совершенствование систем безопасности, в первую очередь, ориентировано на противодействие актуальным угрозам безопасности информации, связанным, как с кибернетическими атаками, так и с утечкой информации ограниченного доступа из КС.

Опыт внедрения систем предотвращения утечек информации, основанных на DLP-решениях, демонстрирует их достаточную высокую эффективность. В то же время, внедрение подобных систем в корпоративных сетях, без интеграции с другими подсистемами системы защиты информации, не является панацеей[2].

В первое время, после появления DLP-систем на рынке средств защиты информации, по мнению некоторых специалистов, предполагалось, что такие системы смогут решить все проблемы утечек информации по техническим каналам связи. Практическое же использование доказало, что это не всегда так. Согласно статистике, в первое время DLP-системы внедрялись по принципу «от конца к началу», т.е. сначала осуществлялось внедрение, а потом выявлялись каналы утечки информации, недостатки политики информационной безопасности. Прежде всего, эти недостатки проявлялись в отсутствии четкого разделения корпоративных данных на открытые данные и данные ограниченного доступа[3]. Такой способ внедрения DLP-системы, как правило, был длительным, поскольку приходилось начинать с исследования уязвимостей информационных систем и построения системы информационной безопасности с самого начала. Кроме того, возникало значительное количество проблем внедрения DLP-систем, прежде всего, заключающихся в необходимости комплексного объединения множества компонентов, на основе DLP-решения. Настройка же правильного взаимодействий внутри СЗИ между средствами и подсистемами защиты позволила бы обеспечить эффект синергичности, а так же обойтись оптимальным набором средств, для достижения требуемого уровня защищенности информации.

КС предприятий и организаций имеют свои отличительные особенности, требования к внедрению, правила внедрения и область действия. Кроме того, особенности КС проявляются в преимуществах и недостатках, влияющих на эффект от внедрения того или иного решения, специальных требований по доступности информации, необходимой для обеспечения бизнес-процессов.

Согласно проведенным исследованиям,

эффективность работы DLP-решений проявляется лучше в системах с количеством сотрудников свыше пяти тысяч человек, поэтому рассмотрение комплексного подхода к внедрению предполагается на примере подобной КС.

Опыт внедрения DLP-решений, с учетом особенностей информационных систем, как правило, позволяет получить максимальный эффект от реализации функций защиты, при оптимальном количестве, используемых программных продуктов. С другой стороны, подобные особенности и обуславливают основные проблемы интеграции DLP-решений в корпоративной сети.

Рассмотрим модель ситуации, когда предполагается внедрение трех программных продуктов A, B, C (рис. 1) для обеспечения информационной безопасности КС. Конкретная система предполагает существование ранжированного перечня угроз безопасности информации. При этом, результат внедрения может быть оценен по различным критериям.

Решение «А» обеспечивает защиту от угроз с максимальным и средним риском, но перекрывает не весь список угроз. Решение «В» обеспечивает защиту от угроз с максимальным риском, но является дорогостоящим. Решение «С» обеспечивает защиту от угроз со средним и минимальным риском.

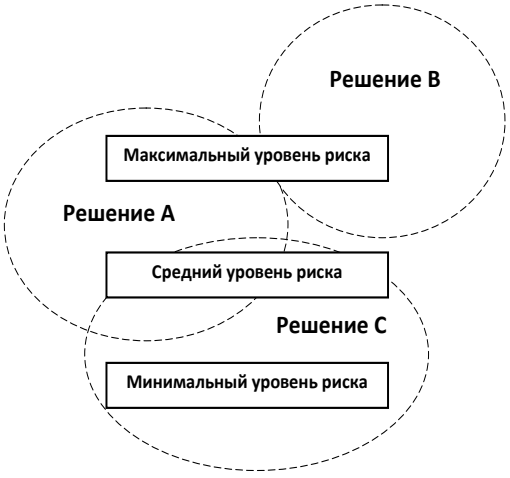

Рис. 1. – Модель реализации вариантов решений по внедрению СЗИ

Даная модель предполагает, что различные комбинации перечисленных средств защиты информации предотвращают различный набор угроз безопасности информации. В данном случае возникает задача выбора такого набора решений, что бы была обеспечена требуемая эффективность при оптимальных затратах. При этом, учет особенностей системы, в которую будет проводиться внедрение, является ключевым фактором, поскольку помогает осуществить корректный выбор.

Основной особенностью КС является строгая организованность административной и производственной деятельности, что порождает территориальную и функциональную распределенность подразделений, большие объемы обрабатываемых данных, высокий уровень регламентации событий в системе[4].

В общем случае корпоративные системы строятся на 6 базовых принципах:

1) системности;
2) совместимости;
3) эффективности;
4) открытости;
5) унификации;
6) единого руководства.

Базовые принципы построения КС порождают требования к системам защиты, внедряемым в такие системы, к основным из которых относятся:

1. Интегрируемости (изменение показателей бизнес-процессов одной части системы должно повлечь за собой изменение связанных с ними характеристик).

2. Автоматизации процессов.

3. Обеспечения дружественного интерфейса по отношению к пользователю, с учетом не предоставлять возможности выполнять больше разрешенного.

4. Логирование (возможность контроля действий пользователей в определенные моменты времени).

В общем случае корпоративная система состоит из следующих компонентов[5]:

1. Ядра системы, содержащего полный набор функциональных модулей для автоматизации задач управления.

2. Автоматизированной системы электронного документооборота.

3. Системы обработки информации.

4. Системы информационной безопасности.

5. Средств и систем обеспечения взаимодействия с пользователем .

6. Сети, локальной и/или внешней.

7. Офисных программных решений.

8. Систем специального назначения, для реализации функций предприятия.

Исходя из выделенных особенностей корпоративных систем, можно провести ана-

лиз и выяснить, по каким причинам внедрение только DLP-решений не может обеспечить качественную защиту информации от утечек.

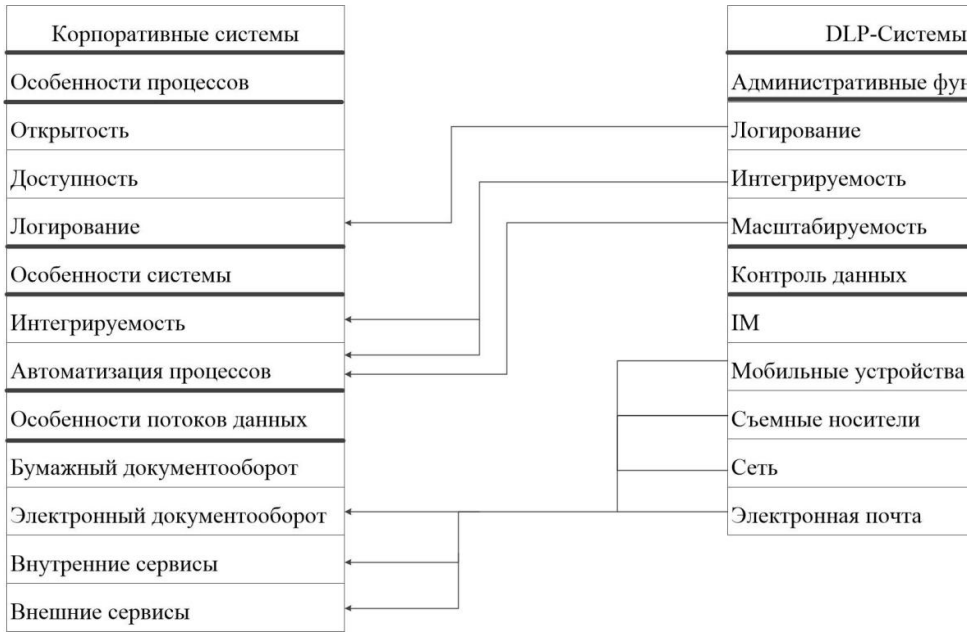

Рис. 2. – Сопоставление особенностей КС и возможностей DLP-решений

На рис. 2 отображены взаимозависимости функций DLP систем и КС, позволяющие сформировать подмножества реализуемых функций. При этом, очевидно, что нереализованные функции по ЗИ должны быть обеспечены иным подмножеством компонентов СЗИ.

Данные предположения обосновывают вывод о необходимости нахождения сбалансированной и эффективной архитектуры КС на основе внедрения комплексной системы защиты. Традиционно, данная система должна включать в себя средства и системы контроля и управления доступом, межсетевого экранирования, средств резервного копирования, средства предотвращения вирусных атак, и ряд других. С другой стороны, возможна интеграция требуемого решения непосредственно в систему защиты информации. При этом, блокирование выявленных каналов утечки, не должно существенно затруднить работу пользователей и не спровоцировать новые возможности для реализации угроз безопасности информации.

Особенности же интеграции DLP-систем в КС, как правило, связаны с возникновением проблемы доступности информационных ресурсов. Внедрение всех необходимых средств защиты информации существенно затрудняет работу сотрудников организации, может повлечь за собой нарушение бизнес-процессов. Кроме того, возможны значительные расходы, связанные со стоимостью внедрения и эксплуатации оборудования для построения подобной системы защиты. Нахождение оптимальных вариантов архитектуры СЗИ, с учетом взаимодействия ее компонентов, предполагает разработку набора модельных представлений.

На рисунке 3 представлена модель взаимодействия подсистем защиты информации в информационной системе КС[6]. Модель сгенерирована для корпоративной организации с количеством сотрудников более 5 000 человек, поскольку при меньших объемах внедрение некоторых подсистем является нерациональным.

В данном случае система защиты представлена совокупностью подсистем СКУД, видеонаблюдения, DLP и SIEM, и межсетевых экранов. Поскольку SIEM системы предназначены для анализа событий, как в реальном времени, так и архивированных, то данные со всех подсистем передаются именно на входы SIEM-систем. Система осуществляет анализ данных на соответствие заданным критериям безопасности, доводит результаты анализа администратору безопасности[7,8]. В частных случаях предполагаются совмещения некоторых функций администрирования системы и

ее безопасности, однако в крупных корпоративных системах, на которые ориентирована рассматриваемая модель, данные функции разделены.

процентном соотношении предполагается на основе зависимостей:

$$E = \xi_n + \xi_v + \xi_s \text{ , где} \quad (1)$$

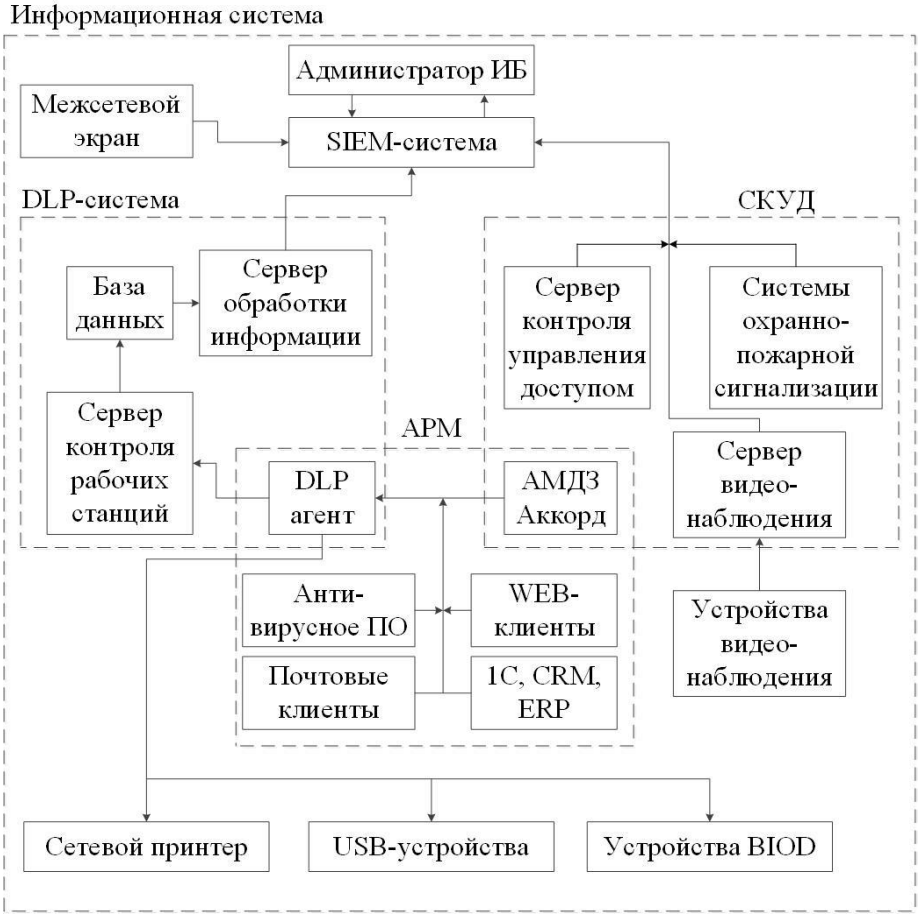

Рис. 3. – Схема взаимодействий подсистем внутри системы защиты информации в КС

Предполагается, что представленный на схеме набор подсистем перекрывает все возможные каналы утечки информации, в том числе и те каналы, которые не выявляются посредством DLP-решения. Например, согласно исследованиям, вероятность реализации технических каналов утечки не исключает возможности утечки традиционных документов и утраты оборудования[8]. То есть, подобные угрозы должны быть ликвидированы за счет других, традиционных решений, например, системы контроля и управления доступом и видеонаблюдения.

Поиск оптимальной архитектуры СЗИ, основанной на внедрении DLP-решения, включает необходимую оценку их эффективности, с точки зрения нахождения требуемых решений по защите информации. Оценить эффективность E, для представленной модели в

$$\xi_n = \left(\frac{(k-x)\cdot \boldsymbol{s} + p\cdot \boldsymbol{s}}{\boldsymbol{s}\cdot y^2} \right) \cdot n \cdot 100\% \quad (2)$$

$$\xi_v = \left(\frac{(k-x)\cdot \boldsymbol{s} + p\cdot \boldsymbol{s}}{\boldsymbol{s}\cdot y^2} \right) \cdot v \cdot 100\% \quad (3)$$

$$\xi_s = \left(\frac{(k-x)\cdot \boldsymbol{s} + p\cdot \boldsymbol{s}}{\boldsymbol{s}\cdot y^2} \right) \cdot s \cdot 100\% \quad (4)$$

Формулы 2,3,4 определяют эффективность данной системы защиты для каждой категории рисков: формула 2 – для низкого риска, формула 3 – для высокого риска, и формула 3 – для среднего риска.

При этом:

k – количество каналов утечки в системе;

sz – количество систем защиты информации;

p – количество каналов утечки перекры-

ваемых несколькими средствами защиты информации;

n – количество каналов утечки с минимальным риском реализации;

s – количество каналов утечки со средним риском реализации;

v – количество каналов утечки с высоким риском реализации;

x – количество каналов не перекрываемых средствами защиты;

y – процентная оценка затруднения реализации пользователями своих функций после внедрения средств защиты.

Таким образом, нахождение оптимальных решений по разработке комплексных СЗИ, на основе внедрения DLP-систем, предполагает их интеграцию с другими подсистемами информационной безопасности, а также учет особенностей и свойств самой корпоративной системы. Поиск оптимальной архитектуры СЗИ требует учета всех функциональных возможностей DLP-систем, с учетом иных подсистем информационной безопасности. Эффективность системы защиты информации определяется набором критериев ее оценки, с учетом необходимости сохранения свойств иерархичности, синергичности и разнородности, используемых компонентов.

Примечания

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

2. Емельянников М.DLP-решения – это не панацея!//Информзащита Системный интегратор: [электр. ресурс]URL: http://www.infosec.ru/news/experts/2527 (дата обращения: 25.10.2017).

3. Безмалый В.Ф. Внедряем DLP?// ITBand: [электр. ресурс] URL: http://itband.ru/2009/08/%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D1%8F%D0%B5%D0%BC-dlp/ (дата обращения:26.10.2017).

4. Корпоративные информационные системы//Конспект лекций: [электр. ресурс] URL: http://sergeeva-i.narod.ru/inform/page501.htm (дата обращения: 27.10.2017).

5. Игнатова Ю.А. Классификация корпоративных информационных систем: реферат по информационному менеджменту. Университет ИТМО. – СПб, 2015. URL: http://iablov.narod.ru/igupit/kislec.htm (дата обращения: 27.10.2017).

6. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP-системы на основе Falcongaze Secure Tower // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2015. – № 4(16). – С. 57-67.

7. Борисов В.И., Шабуров А.С. О применении SIEM-систем для обеспечения безопасности корпоративных сетей // Инновационные технологии: теория, инструменты, практика. – Пермь, 2015. – С. 249-254.

8. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпортаивной сети на основе внелрения SIEM-системы // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2016. – №19. – С. 111-124.

9. Шабуров А.С., Журилова Е.Е. Модель выявления каналов утечки информации в автоматизированных системах на основе симплекс-метода // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2017. – № 4(24).

References

1. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i opredeleniya.

2. Emel'yannikov M.DLP-resheniya – ehto ne panaceya![DLP-solutions is not a panacea] Informzashchita Sistemnyj integrator [Informsecurity System's itnegrator].

3. Bezmalyj V.F. Vnedryaem DLP? [Will we introduce DLP?] ITBand.

4. Korporativnye informacionnye sistemy [Corporate information systems] Konspekt lekcij [Abstract of lectures].

5. Ignatova YU.A. Klassifikaciya korporativnyh informacionnyh system [Classical corporate information system] Referat po informacionnomu menedzhmentu. Universitet ITMO [Essay of information menegment. ITMO University].

6. Shaburov A.S., Zhurilova E.E., Luzhnov V.S. Tekhnicheskie aspekty vnedreniya DLP-sistemy na osnove Falcongaze Secure Tower [Technical aspects of implementation of DLP-systems, based on falcongaze secure tower] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems]. №16. 2015. P. 57-67.

7. Borisov V.I., Shaburov A.S. O primenenii SIEM-sistem dlya obespecheniya bezopasnosti korporativnyh setej [About application of the SIEM-systems for ensuring safety of corporate networks] Innovacionnye

tekhnologii: teoriya, instrumenty, praktika [Innovation technologies: theory, instruments, practice]. P. 249-254.

8. Shaburov A.S., Borisov V.I. Razrabotka modeli zashchity informacii korportaivnoj seti na osnove vnelreniya SIEM-sistemy [Developing model information protection corporate network based on the implementation of SIEM-system] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems].№19. 2016. P.111-124.

9. Shaburov A.S., Zhurilova E.E. Model' vyyavleniya kanalov utechki informacii v avtomatizirovannyh sistemah na osnove simpleks-metoda [Model of identification of information leaks channels in automated systems based on the symplex method] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems].№ 24 2017.

ЖУРИЛОВА Елена Евгеньевна, студент, кафедры автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. Адрес: 614990, Пермь, Комсомольский пр.,29. E-mail:ele11485995@yandex.ru

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета. Адрес: 614990, Пермь, Комсомольский пр.,29. E-mail: shans@at.pstu.ru

ZHURILOVA Elena, student, Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail:ele11485995@yandex.ru

SHABUROV Andrey, Ph.D. of Technical Science at the Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: shans@at.pstu.ru

УДК 004.66 + 004.056 Вестник УрФО № 3(25) / 2017, с. 12–18

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

ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО МОБИЛЬНОГО КОДА НА ОСНОВЕ ЭВРИСТИЧЕСКОГО АНАЛИЗА PDF-ФАЙЛОВ

Описаны методы классификации вредоносных PDF файлов и способы обнаружения мобильных кодов путем статистического анализа. PDF формат файлов позволяет встроить вредоносный контент любого типа вне зависимости от используемого браузера и операционной системы. По этой причине количество угроз этого типа непрерывно растет. Проанализирована выборка из 110000 PDF файлов, часть из которых была заражена. По результатам анализа предложены эффективные способы обнаружения вредоносных мобильных кодов.

Ключевые слова: *Формат PDF, мобильный код, JavaScript, вредоносная программа.*

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

DETECTION OF MALICIOUS MOBILE CODE BASED ON HEURISTIC ANALYSIS OF PDF FILES

Methods of classification of malicious PDF files and ways of detecting mobile codes by the means of statistical analysis described. PDF format allows us to embed malicious content of any type regardless of browser or operation system used. For this reason, number of threats of this type is increasing constantly. Corpus of 110000 PDF files analyzed, some of them were infected. On the basis of the analysis, effective methods of detecting malicious mobile codes suggested.

Keywords: *PDF format, mobile code, JavaScript, malicious software.*

PDF формат существует с 1993 года [1]. До 2004 года он не использовался злоумышленниками как контейнер для распространения вредоносных программ в отличие от форматов, использующих макросы (MS Word, MS Excell). Поэтому во второй половине 1990-х годов PDF формат рекомендовался исследователями как наиболее надежный формат текстовых документов.

С появлением вредоносного ПО (червя) Peachy [2] отношение к PDF формату начало меняться, начались исследования безопасности формата. Peach является классической вредоносной скрипт-программой, написанной на языке Visual Basic Script (VBS). Кроме этого, существует возможность внедрения в PDF-файлы программного кода, написанного на языке JavaScript и другого мобильного кода [3]. С появлением другого червя – Yourde [4], который массово заражал PDF файлы, исследователи в области компьютерной безопасности PDF формату стали уделять большее внимание.

С момента появления PDF формат претерпел множество изменений (с частотой 1 раз в 18 месяцев [5]), позволяющих разработ-

чикам лучше контролировать процесс просмотра. Однако при проведении синтаксического анализа PDF файлов могут возникать проблемы эффективности анализа их структуры (рис. 1).

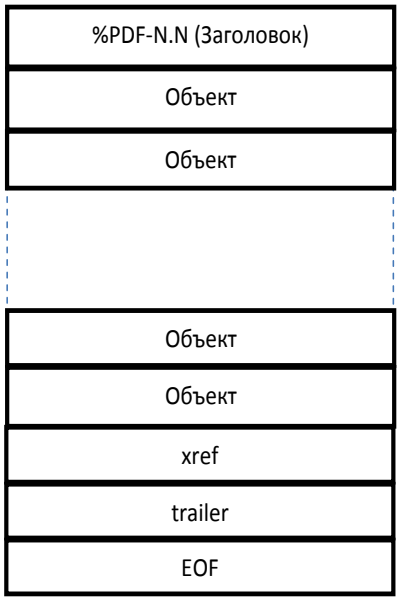

Рис. 1. Структура PDF файла

Заголовок PDF файла обычно находится в его начале, но это необязательное требование. Далее в файле PDF обычно находятся объекты, которые начинаются со строки «N R obj», где N – номер объекта, R – номер ревизии (обычно 0), объект завершается маркером «endobj». Внутри объекта может содержаться сжатый поток данных, который обозначается маркерами начала и конца потока. Таблица перекрестных ссылок (xref) содержит список объектов, их положение и состояние в файле. В файле может находиться несколько xref таблиц. В новом (немодифицированном) PDF файле будет содержаться лишь одна таблица xref, аналогичная приведенной (табл. 1).

Первая запись сообщает, что в таблице содержатся ссылки на 5 объектов, начиная с объекта под номером 0. Нулевой объект – это специальный объект, который имеет смещение в 0 байт, номер ревизии 65535 (-1), а также не используется (флаг f). В остальной части этой таблицы указано, что в файле содержатся четыре объекта со смещениями 10, 120, 189 и 408 байт. Все объекты заданы с номером ревизии 0 и находятся в использовании (флаг n). Такой способ определения объектов может означать, что все объекты уникальны, однако это не обязательно.

Объект типа trailer говорит анализатору как считывать таблицы перекрестных ссылок. В этом объекте обязательно содержится информация о количестве всех объектов в документе (ключ /Size), а также ссылка на корневой объект (ключ /Root). После объекта trailer следуют метка «startxref», величина смещения последней таблицы перекрестных ссылок, а затем метка %%EOF, которая означает «конец файла». Таблица перекрестных ссылок (xref) позволяет разработчикам PDF-анализаторов быстро создавать таблицы позиций объектов в отличие от простого перебора самого файла (что не всегда эффективно).

В рамках исследования была произведена выборка из 110000 PDF файлов, взятых из базы данных SophosLabs с 2014 года. Анализ этих файлов с помощью сканеров Kaspersky, McAfee, Microsoft и Sophos показал, что примерно 70000 из них являются подозрительными или содержат вредоносный мобильный код.

Результаты сканирования файлов введены в базу данных SQLite для последующего их анализа. Собранные данные не являются полными, так как процедура анализа таблицы xref оказалась трудоемкой с точки зрения временных затрат.

За последние несколько лет количество

Таблица 1

Таблица перекрестных ссылок (xref)

	Смещение, байт	**Номер ревизии**	**Флаг использования**
Первая запись	0	5	–
Объект 0	0	65535	f
Объект 1	10	0	n
Объект 2	120	0	n
Объект 3	189	0	n
Объект 4	408	0	n

вредоносных образцов PDF файлов значительно увеличилось. Для иллюстрации были запрошены базы данных SophosLabs по времени поступления PDF файлов, помеченных как вредоносные путем статического сканирования. Динамика роста количества зараженных файлов приведена на рис. 2.

Представленный график отображает натуральный логарифм общего числа вредоносных образцов в зависимости от времени. Во второй части графика, начиная с 2015 года, кривая принимает линейный характер. Если экстраполировать прямую часть представленного графика влево до оси x, то получим дату начала появления зараженных PDF файлов – март 2003 года (появление червя Yourde).

Чтобы показать, что размер PDF файла не является критерием наличия вредоносного мобильного кода, рассмотрим гистограмму из 60000 файлов, имеющих наименьший размер (рис. 3). Файлы сгруппированы в блоки по 512 байт (0-512 байт, 512-1024 байт и т. д.).

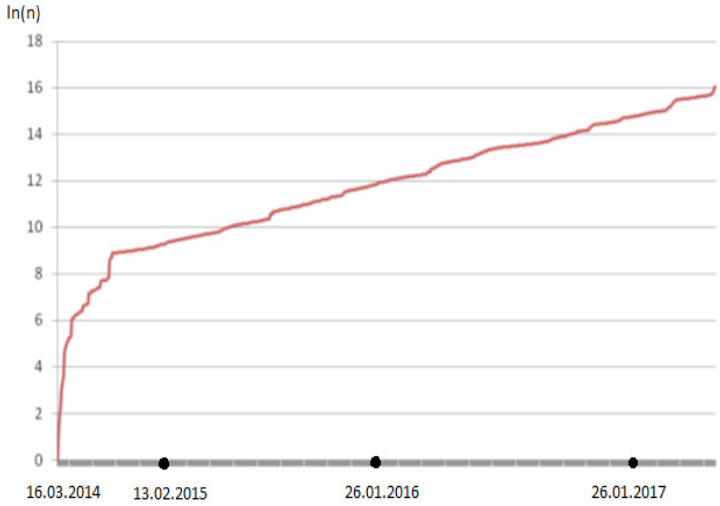

Рис. 2. Динамика роста вредоносных образцов PDF файлов (n – количество вредоносных образцов)

График показывает распределение файлов размером менее 20 КБ: красная полоса – это все файлы (54.05% выборки), а зеленая – только те, которые помечены как вредоносные (83.46%).

Объект, содержащий код на языке JavaScript, может косвенно ссылаться на дру-

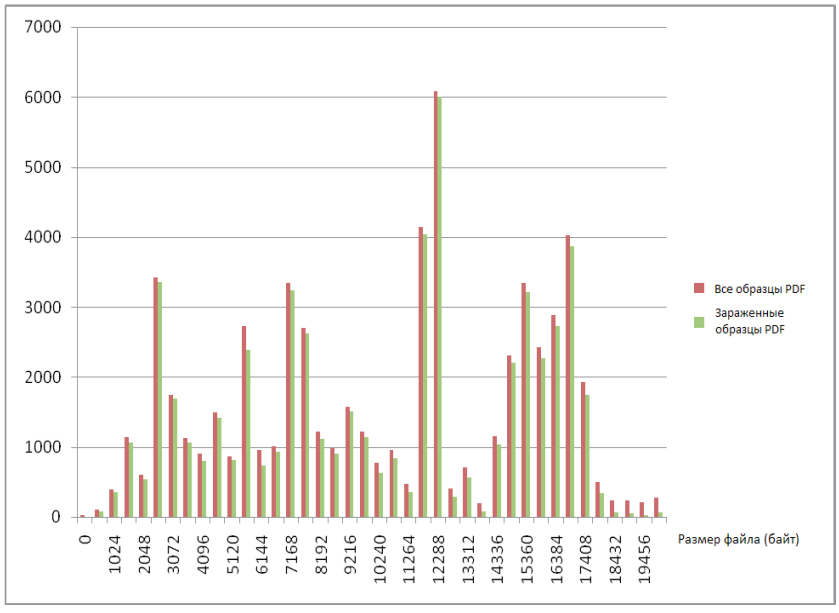

Рис.3. Распределение файлов размером менее 20 КБ

гой объект, содержащий тег /JavaScript. Это означает, что статическое сканирование тега завершится неудачей. Из результатов анализа выборки файлов на наличие тега /JavaScript, представленных в табл. 2, видно, что подавляющее большинство зараженных PDF файлов в отличие от обычных файлов содержат в себе код JavaScript. Таким образом, поиск в файле тега /JavaScript – хороший способ обнаружения вредоносных файлов. Однако, встраивание кода JavaScript – это не единственный способ заражения PDF файлов.

Таблица 2

Наличие тега /JavaScript в файлах

Всего	Вредоносные		Незараженные	
	К-во	%	К-во	%
64616	63523	98,3	1093	1,7

Во вредоносном файле число объектов и потоков может не совпадать с описанным в специальных объектах файла. Сопоставления меток «N R obj» – «endobj» и «stream» – «endstream» должно быть достаточно, чтобы получить истинное число объектов и потоков. В табл. 3 показано, что при выборке из 110000 файлов 10321 файлов имеют несоответствующие объекты, а 2296 – несоответствующие потоки. Процент несовпадений меток во вредоносных файлах значительно выше (84,1% и 69%), чем у незараженных файлов (15,9% и 31%).

Таблица 3

Несовпадающие объекты и потоки в файлах

	Несоответствующие объекты		Несоответствующие потоки	
	К-во	%	К-во	%
Всего файлов	10321	100	2296	100
Вредоносные	8685	84,1	1585	69,0
Незараженные	1636	15,9	711	31,0

В табл. 4 представлена статистика файлов, содержащих уникальные объекты, в выборке из 110000 PDF файлов. Незараженные файлы содержат больше неуникальных объектов по сравнению с вредоносными.

Анализ таблиц перекрестных ссылок (xref) может указывать на то, какой файл может быть заражен: таблица перекрестных ссылок у вредоносных файлов будет иметь недопустимый формат чаще, чем у незараженных файлов (табл. 5).

Таблица 4

Количество уникальных объектов в файлах

	Уникальные объекты		Неуникальные объекты	
	К-во	%	К-во	%
Всего файлов	104749	100	7746	100
Вредоносные	64425	61,7	3078	39,7
Незараженные	40324	38,3	4668	60,3

Таблица 5

Статистика нарушений таблицы перекрестных ссылок (xref)

Типы нарушений таблицы xref	PDF без startxref		Недопустимый xref		xref не сканируется	
	К-во	%	К-во	%	К-во	%
Всего файлов	5506	100	6691	100	91530	100
Вредоносные	5373	97,6	6123	91,5	56114	61,3
Незараженные	133	2,4	568	8,5	35416	38,7

Злоумышленник может закодировать вредоносный контент внутри объекта с помощью фильтров (табл. 6).

Фильтры №№ 1 – 5 обычно используются для всех типов данных, фильтры №№ 6 – 8 – для изображений и носителей, фильтры №№ 9 – 10 используются Adobe для защиты данных. Статистика распределения фильтров внутри выборки из 110000 файлов показаны в табл. 7.

Формат PDF позволяет записывать в файл символы, отличные от ASCII и не запрещает использование их шестнадцатеричного представления. Например, последовательность символов обфусцированного тега /Filter выглядит как:

Таблица 6

Типы кодирования внутри фильтров

№ п/п	Тип кодирования	Имя в фильтре
1.	Flate	FlateDecode
2.	LZW	LZWDecode
3.	ASCII85	ASCII85Decode
4.	ASCIIHex	ASCIIHexDecode
5.	RunLength	RunLengthDecode
6.	JBIG2 J	JBIG2Decode
7.	RichMedia	RichMedia
8.	DCT	DCTDecode
9.	Crypt	Crypt
10.	Encrypt	Encrypt

Вредоносные PDF файлы могут также содержать в себе другие теги, которые используются для запуска мобильного кода:

• OpenAction – определяет, что должна делать программа для просмотра PDF файлов при открытии документа;

• Launch [6] – позволяет запускать медиа объекты и скрипты при открытии PDF файла;

• «AA» (additional action) – определяет действия в ответ на «событие триггера» внутри объектов;

• Acroform – интерактивная форма, которая используется вредоносными PDF-файлами, где она переопределяет объект как исполняемый JavaScript код.

• Год от года количество обнаруженных заражений PDF файлов растет. Сложность формата файла и его способность запускать мобильный код означает, что эта тенденция, скорее всего, будет развиваться. Полученная статистика позволяет сделать заключение о признаках заражения PDF файла. Чтобы файл отнести к подозрительным, необходимо выполнение одного из условий:

Таблица 7

Статистика распределения фильтров в файлах

Фильтр	Всего	Вредоносные		Незараженные	
		К-во	%	К-во	%
FlateDecode	92277	52342	56,7	39935	43,3
LZWDecode	5907	319	5,0	5588	95,0
ASCII85Decode	6174	841	13,6	5333	86,4
ASCIIHexDecode	6451	6404	99,3	47	0,7
RunLengthDecode	371	159	42,9	212	57,1
JBIG2Decode	689	525	76,2	164	23,8
RichMedia	178	178	100	0	0
DCTDecode	20666	1404	6,8	19262	93,2
Crypt	234	28	11,9	206	88,1
Encrypt	5478	614	11,2	4864	88,8

/Filter [/A#53#43#49#48#65#78Dec#6f#6 4 e / # 4 c # 5 a W # 4 4 # 6 5 c # 6 f d e /#41S#43I#4985Decod#65/R#75n#4ce#6e#67#74#68D#65#63o#64e /FlateDecode]

Обфусцированный тег декодируется средствами просмотра PDF файлов в последовательность символов:

/Filter [/ASCIIHexDecode /LZWDecode / ASCII85Decode

/RunLengthDecode /FlateDecode]

Этот пример демонстрирует, что значение тега /Filter может быть обфусцировано с целью скрытия в нем фильтров, которые могут использоваться во вредоносных файлах. Для поиска обфусцированных тегов можно использовать регулярное выражение:

Filter\s+\[\s+[^\]]+#

• наличие тега /JavaScript;

• несовпадение меток потоков и объектов в файле;

• содержит больше неуникальных объектов;

• содержит любой из видов нарушений таблицы перекрестных ссылок (xref)

• содержит фильтры FlateDecode и ASCIIHexDecode.

Таким образом, для ограничения возможностей запуска вредоносного мобильного

кода, содержащегося в PDF файле, рекомендуется при использовании средств просмотра:

• запускать только подписанный JavaScript код (и другие функции);

• запускать только подписанные встроенные файлы;

• отключать JavaScript в плагинах браузера;

• реализовывать строгий режим синтаксического анализа, например, чтобы не допустить запутывания фильтров.

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

Примечания

1. История формата PDF (сайт компании Adobe) [Электронный ресурс] //http://www.adobe.com/pdf/about/history/. (Дата обращения: 13.10.2017).

2. История вредоносного контента встраиваемого в PDF файлы (сайт компании McAfee) [Электронный ресурс] //http://vil.nai.com/vil/content/v_99179.htm. (дата обращения: 13.10.2017).

3. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности [Текст]: ГОСТ Р МЭК 62443-3-3 – 2016. – Введ. 2017–04–01. – М. : Стандартинформ, 2016.

4. Анализ вредоносного контента в PDF файлах (сайт компании Sophos) [Электронный ресурс] // http://www.sophos.com/security/analyses/viruses-andspyware/jsyourdea.html#table4. (дата обращения: 13.10.2017).

5. История формата PDF. Блог Леонарда Орра [Электронный ресурс] // http://www.acrobatusers.com/blogs/leonardr/history-of-pdfopenness/.(дата обращения: 15.10.2017).

6. Запуск вредоносного контента из PDF файлов (сайт компании Sophos) [Электронный ресурс] // http://www.sophos.com/blogs/sophoslabs/?p=9301. (дата обращения: 13.10.2017).

References

1. Istoriya formata PDF (sayt kompanii Adobe) [Elektronnyy resurs] //http://www.adobe.com/pdf/about/history/. (Data obrashcheniya: 13.10.2017).

2. Istoriya vredonosnogo kontenta vstraivayemogo v PDF fayly (sayt kompanii McAfee) [Elektronnyy resurs] //http://vil.nai.com/vil/content/v_99179.htm. (data obrashcheniya: 13.10.2017).

3. Seti promyshlennoy kommunikatsii. Bezopasnost' setey i sistem. Chast' 3-3. Trebovaniya k sistemnoy bezopasnosti i urovni bezopasnosti [Tekst]: GOST R MEK 62443-3-3 – 2016. – Vved. 2017–04–01. – M. : Standartinform, 2016.

4. Analiz vredonosnogo kontenta v PDF faylakh (sayt kompanii Sophos) [Elektronnyy resurs] //http://www.sophos.com/security/analyses/viruses-andspyware/

jsyourdea.html#table4. (data obrashcheniya: 13.10.2017).

5. Istoriya formata PDF. Blog Leonarda Orra [Elektronnyy resurs] // http://www.acrobatusers.com/blogs/leonardr/history-of-pdfopenness/.(data obrashcheniya: 15.10.2017).

6. Zapusk vredonosnogo kontenta iz PDF faylov (sayt kompanii Sophos) [Elektronnyy resurs] // http://www.sophos.com/blogs/sophoslabs/?p=9301. (data obrashcheniya: 13.10.2017).

БУХАРЕВ Дмитрий Александрович, студент кафедры 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: needleinspace@gmail.com

ВАГИН Сергей Владиславович, студент кафедры 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: 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: ANSokolov@inbox.ru

BUKHAREV Dmitrii, student 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: needleinspace@gmail.com

VAGIN Sergey, student 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: vaginserg.96@mail.ru

SOKOLOV Alexander, Candidate of Engineering Science, Docent, 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: ANSokolov@inbox.ru

УДК 004.048 + 004.032.26 Вестник УрФО № 3(25) / 2017, с. 19–23

Асяев Г. Д., Рагозин А. Н.

ОПРЕДЕЛЕНИЕ МИНИМАЛЬНОГО НАБОРА ВХОДНЫХ ДАННЫХ ДЛЯ КОРРЕКТНОЙ АУТЕНТИФИКАЦИИ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

В статье проводится обзор биометрических динамических характеристик человека, параметров по которым будет происходить аутентификация по клавиатурному почерку. Экспериментальным образом определяется тип нейронной сети, который оптимально проводит операцию аутентификации по клавиатурному почерку, проводится экспериментальное исследование минимального количества входных данных на основе произвольного текста для корректного распознавания зарегистрированного пользователя. Определены границы параметров системы идентификации и их обоснование при практической реализации, выбран алгоритм распознавания на основе нейронной сети.

Ключевые слова: *Безопасность, аутентификация, парольное слово, клавиатурный почерк, аудит, ошибки второго рода.*

DETERMINATION OF THE MINIMUM SET OF INPUT DATA FOR CORRECT KEY-BASED AUTHENTICATION USING A NEURAL NETWORK

The article reviews the biometric dynamic characteristics of a person whose parameters will be used to authenticate using the keyboard handwriting. The type of the neural network is determined experimentally which optimally performs the authentication operation using the keyboard handwriting, an experimental study of the minimum amount of input data on the basis of arbitrary text is performed to correctly recognize the registered user. The boundaries of the parameters of the identification system and their justification for practical implementation are determined, and the recognition algorithm based on the neural network is chosen.

Keywords: Security, authentication, password, keyboard handwriting, audit, errors of the second kind.

Отождествление пользователя ЭВМ является первостепенной задачей при обеспечении информационной безопасности объекта. Это можно сделать как при помощи традиционной парольной защиты, так и про помощи проверки физических и психофизических параметров человека. В данной статье рассмотрена биометрическая система аутентификации, анализирующая динамический образ, который в свою очередь построен на анализе клавиатурного почерка.

Клавиатурный почерк - динамическая биометрическая характеристика, которую описывают: динамика и скорость ввода, частота возникновения ошибки. В ходе выполнения исследования было разработано программное обеспечение, которое регистрирует все характеристики, описанные выше. В качестве парольной фразы могут быть как несвязные по смыслу буквы (20 - 42), так и произвольно генерируемый текст. Данная система может находиться в 3 этапах: получение информации, обработка информации, разрешение или запрет на получение ресурсов пользователю на основе аутентификации. В ходе проведения эксперимента было написано программное обеспечение, которое регистрирует временные интервалы между нажатиями клавиш и направляет выходные данные программы на вход нейронной сети.

Использование нейронной сети для аутентификации было выбрано в связи с обладанием ряда преимуществ по сравнению с обычными статистическими моделями:

1. В силу физической и психической особенности человека невозможно получить одни и те же параметры клавиатурной аутентификации при одинаковых условиях. Именно применение нейронной сети делает систему устойчивой к отклонениям входных данных. Отсутствует необходимость в проведении предварительной обработки шумов входных данных.

2. В силу психического состояния человека нейронная сеть способна адаптироваться к изменениям в поведении и темпу набора парольной фразы на клавиатуре.

3. Нейронные сети обладают высоким быстродействием из-за параллелизма обработки информации.

Во время исследования рассматривалось 4 типа нейронной сети:

1. Нейронная сеть с прямым распространением сигнала и обратным распространением ошибки1. В результате эксперимента выяснилось, что сеть успешно распознала всех пользователей. Неточность в определении пользователя определяется недостаточным выбором метрики нейронной сети с прямым распространением сигнала и обратным распространением ошибки и, как следствие, неправильное вычисление весовых коэффициентов. Данный тип нейронной сети корректно работает при количестве зарегистрированных пользователей до 20.

2. Самоорганизующаяся карта Кохонена[1]. В ходе эксперимента выяснилось, что данный подход имеет существенный недостаток: аутентификация по клавиатурному почерку с помощью нейронной сети Кохонена возможна при обязательном использовании парольной защиты, либо другой аутентификации, исключающей доступ к ЭВМ незарегистрированных лиц. Исходя из этого основным применением данной сети является скрытый мониторинг информационных систем безопасности.

3. Иерархическая сеть. Максимальное количество пользователей при котором возможна корректная аутентификация, вследствие подчинённости иерархии, составило 50 человек.

4. Нейронная сеть, у которой количество входов равняется количеству выходов. В ходе проведённого эксперимента выяснилось, что она обладает достаточной устойчивостью и оптимально распознаёт зарегистрированных пользователей. Большим плюсом является большое количество пользователей при котором возможна корректная аутентификация.

В качестве алгоритма для идентификации пользователя применим нейронную сеть, у которой количество входов равняется количеству выходов. Функцией активации была выбрана единичная функция активации с жёстким ограничением. Она передаёт "1" на выход нейронной сети, который соответствует входным параметрам пользователя.

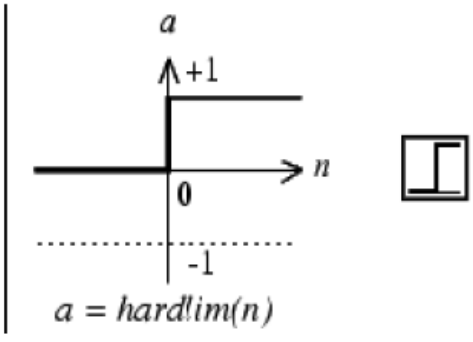

Рис. 1. Функция активации с жестким ограничением

Вычисление коэффициентов осуществляется по следующему принципу:

$$X_i = WX_i, \text{ где} \quad (1)$$

X_i – запомненные образы;

Весовые коэффициенты настраиваются один раз и больше не изменяются. Именно, когда матрица весов удовлетворяет условию, описанному выше, Xi становится максимально устойчивым, что позволяет сети при попадании в такое состояние там и остаться[2].

Алгоритм работы сети[3]:

1. Каждое значение элемента вектора входа умножается на вес этого вектора W_{1j};

2. Полученные взвешенные элементы суммируются и подаются на вход функции активации;

3. Если на вход функции активации поступило *n>0*, то нейрон возвращает *1*;

4. Если на вход функции активации поступило *n<0*, то нейрон возвращает *0*.

Упрощённая модель нашей схемы представлена на рисунке.

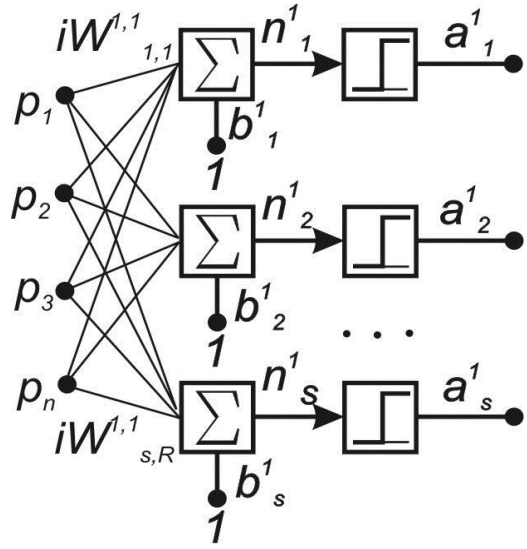

Рис.2. Упрощенная структура схемы

Каждому пользователю отведён свой выходной слой. Это позволяет исключить ошибки второго рода. Из каждого набора входных слоёв выбирается ровно один вектор, который и характеризует данный слой. При этом чем больше количество повторений временных интервалов для каждого субъекта при обучении, тем корректнее работает данная сеть[2]. Вследствие того, что каждому входу соответствует ровно один выход, то количество зарегистрированных пользователей может быть больше 60. Данный тип нейронной сети хорошо применим для организаций с большим штатом сотрудников. Для данного алгоритма данные о количестве нажатий составляют 60% от общего массива данных, что является недопустимым для реализации в конечном программном продукте. Очевидно, что при уменьшении количества нажатий корректность идентификации будет умень-

шаться. Основной же задачей исследования является определить минимальное количество входных данных при котором пользователь будет корректно распознаваться для данной модели алгоритма с заданной точностью – 95%. Остальные 5% - психофизическое состояние человека. Параметры, влияющие на корректность идентификации:

1. Количество нажатий на клавиши;

2. Временной интервал между нажатиями клавиш;

3. Количество ошибок при наборе произвольного текста.

рода. При размере входных данных составляющем 13 символов – 25%, возникали ошибки второго рода. При размере входных сигналов составляющих 16 символов из 8 попыток идентификации все 8 были успешны.

В ходе проведения эксперимента был написан алгоритм распознавания пользователей по временному интервалу между нажатиям клавиш, определён минимальный набор входных данных при котором пользователь будет корректно распознаваться для нейронной сети у которой количество входов равняется количеству выходов. Исходя из результатов экспери-

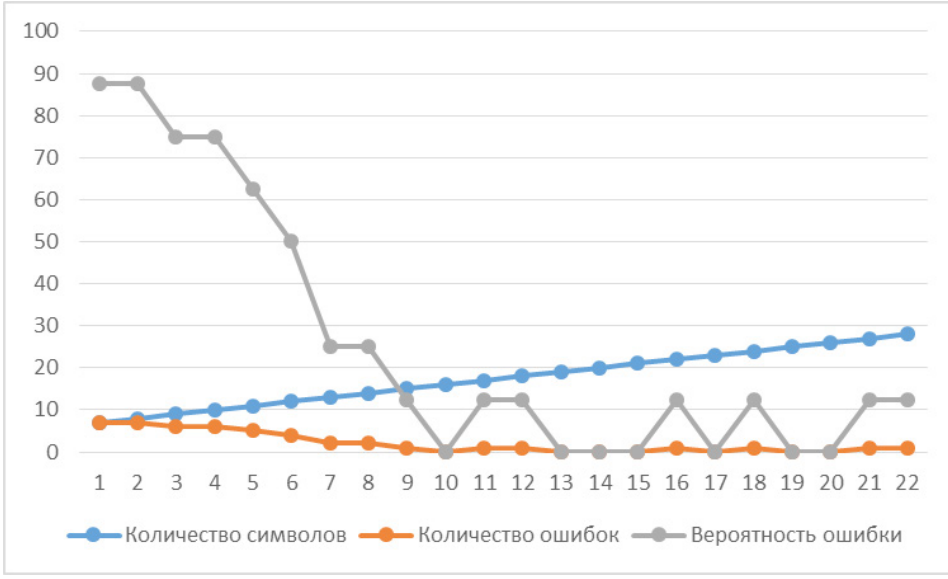

Рис. 3. График зависимости количества введённых символов от вероятности ошибки

В ходе проведения эксперимента было зарегистрировано 8 пользователей. Знаки пунктуации в произвольном тексте были исключены. При входном наборе равным 6 символов вероятность ошибки составила 87,9%, возникали ошибки как первого, так и второго

мента 16 символов парольной фразы является оптимальным количеством для успешной аутентификации. При меньшем наборе входных данных наблюдались ошибки первого и второго рода, а при количестве символов больше 16 наблюдается избыточность входных данных.

Примечания

1. Мищенко Е. Ю., Соколов А. Н. Количественный анализ процедуры обезличивания персональных данных. Метод перемешивания // Вестник УрФО. Безопасность в информационной сфере /№ 3(21) / 2016, с. 30–37.

2. Хайкин С. Нейронные сети: полный курс. – М.: Вильямс, 2006. – С. 1104.

References

1. Mishchenko E. Yu., Sokolov A. N Quantitative analysis of the depersonalization procedure. Method of mixing//.Bulletin of the Ural Federal District Security in the Sphere of Information No. 3(21) / 2016, p. 30–37.

2. Haykin S. Neural networks: a full course. - M .: Williams, 2006. – P. 1104.

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

РАГОЗИН Андрей Николаевич, научный рук., кандидат технических наук, доцент кафедры «Защита информации» , доцент кафедры инфокоммуникационных технологий ФГАОУ ВО «Южно-Уральский Государственный Университет» (Национальный исследовательский университет). Россия, 454080, г.Челябинск, проспект Ленина, д 76. E-mail: asyaev1996@mail.ru

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

RAGOZIN Andrey, scientific chief., Ph.D., Candidate of Technical Sciences, assistant professor of information security , assistant professor of information and communication technologies FGAOU «South Ural State University» (National Research University). Russia, 454080, Chelyabinsk, Prospekt Lenina, 76. E-mail: asyaev1996@mail.ru

УДК 004.056 + 658.1:622 + 681.518 Вестник УрФО № 3(25) / 2017, с. 24–33

Захаров А. А., Римша А. С., Харченко А. М., Зулькарнеев И. Р.

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ ПРОЦЕССАМИ ГАЗОДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ

В настоящее время на предприятиях газодобывающей отрасли используют автоматизированные системы, позволяющие повысить эффективность и контроль технологического процесса. Эти предприятии являются частью критической информационной инфраструктуры России, опасным производственным объектом, при эксплуатации которого могут возникнуть аварийные ситуации, причиной которых может быть, в том числе, и недостаточная защищенность автоматизированных систем управления технологическими процессами.

Для анализа защиты типовой иерархической структуры предприятия по добыче газа предложена математическая модель его информационной инфраструктуры. Рассматривается принцип работы каждого уровня такой системы, идентифицируются активы и определяется технология моделирования средств защиты информации. Приводится перечень основных уязвимостей системы. Формулируются этапы оценки уязвимости, на основе которых выделяются основные угрозы. После идентификации рисков проводится оценка их величины. Рассматриваются этапы внедрения средств защиты и их влияние на сокращение возможного ущерба.

Ключевые слова: *газодобывающая организация, критическая информационная инфраструктура, информационная безопасность, математическая модель, оценка рисков.*

Zakharov A. A., A.S. Rimsha, A.M. Kharchenko, I.R. Zulkarneev

ANALYSIS OF INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS FOR TECHNICAL PROCESSES OF A GAS PRODUCING ENTERPRISE

At present, the enterprises of the gas industry are using automated systems to a greater or lesser extent, which make it possible to increase the efficiency and control the technological process. The principle of operation of automation systems of technological processes at a gas producing enterprise is in many respects like the solutions used in other industrial enterprises, but they also have their own peculiarities. They represent a dangerous production facility, during the operation of which there can be emergencies, caused, including by the incorrect operation of automated systems.

This paper is devoted to the construction of a mathematical model for analysis of the protection of a typical hierarchical structure of the automated process control system for gas production. The principle of operation of each level of such a system is considered, the assets of the whole system are identified. The technology of modeling IIS is determined. The list of the main vulnerabilities of the system is given. The stages of vulnerability assessment are formulated based on which the main threats to the process control system are highlighted. After identifying the risks, a risk analysis is performed, the result of which is the overall estimated risk value. The stages of implementation of IIS measures, as well as their impact on possible damage, are considered.

Keywords: gas producing organization, critical information infrastructure, information security, mathematical model, risk assessment.

Введение

Для автоматизации технологических процессов в газодобывающей отрасли используются автоматизированные системы управления технологическим процессом (АСУ ТП), построенные на базе промышленных логических контроллеров (ПЛК) [1].

Одной из задач корректного функционирования АСУ ТП является обеспечение информационной безопасности (ИБ) этих систем. Проблемы защиты АСУ ТП от вредоносного программного обеспечения (ПО) Stuxnet, Duqu, Flame и другие обсуждаются в работах [2-4].

Важно подчеркнуть бытовавшее представление о том, что функционирование АСУ ТП сложно нарушить благодаря следующим обстоятельствам:

– ПО каждой АСУ ТП, как правило, проприетарное и закрытое;

– в локальной сети пользователей на верхнем уровне АСУ ТП проблемы с безопасностью можно решить организацией корректной политики ограничения доступа;

– проникновение в АСУ ТП связано с большими интеллектуальными затратами, а выгода для злоумышленника не очевидна.

Однако недавние инциденты с заражением компьютеров предприятий, занимающихся добычей нефти и газа, в «Роснефть», «Башнефть» [5] вирусами типа WannaCry [6] или Petya, использующими уязвимость устаревшего протокола SMBv1, свидетельствуют об обратном. Более того, тот факт, что предприятия передают данные по Ethernet во внешние сети (например, в центральный офис), показывают, что такие системы необходимо защищать, в том числе, и по причине возможного использования информационных технологий как инструмента давления и противобор-

ства. Это нашло свое отражение в Доктрине информационной безопасности Российской Федерации 2016 года и Стратегии национальной безопасности США 2015 года.

Отметим, что, даже отделив физически технологическую сеть АСУ ТП от сетей общего пользования, нельзя исключать возможность заражения вирусом, случайно принесенным пользователем на внешнем носителе. Все это заставляет по-новому поставить вопросы, связанные с информационной безопасностью предприятий, использующих АСУ ТП.

В соответствии с последними изменениями законодательства о ключевой информационной инфраструктуре (КИИ) от 26 июля 2017 г., принятыми федеральными законами 183-ФЗ, 193-ФЗ и 194-ФЗ, АСУ ТП относятся к КИИ и подлежат обязательной категоризации и защите [7] в соответствии с требованиями нормативно-правовых актов, обязательному контролю со стороны соответствующих ФОИВ. Также вводится уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, содержащейся в КИИ [8].

Предварительный анализ типовых информационных системы АСУ ТП газодобывающего предприятия, протоколов передачи информации и информационных ресурсов показывает сложность их взаимодействий и, как следствие, потенциальную возможность реализации тех или иных угроз ИБ [9, 10].

Поскольку статистику по инцидентам, связанным с нарушением ИБ, трудно собрать в должном объеме, то актуальной задачей представляется моделирование системы защиты ИС АСУ ТП типового газодобывающего предприятия, с целью оценки рисков информационной безопасности, оптимизации расходов на ИБ и конкретизации рекомендаций к организационным и технологическим мероприятиям, повышающим защищенность ИС АСУ ТП [11].

Существуют различные подходы к моделированию систем защиты информации (СЗИ), отражающие те или иные аспекты систем защиты [9, 12 - 15]:

– обобщенные модели систем защиты;

– модели, использующие подходы теории вероятности и нейронных сетей;

– модели, построенные с использованием теории сетей Петри–Маркова;

– модели, основанные на теории конечных автоматов;

– модели, построенные с использованием теории графов;

– модели, использующие теорию нечетких множеств;

– модели, построенные с использованием энтропийного подхода.

Модели, использующие теорию вероятности и нейронные сети, идеально работают, например, при анализе аномалий сетевого трафика из внешней сети, когда можно на основе статистики классифицировать аномалию и принять решение о блокировке определенного трафика.

Модели на основе сетей Петри–Маркова, как и модели, использующие автоматы Мура, хорошо себя зарекомендовали для анализа управления вероятностью успешной реализации НСД по времени (с использованием статических данных) [16,17].

Модели ИБ, использующие теорию графов, хорошо работают в системах поддержки принятия решений с использованием экспертов, когда, например, необходимо оценить безопасность того или иного пути реализации процесса, а для оптимизации выбора наиболее безопасного маршрута используется модифицированный алгоритм Дейкстры [18].

Модели на основе нечетких множеств (модель Мамдани, TSK- модели и др.) можно использовать для оценки рисков ИБ с помощью хорошо спланированных экспериментов и экспертов, способных грамотно оценить результат работы модели, т.е. полученный риск, по входным данным. Обычно хорошо работают для конкретных информационных процессов в защищаемой ИС [19].

Модели ИБ, построенные на основе энтропийного подхода, используются для выявления возможности идентификации пользователей веб-ресурсов [20].

Как правило, подход к моделированию выбирают, ориентируясь на параметры, используемые в качестве входной информации, и те результаты расчетов, которые получены на выходе. Обычно входная информация базируется на имеющейся статистике для существующих ИС и/или данных экспертов. Модели могут использоваться на этапе проектирования ИС, но чаще их используют на этапах эксплуатации и сопровождения, проведения мониторинга и аудита систем защиты информации.

Предлагаемая методология

Для выбора конкретной технологии мо-

делирования защиты ИС АСУ ТП формализуем бизнес-процессы типового газодобывающего предприятия, которое представляет собой территориально распределенную структуру, начинающуюся от кустов газовых скважин и заканчивающуюся центральным диспетчерским пунктом.

Управление технологическим процессом требует применения специальных технологических решений построения сетей передачи данных. Упрощенная структура АСУ ТП типового предприятия газодобывающей отрасли строится по иерархическому принципу. Обычно в промышленных АСУ ТП выделяют три уровня [1, 21]:

– *нижний уровень, или уровень ввода данных, исполнительных устройств* — датчики (датчики температуры, давления, расхода, и т.д.) и исполнительных механизмов (регулирующая и запорная арматура);

– *средний уровень, или уровень автоматического управления* — промышленные контроллеры, управляющие исполнительными механизмами и, при необходимости, передающие данные с датчиков на верхний уровень;

– *верхний уровень, или уровень операторского управления* — централизованное дистанционное управление, основанное на SCADA (supervisory control and data acquisition) и современных разработках в области информационных технологий (сервера ввода/вывода, коммутационное оборудование, рабочие места операторов и диспетчеров, базы данных, ПО для сбора данных, визуализации и мониторинга хода технологического процесса).

Введем основные обозначения:

$c^{sensor} = \{c_1^{sensor}, \dots, c_{a_1}^{sensor}\}$ - множество всех датчиков, используемых в технологическом процессе;

$c^{mechanism} = \{c_1^{mechanism}, \dots, c_{a_2}^{mechanism}\}$ - множество исполнительных механизмов;

$c^{PLC} = \{c_1^{PLC}, \dots, c_{a_3}^{PLC}\}$ - множество всех ПЛК;

$c^{server} = \{c_1^{server}, \dots, c_{a_4}^{server}\}$ - множество серверов ввода/вывода;

$c^{network} = \{c_1^{network}, \dots, c_{a_5}^{network}\}$ - множество элементов сетевого оборудования;

$c^{workstation} = \{c_1^{workstation}, \dots, c_{a_6}^{workstation}\}$ - множество автоматизированных рабочих мест (АРМ).

Тогда все многообразие компонентов, используемых в АСУ ТП газодобывающего предприятия, можно представить в виде множества $C = \{c^{sensor}, c^{mechanism}, c^{PLC}, c^{server}, c^{network}, c^{workstation}\}$. (1)

На физическом уровне для передачи данных между компонентами используется четыре типа сетей связи:

– электрические линии — $electrical$;

– волоконно-оптические линии — $fiber$;

– беспроводная связь — $wireless$;

– многопарные медные линии — UTP.

Таким образом, множество типов связи между компонентами c_i и c_j для передачи данных можно представить:

$$s_{ij} = \{electrical, fiber, wireless, UTP\}. \quad (2)$$

Множество типов связи между всеми компонентами образует многомерный массив, размерность которого определяется числом компонентов системы и представляет собой матрицу типов связи:

$$S = \begin{vmatrix} 0 & \cdots & s_{1j} & \cdots & s_{1i} & \cdots & s_{1n} \\ \cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{j1} & \cdots & 0 & \cdots & s_{ji} & \cdots & s_{jn} \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ s_{i1} & \cdots & s_{ij} & \cdots & 0 & \cdots & s_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \cdots \\ s_{n1} & \cdots & s_{nj} & \cdots & s_{ni} & \cdots & 0 \end{vmatrix}. \quad (3)$$

На логическом уровне в зависимости от производителя и типа оборудования используются промышленные протоколы (семейство протоколов Modbus, промышленная сеть PROFIBUS и т.д.). Между рабочими станциями и сетевым оборудованием, используется Ethernet. Сигналы, передающиеся по электрическим линиям, можно разделить на аналоговые, дискретные и цифровые. Обозначим множество способов передачи данных между компонентами c_i и c_j

$$pr_{ij} = \{pr_1, \dots, pr_b\}. \quad (4)$$

По аналогии с (3) множество способов передачи данных между всеми компонентами представим в виде матрицы:

$$Pr = \begin{vmatrix} 0 & \cdots & pr_{1j} & \cdots & pr_{1i} & \cdots & pr_{1n} \\ \cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ pr_{j1} & \cdots & 0 & \cdots & pr_{ji} & \cdots & pr_{jn} \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ pr_{i1} & \cdots & pr_{ij} & \cdots & 0 & \cdots & pr_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \cdots \\ pr_{n1} & \cdots & pr_{nj} & \cdots & pr_{ni} & \cdots & 0 \end{vmatrix}. \quad (5)$$

Исходя из этого, связь между компонентами c_i и c_j будет иметь вид упорядоченной пары: тип связи и способ передачи данных – (s_{ij}, pr_{ij}).

Таким образом, ПЛК c_i^{PLC}, получив по од-

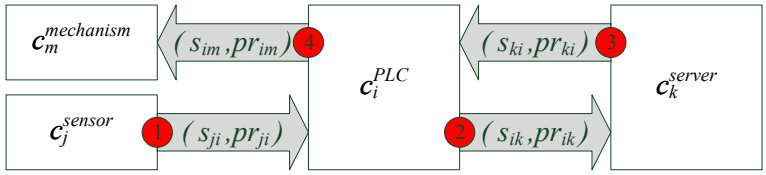

Рис. 1. Схема взаимодействия компонентов

ному из типов связи s_{ji} и соответствующим способом передачи данных pr_{ji} информацию от датчика c_j^{sensor}, отправляет информацию на верхний уровень c_k^{server} через (s_{ik}, pr_{ik}) и в зависимости от встроенных алгоритмов или указаний от *SCADA*-системы через (s_{ki}, pr_{ki}), отправляет по (s_{im}, pr_{im}) команду на выполнение определенных операций исполнительному механизму $c_m^{mechanism}$ (рис. 1).

Всем существенным с точки зрения защиты технологического процесса активам соответствует некая ценность, зависящая от степени его влияния на прибыль организации и уровнем ущерба (в финансовом, репутационном, социальном, промышленном и других планах), который может понести организация при выводе из строя, компрометации или некорректном функционировании данного актива. Объединим ценность активов во множество

$$A = \{A_1, \dots, A_o\}. \quad (6)$$

Согласно (1), (3) и (5) мощность такого множества будет равна $\boldsymbol{o = |C| + |S| + |Pr|}$.

Для выбора конкретной технологии моделирования защиты АСУ ТП в первую очередь будем использовать формализованную структуру компонентов и связей АСУ ТП (1-6) и такие критерии как:

– простота определения входных параметров модели (модель может использовать различные данные в качестве исходных, однако возможности получения этих данных могут быть задачами различной сложности);

– уровень подготовки и оснащенности злоумышленника;

– вероятность реализации той или иной угрозы, риски, связанные с этой угрозой и возможность рассчитать вероятный ущерб в результате реализации угрозы;

– возможность учесть разнородность компонентов системы каждого уровня (1-3) и связь между ними.

– возможность учета требования по защите АСУ ТП в соответствии с действующим законодательством;

– возможность рассчитать время обнаружения атаки в зависимости от используемых средств защиты, уязвимостей в них и уровня подготовки и оснащенности злоумышленника;

– при атаках на функционирующую систему возможна ситуация, когда на определенном этапе с помощью технологий обнаружения вторжения и/или оперативных действий персонала по соответствующему регламенту атака будет заблокирована. Важно определить среднее время от начала атаки до ее блокировки.

Анализ приведенных критериев показывает, что на первом этапе можно воспользоваться обобщенной моделью АСУ ТП типового газодобывающего предприятия вида:

$$K = \{C, S, Pr, A, T, V, P, D, R, L\},$$

где ***C*** – множество компонентов системы;

S – множество типов связи между всеми компонентами;

Pr – множество способов передачи между компонентами;

A – множество стоимостей всех активов организации;

T – множество угроз;

$\boldsymbol{V_i}$ – множество уязвимостей угрозы ;

P – множество характеристик угроз в виде вероятностных показателей;

D – множество мероприятий по снижению риска;

R – множество оценочных величин риска;

L – множество требований законодательства по защите АСУ ТП.

Поскольку в газодобывающем предприятии конфиденциальность не является критическим объектом защиты [22], то далее под уязвимостью будем понимать проблемы безопасности, которые позволяют нарушить целостность и доступность информации в системе АСУ ТП. Множество уязвимостей обозначим $\boldsymbol{V = \{V_1, \dots, V_m\}}$.

Каждая уязвимость может по-разному влиять на отдельный актив [23]. Таким образом, влияние уязвимостей на активы можно представить в виде матрицы уязвимостей и их влияние на актив.

	V_1	V_2	...	V_m
A_1	v_{11}	v_{12}	...	v_{1m}
A_2	v_{21}	v_{21}	...	v_{2m}
...	...	...	...	
A_o	v_{o1}	v_{o2}	...	v_{om}

Влияние одной уязвимости на множество активов можно рассчитать по следующей формуле:

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i \qquad (7)$$

где v_{ij} – воздействие уязвимости V_j на актив A_i.

Обозначим через множество угроз, а множество характеристик угроз в виде вероятностных показателей через . Каждая угроза представляет собой совокупность уязвимостей, но каждая уязвимость может по-своему влиять на реализацию угрозы, поэтому введем коэффициент потенциального воздействия уязвимости на угрозу – *d*.

При реализации угрозы нарушается технологический процесс, результатом которого может быть выход из строя компонентов системы. Под ущербом, нанесенным в таком случае, будем понимать совокупность всех уязвимостей конкретной угрозы с учетом потенциального воздействия каждой [24]. Определим матрицу угроз, которая отражает взаимосвязь угроз с уязвимостями.

	V_1	V_2	…	V_m
T_1	t_{11}	t_{12}	…	t_{1m}
T_2	t_{21}	t_{21}	…	t_{2m}
…	…	…	…	
T_g	t_{g1}	t_{g2}	…	t_{gm}

Так как под ущербом мы подразумеваем реализацию угрозы, то оценка ущерба от конкретной угрозы будет определяться совокупностью уязвимостей, которые с ней связаны:

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right) \qquad (8)$$

где t_{hj} – воздействие уязвимости V_j на угрозу T_h.

Определим риск, как возможность того, что произойдет неблагоприятное событие, имеющее последствие (ущерб) T_h с вероятностью наступления этого события p_h [25]. Далее будем подразумевать, что риск зависит от реализации угрозы T_h. Таким образом, общая оценка величины риска системы будет представлять сумму последствий реализации всех угроз:

$$R = \sum_{i=1}^{g} R_i = \sum_{i=1}^{g} p_i \times T_i \qquad (9)$$

Для полной оценки величины ущерба организации необходимо учитывать не только величину риска в зависимости от реализации угроз, но и возможный ущерб от игнорирования требований законодательства по защите АСУ ТП и КИИ. Так как данный ущерб оценивается не только количественно, но и качественно, а требования являются обязательными для выполнения организациями, эксплуатирующих КИИ, то дополнительно следует учитывать затраты на реализацию этих требований как сумму затрат на выполнение конкретного требования L_i:

$$L = \sum_{i=1}^{l} L_i \qquad (10)$$

При этом надо учитывать, что в случае, если величина ущерба R_i от реализации угрозы T_i будет меньше величины затраты L_i, то целесообразно использовать компенсирующую меру, которая позволит сделать стоимость затрат меньшей, чем величина ущерба. В случае отсутствия подобной компенсирующей меры необходимо обосновать неприменимость этого требования и исключить его из общего множества. После оценки затрат на реализацию требований и оптимизации затрат с использованием компенсирующих мер и исключением неприменимых делается новая оценка величины *L*.

Общую оценочную величину затрат на реализацию СЗИ обозначим как *C*. Под допустимым риском будем понимать риск, потери по которому не превышают определенной суммы прибыли, установленной в организации. Определим следующие условия:

1) минимальное значение *C* должно быть равно *L* для выполнения требований законодательства;

2) если $C < L + R$, то процесс внедрения мер СЗИ на этом шаге пропускается и осуществляется мониторинг системы;

2) если $C \geq L + R$, то необходимо разрабатывать программу мероприятий по снижению ущерба при реализации угроз;

Комплекс таких мероприятий, организационных и технических, называется мероприятиями СЗИ. Каждое мероприятие из СЗИ будет оказывать определенное влияние на совокупность угроз. С оставим матрицу СЗИ с учетом применения требований законодательства *L*.

	L_1	L_2	…	L_l
T_1	l_{11}	l_{12}	…	l_{1l}
T_2	l_{21}	l_{21}	…	l_{2l}
…	…	…	…	
T_g	l_{g1}	l_{g2}	…	l_{gl}

Исходя из матрицы СЗИ, можно рассчитать ущерб от угрозы T_h после внедрения l мероприятий СЗИ:

$$T_h^{'} = \sum_{i=1}^{l} l_{hi} \times T_h \qquad (11)$$

где l_{hi} – воздействие определенных законом мер L_i на угрозу T_h.

После внедрения СЗИ вероятность реализации угрозы T_h изменяется, принимая вид p'_h. Таким образом, после внедрения мер, определенных законодательством, меняется и оценочная величина риска R'_h. Далее необходимо провести разработку мероприятий по защите системы исходя из реализованных мер с учетом обновленных величин от реализации угроз T'_h. С учетом этих мероприятий итоговая матрица мер СЗИ будет выглядеть так:

	D_1	D_2	...	D_l
$T_1^{'}$	d_{11}	d_{12}	...	d_{1l}
$T_2^{'}$	d_{21}	d_{21}	...	d_{2l}
...	...	...	...	
$T_g^{'}$	d_{g1}	d_{g2}	...	d_{gl}

Исходя из матрицы СЗИ, можно рассчитать ущерб от угрозы T'_h после внедрения l мероприятий СЗИ:

$$T_h^{''} = \sum_{i=1}^{l} d_{hi} \times T_h^{'}$$

где d_{hi} – воздействие СЗИ на угрозу T'_h.

Соответственно меняется и оценочная величина риска R''_h.

Выводы

Перед внедрением мер важно рассчитать стоимость их реализации, исходя из выделенного бюджета ИБ и требований законодательства. Если стоимость мероприятий превышает допустимые расходы – необходимо скорректировать риски: отложить маловероятные на следующий цикл, а наиболее опасные риски понизить в рамках текущего бюджета.

Процесс управления рисками будет происходить до тех пор, пока значение общей оценочной величины риска R не опустится ниже допустимого уровня, установленного в организации, и стоимость внедрения таких мероприятий не превысит допустимые расходы.

Предложенная модель позволяет выполнить анализ и оценить риски информационной безопасности. Установив допустимый уровень общей оценочной величины риска, принимается решение о необходимости внедрения СЗИ. Процесс происходит до тех пор, пока оценочная величина риска не примет допустимый уровень.

Модель была использована для анализа рисков АСУ ТП газодобывающего предприятия, что позволило учесть влияние каждой уязвимости и на компоненты каждого уровня АСУ ТП и на связь между ними. Благодаря этой особенности были сделаны расчеты ущерба при некорректном функционировании всей системы в результате реализации даже одной угрозы.

Примечания

1. Сергеев Н. Е., Добровольский С. В. АСУ ТП цеха добычи нефти и газа // Известия ЮФУ. Технические науки. 2000. — №1. — С. 159

2. Shearer J., Symantec. W32.Stuxnet. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

3. Symantec Corporation, Duqu: следующий Stuxnet. URL: http://www.symantec.com/ru/ru/outbreak/?id=stuxnet

4. Gostev À., Securelist, The Flame: Questions and Answers. URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

5. Кречетова А., Forbes Staff, Petya в «Роснефти»: нефтяная компания пожаловалась на мощную хакерскую атаку. URL: http://www.forbes.ru/kompanii/346997-rosneft-pozhalovalas-na-moshchnuyu-hakerskuyu-ataku

6. ProSoft, Разбудит ли вирус WannaCry промышленную Кибербезопасность. URL: https://tp.prosoft.ru/news/obzory-issledovaniya-analitika/175645/

7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

8. Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Рос-

сийской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

9. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Доклады ТУСУР. 2013. — №2 (28). — С. 112-115

10. Крымский В. Г., Жалбеков И. М., Имильбаев Р. Р., Юнусов А. Р. Автоматизация управления технологическими процессами в газораспределительных сетях: проблемы, тенденции и перспективы // Электротехнические и информационные комплексы и системы. 2013. — №2. — С. 70-79

11. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. — №1 (9). — С. 73-79

12. Арьков П. А. Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия ЮФУ. Технические науки. 2008. — №8. — С. 30-36

13. Данилова Е.А., Хохоля А.С., Золотарев В.В. Построение и анализ математических моделей эффективности и безопасности автоматизированных систем // Актуальные проблемы авиации и космонавтики. 2010. — №6. — С. 392-393

14. Варлатая С.К., Шаханова М.В. Математические модели динамики возникновения и реализации угроз информационной безопасности // Доклады ТУСУР. 2012. — №1-2 (25). — С. 7-11

15. Бондарь И.В. Методика построения модели угроз безопасности информации для автоматизированных систем // Вестник СибГУ им. М.Ф. Решетнева. 2012. — №3 (43). — С. 7-10

16. Миронова В. Г., Шелупанов А. А., Сопов М. А. Сети Петри-Маркова как инструмент создания аналитических моделей для основных видов несанкционированного доступа в информационной системе // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. — №. 1-2 (25). — С. 20-24

17. Меньших В.В., Петрова Е.В. Теоретическое обоснование и Синтез математической модели защищенной информационной системы ОВД как сети автоматов // Вестник ВИ МВД России. 2010. — №3. — С. 134-143

18. Ефимов Б. И. Применение алгоритмов теории графов для решения задач, связанных с обеспечением информационной безопасности в системах принятия решений //Системы управления и информационные технологии. 2009. Т. 35. — №. 1.3. — С. 342-346

19. Булдакова Т. И., Миков Д. А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2013. — №11. — С. 295-310

20. Захаров И.В., Забузов В.С., Фомин С.И., Фомин С.И., Эсаулов К.А. Способ априорной оценки возможности идентификации пользователей веб-ресурсов на основе энтропийного подхода // Современные проблемы науки и образования. 2014. — № 1. — С. 1-7

21. Чуркин Г. М., Великанов А. М., Тырин Е. А. К вопросу о выборе средств автоматизации АСУ ТП // Вестник СГТУ. 2013. — №1 (70). — С. 151-158

22. Духвалов А.П. Кибератаки на критически важные объекты вероятная причина катастроф // Вопросы кибербезопасности. 2014. — №3 (4). — С. 50-53

23. Дружинин Е., Карпов И., Гнедин Е., Бойко И., Симонова Ю. Безопасность АСУ ТП в цифрах // Москва: Positive Technologies, 2016. — С. 9

24. Пищик Б.Н. Безопасность АСУ ТП // ЖВТ. 2013. — №.5 — С. 170-175

25. Баранова Е.К., Мальцева А.Н. Анализ рисков информационной безопасности для малого и среднего бизнеса // Директор по безопасности. 2015. — №9 (69). — С. 58-63

References

1. Sergeev N. E., Dobrovolskii S. V. ASU TP tsekha dobychi nefti i gaza [APCS plant oil and gas] // Izvestiia IuFU. Tekhnicheskie nauki [Proceedings of the SFU. Technical science]. 2000. №1. P.159

2. Shearer J., Symantec. W32.Stuxnet. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

3. Symantec Corporation, Duqu: sleduiushchii Stuxnet. URL: http://www.symantec.com/ru/ru/outbreak/?id=stuxnet

4. Gostev À., Securelist, The Flame: Questions and Answers. URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

5. Krechetova A., Forbes Staff, Petya v «Rosnefti»: neftianaia kompaniia pozhalovalas na moshchnuiu khakerskuiu ataku [Petya in Rosneft: the oil company complained of a powerful hacker attack]. URL: http://www.forbes.ru/kompanii/346997-rosneft-pozhalovalas-na-moshchnuyu-hakerskuyu-ataku

6. ProSoft, Razbudit li virus WannaCry promyshlennuiu Kiberbezopasnost [Will the WannaCry virus wake industrial Cybersecurity?]. URL: https://tp.prosoft.ru/news/obzory-issledovaniya-analitika/175645/

7. Federalnyi zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [On the Security of the Critical Information Infrastructure of the Russian Federation]

8. Federalnyi zakon ot 26.07.2017 № 194-FZ «O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i statiu 151 Ugolovno-protsessualnogo kodeksa Rossiiskoi Federatsii v sviazi s priniatiem Federalnogo zakona «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation in connection with the adoption of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation"]

9. Kirsanov S.V. Metod otsenki ugroz informatsionnoi bezopasnosti ASU TP gazovoi otrasli [The method of assessing threats to information security of the automated process control system of the gas industry] // Doklady TUSUR [TUSUR reports]. 2013. №2 (28). P.112-115

10. Krymskii V. G., Zhalbekov I. M., Imilbaev R. R., Iunusov A. R. Avtomatizatsiia upravleniia tekhnologicheskimi protsessami v gazoraspredelitelnykh setiakh: problemy, tendentsii i perspektivy [Automation of process control in gas distribution networks: problems, trends and prospects] // Elektrotekhnicheskie i informatsionnye kompleksy i sistemy [Electrical and information complexes and systems]. 2013. №2. P.70-79

11. Baranova E.K. Metodiki analiza i otsenki riskov informatsionnoi bezopasnosti [Methods of analysis and assessment of information security risks] // Obrazovatelnye resursy i tekhnologii [Educational resources and technologies]. 2015. №1 (9). P.73-79

12. Arkov P. A. Kompleks modelei dlia poiska optimalnogo proekta sistemy zashchity informatsii [A set of models for finding the optimal project of an information security system] // Izvestiia IuFU. Tekhnicheskie nauki [Proceedings of the SFU. Technical science]. 2008. №8. P.30-36

13. Danilova E.A., Khokholia A.S., Zolotarev V.V. Postroenie i analiz matematicheskikh modelei effektivnosti i bezopasnosti avtomatizirovannykh system [Construction and analysis of mathematical models of efficiency and safety of automated systems] // Aktualnye problemy aviatsii i kosmonavtiki [Actual problems of aviation and cosmonautics]. 2010. №6. P.392-393

14. Varlataia S.K., Shakhanova M.V. Matematicheskie modeli dinamiki vozniknoveniia i realizatsii ugroz informatsionnoi bezopasnosti [Mathematical models of the dynamics of the emergence and implementation of threats to information security] // Doklady TUSUR [TUSUR reports]. 2012. №1-2 (25). P.7-11

15. Bondar I.V. Metodika postroeniia modeli ugroz bezopasnosti informatsii dlia avtomatizirovannykh system [The method of constructing a model of information security threats for automated systems] // Vestnik SibGU im. M.F. Reshetneva [Bulletin of SibSU. M.F. Reshetnev]. 2012. №3 (43). P.7-10

16. Mironova V. G., Shelupanov A. A., Sopov M. A. Seti Petri-Markova kak instrument sozdaniia analiticheskikh modelei dlia osnovnykh vidov nesanktsionirovannogo dostupa v informatsionnoi sisteme [Petri-Markov networks as a tool for creating analytical models for the main types of unauthorized access in the information system] // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics]. 2012. №. 1-2 (25). P.20-24

17. Menshikh Valerii Vladimirovich, Petrova Elena Vladilenovna Teoreticheskoe obosnovanie i Sintez matematicheskoi modeli zashchishchennoi informatsionnoi sistemy OVD kak seti avtomatov [Theoretical justification and Synthesis of the mathematical model of the protected information system of ATS as a network of automats] // Vestnik VI MVD Rossii [Bulletin of the Ministry of Internal Affairs of Russia]. 2010. №3. P.134-143

18. Efimov B. I. Primenenie algoritmov teorii grafov dlia resheniia zadach, sviazannykh s obespecheniem informatsionnoi bezopasnosti v sistemakh priniatiia reshenii [Application of algorithms of graph theory for solving problems related to ensuring information security in decision-making systems] // Sistemy upravleniia i informatsionnye tekhnologii [Control Systems and Information Technology]. 2009. T. 35. №. 1.3. P. 342-346

19. Buldakova T. I., Mikov D. A. Otsenka informatsionnykh riskov v avtomatizirovannykh sistemakh s pomoshchiu neiro-nechetkoi modeli [Assessment of information risks in automated systems using a neural-fuzzy model] // Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana [Science and Education: a scientific edition of the MSTU. N.E. Bauman]. 2013. №11. P.295-310

20. Zakharov I.V., Zabuzov V.S., Fomin S.I., Fomin S.I., Esaulov K.A. Sposob apriornoi otsenki vozmozhnosti identifikatsii polzovatelei veb-resursov na osnove entropiinogo podkhoda [A method of a

priori assessment of the possibility of identifying users of web resources based on the entropy approach] // Sovremennye problemy nauki i obrazovaniia [Modern problems of science and education]. 2014. № 1. P.1-7

21. Churkin G. M., Velikanov A. M., Tyrin E. A. K voprosu o vybore sredstv avtomatizatsii ASU TP [On the issue of choosing automation means for process control systems] // Vestnik SGTU [Bulletin of the CSTU]. 2013. №1 (70). P.151-158

22. Dukhvalov A.P. Kiberataki na kriticheski vazhnye obieekty veroiatnaia prichina katastrof [Cyberattacks on critical objects probable cause of accidents] // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. №3 (4). P.50-53

23. Druzhinin E., Karpov I., Gnedin E., Boiko I., Simonova Iu. Bezopasnost ASU TP v tsifrakh [Safety of automated control systems in figures] // Moskva: Positive Technologies, 2016. P.9

24. Pishchik B.N. Bezopasnost ASU TP [Safety of automated process control system] // ZhVT. 2013. №. P.170-175

25. Baranova E.K., Maltseva A.N. Analiz riskov informatsionnoi bezopasnosti dlia malogo i srednego biznesa [Analysis of information security risks for small and medium businesses] // Direktor po bezopasnosti [Director of Security]. 2015. №9 (69). P.58-63

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: azaharov@utmn.ru

РИМША Андрей Сергеевич, аспирант кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaAndrew@gmail.com

ХАРЧЕНКО Анастасия Михайловна, инженер ИТ отдела КИПиА и АСУ ТП АО «Ачимгаз». 629303, г. Новый Уренгой. мкр. Советский 7/2а. E-mail: Kharchenkoam.86@gmail.com

ЗУЛЬКАРНЕЕВ Искандер Рашитович, старший преподаватель кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: i.r.zulkarneev@utmn.ru

ZAKHAROV Alexander, Doctor of Technical Sciences, Professor of the Department of Information Security. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: azaharov@utmn.ru

RIMSHA Andrew, post-graduate student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaAndrew@gmail.com

KHARCHENKO Anastasia, IT Engineer of the Instrumentation and Control Systems Department of Achimgaz JSC. Bld. 7/2a, Soviet Mdst., Noviy Urengoy, 629303. E-mail: Kharchenkoam.86@gmail.com

ZULKARNEYEV Iskander, senior lecturer of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: i.r.zulkarneev@utmn.ru

УДК 004.4.056 + 681.518 + 005.334 Вестник УрФО № 3(25) / 2017, с. 34–42

Баринов А. Е., Скурлаев С. В., Соколов А. Н.

МЕТОДИКА ОЦЕНКИ РИСКОВ, ВЫЗВАННЫХ УЯЗВИМОСТЯМИ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

В последнее время существенно участились атаки на автоматизированные системы управления технологическими процессами (АСУ ТП), вызванные уязвимостями в их программном обеспечении (ПО). Однако специфика АСУ ТП такова, что зачастую невозможно мгновенно установить исправление ПО даже при его наличии, а внеплановая остановка АСУ ТП для обслуживания является затратным мероприятием. Поэтому актуальным является вопрос оценки критичности уязвимостей в целях планирования установки исправлений. В статье описана модель влияния информационных потоков на технологические процессы (ТП) в АСУ ТП и предложена методика оценки критичности уязвимости, содержащая временной параметр, а также степень влияния на управляемые технологические функции.

Ключевые слова: *информационная безопасность АСУ ТП, метрика, уязвимость, оценка рисков, управление рисками, управление исправлениями, информационный поток.*

Barinov A. E., Skurlaev S. V., Sokolov A. N.

METHOD FOR RISK ASSESSMENT CAUSED BY VULNERABILITIES IN ICS SOFTWARE

Recently, attacks on ICS and SCADA caused by vulnerabilities in software have increased significantly. However, the specificity of ICS is that it is often impossible to immediately install the patch, even if it exists, and the unplanned stop of process control systems for maintenance is a costly event. Therefore, the issue of assessing the criticality of vulnerabilities for the purpose of planning the installation of patches is relevant. This paper describes the model of the influence of information flows on industrial process in the ICS and suggests a methodology for assessing the criticality of the vulnerability, containing time parameters, and the degree of influence on managed technological functions.

Keywords: *ICS Security, metric, vulnerability, risk assessment, risk management, patch management, information flow.*

АСУ ТП довольно давно используются во многих отраслях промышленности, однако актуальность их информационной безопасности существенно возросла лишь в последнее время с учащением инцидентов в промышленных системах. Обеспечение безопасности информации АСУ ТП наиболее критично для предприятий топливно-энергетического комплекса, поскольку инциденты информационной безопасности на таких объектах могут привести не только к серьезным экономическим последствиям (нарушение поставок нефти и газа, перебои в электроснабжении населения и т.п.), но и к экологическим или гуманитарным катастрофам. Кроме того, уязвимыми являются различные транспортные системы[1], металлургические, химические, ядерные производства, инфраструктура связи и т.п. Приведем лишь некоторые известные примеры кибератак на АСУ ТП, приведших к значительным негативным последствиям:

• Stuxnet (первая атака на АСУ ТП, поразившая ядерные объекты Ирана)[2];

• Crouching Yeti (атака на предприятия энергетики, машиностроения, фармацевтического сектора США и стран Евросоюза с целью кражи конфиденциальной информации о ТП)[3];

• BlackEnergy (семейство атак на украинскую энергетическую систему, вызвавших её сбой)[4].

Некоторые из угроз реализуются в промышленных сетях в силу их недостаточной изоляции от корпоративных сетей (BlackEnergy)[4] или через внешние носители (Stuxnet)[2]. Кроме того, уязвимости могут возникать непосредственно в оборудовании промышленных сетей: PLC, HMI и т.д. По имеющимся данным[5], за 2016 год обнаружено свыше 180 таких уязвимостей.

Специфика обеспечения информационной безопасности АСУ ТП в отличие от корпоративных систем имеет следующие особенности:

• индустриальные информационные системы могут работать годами, их остановка либо неприемлема, либо невозможна. Это усложняет установку исправлений для ПО с целью устранения уязвимостей;

• каждая АСУ ТП специфична по критичности ТП, степени потенциального ущерба и т.д.;

• многие АСУ ТП используют закрытые проприетарные протоколы, их производители либо не реализуют адекватных политик поиска, устранения и сопровождения уязвимостей, либо соответствующие релизы сняты с поддержки.

Вышеперечисленное приводит к тому, что при обеспечении информационной безопасности АСУ ТП необходимы постоянный аудит и оценка рисков.

Установка исправления является критичным процессом, требующим принятий целого комплекса мер по тестированию исправления, вводу его в АСУ ТП, анализа необходимости остановки ТП и т.д.

Известны рекомендации[6], где предложен алгоритм принятия решения по установке исправления (рис. 1). Однако предложенный алгоритм не учитывает снижение эффективности системы при применении обходного решения, а также не предоставляет аналитического аппарата для проведения анализа рисков информационной безопасности и его сопоставления с операционными рисками.

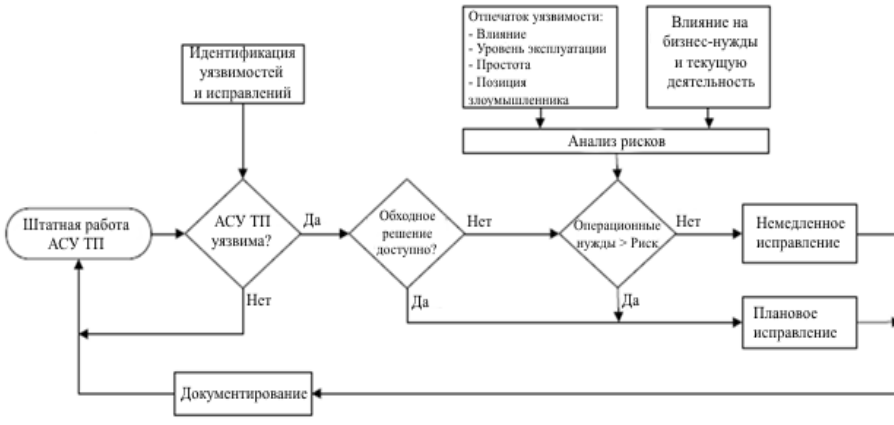

Рис. 1. Алгоритм принятия решения об установке исправления

Документ[6] вводит понятие отпечаток уязвимости на основе таких метрик, как:

• *уровень эксплуатации (D)* – доля узлов, подверженных рассматриваемой уязвимости (при этом допускается применение весов для определения приоритетов, подверженных уязвимости узлов);

• *влияние (I)* – степень контроля над системой и степень потенциально наносимого ей ущерба;

• *позиция злоумышленника (E)* – (включая его местоположение по отношению к периметру, требуемым привилегиям и т.д.);

• *простота (S)* – степень доступности средств для эксплуатации уязвимости и степень навыков злоумышленника.

3) описанный подход не сопоставляет время обнаружения уязвимости и расписание сервисных окон с целью определения оптимального момента для устранения уязвимостей.

Целью настоящей работы является построение модели оценки критичности уязвимости для формализации процесса её устранения.

В результате анализа процессов обработки информации в АСУ ТП и информационных потоков[7,8] разработана модель АСУ ТП (рис. 2), представленная в виде диаграммы классов UML.

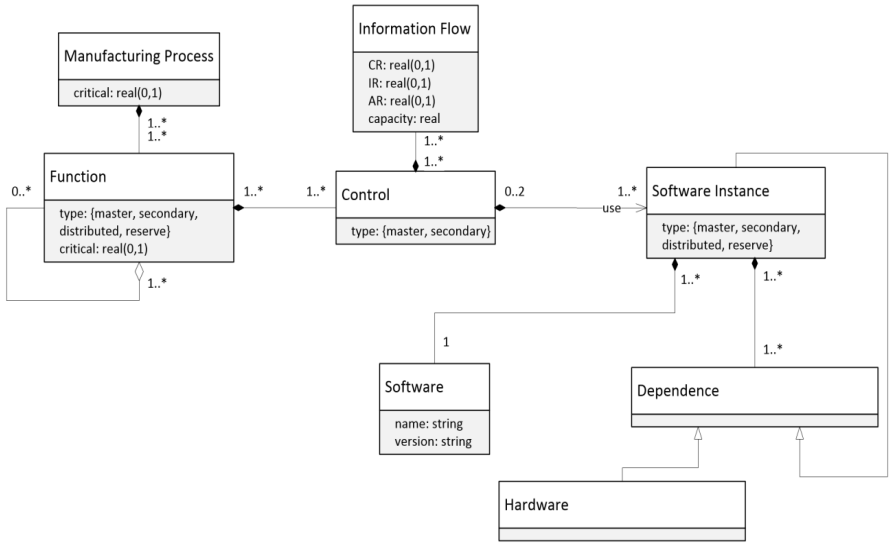

Рис. 2. Модель АСУ ТП

При формировании значений для этих составляющих документ[6] полагается на экспертную оценку значений по шкале с градациями: *низкая, средняя, высокая*. Это не позволяет полноценно выполнить процесс анализа рисков и сопоставить его с функциональными нуждами АСУ ТП. Поэтому очевидны следующие недостатки:

1) низкая степень гранулярности показателей не даёт возможности приоритезации для двух уязвимостей со сходными показателями, появившихся почти одновременно;

2) экспертная оценка показателей не позволяет адекватно сопоставить риск, вносимый рассматриваемыми уязвимостями, и риск функциональных нарушений в АСУ ТП. Таким образом, сложно оценить, какие именно производственные функции и процессы деградируют, а также степень их деградации. Кроме того, для сопоставления с числовыми значениями используется устаревший стандарт CVSS 2.0;

Под технологическим процессом (Manufacturing Process) будем понимать относительно автономную часть производства, выполняющую совокупность функций, направленных на реализацию продукта. Промышленное предприятие может реализовывать несколько независимых ТП, для которых, как правило, можно выделить независимые АСУ ТП. Критичность (Critical) отдельно взятого ТП может характеризовать степень ущерба при нарушении его нормальной работоспособности.

В настоящее время крупные страны имеют рекомендательные документы по классификации АСУ ТП. В частности, в России и США подобная классификация производится по величине потенциального финансового ущерба и количеству потенциальных жертв. В рамках представленной модели оценку предлагается производить величиной, верхнее значение которой соответствует максимально возможному уровню критичности.

Функция (function) в представленной модели определена как физический элемент технологического процесса (включая производственное, контрольное оборудование и т.п.). Функции образуют иерархическую структуру. Такой подход обеспечивает:

• возможность разбиения каждой функции верхнего уровня (например, подачи железной руды в доменном производстве) на более простые функции, контролируемые отдельными автоматизированными системами (например, очистку руды и т.п.);

• повторяемость использования функций (например, общие производственные функции (электроснабжение, вентиляция) могут обслуживать несколько технологических процессов). Эти общие функции считаются основными для того же уровня, который они обслуживают.

В модель также включены функции:

• *резервные* (reserve) – задействуются при отказе основных (master);

• *распределённые* (distributed) – работают параллельно (например, несколько одновременно работающих линий подачи);

• *вспомогательные* (secondary) – нарушение их работы на некоторый интервал времени не оказывает существенного влияния на ТП. К таким функциям можно отнести, например, функцию мониторинга температуры технологического оборудования.

Под *элементом контроля* (control) понимается промышленный контроллер или его автономная часть, принимающая сигналы от контролируемых функций и передающая им команды управления. При этом функции верхнего уровня контролируются программными средствами, обеспечивающими координацию всего ТП, а функции низовой автоматизации – программным обеспечением исполняющих устройств и средств, ими управляющих. Вполне очевидно, что элемент контроля может контролировать несколько функций, а одна функция может принимать сигналы (или отправлять данные) более чем одному элементу контроля. Элемент контроля для исполнения своих функций создаёт *информационные потоки* (Information Flow), обрабатываемые программным обеспечением или получаемые от него для передачи другим элементам контроля или для хранения с целью повторного использования. В свою очередь элемент контроля использует некоторое множество *установок ПО* (Software Instance) определённых версий и конфигураций. При этом каждая установка ПО может обслуживать не более двух элементов контроля (основной и резервный) или не обслуживать ни один, если является зависимостью (различное обеспечивающее ПО, например, СУБД для SCADA, операционные системы и т.п., и оборудование, на которое установлено ПО). Элемент контроля может быть *основным* (master), который непосредственно обслуживает производственные функции или *вспомогательным* (secondary). Наиболее очевидный пример вспомогательного элемента контроля – самодиагностика систем.

В понятие *информационный поток* (Information Flow) входят:

• поток данных, формируемый функциями или элементом контроля;

• поток данных, формируемый командами, получаемыми от ПО;

• набор данных, хранящихся непосредственно на контролирующем элементе.

Информационные потоки предназначаются для обмена информацией между различными элементами контроля ТП или реализации элементами контроля своих внутренних функций (например, данные о текущем состоянии ТП, хранящиеся внутри контроллера, его конфигурация и т.д.). Очевидно, что один элемент контроля может производить и потреблять разнородные информационные потоки, например основной поток команд для оборудования, данные о текущем состоянии, информацию о структуре АСУ ТП для взаимодействия с другими элементами контроля и т.д. Можно отметить, что информационная ёмкость (capacity) этих потоков является различной, также как и требования по обеспечению различных метрик информационной безопасности: *конфиденциальности* (CR), *целостности* (IR) и *доступности* (AR). Любая информация в АСУ ТП может быть представлена в виде некоторого информационного потока. Кроме того, получать и использовать один информационный поток могут несколько контролирующих элементов.

Управляющую роль для элемента контроля исполняет *установка ПО* (Software Instance). Установка ПО реализует свою работу посредством ПО (Software) определённой версии и конфигурации, а также и его зависимостей. Установка ПО может быть *основной* (master), если её отказ приводит к нарушению работы соответствующего элемента контроля, *резервной* (reserve) и *параллельной* по аналогии с функциями (distributed). С целью

упрощения модели характеристики оборудования детально не анализируются.

Выше отмечено, что к составляющим отпечатка уязвимости относятся такие метрики как *уровень эксплуатации* (D), *влияние* (I) , *позиция злоумышленника* (E), *простота* (S).

Стоит отметить, что две последние метрики отражают характеристики злоумышленника и могут быть относительно легко сформированы из описания данных уязвимости в CVSS 3.0. Первые две метрики являются более сложными. Рассмотрим процесс формирования этих метрик. Здесь и далее будем полагать, что значение 0 означает неприменимость метрики или отсутствие риска, а 1 – полный контроль над системой со стороны злоумышленника.

Уязвимое ПО может использоваться в работе функции только посредством контролирующих элементов, а контролирующий элемент, в свою очередь, может обслуживать разные по критичности функции и различные по требованиям информационной безопасности информационные потоки. Поэтому параметры влияния и уровень эксплуатации должны рассчитываться отдельно для каждого контролирующего элемента.

Для каждого информационного потока характерно 3 метрики информационной безопасности: *конфиденциальность* (CR), *целостность* (IR) и *доступность* (AR). Оценка критичности каждой из этих метрик необходима для оценки общего влияния уязвимости на АСУ ТП. Каждая метрика информационного потока оказывает влияние на характеристики эффективности *производственных функций f(j)*. Обозначим *показатели эффективности производственных функций как* $p_{if(j)}$. Каждый показатель $p_{if(j)}$ зависит от параметров информационных потоков, которые на него влияют, а также имеет предельное значение $p_{if(j)t}$, при котором производственная функция деградирует. Поскольку каждый информационный поток входит в несколько производственных функций, а информационная ёмкость потока может меняться со временем эксплуатации системы, задача определения оптимальных параметров информационных потоков носит статистический и оптимизационный характер. Определим базовые параметры информационных потоков и метрики информационной безопасности, которые они формируют.

Метрика *доступности* (AR) – является одной из самых очевидных и определяет уровень доступности как долю времени работы системы с заданными характеристиками. Эта метрика формируется на этапе проектировании системы, поэтому при оценке величины AR можно опираться на проектные значения.[9] Исследование зависимости показателей эффективности производственных функций от значения метрики доступности является широко исследованным вопросом, например[7].

Метрика *целостности* (IR) – может быть представлена на основе двух составляющих: минимальной *доли информации*, которая является *достаточной для управления ТП* ($\delta_{\varepsilon m}$) и *способности информации к восстановлению* ($\delta_{\varepsilon r}$). Формирование первой составляющей ($\delta_{\varepsilon m}$) можно наглядно продемонстрировать на следующем примере: при ежесекундном измерении температуры для получения сведений о динамике процесса зачастую достаточно одного из десяти измерений, следовательно, $\delta_{\varepsilon m} = 0{,}1$. Вторая составляющая ($\delta_{\varepsilon r}$) характеризует способность информации восстанавливаться либо за счёт встроенной избыточности (на уровне логики или избыточного кодирования), либо за счёт переотправки без потери производительности. В итоге, значение метрики IR можно определить как

$$IR = \delta_{\varepsilon m} \times \delta_{\varepsilon r}. \quad (1)$$

Метрика *конфиденциальности* (CR) является одной из самых сложных и чаще всего оценивается экспертным путём. Имеются работы, оценивающие конфиденциальность только на основе вероятностных характеристик[10] или стоимости информации. Оба метода не в полной мере могут подходить для АСУ ТП, так как для большинства ТП нарушение конфиденциальности информации не является критичным в краткосрочной перспективе (по сравнению с доступностью). С другой стороны, получая доступ к технологической информации, злоумышленник может получить не только информацию о ноу-хау, но и изучить структуру системы, что при нечастых исправлениях в АСУ ТП может облегчить ему дальнейшие атаки. Поэтому в предположении, что информация устаревает по экспоненте[11], определим следующие параметры:

• k – доля полезной информации в текущем информационном потоке. К полезной не относится служебная информация, по которой нельзя получить сведения о структуре системы, информация о ноу-хау и т.д. (оценивается экспертно);

a – постоянная устаревания информации;

CR_B – базовый критерий конфиденциаль-

ности, определённый для данного информационного потока исходя из требований организации.

Вводя нормировку $\{k;\ \alpha;\ CR_B\} \in [0;1]$, получим значение метрики CR в виде

$$CR = \frac{\log_\alpha k \int_{t_c}^{t_i} v(t)dt + k\int_{t_c}^{t_i}\left(\int_{t_c}^{t} v(t)dt\right)\left(1-\alpha^t\right)dt}{(t_i - t_c + 1\log_\alpha k)\int_{t_c}^{t_i} v(t)dt} \times CR_B, \qquad (2)$$

где t_c – текущее время, t_i – предполагаемое время прекращения угрозы утечки информации, $v(t)$ – потенциальная скорость утечки информации, определяемая из статистических наблюдений за пропускной способностью потенциального канала утечки, учитывая его ёмкость и прогнозируемую загруженность.

Тогда оценка влияния уязвимости I_{if} на конкретный информационный поток *if* может быть выполнена, как[12]

$$I_{if}=1-(1-CR\times R_{CR})(1-IR\times R_{IR})(1-AR\times R_{AR}), \qquad (3)$$

где IR и CR определены, соответственно, в (1) и (2), а веса ранее определенных метрик R_{CR}, R_{IR}, R_{AR} связаны соотношением[13]

$$R_{CR}+R_{IR}+R_{AR}=1.$$

Итоговую оценку влияния I_m для m-го элемента контроля можно выполнить исходя из известного соотношения

$$I_m=1-\Pi^n_{if=1}(1-I_{if}), \qquad (4)$$

где n – число информационных потоков, а значение I_{if} определено в (3).

Очевидно, что влияние уязвимости тем выше, чем

- большее число узлов, реализующих ту или иную функцию, подвержено уязвимости,
- большее число функций обслуживается уязвимым ПО.

В этом случае *уровень эксплуатации* D_m для m-го элемента контроля может быть рассчитан как

$$D_m = D_{fm} \times D_{sm}, \qquad (5)$$

где D_{fm} – уровень функциональной эксплуатации, а D_{sm} – уровень программной эксплуатации.

На рис. 2 видно, что функция представляет собой древовидную структуру. Критичность основной функции D_i технологического процесса определяется его критичностью $T \in [0;1]$. Для формирования критичности конкретной функции дерево обходится вниз.

Если входящая в функцию подфункция является *основной*, то её критичность соответствует критичности функции верхнего уровня, (например конвейер – критичность всех элементов одинакова, т.к. остановка одного приводит к остановке всего конвейера).

Если функция f_i реализуется набором параллельных функций, то критичность каждой из них будет являться $D_i=m/n$, где n – число параллельных подфункций, реализующих данную функцию, а m – их минимальное число, необходимое для реализации функции на необходимом уровне.

Если функция является *вспомогательной* (например, мониторинг), то оценивается его степень влияния на основную функцию k, а критичность вспомогательной функции определяется как kD_i.

Для *резервной* функции критичность определяется как $F(t_i) \times D_i$,где $F(t_i)$ – функция распределения отказов резервируемого элемента, полученная статистически. Для резервируемого элемента, критичность, соответственно, имеет вид $(1 – F(t_i)) \times D_i$. При этом если функция оказывается *подфункцией* для нескольких технологических процессов или функций, то её критичность определяется максимальной из расчётных критичностей. Если один контролирующий элемент управляет несколькими функциями с разной степенью критичности, то уровень функциональной эксплуатации может быть рассчитан, как

$$D_{fm}=\Pi^n_{i=1}(1-D_i).$$

Программное обеспечение также можно представить древовидной структурой. Расчет уровня программной эксплуатации D_{si} можно выполнить по следующему алгоритму:

1) если уязвимое ПО является *основным* компонентом, подверженным уязвимости, то уровень эксплуатации D_{si} считается равным 1;

2) если основной компонент резервируется другим компонентом на другом стеке ПО, то его уровень эксплуатации $D_{si}= m/n$, где m – сумма уровней эксплуатации уязвимых стеков ПО, а n – число суммарное число компонентов резервных и резервируемых;

3) если ПО является распределенным, то уровень программной эксплуатации $D_{si} \times F_s(t_i)$ соответствует доле установок ПО, потенциально подверженных атаке на основе статистических наблюдений;

4) если установка ПО – *вспомогательная* (например, для мониторинга состояния сервера, на котором установлено ПО управления АСУ ТП), то его влияние может быть оценено через коэффициент, то есть kD_{si};

5) если установка ПО – *резервная*, то уровень его программной эксплуатации может быть рассчитан как $D_{si} \times F_{se}(t_i)$, где $F_{se}(t_i)$ – распределение отказов основных компонентов,

и, соответственно, переходов на резервный компонент;

6) если установка ПО является *зависимостью* для нескольких стеков ПО, то уровень её программной эксплуатации определяется максимальным из уровней.

Итоговый уровень эксплуатации для элемента контроля определяется значением, появившимся на вершине дерева при обходе его снизу вверх.

Простота (S) является характеристикой не инфраструктуры, а непосредственно уязвимости. Исходя из анализа[6,12], можно выразить *простоту* как

$$S = (AC - 0{,}44) \times 1{,}52 + (ECM \times RC - 0{,}83) \times 6{,}14, \quad (6)$$

где AC – показатель сложности проведения атаки, ECM – зрелость кода для эксплуатации уязвимости, RC – степень детальности описания уязвимости. Указанные значения берутся из описаний уязвимостей в репозиториях и интерпретируются в соответствии с CVSS 3.0, либо модифицируются на уровне организации путём экспертных оценок. Переводные коэффициенты получены с учетом того, что параметр S находится в диапазоне [0;1].

Аналогично параметру S, выразим *позицию злоумышленника (E)* как

$$E = (AV \times PR \times UI - 0{,}03) \times 1{,}71, \quad (7)$$

где AV – вектор атаки, PR – требуемые для эксплуатации уязвимости привилегии, UI – требуемое для эксплуатации уязвимости пользовательское взаимодействие.

Таким образом, для каждого элемента контроля имеем 4 параметра *I, D, E, S*, рассчитанных для конкретной уязвимости в (4), (5), (6) и (7).

Оценку риска для j-го элемента контроля, подверженного конкретной уязвимости, можно оценить при этом как[14]:

$$C_j = \frac{\lfloor 10I_j \rfloor + \lfloor 10D_j \rfloor}{18} \times \frac{\lfloor 10S \rfloor + \lfloor 10E \rfloor}{18}.$$

Суммарная оценка риска по всем элементам контроля вычисляется как

$$C = \frac{\lfloor 10S \rfloor + \lfloor 10E \rfloor}{18} \times \sum_{j=1}^{n} \frac{\lfloor 10I_j \rfloor + \lfloor 10D_j \rfloor}{18},$$

где n – число элементов, контролирующих стеки, ПО которых подвержены данной уязвимости.

Таким образом, возможность расчёта риска для отдельно взятого элемента контроля позволяет выделить те участки инфраструктуры, где устранение уязвимости необходимо выполнить в первую очередь. Разработанная методика при этом позволяет провести оценку влияния уязвимостей программного обеспечения на информационную безопасность АСУ ТП с целью их приоритезации и последующего устранения. Представленная модель является многопараметрической. В качестве одного из параметров базовых аналитических выражений используется параметр t_i – предполагаемый момент времени прекращения угрозы утечки информации. Он позволяет оценить интервал времени воздействия потенциальной угрозы с момента возникновения до сервисных окон обслуживания, если для установки исправления требуется остановка технологического процесса. Такой подход позволяет адекватно спланировать установку исправлений и ответить на вопрос, нужно ли проводить исправления в срочном порядке или следует выбрать для этого соответствующее сервисное окно.

Оценки параметров эффективности производственных функций, используемые в модели, позволяют также оценить критичность уязвимости в зависимости от степени деградации производственных функций. Перспективным направлением моделирования представляется оценка взаимного влияния уязвимостей, когда в системе действует несколько уязвимостей низкого риска, но совместное их воздействие может спровоцировать высокий риск для инфраструктуры. Имеющиеся в этой области работы либо не отражают специфику АСУ ТП[13], либо оценивают влияние уязвимостей на количественных характеристиках без учёта особенностей применимости к конкретной системе.

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

Примечания

1. Андрей Заикин. Почему защита АСУ ТП сегодня стала критически важной? [Электронный ресурс] // https://www.securitylab.ru/analytics/484730.php. (Дата обращения: 30.10.2017).

2. Keizer, Greg. Is Stuxnet the 'best' malware ever? Infoworld. 16 September 2010. [Электронный ресурс] // https://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html. (Дата обращения: 30.10.2017).

3. KL ICS CERT. Nigerian phishing: industrial companies under attack [Электронный ресурс] // https://ics-cert.kaspersky.com/reports/2017/06/15/nigerian-phishing-industrial-companies-under-attack/. (Дата обращения: 30.10.2017).

4. Securelist. Kaspersky Lab's Global Research & Analysis Team. BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents [Электронный ресурс] // https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/. (Дата обращения: 30.10.2017).

5. ICS-CERT Monitor November/December 2016, National Cybersecurity and Communications Integration Center, 2016.

6. Recommended Practice for Patch Management of Control Systems (December 2008). U.S. Department of Homeland Security.

7. Friedberg, I. Towards a Resilience Metric Framework for Cyber-Physical Systems. 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Queen's Belfast University, UK, 23 - 25 August 2016, pp. 19-22.

8. Tebbe, C. Ontology and life cycle of knowledge for ICS security assessments. 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Queen's Belfast University, UK, 23 - 25 August 2016, pp. 32-41.

9. ITIL Service Design TSO, Norwich, United Kingdom, 2011.

10. Jonsson, E. An attempt to quantitative modelling of behavioural security, 11th International Information Security Conference, Cape Town, South Africa, May 1995.

11. Cobb, J. What is the half-life of your information? [Электронный ресурс] // http://captricity.com/blog/half-life-information/. (Дата обращения: 30.10.2017).

12. Common Vulnerability Scoring System v3.0: Specification Document (v1.7).

13. Баринов А.Е., Рябцева О.В., Соколов А.Н. Адаптивная оценка клиентского риска в облачных инфраструктурах. Вестник УрФО. Безопасность в информационной сфере. № 1(23) / 2017, с. 14–19.

14. Cayirci, E., Garaga, A., Santana de Oliveira, A. et al. J Cloud Comp (2016) 5: 14. doi:10.1186/s13677-016-0064-x.

References

1. Andrey Zaikin. Pochemu zashchita ASU TP segodnya stala kriticheski vazhnoy? [Elektronnyy resurs] // https://www.securitylab.ru/analytics/484730.php. (Data obrashcheniya: 30.10.2017).

2. Keizer, Greg. Is Stuxnet the 'best' malware ever? Infoworld. 16 September 2010. [Elektronnyy resurs] // https://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html. (Data obrashcheniya: 30.10.2017).

3. KL ICS CERT. Nigerian phishing: industrial companies under attack [Elektronnyy resurs] // https://ics-cert.kaspersky.com/reports/2017/06/15/nigerian-phishing-industrial-companies-under-attack/. (Data obrashcheniya: 30.10.2017).

4. Securelist. Kaspersky Lab's Global Research & Analysis Team. BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents [Elektronnyy resurs] // https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/. (Data obrashcheniya: 30.10.2017).

5. ICS-CERT Monitor November/December 2016, National Cybersecurity and Communications Integration Center, 2016.

6. Recommended Practice for Patch Management of Control Systems (December 2008). U.S. Department of Homeland Security.

7. Friedberg, I. Towards a Resilience Metric Framework for Cyber-Physical Systems. 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Queen's Belfast University, UK, 23 - 25 August 2016, pp. 19-22.

8. Tebbe, C. Ontology and life cycle of knowledge for ICS security assessments. 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Queen's Belfast University, UK, 23 - 25 August 2016, pp. 32-41.

9. ITIL Service Design TSO, Norwich, United Kingdom, 2011.

10. Jonsson, E. An attempt to quantitative modelling of behavioural security, 11th International Information Security Conference, Cape Town, South Africa, May 1995.

11. Cobb, J. What is the half-life of your information? [Elektronnyy resurs] // http://captricity.com/blog/half-life-information/. (Data obrashcheniya: 30.10.2017).

12. Common Vulnerability Scoring System v3.0: Specification Document (v1.7).

13. Barinov A.Ye., Ryabtseva O.V., Sokolov A.N. Adaptivnaya otsenka kliyentskogo riska v oblachnykh infrastrukturakh. Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. № 1(23) / 2017, s. 14–19.

14. Cayirci, E., Garaga, A., Santana de Oliveira, A. et al. J Cloud Comp (2016) 5: 14. doi:10.1186/s13677-016-0064-x.

БАРИНОВ Андрей Евгеньевич, старший преподаватель кафедры защиты информации, младший научный сотрудник, и.о. директора НОЦ «Информационная безопасность» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: barinovae@susu.ru

ANDREY Barinov, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: barinovae@susu.ru

СКУРЛАЕВ Сергей Вадимович, старший преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: svskurlaev@susu.ru

SERGEY Skurlaev, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: svskurlaev@susu.ru

СОКОЛОВ Александр Николаевич, канд. техн. наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: ANSokolov@inbox.ru

ALEXANDER Sokolov, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: ANSokolov@inbox.ru

УДК 004:34 + 34.03 Вестник УрФО № 3(25) / 2017, с. 43–49

Минбалеев А. В.

РАЗВИТИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ: СТРАТЕГИЯ И ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

В статье анализируются актуальный акт информационного законодательства – Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. Стратегия определяет основные направления развития информационного общества в России и постепенный переход России в общество знаний. В документе содержится достаточно разнообразный набор средств и методов государственного регулирования развития информационного общества. Автор анализирует данный документ и выделяет основные направления совершенствования российского законодательства, направленные на развитие информационного общества в России.

Ключевые слова: *информационное общество, общество знаний, стратегия, информационные технологии.*

Minbaleev A. V.

THE DEVELOPMENT OF THE LEGAL REGULATION OF THE INFORMATION SOCIETY IN RUSSIA: THE STRATEGY AND THE MAIN DIRECTIONS FOR IMPROVING LEGISLATION

The article analyzes the current act of information legislation - the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030. The strategy defines the main directions of the development of the information society in Russia and the gradual transition of Russia to the knowledge society. The document contains a rather diverse set of tools and methods for state regulation of the development of the information society. The author analyzes this document and outlines the main directions for improving Russian legislation aimed at developing the information society in Russia.

Keywords: *information society, knowledge society, strategy, information technology.*

Указом Президента Российской Федерации от 9 мая 2017 г. № 203 утверждена Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (далее – Стратегия развития информационного общества). В ранее действующей Стратегии развития информационного общества государство основной акцент делало на основные направления ее реализации, в результате было положено начало интенсивному использованию органами государственной власти Российской Федерации, бизнесом и гражданами информационно-коммуникационных технологий.

В новом документе принципиально меняется подход в стратегическом видении государством последующего развития информационного общества в России: закрепляются принципы, на которых функционирует Стратегия развития информационного общества; даются определения основных понятий тех или иных явлений, объектов, сфер и институтов информационного общества, которые ранее практически не определялись законодательно или же были существенно подкорректированы с учетом особенностей современного уровня развития информационно-коммуникационных технологий; устанавливается современное состояние развития информационного общества в мире и в России, а также обозначаются ряд проблем, в том числе необходимости интенсификации использования самих технологий, стремительного регулирования «на ходу» сферы информации и информационных технологий в условиях новых технологий; устанавливается цель документа и стратегические национальные приоритеты Российской Федерации при развитии информационного общества, а также приоритетный сценарий развития информационного общества в России, перечень показателей реализации Стратегии развития информационного общества и этапы ее реализации. В Стратегии развития информационного общества также закрепляются вопросы управления ее реализацией, источники и механизмы ресурсного обеспечения мероприятий по ее реализации, задачи, функции и порядок взаимодействия государственных органов, органов местного самоуправления и организаций при ее реализации. Все это свидетельствует о более обоснованном, методологическом подходе государства к выстраиванию основных приоритетных направлений развития информационного общества.

Развитие информационного общества рассматривается не как самоцель, а как важнейшее средство для достижения более гло-

бальной цели Стратегии развития информационного общества – создание условий для формирования в Российской Федерации общества знаний, следующего этапа развития общества, заложенного Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003 год), Планом действий Тунисского обязательства (2005 год). Общество знаний, как устанавливает Стратегия развития информационного общества, представляет собой общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации. Таким образом, Российская Федерация, основываясь на принципе обеспечения прав граждан на доступ к информации, стремится к обществу достоверной информации.

Что же следует понимать под информационным обществом? Стратегия развития информационного общества впервые официально определяет его как общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.

Основными принципами, на которые опирается Стратегия развития информационного общества, являются следующие: обеспечение прав граждан на доступ к информации; обеспечение свободы выбора средств получения знаний при работе с информацией; сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг; приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий; обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях; обеспечение государственной защиты интересов российских граждан в информационной сфере.

Стратегия призвана способствовать обеспечению следующих национальных интересов: развитие человеческого потенциала; обеспечение безопасности граждан и государства; повышение роли России в мировом гуманитарном и культурном пространстве; развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления; повышение эффективности государственного управления, развитие экономики и социальной сферы; формирование цифровой экономики.

Обеспечение национальных интересов при развитии информационного общества согласно Стратегии развития информационного общества осуществляется путем реализации ряда приоритетов. С точки зрения перспектив правового регулирования информационного общества можно выделить следующие направления совершенствования законодательства в рамках каждого из выделяемых приоритетов:

1) Формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений. В рамках данного приоритета можно выделить следующие направления совершенствования законодательства:

– развитие законодательства об обеспечении доступа к информации в соответствии с заявляемыми целями формирования информационного пространства, основанного на знаниях (далее – информационное пространство знаний), к которым относятся обеспечение прав граждан на объективную, достоверную, безопасную информацию и создание условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора. Таким образом, явно выделяется необходимость установления и конкретизации в целом ряде нормативных правовых актов гарантий по обеспечению прав граждан именно на объективную, достоверную и безопасную информацию;

– дальнейшее развитие законодательства с целью обеспечения безопасной информационной среды для детей;

– закрепление в законодательстве механизмов, обеспечивающих доступ максимально широкого круга пользователей к Национальной электронной библиотеке и иным государственным информационным системам, включающих в себя объекты исторического, научного и культурного наследия народов Российской Федерации;

– развитие административной и уголовной ответственности за незаконное исполь-

зование информационных технологий в различных сферах общественной жизни, в первую очередь, – экономической;

– обеспечение создания и развития систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления;

– совершенствование на уровне федеральных законов механизмов ограничения доступа к информации, распространение которой в Российской Федерации запрещено федеральными законами, и механизмов быстрого ограничения доступа к ней и (или) удаления;

– совершенствование регулирования деятельности средств массовой информации в условиях информационного пространства знаний, а также средств обеспечения доступа к информации, которые по многим признакам могут быть отнесены к средствам массовой информации, но не являются таковыми (интернет-телевидение, новостные агрегаторы, социальные сети, сайты в сети «Интернет», мессенджеры);

– законодательное обеспечение функционирования и использования современных информационных платформ для распространения достоверной и качественной информации и информационных продуктов российского производства;

– установление в законодательстве льгот и преференций для выпуска отечественных медиапродуктов и сервисов российского производства, а также для поддержки традиционных средств распространения информации (радио-, телевещание, печатные средства массовой информации, библиотеки).

2) Развитие информационной и коммуникационной инфраструктуры Российской Федерации. К основным направлениям совершенствования законодательства в рамках данного приоритета необходимо выделить:

– развитие законодательства в сфере обеспечения свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации, подлежащей свободному обращению, на всех этапах ее создания и распространения;

– развитие законодательства, направленного на недопущение подмены, искажения, блокирования, удаления, снятия с каналов связи и иных манипуляций с информацией на уровне программного обеспечения и сервисов, предоставляемых с использованием сети «Интернет»; информационных систем и центров обработки данных; сетей связи (линии и средства связи, инфраструктура российского сегмента сети «Интернет», технологические и выделенные сети связи, сети и оборудование интернета вещей);

– обеспечение устойчивого функционирования информационной инфраструктуры Российской Федерации, предполагающее создание единства государственного регулирования, централизованных мониторинга и управления функционированием информационной инфраструктуры Российской Федерации на уровне информационных систем и центров обработки данных, а также на уровне сетей связи;

– закрепление в законодательстве дополнительных мер, стимулирующих: переход государственных органов и органов местного самоуправления к использованию инфратруктуры электронного правительства как части информационной инфраструктуры Российской Федерации; использование российских криптоалгоритмов и средств шифрования при электронном взаимодействии федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления между собой, а также с гражданами и организациями; замену импортного оборудования, программного обеспечения и электронной компонентной базы российскими аналогами в целях обеспечения технологической и производственной независимости и информационной безопасности;

– закрепление в законодательстве мер, направленных на создание российского общесистемного и прикладного программного обеспечения, телекоммуникационного оборудования и пользовательских устройств и расширения использования их гражданами, субъектами малого, среднего и крупного предпринимательства, государственными органами и органами местного самоуправления, в том числе на основе обработки больших объемов данных, применения облачных технологий и интернета вещей, технологии блокчейн;

– совершенствование нормативного правовое регулирования в сфере обеспечения

безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих технологий и интересам общества;

– закрепление в законодателсьтве принципа обеспечения баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая права на неприкосновенность частной жизни и права на личную и семейную тайну;

– развитие нормативного правового регулирования обеспечения обработки данных российских граждан и организаций на российских серверах при электронном взаимодействии лиц, находящихся на территории Российской Федерации, а также передачи таких данных на территории Российской Федерации с использованием сетей связи российских операторов;

– обеспечение государственного регулирования и координации действий при создании и ведении информационных ресурсов в Российской Федерации в целях соблюдения принципа разумной достаточности при обработке данных;

– усиление ответственности за незаконную обработку и сбор сведений о гражданах, в том числе персональных данных граждан, на территории Российской Федерации, а также установление дополнительных требований по проведению мероприятий по противодействию незаконной обработки и сбора сведений о гражданах, в том числе персональных данных граждан, на территории Российской Федерации неуполномоченными и неустановленными лицами, а также используемым ими техническим средствам;

– правовое регулирование создания и использования централизованной системы мониторинга и управления единой сетью электросвязи Российской Федерации; системы, обеспечивающей возможность устойчивого, безопасного и независимого функционирования российского сегмента сети «Интернет»;системы мер по обеспечению устойчивого функционирования российского сегмента сети «Интернет»;

– развитие законодательства, направленного на реализацию государственную политику в части, касающейся государственного управления инфраструктурой российского сегмента сети «Интернет»;

– выработка законодательных мер по предотвращению нарушений работы сети «Интернет» и отдельных ее ресурсов на территории Российской Федерации в результате целенаправленных действий;

– законодательное закрепление проведения ряда мероприятий на международном уровне, в том числе: отстаивание суверенного права государства определять информационную, технологическую и экономическую политику в национальном сегменте сети «Интернет»; ведение работы, направленнуюой против использования сети «Интернет» в военных целях; интеграция российских стандартов в сфере информационных и коммуникационных технологий в соответствующие международные стандарты, а также обеспечение гармонизации межгосударственной и национальной систем стандартов в данной сфере; создание новых механизмов партнерства, призванных с участием всех институтов общества выработать систему доверия в сети «Интернет», гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации и исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети «Интернет»;

– разработка норм международно-правового регулирования, касающихся безопасного и устойчивого функционирования и развития сети «Интернет», включая вопросы юрисдикции и определения субъектов правоотношений, на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы.

3) Создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне. При реализации данного приоритета неоходимо выделить следующие направления:

– закрепеление в законодательстве стимулов для создания и развития российских информационных и коммуникационных технологий осуществляется в целях получения государством и гражданами новых технологических преимуществ, использования и обработки информации, доступа к ней, получения знаний, формирования новых рынков и обеспечения лидерства на них. Основными приоритетными направлениями развития российских информационных и коммуника-

ционных технологий на ближайшую перспективу закрепляются: конвергенция сетей связи и создание сетй связи нового поколения; обработка больших объемов данных; искусственный интеллект; доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере; облачные и туманные вычисления; интернет вещей и индустриальный интернет; робототехника и биотехнологии;радиотехника и электронная компонентная база; информационная безопасность. В качестве перспективных также необходимо отнести использование технологии блокчейн;

– законодательное стимулирование создания российских организаций, осуществляющих деятельность, направленную на развитие всего спектра сервисов цифровой экономики, и способных лидировать на внутреннем и внешнем рынках; трансфера иностранных технологий и применение лучшего зарубежного опыта в сфере информационных технологий.

4) Формирование новой технологической основы для развития экономики и социальной сферы предполагает следующие основные направления развития законодательства:

– законодательное совершенствование механизмов предоставления финансовых услуг в электронной форме и обеспечение их информационной безопасности;

– стимулирование российских организаций в целях обеспечения работникам условий для дистанционной занятости;

– совершенствование механизмов электронной демократии, в том числе обеспечение возможности использования информационных и коммуникационных технологий при проведении опросов и переписи населения;

– законодательное закрепление стимулирования использования электронного документооборота в организациях, создание условий для повышения доверия к электронным документам, осуществление в электронной форме идентификации и аутентификации участников правоотношений; создания электронной системы представления субъектами хозяйственной деятельности отчетности в органы государственной власти Российской Федерации и органы местного самоуправления, а также сохранение возможности представления документов традиционным способом.

5) Обеспечение национальных интересов в области цифровой экономики. К ключевым направлениям совершенствования законодательства в рамках данного приоритета необходимо выделить:

– совершенствование антимонопольного законодательства, в том числе при предоставлении программного обеспечения, товаров и услуг с использованием сети «Интернет» лицам, находящимся на территории Российской Федерации;

– законодательное закрепление условий для развития крупных российских организаций в сфере информационных и коммуникационных технологий (экосистемы цифровой экономики); для создания кросс-отраслевых консорциумов в сфере цифровой экономики на базе крупнейших российских интернет-компаний, банков, операторов связи (в том числе почтовой), операторов платежных систем, участников финансового рынка, государственных компаний и корпораций;

– стимулирование государством локализации иностранными организациями на территории Российской Федерации процессов производства и использования продукции в сфере информационных и коммуникационных технологий;

– законодательно регламентировать доступ организаций к данным о гражданах и юридических лицах, в том числе содержащимся в государственных информационных системах, порядок обработки данных, а также порядок государственной защиты персональных данных граждан на территории Российской Федерации;

– расширение таможенного контроля в отношении товаров, заказанных с использованием сети «Интернет»;

– законодательное закрпеление сертификации и лицензирования отдельных товаров и услуг, ввозимых в Российскую Федерацию, в том числе приобретаемых с использованием сети «Интернет»;

– закрепление мер по ограничению доступа к программному обеспечению, товарам и услугам, предоставляемым с использованием сети «Интернет» на территории Российской Федерации иностранными организациями, допустившими нарушение законодательства Российской Федерации;

– законодательное обеспечение защиты интересов и безопасности российских участников электронной торговли с учетом соблюдения требований идентификации, под-

твержденія достоверности и подлинности используемых документов; осуществления расчетов между участниками электронной торговли через российскую платежную систему.

В рамках обеспечения национальных интересов в области цифровой экономики достаточно большое количество направлений и конкретные законодательные мероприятия закреплены в утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 года №1632-р программе «Цифровая экономика Российской Федерации».

Все указанные направления развития законодательсьтва в условиях развития информационного общества учитывают стратегические цели, которые стоят перед российским государством в целом на ближайшие годы. В то же время необходимо учитывать, что, в связи с активным развитием информационных процессов в условиях развити яинформационного общества, возникает необходимость системного совершенствования всего информационного законодательства. Анализ последнего свидетельствует о том, что оно не отвечает потребностям соврменных субъектов информационных отношений и требует обновления на основе стратегических целей и задач, а также развития информационных и коммуникационных технологий.

МИНБАЛЕЕВ Алексей Владимирович , доктор юридических наук, профессор кафедры теории государства и права, конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет), г. Челябинск. E-mail: alexmin@bk.ru.

MINBALEEV Aleksey Vladimirovich, Doctor of Law, Professor Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University (National Research University), Chelyabinsk, Russian Federation. E-mail: alexmin@bk.ru.

УДК 659.1:34 + 004.738.5:659.1 Вестник УрФО № 3(25) / 2017, с. 50–55

Меликов У. А.

ПРАВОВЫЕ АСПЕКТЫ РЕКЛАМЫ В ИНТЕРНЕТЕ

Реклама в сети интернет является основным источником доходов. Интернет выступает как информационно- коммуникационная технология для распространения рекламы в интернете. Размещение и распространение рекламы в СМИ, интернете, транспортных средствах, зданиях и других источниках имеет свои особенности. В законодательстве Республики Таджикистан не предусматриваются специальные нормы о распространении рекламы посредством интернета. Такая ситуация усложняет решение проблем связанных с рекламой. В статье рассматривается понятие рекламы, его соотношение с офертой, особенности ограничения касающихся рекламы в интернете, запрета спама и т. д. Отмечается, что при решении этих вопросов важную роль играет место нахождения рекламодателя и рекламораспространителя. Автор приходит к выводу о том, что в законодательстве Республики Таджикистан необходимо предусмотреть нормы об особенности рекламы в интернете.

Ключевые слова: *право, интернет, реклама, оферта, ограничение, закон, рекламодатель, рекламораспространитель, спам, запрет.*

Melikov U. A.

LEGAL ASPECTS OF ADVERTISING ON THE INTERNET

Advertising on the Internet is the one of source of income. Internet is information and communication technology for the distribution of advertising. Advertising on media, internet, transports, buildings and other sources has its own particularity. The legislation of the Republic of Tajikistan does not specific rules on the distribution of advertising on the Internet. This situation complicates the solution of problems related to advertising. Author analyzed in the article definition of advertising, its relation to the offer, particularly limitations relating to advertising on the Internet, banning spam. Location of the advertiser and advertisement is criterion for solution issues relation to advertising on internet. Author concludes that in the legislation of Republic of Tajikistan is necessary to provide rules on the particular advertising on the Internet.

Keywords: *law, internet, advertising, offer, limit, law, advertiser, advertisements, spam ban.*

Рекламная деятельность в интернете является в настоящий момент основным источником доходов, получаемых в сети. С рекламой в интернете так или иначе связана деятельность студий веб-дизайна, рекламных интернет-агентств, порталов, поисковых систем, целого ряда других субъектов сетевого бизнеса[1]. Реклама в интернете отражает коммерческие интересы не только рекламодателя, но и правообладателя сайта. Поэтому мы специально остановимся на рассмотрении данного вопроса.

Понятие «реклама» по-разному трактуется в юридической литературе. Одни авторы считают, что реклама - это разновидность информации[2], другие рассматривают ее как деятельность или услугу[3], третьи - как информацию и результат интеллектуальной дея-

тельности[4]. Причиной неоднозначного толкования этого понятия является отсутствие единого подхода к определению понятия информации.

В ст. 2 Закона РТ «О рекламе» дается такое определение: «реклама - распространяемая в любой форме, с помощью любых видов средств информация о физическом или юридическом лице, товарах, идеях и начинаниях (рекламная информация), которая предназначена для неопределенного круга лиц и призвана формировать или поддерживать интерес к физическим и юридическим лицам, товарам, идеям и начинаниям и способствовать реализации товаров, идей и начинаний».

В этом же законе, в зависимости от средств распространения рекламы, предусмотрен ряд норм: реклама в печатных СМИ, реклама в телевидении и радиовещании; реклама на транспорте, реклама на зданиях и т.п. Однако в данном законе нет ни слова об интернете или сайтах. Отсутствуют в нем и специальные нормы, регулирующие рекламу в интернете. Но, исходя из понятия рекламы, где о ней говорится как информации, «распространяемой в любой форме, с помощью любых видов средств……», можно сделать вывод, что в «любые виды средств» входит и интернет. Между тем правовое регулирование рекламы в интернете имеет свои специфические проблемы.

Одна из них – это действие законодательства в пространстве. Проблема заключается в недостаточно глубоко разработанной концепции «интернет – территории». Условно территории в интернете ограничиваются доменами верхнего уровня, который создан на основе кодирования названий стран. Такое решение вопроса имеет технический характер, юридические же проблемы пока остаются нерешенными.

Многие сайты находятся в зарубежных доменах и серверах, поэтому, например, применить здесь, требование ст. 13 Закона РТ «О государственном языке Республики Таджикистан» (от 5 октября 2009 г., № 553 [5]) о том, что «в Республике Таджикистан объявления и рекламы распространяются на государственном языке. Объявления и реклама могут распространяться в соответствии с законодательством Республики Таджикистан и на других языках», достаточно сложно.

Для пользователя нет разницы в том, из какого источника он получает рекламу - от сайтов, находящихся в доменах TJ, или других сайтов. Реклама всегда направлена на результат, а с какого сайта, какого домена или сервера она распространяется, это вопрос технического характера. Поэтому при определении правового регулирования в данной сфере необходимо учитывать указанные моменты.

Реклама и оферта часто схожи по содержанию. В законодательстве Республики Таджикистан дается два следующих понятия оферты: офертой признается адресованное одному или нескольким конкретным лицам предложение, которое достаточно определенно и выражает намерение лица, сделавшего предложение, считать себя заключившим договор с адресатом, которым будет принято предложение. Оферта должна содержать существенные условия договора (ст. 467 ГК РТ); оферта - предложение о заключении договора, направленное одному или нескольким конкретным лицам и охватывающее основные требования договора (ст. 2 Закона РТ «О рекламе»).

В обоих понятиях отмечены два важных моментов: 1) волеизъявление лица, которое предлагает оферту о заключении договора; 2) изложение существенных условий договора. В ст. 2 Закона «О рекламе» вместо «существенные условия договора» приводятся «основные требования договора». В отличие от существенных условий договора, основные требования договора в гражданском законодательстве не предусматриваются. Существенные условия договора рассматриваются в трех аспектах: для всех договоров - предмет договора (ст. 464 ГК РТ); для отдельных видов договоров – конкретно предусматривается в соответствующих нормативно-правовых актах (например, существенные условия авторских договоров предусматриваются в ст. 26 Закона РТ «Об авторском праве и смежных правах»); 3) по соглашению сторон.

Реклама, призывающая совершить оферту и публичную оферту, является как бы предпосылкой этого действия. Если реклама охватывает существенные условия договора, то она переплетается с офертой, и, соответственно, на последнюю распространяются не только нормы рекламного законодательства, но и нормы гражданского законодательства о договорах.

Гражданский кодекс РТ рассматривает рекламу как приглашение к оферте. Приглашение совершить оферту (ст. 469 ГК РТ) и реклама не имеют договорно – правовых последствий. Если и та, и другая охватывают

существенные условия договора, то обе становятся офертой и приобретают договорно – правовые последствия.

Законодатель требует, чтобы рекламодатель обязательно указывал срок действия как рекламы, выступающей в качестве приглашения делать оферты, если в рекламе сообщается хотя бы одно из существенных условий, так и рекламы, выступающей в качестве публичной оферты (ст. 26 Закона «О рекламе»).

Таким образом, соотношение рекламы и оферты в законодательстве РТ сводится к следующему: 1) приглашение делать оферты не имеет договорно-правовых последствий; 2) если реклама имеет хотя бы одно существенное условие договора, то должен быть указан срок ее действия; 3) если реклама охватывает все существенные условия договора, то она считается офертой (публичная оферта) и приобретает договорно - правовые последствия.

Данное положение законодательства не всегда соответствует фактическим рекламным отношениям в связи с тем, что осуществление данного требования ставит иногда рекламодателей в «сложное» положение. Пока ни в одной из реклам мы не встречали указания на срок ее действия.

Данный вопрос основательно решен в ст. 11 Закона РФ «О рекламе»: «Если в соответствии с Гражданским кодексом Российской Федерации реклама признается офертой, такая оферта действует в течение двух месяцев со дня распространения рекламы при условии, что в ней не указан иной срок».

Возложить на рекламодателя обязательство об указании срока действия рекламы нереально. Более правильное решение вопроса – ограничить срок оферты (а не рекламы) двумя месяцами с момента распространения рекламы. Это снимает излишнее обязательство с участников рекламных отношений. Если же сами рекламодатели заинтересованы в указании определенного срока действия рекламы, то это их субъективное право.

Рассмотренные выше проблемы характерны и рекламе в интернете. На сайте предпринимателя вполне может быть размещена реклама, которая имеет хотя бы одно существенное условие договора. Уже сам предмет договора является существенным его условием. В большинстве случаев реклама охватывает именно предмет договора. Например, на сайте ООО «Исател» - isatel.tj размещены разные рекламные баннеры: доступный WIMAX интернет, спутниковый интернет VSAT и т.д. Из них следует, что данная компания предлагает услуги WIMAX интернет, спутниковый интернет VSAT. В их рекламе уже есть одно из существенных условий договора – предмет договора. Другие условия – цена, объем трафика и т.п., далее будут конкретизированы в договоре.

Насколько целесообразно в такой рекламе предусматривать срок действия рекламы? Реклама имеет такие особенности, как краткость, простота, доступность и т.п. Указание на срок действия рекламы в самой рекламе, которая, например, состоит всего из трех слов «Доступный WIMAX интернет», «Спутниковый интернет VSAT», превращает ее в «не - рекламу». Следовательно, целесообразно усовершенствовать положение Закона РТ «О рекламе», касающееся данного вопроса, что будет способствовать не только развитию рекламы в интернете, но и рекламы в других источниках информации.

Другая проблема, которая часто дискутируется среди специалистов, - это спам. Согласно п. 17 Правил предоставления услуг интернета на территории Республики Таджикистан, утвержденых постановлением Правительства Республики Таджикистан (от 8 августа 2001 г., № 389), абонент обязан «не совершать массовую рассылку предварительно не согласованных электронных сообщений (spam), а также не посылать сообщения адресатам, высказавшим ранее явное нежелание получать эти сообщения. Касаясь проблемы ограничения рекламы в интернете, О.А. Филатовапишет: «В связи с наличием в интернете большого количества рекламы, носящей порнографический характер, представляется целесообразным ограничить доступ к такой рекламе. Для этого предлагается принять следующие меры: а) вынести такие сайты в отдельный определенный домен, что даст возможность запретить доступ к этим сайтам на отдельных компьютерах; б) законодательно обязать регистрировать сайты именно в этом домене; в) запретить рекламу этих материалов и определенных услуг, связанных с ними, на сайтах, в каталогах и поисковых системах»[6]. Такие меры могут временно положительно повлиять на ограничение противозаконной реклам, но они же могут привести и к обратному результату. Во-первых, когда вся порнореклама будет генерироваться в одном домене, это, наоборот,

будет способствовать «рекламе» такого домена. Например, почти каждый пользователь интернета знает домен youtube.com, где размещаются все видеоматериалы. Во - вторых, широко доступны пользователям прокси-серверы для обходов таких технических ограничений. В-третьих, практика показывает, что ограничение доступа к тому или иному материалу в интернете, наоборот, делает его более популярным, интерес пользователей к нему увеличивается. Получается обратный эффект. Следовательно, при применении таких юридико- технических мер, необходимо учитывать все стороны вопроса и последствия его решения.

Реклама в интернете выражается в разных формах: это баннеры, текстовые блоки, мини-сайты и др. Они прикрепляются к сайтам и становятся доступными пользователям. Согласно рекламному законодательству, реклама в печатных и электронных СМИ, в транспорте и все другие виды рекламы имеют свои ограничения по времени, по объемам и другим критериям. Но касательно интернета в Таджикистане пока таких ограничении нет (за исключением ограничения спама, о чем мы писали выше).

Заслуживает внимания правоприменительная практика регулирования отношений в интернете в ряде стран (таких, как Япония, Южная Корея, Аргентина, а также в Евросоюзе). В Южной Корее, например, начиная с 2002 г., действует «Закон о защите в электронной коммерции», который накладывает запрет на слишком большие рекламные сообщения и определяет судебную ответственность вплоть до лишения лицензии на коммерческую деятельность за нарушения данного законодательства. В 18 - ти штатах США действует запрет на распространение спама. В них проводятся успешно судебные процессы по этому поводу. В других странах рассылка спама разрешена только при соблюдении рекламодателем определенных требований. Например, японское и южнокорейское законодательства определяют, что получатель спама должен быть определенно уведомлен о том, что полученное им письмо содержит материалы рекламного характера. Кроме того, в Японии имеет место следующее положение: если адресат не пожелает более получать аналогичные электронные письма, рассылка должна быть немедленно прекращена [7].

При правовом регулировании рекламной деятельности в интернете должны учитываться частные и публичные интересы, поэтому необходимо «взаимодействие диспозитивного и императивного методов регулирования»[8]. Правовое средство, которое направлено на регулирование деятельности по созданию и распространению рекламы, - это правовые нормы, в которых установлены правовые ограничения. А. В. Малько отмечает, что «в зависимости от того, в каких элементах нормы права они содержатся, можно выделить: юридический факт-ограничение (гипотеза), запрет, приостановление, обязанность и т. п. (диспозиция), меры наказания (санкция)»[9]. В Законе РТ «О рекламе» установлен ряд ограничений при осуществлении рекламной деятельности, среди которых особое внимание вызывают запреты и обязанности. Эти ограничения, прежде всего, отражают сочетание интересов участников рекламной деятельности, но применить их в отношении рекламы в интернете возможно лишь в определенных случаях.

Например, согласно ст. 6 Закона РТ «О рекламе» запрещается недобросовестная реклама, в том числе реклама, которая содержит некорректные сравнения рекламируемого товара с товаром (товарами) других физических или юридических лиц, а также высказывания, образы, порочащие честь, достоинство или деловую репутацию конкурента (конкурентов). Соблюдение данного запрета можно требовать от рекламораспространителей в интернете, которые находятся в Таджикистане. Но если домен не в зоне TJ, а сервер находится за рубежом, то проблему решить труднее. Несмотря на это, на наш взгляд, основным критерием применения закона должно быть действие субъекта, который находится в пространстве Таджикистана. Нахождение им сайта, сервера или домена – это скорее всего результат именно его работы.

О.А. Филатова, рассматривая данный вопрос, предлагает внести в законодательство положение об ответственности рекламораспространителя – владельца сайта, который размещает ссылку с противоправной информацией[10]. Определение противоправной информации весьма широко, и иногда даже в суде трудно доказать противоправность того или иного вида информации. Поэтому любой вид ответственности должен быть применим на основе конкретных фактов и норм.

Рекламная деятельность состоит из двух взаимосвязанных этапов - создания и распространения рекламы. На стадии создания

рекламы правовые ограничения касаются содержания информации[11], а на стадии распространения - времени и объема распространения[12]. Анализируя положения правового регулирования рекламной деятельности в интернете и правоприменительную практику, невозможно не остановиться на некоторых запретах и позитивных обязанностях, установленных законодательством относительно рекламы.

В п. 9 Порядка единых требований для сайтов и локально-вычислительных сетей государственных органов управления, утвержденных постановлением Правительства Республики Таджикистан (от 1 апреля 2011 г., № 166), отмечается, что «официальный сайт государственного органа не должен размещать в себе рекламные ролики, ссылки на различные разделы одного сайта, непроверенные или недостоверные материалы и подобные им материалы, в ней должна быть размещена содержательная информация с указанием источников. Услуги по предоставлению рекламных роликов через сеть Интернета должны действовать в рамках действующего законодательства с указанием и размещением даты и номера договора».

Регулирование рекламы на государственных сайтах не вызывает трудностей, но проблемы возникают при их регулировании в случае, когда эта реклама распространяется на зарубежных сайтах. Например, на сайте www.mail.ru, когда открывается почта в Таджикистане, распространяется реклама на таджикском языке. Рекламодателями являются субъекты – предприниматели, которые находятся в Таджикистане, а рекламораспространителями-резиденты России. Реклама в данном случае ориентирована на потребителя в Таджикистане. В отношении рекламодателя можно применить требование законодательства РТ, но в отношении рекламораспространителя вопрос сложнее. Проблема имеет трансграничный характер. Следовательно, необходим комплексный подход к регулированию рекламы на международном, региональном уровнях или хотя бы на уровне двусторонних соглашений.

Примечания

1. Винтонива Н. И., Клименко С. А. Основные юридические проблемы при оказании рекламных и маркетинговых услуг в Интернете: особенности правового регулирования. Развитие российского права и права стран АТР в условиях конституционного реформирования : Материалы региональной научно-практической конференции, 29 ноября 2003 г. - Владивосток : Изд. ВГУЭС, 2004. - С. 28 – 31. URL: http://www.law.edu.ru/doc/document.asp?docID=1149960 (дата обращения 14. 05. 2015)

2. См.: Жилинский С. Э. Предпринимательское право (правовая основа предпринимательской деятельности): Учебник для вузов. 3-е изд., изм. и доп. - М.: НОРМА – ИНФРА- М, 2002. - С. 517; Кузнецова О.Б. Правовое регулирование отношений, возникающих в области рекламы. Автореф. дисс.... к. ю. н. - М., 1999. - С. 10; Минбалеев А.В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества. - Челябинск, 2012. - С. 106.

3. См.: Страунинг Э.Л. Соотношение понятий «реклама» и «информация» URL: http://www.yurclub.ru/docs/pravo/1003/9.html (дата обращения 25.07.2016); Его же. Реклама как объект гражданских прав. URL: http://www.yurclub.ru/docs/pravo/1203/11.html (дата обращения 25. 07. 2016); Жуковская Л.М. Гражданско–правовое регулирование рекламной деятельности в Российской Федерации. Автореф. дисс....к. ю. н. - М., 2007. - С. 19.

4. См.: Куликова Ю.С. Ненадлежащая реклама как форма недобросовестной конкуренции. Дисс...к. ю. н. -М., 2003. - С. 58-59; Шугаибов З.Ш. Гражданские правоотношения в сфере российского рынка рекламы. Автореф. дисс...к. ю. н. - М., 2006. - С. 18; Малеина М. Н. Право на рекламу // Правоведение. -1991. - № 1. - С. 15 – 25.

5. Ахбори Маджлиси Оли Республики Таджикистан. – 2009. - №9-10. – С. 125- 129.

6. Филатова О.А. Гражданско - правовые особенности рекламы в Интернете: Автореф. дисс… к.ю.н. - М., 2003. - С. 11.

7. См.: Шмавганец Т.А. Проблемные аспекты правового регулирования рекламы в Интернет-сети. URL: http://repository.hneu.edu.ua/jspui/bitstream/123456789/4726/1/%D0%A8%D0%BC%D0%B0%D0%B2%D0%B3%D0%B0%D0%BD%D0%B5%D1%86%D1%8C%20%D0%A2.%D0%90.%20%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%BD%D1%8B%D0%B5%20%D0%B0%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D1%8B%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20%D1%80%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D1%8B%20%D0%B2%20%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%81%D0%B5%D1%82%D0%B8.pdf (дата обращения: 6. 02. 2016).

8. Черячукин Ю. В. Проблемы правового регулирования рекламной деятельности в России и зарубежных государствах. Дисс... д. ю. н. - Волгоград, 2002. Указ. раб. - С. 35.

9. Малько А.В. Стимулы и ограничения в праве. 2-е изд., перераб. и доп. - М.: Юристь, 2004. - С. 94.

10. Филатова О.А. Указ. раб. - С. 13.

11. В СМИ запрещается, прежде всего, ненадлежащая реклама (недобросовестная, недостоверная, неэтичная, заведомо ложная, скрытая реклама), реклама алкогольных напитков, табака и табачных изделий, порнографических аудио-, видео- и печатных материалов, а также наркотических веществ, психотропных препаратов и прекурсоров (ст. 5-10 Закона РТ «О рекламе»).

12. Данные запреты направлены на ограничение распространения рекламы в эфире, на газетной площади (ст. 11-12 Закона РТ «О рекламе»).

References

1. Vintoniva N. I., Klimenko S. A. Osnovnyie yuridicheskie problemyi pri okazanii reklamnyih i marketingovyih uslug v Internete: osobennosti pravovogo regulirovaniya. Razvitie rossiyskogo prava i prava stran ATR v usloviyah konstitutsionnogo reformirovaniya : Materialyi regionalnoy nauchno-prakticheskoy konferentsii, 29 noyabrya 2003 g. - Vladivostok : Izd. VGUES, 2004. - S. 28 – 31. URL: http://www.law.edu.ru/doc/document.asp?docID=1149960 (data obrascheniya 14. 05. 2015)

2. Sm.: Zhilinskiy S. E. Predprinimatelskoe pravo (pravovaya osnova predprinimatelskoy deyatelnosti): Uchebnik dlya vuzov. 3-e izd., izm. i dop. - M.: NORMA – INFRA- M, 2002. - S. 517; Kuznetsova O.B. Pravovoe regulirovanie otnosheniy, voznikayuschih v oblasti reklamyi. Avtoref. diss.... k. yu. n. - M., 1999. - S. 10; Minbaleev A.V. Teoreticheskie osnovaniya pravovogo regulirovaniya massovyih kommunikatsiy v usloviyah razvitiya informatsionnogo obschestva. - Chelyabinsk, 2012. - S. 106.

3. Sm.: Strauning E.L. Sootnoshenie ponyatiy «reklama» i «informatsiya» URL: http://www.yurclub.ru/docs/pravo/1003/9.html (data obrascheniya 25.07.2016); Ego zhe. Reklama kak ob'ekt grazhdanskih prav. URL: http://www.yurclub.ru/docs/pravo/1203/11.html (data obrascheniya 25. 07. 2016); Zhukovskaya L.M. Grazhdansko–pravovoe regulirovanie reklamnoy deyatelnosti v Rossiyskoy Federatsii. Avtoref. diss....k. yu. n. - M., 2007. - S. 19.

4. Sm.: Kulikova Yu.S. Nenadlezhaschaya reklama kak forma nedobrosovestnoy konkurentsii. Diss...k. yu. n. -M., 2003. - S. 58-59; Shugaibov Z.Sh. Grazhdanskie pravootnosheniya v sfere rossiyskogo ryinka reklamyi. Avtoref. diss...k. yu. n. - M., 2006. - S. 18; Maleina M. N. Pravo na reklamu // Pravovedenie. -1991. - # 1. - S. 15 – 25.

5. Ahbori Madzhlisi Oli Respubliki Tadzhikistan. – 2009. - #9-10. – S. 125- 129.

6. Filatova O.A. Grazhdansko - pravovyie osobennosti reklamyi v Internete: Avtoref. diss…k.yu.n. - M., 2003. - S. 11.

7. Sm.: Shmavganets T.A. Problemnyie aspektyi pravovogo regulirovaniya reklamyi v Internet-seti. URL: http://repository.hneu.edu.ua/jspui/bitstream/123456789/4726/1/Shmavganets T.A. Problemnyie aspektyi pravovogo regulirovaniya reklamyi v Internet-seti.pdf (data obrascheniya: 6. 02. 2016).

8. Cheryachukin Yu. V. Problemyi pravovogo regulirovaniya reklamnoy deyatelnosti v Rossii i zarubezhnyih gosudarstvah. Diss... d. yu. n. - Volgograd, 2002. Ukaz. rab. - S. 35.

9 .Malko A.V. Stimulyi i ogranicheniya v prave. 2-e izd., pererab. i dop. - M.: Yurist, 2004. - S. 94.

10. Filatova O.A. Ukaz. rab. - S. 13.

11. V SMI zapreschaetsya, prezhde vsego, nenadlezhaschaya reklama (nedobrosovestnaya, nedostovernaya, neetichnaya, zavedomo lozhnaya, skryitaya reklama), reklama alkogolnyih napitkov, tabaka i tabachnyih izdeliy, pornograficheskih audio-, video- i pechatnyih materialov, a takzhe narkoticheskih veschestv, psihotropnyih preparatov i prekursorov (st. 5-10 Zakona RT «O reklame»).

12. Dannyie zapretyi napravlenyi na ogranichenie rasprostraneniya reklamyi v efire, na gazetnoy ploschadi (st. 11-12 Zakona RT «O reklame»).

МЕЛИКОВ Умрилло Асадуллоевич, начальник отдела гражданского, предпринимательского и семейного законодательства Национального центра законодательства при Президенте Республики Таджикистан, кандидат юридических наук. 734024, г. Душанбе. ул. Академика А. Адхамова 13 А. Тел: (+992) 372274678 E-mail: umrillo@mail.ru

MELIKOV Umrillo Asadulloevich, head of the department of civil, business and family law the National Center for Legislation under the President of the Republic of Tajikistan, candidate of Legal Science. 734024, Dushanbe. str. Akademik A. Adhamov 13 A. Tel: (+992) 372274678 E-mail: umrillo@mail.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

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

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

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

УДК
ББК

ОБРАЗЕЦ

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

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

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

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

Рисунки

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

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

Формулы

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

Таблицы

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

Примечания

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

Статья публикуется впервые
Подпись, дата

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

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

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

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

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

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

Библиографические ссылки

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

Ниже приводятся образцы оформления сносок:

а) на монографии:

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

б) на статьи из сборников:

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

в) статьи из журналов и продолжающихся изданий:

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

г) авторефераты диссертаций:

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

д) интернет-страницы:

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

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

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

Поступившие в редакцию материалы возврату не подлежат.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Экспертная комиссия в составе _____

в период с «___»_____20___г. по «___»_____20___г. провела экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспертном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011г, № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., экспертная комиссия установила:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Председатель комиссии (Ф.И.О., подпись)

Члены ЭК : (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 3(25) / 2017

Дата выхода в свет 29.09.2017. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,25. Тираж 100 экз. Заказ 386/638.
Цена свободная.

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

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 3(25) / 2017

Date of publication of the 29.09.2017. Format 70×108 1/16. Screen printing.
Conventional printed sheet 5,25. Circulation – 100 issues. Order 386/638. Open price.

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