ISSN 2074-7128(print), ISSN 2074-7136(on-line)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Том 25, № 4 (2018)

(IT Security)

Периодический рецензируемый научный журнал «Безопасность информационных технологий», освещающий широкий спектр проблем обеспечения информационной безопасности, в том числе технологические, организационно-правовые и образовательные аспекты.

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати.
Свидетельство № 017789.
Издается с 1994 г.

С момента основания и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников 05.13.00 – информатика, вычислительная техника и управление, по которой журнал входит в этот перечень.

Основные тематические направления журнала:
•Концептуальные основы обеспечения информационной безопасности автоматизированных систем;
•Методические подходы к анализу и оценке рисков информационной безопасности, технологии поиска уязвимостей в программном обеспечении;
•Оценка уровня защищенности автоматизированных систем;
•Программно-технические способы и средства обеспечения информационной безопасности.

Журналом приветствуются статьи на русском и английском языках.

Редакционная коллегия:
Жуков И.Ю. (главный редактор, ООО «Национальный Мобильный Портал», Москва, Россия; Author ID: 55229487100);
Дураковский А.П. (зам. главного редактора, Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; Author ID: 56893817400);
Горбатов В.С. (отв. секретарь, Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; Author ID: 36766363500);
Будзко В.И. (Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия; Author ID: 56879039000);
Тарасов А.М. (ЗАО «Лаборатория Касперского», Москва, Россия; Author ID(РИНЦ): 448352);
Кулик С.Д. (Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; Author ID: 56565032900);
Труфанов А.И. (Иркутский национальный исследовательский технический университет, Иркутск, Россия; Author ID: 56439267200);
Зегжда П.Д. (Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия; Author ID: 55872378100);
Епишкина А.В. (Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; Author ID: 56669752600);
Грушо А.А. (Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия; Author ID: 13104337000);
Мещеряков Р.В. (Томский государственный университет систем управления и радиоэлектроники, Томск, Россия); Author ID: 23035794100);
Макаревич О.Б. (Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Таганрог, Россия; Author ID: 22950974400);
Matt Bishop (University of California at Davis – USA, Davis; Author ID: 7201415965);
Maria Dubovitskaya (Security & Privacy Group, IBM Research – Switzerland, Zurich; Author ID: 35338862600);
Steven Furnell (School of Computing, Electronics and Mathematics (Faculty of Science and Engineering) – UK, Plymouth; Author ID: 7003551084);
Lech Janczewski (University of Auckland – New Zealand, Auckland; Author ID: 6603473186);
Christos Kalloniatis (Lab. of Cultural Informatics, Dept. of Cultural Technology and Communication, University of the Aegean – Greece, Mytilene; Author ID: 8935567300);
Valentin Kisimov (University of National and World Economy – Bulgaria, Sofia; Author ID: 56628657100);
Edgar Weippl (Vienna University of Technology (CISSP, CISA, CISM) – Austria, Vienna; Author ID: 8925433900)

Состав редакционного совета:
Старовойтов А.В. (председатель редакционного совета, Центр информационных технологий и систем органов исполнительной власти (ЦИТиС), Москва, Россия);
Дворянкин С.В. (зам. председателя редакционного совета, Финансовый университет при Правительстве Российской Федерации, Москва, Россия; Author ID: 57170853500);
Конявский В.А. (Центр экспертизы и координации информатизации (ЦЭКИ) Минкомсвязи России, Москва, Россия; Author ID: 57192434900);
Милославская Н.Г. (Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; Author ID: 22950974400);
Mark Manulis (Faculty of Engineering and Physical Sciences, University of Surrey – UK, Guildford; Author ID: 8690445500);
Erik Moore (College of Computer & Information Sciences, Regis University – USA, Denver; Author ID: 55426010100);
Corey Schou (College of Business, Idaho State University, National Information Assurance Training and Education Center (NIATEC) and the Simplot Decision Support Center (SDSC) – USA, Pocatello; Author ID: 7006835719);

IT Security(Russia)

IT Security is a periodic peer-reviewed scientific journal publishing papers on a wide range of information security topics, including technological, organizational, legal and educational problems.

Since its establishment in 1994 (registration certificate No. 017789 by the State Committee for Press of the Russian Federation), the journal has been publishing by the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University, a.k.a. "MEPhI" (Moscow Engineering Physics Institute).

Papers in Russian and English are equally welcome.

Focus topics:
•Fundamentals of information security of automated systems;
•Methodology of assessing the information security risks;
•Technology of detecting software vulnerabilities;
•Evaluation of the security level of automated systems;
•Soft- and hardware means of ensuring information security.

Editorial Board
I. Yu. Zhukov, Editor in chief, Ltd. "The National Mobile Portal", Moscow, Russian Federation, Author ID: 55229487100;
A. P. Durakovskiy, Deputy chief editor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation, Author ID: 56893817400;
V. S. Gorbatov, The responsible Secretary of edition, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation, Author ID: 36766363500;
V. I. Budzko, Federal Research Center "Informatics and Management" Russian Academy of Sciences, Moscow, Russian Federation, Author ID: 56879039000;
A. M. Tarasov, Kaspersky Lab, Moscow, Russian Federation; Author ID(RSI): 448352
S. D. Kulik, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation, Author ID: 56565032900;
A. I. Trufanov, Irkutsk National Research Technical University, Irkutsk, Russian Federation, Author ID: 56439267200;
P. D. Zegzhda, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation, Author ID: 55872378100;
A. V. Epishkina, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation, Author ID: 56669752600;
A. A. Grusho, Federal Research Center "Informatics and Management" Russian Academy of Sciences, Moscow, Russian Federation, Author ID: 13104337000;
R. V. Mescheryakov, Tomsk State University of Control Systems and Radioelectronics, Tomsk, Author ID: 23035794100;
O. B. Makarevich, Southern Federal University, Institute of Computer Technologies and Information Security, Taganrog, Russian Federation, Author ID: 22950974400;
Matt Bishop (University of California at Davis – USA, Davis; Author ID: 7201415965);
Maria Dubovitskaya (Security & Privacy Group, IBM Research – Switzerland, Zurich; Author ID: 35338862600);

Steven Furnell (School of Computing, Electronics and Mathematics (Faculty of Science and Engineering) – UK, Plymouth; Author ID: 7003551084);
Lech Janczewski (University of Auckland – New Zealand, Auckland; Author ID: 6603473186);
Christos Kalloniatis (Lab. of Cultural Informatics, Dept. of Cultural Technology and Communication, University of the Aegean – Greece, Mytilene; Author ID: 8935567300);
Valentin Kisimov (University of National and World Economy – Bulgaria, Sofia; Author ID: 56628657100);
Edgar Weippl (Vienna University of Technology (CISSP, CISA, CISM) – Austria, Vienna; Author ID: 8925433900)

Editorial Council
A. V. Starovoytov, Editorial Council chairman, Center of information technologies and systems of Executive authorities, Moscow, Russian Federation;
S. V. Dvoryankin, Deputy Chairman of the editorial council, Financial University under Government of Russian Federation, Moscow, Russian Federation;
V. A. Konyavsky, Center for expertise and coordination of informatization of the Russian Ministry of Communications, Moscow, Russian Federation;
N. G. Miloslavskaya, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation;
Mark Manulis, Faculty of Engineering and Physical Sciences, University of Surrey, United Kingdom;
Erik Moore, College of Computer & Information Sciences, Regis University, United States;
Corey Schou, Information Systems, Associate Dean, College of Business, Idaho State University & Director of the National Information Assurance Training and Education Center (NIATEC) and the Simplot Decision Support Center (SDSC), United States.

СОДЕРЖАНИЕ

CONTENT

Евгений Б. Белов[1], Владимир П. Лось[2], Анатолий А. Малюк[3]
[1]ФУМО ВО ИБ,
Мичуринский просп., 70, г. Москва, Россия
e-mail: umoib@yandex.ru*, https://orcid.org/0000-0003-4854-1220*
[2]Центр исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА,
Вернадского просп., 78, г. Москва, Россия
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

ЦИФРОВАЯ ЭКОНОМИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.01

Аннотация. Тенденции развития глобального информационного общества свидетельствуют о возрастании потребности в специалистах, обладающих высокой информационной культурой, в том числе обладающих знаниями и навыками обеспечения информационной безопасности. В Доктрине информационной безопасности Российской Федерации развитие и совершенствование системы соответствующей подготовки кадров заявлено в качестве одного из первоочередных мероприятий по реализации государственной политики в области формирования цифровой экономики. Подготовка кадров в данном случае должна предусматривать два направления – профессиональное и массовое обучение. В свою очередь, профессиональное обучение может быть основным и дополнительным. Основная цель массового обучения – формирование в обществе культуры информационной безопасности, недостаточный уровень которой отмечен в Доктрине информационной безопасности как одна из основных информационных угроз. Исходя из этого, в статье рассматриваются все актуальные сегодня проблемы как профессионального, так и массового обучения. При этом подчеркивается важность реализации парадигмы непрерывного образования (образования в течение всей жизни).

Таким образом, основная цель данной статьи заключается в раскрытии важнейших проблем обеспечения непрерывного процесса формирования современной культуры информационной безопасности с использованием возможностей всех звеньев образовательной системы.

Ключевые слова: информационная безопасность, кадровое обеспечение отрасли информационной безопасности, осведомленность по вопросам информационной безопасности, профессиональное и массовое обучение в области информационной безопасности, культура информационной безопасности.

Для цитирования: БЕЛОВ, Евгений Б.; ЛОСЬ, Владимир П.; МАЛЮК, Анатолий А. ЦИФРОВАЯ ЭКОНОМИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 6-22, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1157>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.01.

Evgeny B. Belov [1], Vladimir P. Los [2], Anatoly A. Malyuk [3]
[1]FUMO VO IB,
Michurinsky prosp., 70, Moscow, Russia
e-mail: umoib@yandex.ru, https://orcid.org/0000-0003-4854-1220
[2]Center for the Study of the Problems of Personnel Supply in the Information Security Industry RTU MIREA,
Vernadsky prosp.,78, Moscow, Russia
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048

[3]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute)
Kashirskoe sh.,31, Moscow, Russia
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

The digital economy and actual problems of the improvement of the training system in the field of information security

DOI: http://dx.doi.org/10.26583/bit.2018.4.01

Abstract. Trends in the development of the global information society indicate an increasing need for professionals with well established information culture, including those with knowledge and skills to ensure information security. The development and improvement of the system of appropriate training is stated in the Doctrine of information security of the Russian Federation as one of the priority measures for the implementation of the state policy in the field of digital economy. Training in this case should include both professional and mass training. In turn, the professional training can be basic and additional. The main goal of mass education is to form a culture of information security in society, which insufficient level of was noted in the Doctrine of information security as one of the main information threats. Therefore, the paper deals with the whole spectrum of the current problems of both professional and mass training. The importance of implementing the paradigm of continuous education ("lifelong learning") is emphasized.
Thus, the main purpose of this paper is to reveal the most important problems of ensuring the continuous process of formation of modern culture of information security using the capabilities of all components of the educational system.

Keywords: information security, staffing of the information security industry, information security awareness, professional and mass training in the field of information security, information security culture.
For citation: BELOV, Evgeny B.; LOS, Vladimir P.; MALYUK, Anatoly A. The digital economy and actual problems of the improvement of the training system in the field of information security. IT Security (Russia), [S.l.], v. 25, n. 4, p. 6-22, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1157>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.01.

Введение

Процесс формирования глобального информационного общества развивается нарастающими темпами. Сегодня мы являемся свидетелями широкого внедрения принципиально новых инструментов управления экономическими системами как на уровне отдельных государств, так и во всемирном масштабе. Появился даже новый термин «цифровая экономика», подразумевающий использование возможностей современных информационно-коммуникационных технологий (ИКТ) в обеспечении функционирования экономической системы. С другой стороны, цифровая экономика подразумевает также реализацию на основе концепции искусственного интеллекта систем поддержки принятия решений, базирующихся на широком спектре цифровых прогностических моделей.

Понятно, что указанные процессы с новой силой ставят проблему обеспечения информационной безопасности. Положительный эффект от реализации процессов цифровизации экономики возможен только в безопасной информационной среде. Иначе последствия такой «цифровизации» могут оказаться просто катастрофическими.

В Доктрине информационной безопасности Российской Федерации, принятой в декабре 2016 года, четко констатируется тот факт, что проблемы информационной безопасности (ИБ) перестали сегодня быть узкой областью исключительной компетенции специальных служб и все больше становятся предметом внимания достаточно образованной части населения. Тенденции информатизации мирового сообщества свидетельствуют о возрастании потребности в специалистах, обладающих высокой информационной культурой, владеющих новейшими информационными технологиями, умеющих применять их в своей профессиональной деятельности и обладающих знаниями и навыками обеспечения ИБ. Согласно Доктрине развитие и совершенствование системы соответ-

ствующей подготовки кадров, работающих как собственно в сфере обеспечения ИБ России, так и в других сферах экономики, широко использующих ИКТ, является одним из первоочередных мероприятий по реализации государственной политики в области формирования цифровой экономики. Подобная подготовка должна в том числе частично компенсировать повсеместное использование импортных средств вычислительной техники, телекоммуникаций и программного обеспечения. Хотя, конечно же, это не снимает остроты проблемы импортозамещения в этой области.

Таким образом, не вызывает никаких сомнений высокая актуальность проблемы кадрового обеспечения сферы ИБ, а также формирования в обществе культуры информационной безопасности с использованием концепции непрерывного образования [1, 2].

При этом в системе высшего образования базовыми центрами формирования культуры информационной безопасности могут стать:

региональные учебно-научные центры по проблемам информационной безопасности, созданные в 1997 году на базе ведущих учебных заведений;

планируемые к созданию в рамках федерального проекта «Цифровая экономика» многофункциональные окружные учебно-научные (производственные) центры по проблемам обеспечения информационной безопасности для задач цифровой экономики в каждом федеральном округе на базе ведущей образовательной организации высшего образования, реализующей основные образовательные программы в области информационной безопасности;

планируемые к созданию в рамках федерального проекта «Цифровая экономика» межрегиональные центры в области информационной безопасности в системе среднего профессионального образования.

Обозначенные нами проблемы и являются предметом рассмотрения данной статьи.

1. Исторический очерк

Подготовка специалистов – профессионалов в области информационной безопасности в стране имеет, по крайней мере, 70-летнюю историю, если иметь в виду такую ее важнейшую составляющую, как криптография. Однако как целостная система такая подготовка стала складываться только в начале 90-х годов прошлого века. Этому способствовал целый ряд обстоятельств – развитие новых ИКТ, включая глобальные компьютерные сети, повсеместное использование этих технологий частными компаниями и гражданами и т.д. Как следствие, появился, например, большой интерес в негосударственном секторе к вопросам криптографии (особенно сюда следует отнести криптографию с открытым ключом), а также к компьютерной безопасности. Происходившая одновременно реформа высшего образования в стране, состоявшая, в частности, в переходе профессионального образования на Государственные образовательные стандарты (ГОС) в определенной степени стимулировала возникновение отдельного направления подготовки кадров «Информационная безопасность».

Сегодня, по прошествии более 20 лет, нам достаточно понятны процессы в естественнонаучном и техническом направлениях подготовки кадров в области ИБ. Существенно менее понятны они в гуманитарном направлении и на стыке указанных выше. Такая ситуация, по-видимому, достаточно естественна. Действительно, имеется прорыв по техническим составляющим новых информационных технологий. Вопросы же реализации заложенных в этих технологиях возможностей, с одной стороны, в значительной степени зависят от такого социально-экономического фактора, как возможность граждан получить доступ к ним, и от подходов к вопросам управления информационными сетями. С другой стороны, в мировом сообществе имеются различные точки зрения на роль государства в этих вопросах. В том числе высказывается и мнение, что государство несет ответственность за решение проблем, связанных с обеспечением неприкосновенности частной жизни, соблюдением авторских прав, содержанием передаваемой информации и доступом к ней, за электронной торговлей и компьютеризацией образования. При этом указанные проблемы должны решаться одновременно на национальном, региональном и международном уровнях. В настоящее

время идет непростой процесс осознания нетехнических составляющих формирующегося информационного общества, а также возможностей, прав и обязанностей личности, общества и государства в нем.

Отметим далее, что к настоящему времени в системе Министерства науки и образования Российской Федерации сложились основы дееспособной системы подготовки специалистов, способных решать задачи обеспечения ИБ страны. Эта стройная, на наш взгляд, система опирается на Федеральное учебно-методическое объединение по образованию в области информационной безопасности (ФУМО ИБ), созданное в 1996 году на базе крупнейшего и известнейшего учебного заведения в этой области – Института криптографии, связи и информатики (ИКСИ) Академии Федеральной службы безопасности Российской Федерации, а также на сеть региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы, созданную Министерством общего и профессионального образования Российской Федерации в 1997 году.

Следует отметить, что российская система подготовки кадров в области ИБ занимает по ряду позиций ведущее положение, по крайней мере, среди европейских стран, о чем свидетельствуют материалы регулярно проводимой международной конференции по образованию в области информационной безопасности (*World Conference on Information Security Education*) [3 - 5].

На сегодняшний день эта система включает в себя следующие составляющие [6]:

- пять федеральных государственных образовательных стандартов (ФГОС) высшего образования и разработанных на их базе основных образовательных программ подготовки специалистов в области ИБ по специальностям: «Компьютерная безопасность», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Информационно-аналитические системы безопасности», «Безопасность информационных технологий в правоохранительной сфере»;
- два федеральных государственных образовательных стандарта высшего образования по направлению «Информационная безопасность» (подготовка бакалавров и магистров);
- три федеральных государственных образовательных стандарта среднего профессионального образования по специальностям: «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем», «Организация и технология защиты информации»;
- федеральное учебно-методическое объединение вузов России по образованию в области ИБ на базе ИКСИ Академии ФСБ России;
- более 100 вузов России различной ведомственной принадлежности, которые ведут образовательную деятельность по подготовке специалистов по указанным специальностям и направлениям;
- 12 министерств и ведомств и их органов управления профессиональным образованием, а также научные организации и учреждения, ведущие научные исследования в данной области, в том числе два головных центра – МГУ

им. М.В. Ломоносова и Академия криптографии РФ;

- специальности и направления подготовки (соответствующие образовательные программы, включающие вопросы ИБ), реализуемые в рамках других УМО, смежных с входящими в группу по ИБ;
- 28 региональных учебно-научных центров по проблемам ИБ в системе высшей школы;
- образовательные программы дополнительного образования и соответствующие различные ведомственные курсы переподготовки и повышения квалификации;
- образовательные программы послевузовского образования в данной области (подготовка кадров высшей квалификации по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»).

Таким образом, сегодня можно с уверенностью говорить о сформированном вузовском сегменте образования. Хотя необходимо признать, что здесь еще недостаточна или просто отсутствует

координация усилий между различными УМО, а порой и основными заинтересованными ведомствами. Нет обоснованных решений по сочетанию различных схем и уровней подготовки, увязанных с потребностями соответствующих секторов экономики страны. Остаются проблемы и в области нормативного обеспечения функционирования системы. Все это будет рассмотрено нами ниже в соответствующих разделах данной статьи.

2. Проблемы профессионального обучения

В соответствии с Общероссийским классификатором специальностей по образованию (ОКСО) все интересующие нас ФГОС объединены в настоящее время в отдельную группу специальностей и направлений подготовки в области информационной безопасности (код 2.10.00.00). При этом в классификаторе предусмотрены все уровни подготовки: среднее профессиональное образование, бакалавриат, магистратура, специалитет и аспирантура.

С учетом задач развития цифровой экономики рассмотрим содержательное наполнение актуальных сегодня конкретных программ подготовки (специалитет, бакалавриат, магистратура). Результаты анализа приводят нас к следующим выводам. Особенностью практически всех программ является то, что содержание блока общих математических и естественнонаучных дисциплин отражает более глубокие требования к уровню базовой математической и естественнонаучной подготовки специалиста по информационной безопасности. Дополнительно к присутствовавшим в предыдущих поколениях стандартов математике, информатике, физике и экологии повсеместно добавлены дисциплины «Дискретная математика», «Математическая логика и теория алгоритмов», а также «Теория информации». Введение этих дисциплин в блок фундаментальной подготовки отражает принципиальную ориентацию обучающихся на овладение дискретными моделями, характеризующими информационные процессы, и специфическими для области методами их познания. Это вполне соответствует сформулированным нами компетенциям, требующимся для реализации задач цифровой экономики.

В группе дисциплин программного обеспечения информационных технологий в последнее время формируется более системный взгляд на сущность процессов построения программных комплексов. Программное обеспечение операционных систем и средств их интеграции, систем управления базами данных изучается не столько с функциональной точки зрения, сколько с аналитических позиций. Во главу угла поставлены архитектурные и основные технологические решения, их анализ с точки зрения обеспечения безопасности базирующихся на них информационных технологий. Увеличение числа рассматриваемых вопросов повлекло за собой увеличение общего числа часов, отводимых на изучение перечисленных выше дисциплин.

Ядро всех без исключения учебных программ определяет комплекс общепрофессиональных дисциплин, составляющих научный базис специалиста технологического профиля. Выделение общепрофессионального ядра является принципиальным моментом, характеризующим указанные программы.

Характерной чертой всех проанализированных нами программ является также введение в них общей дисциплины «Основы информационной безопасности», которая задумана как научный и методический фундамент всех дисциплин ядра. В процессе изучения этой дисциплины у студента должно сформироваться общее представление о структуре объекта изучения и основных понятиях теории информационной безопасности, содержании и взаимосвязи вопросов, изучаемых в остальных дисциплинах ядра. Присутствующая во многих программах дисциплина «Теоретические основы компьютерной безопасности» развивает и конкретизирует содержание методов обеспечения безопасности функционирования электронных систем обработки данных. Объектом изучения этой дисциплины является и технология проведения исследования и проектирования подсистем защиты автоматизированных систем, и методы управления функционированием системы обеспечения безопасности.

Дисциплины «Криптографические методы защиты информации», «Технические средства и методы защиты информации» и «Программно-аппаратные средства обеспечения информационной без-

опасности» призваны сформировать основной профессиональный инструментарий специалиста по защите информации. Особенностями данных курсов является обязательность проведения практических и лабораторных занятий, на которых студенты должны приобрести реальные навыки применения современных программных и аппаратных средств, изучаемых в соответствующих курсах.

Особые задачи дальнейшего совершенствования содержательного наполнения дисциплин образовательных программ стоят перед дисциплинами «Организационное обеспечение информационной безопасности» и «Правовое обеспечение информационной безопасности». Эти дисциплины имеют своим объектом анализ человеческого фактора как неотъемлемой, а часто и решающей части комплекса мероприятий по обеспечению информационной безопасности любой системы. Анализ многих, в том числе и наиболее громких событий, связанных с нарушением нормальной работы автоматизированных систем, показывает, что прекрасно спроектированные с технической точки зрения системы оказываются достаточно уязвимыми для противоправной деятельности, нацеленной на персонал. Знание основных организационных мер обеспечения защиты объекта и наличие элементарной правовой культуры является необходимым требованием к любому специалисту по защите информации.

В целом анализ современных ФГОС и конкретных образовательных программ по специальностям и направлениям группы 2.10.00.00 позволяет сформулировать следующие выводы.

1. Все образовательные программы в области информационной безопасности характеризует явно выраженная общность структур общеобразовательного цикла дисциплин, что подтверждает их общую идеологию, необходимость их дальнейшего развития в рамках единой организационной структуры. Это основной принцип формирования программ данной группы. Он, вообще говоря, отличается от используемых при формировании образовательных программ других групп специальностей и направлений подготовки.

2. Характерным для всех программ ИБ является наличие в блоке общепрофессиональных дисциплин групп дисциплин, ориентированных на изучение тех или иных методов и средств обеспечения ИБ. К указанным группам относятся:

- дисциплины по общим вопросам обеспечения информационной безопасности;
- дисциплины по организационно-правовым методам обеспечения ИБ;
- дисциплины по криптографическим методам защиты информации;
- дисциплины по инженерно-техническим методам защиты информации;
- дисциплины по безопасности информационных технологий.

Общий объем указанных дисциплин для различных программ составляет в среднем около 30 % от объема блока общепрофессиональных дисциплин.

3. Цикл общепрофессиональных дисциплин базируется на достаточно специализированном естественнонаучном цикле. Характерно, что, по сравнению, например, с родственными программами в области компьютерной техники и информационных технологий, естественнонаучный цикл для специальностей и направлений в области ИБ отличается большим объемом и существенной дискретно-математической составляющей, включающей, как правило, дополнительно 2-3 дисциплины.

4. В то же время, в каждой программе в общепрофессиональном и естественнонаучном циклах имеется блок дисциплин, отражающий специфику предметной области подготовки специалистов, соответствующий профилю их профессиональной деятельности. Это отличие по содержанию различных образовательных программ составляет примерно 25 – 30 % от объема блоков общепрофессиональных и естественнонаучных дисциплин.

5. Практика показывает, что в соответствии с запросами работодателей в качестве траектории образования наиболее востребованной все-таки оказывается подготовка дипломированных специалистов. Таким образом, с учетом разнообразия предметной области подготовки, различных квалификаций и сроков реализации образовательных программ возникают определенные сложности в формировании направления подготовки бакалавров и магистров. Более того, как вузы, так

и потребители особо остро данную проблему не ставят. Вместе с тем с учетом общей концепции развития в стране системы образования ФУМО ИБ совместно с вузами и потребителями специалистов, очевидно, необходимо провести научную проработку вопроса о месте подготовки бакалавров и магистров в решении задач формирования цифровой экономики.

Учитывая, что удовлетворить потребность в специалистах в области обеспечения информационной безопасности можно только на основе комплексного использования возможностей среднего, высшего и дополнительного профессионального образования, как вариант можно было бы предложить систему подготовки и переподготовки кадров по ИБ, представленную на рис. 1. Указанная система создает, на наш взгляд, все необходимые условия для реализации концепции непрерывного образования в данной области.

Как известно, в Доктрине информационной безопасности Российской Федерации (2016 г.) большое внимание уделено анализу угроз информационной безопасности в различных сферах деятельности личности, общества и государства. В современных условиях важное место среди этих угроз занимают:

• деятельность иностранных разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

• разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Противодействие именно этим угрозам является, на наш взгляд, основным направлением дальнейшего развития группы 2.10.00.00. Кое-что в этом направлении на сегодняшний день уже сделано. В частности, сюда можно отнести специальность «Противодействие техническим разведкам».

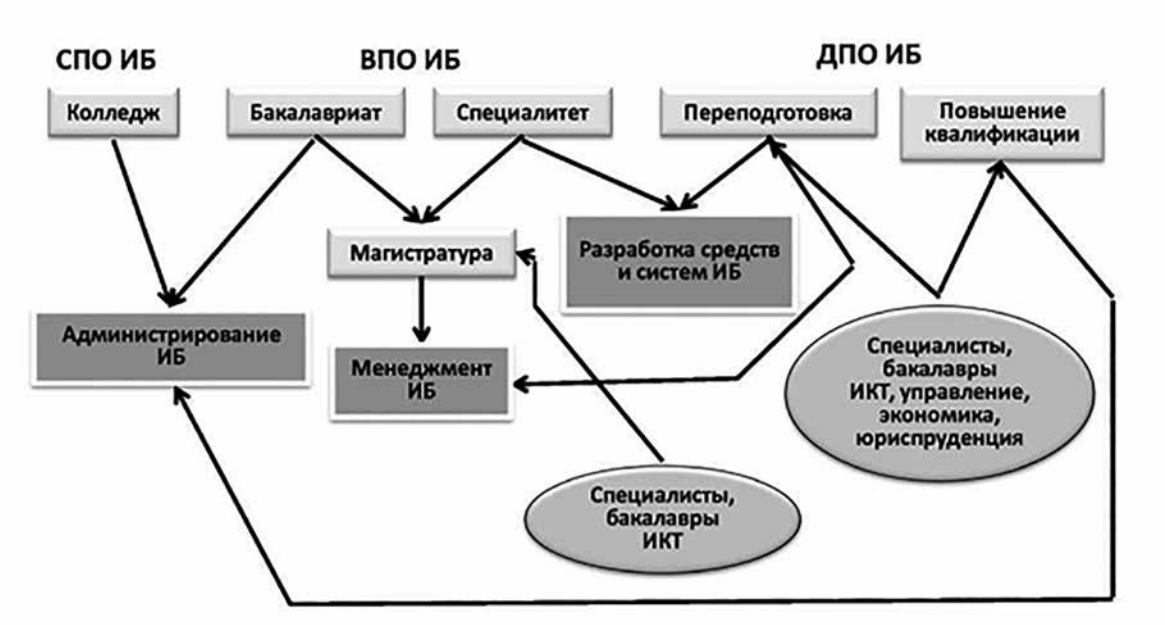


Рис. 1. Система подготовки и переподготовки кадров по ИБ
(Fig. 1. The system of training and retraining of personnel in the field of information security)

Новым направлением здесь может стать специальность с условным наименованием «Технические системы и средства информационного противоборства». Содержание образовательной программы здесь должно определяться моделью противоборства двух противостоящих друг другу контуров управления критическими системами, каждый из которых преследует цель дезорганиза-

ции управления противостоящей стороны и сохранения устойчивости своего управления. В рамках такой модели должны рассматриваться различные методы информационного воздействия на технические системы и человека и определяться пути обеспечения информационной безопасности.

В указанных специальностях неминуемо существенно увеличивается роль гуманитарной составляющей. Очевидно, если такие решения будут приняты, то возникает необходимость формирования специального модуля образовательной программы – «Гуманитарные проблемы информационной безопасности».

Нельзя не остановиться и на проблемах ИБ в гуманитарных специальностях и направлениях подготовки, входящих в ОКСО. Еще раз подчеркнем, что сегодня важнейшей задачей является увеличение подготовки специалистов по информационной безопасности гуманитарного профиля. Отметим, что в этом направлении уже более 20 лет активно работает Российский государственный гуманитарный университет, к которому подключился еще ряд вузов (НИЯУ МИФИ, МГУ, СПбГУ), создано несколько специализированных кафедр. Движение здесь очевидно, но, к сожалению, темпы развития этой тематики не соответствуют требованиям, изложенным в Доктрине информационной безопасности Российской Федерации. Не хватает нормативно-правовой базы по отдельным аспектам данной проблемы.

Серьезного внимания заслуживает проблема подготовки кадров для правоохранительных органов по расследованию преступлений в сфере компьютерной информации. Здесь можно отметить работу ряда вузов МВД, открывших вузовскую подготовку юристов с профилем в области ИБ. Однако активность в этом направлении в последнее время снижается, хотя появилась даже новая специальность «Безопасность информационных технологий в правоохранительной сфере». В чем здесь дело? Это тема для отдельного разговора, поскольку не понятно какое полушарие головного мозга должно преобладать при расследовании компьютерных преступлений или в разработке правового регулирования в киберпространстве, гуманитарное или техническое. На наш взгляд, заслуживает внимания симметричный подход, а именно – на базе технического направления давать юридическую специализацию или второе (юридическое) образование.

Другой возможный подход – разработка стандарта на стыке двух направлений (условно «Прикладная юриспруденция»). Подобный стандарт, по-видимому, мог бы быть взят за основу при подготовке специалистов для оперативных подразделений МВД, ФСБ и других силовых структур.

Аналогичную картину можно наблюдать и в области других гуманитарных направлений. Например, в философии – область этических проблем постиндустриального информационного общества или культура информационной безопасности. Можно также говорить о специализациях в области ИБ на базе специальностей и направлений по психологии и социологии.

3. Массовое обучение, формирование культуры информационной безопасности

Как уже отмечалось, формирование глобального информационного общества порождает широчайший спектр новых вызовов и угроз, связанных с активным внедрением современных ИКТ во все сферы деятельности. Чтобы успешно противостоять всему этому потоку негативных воздействий, каждому члену информационного общества необходимо обладать определенным минимумом знаний, соответствующей культурой информационной безопасности и быть готовым к активной борьбе за чистоту ИКТ.

Решению этой задачи может способствовать массовое введение во все образовательные стандарты (общего и профессионального образования, независимо от специальностей и направлений подготовки) компетенций в области основ обеспечения информационной безопасности. Это даст возможность подготовить обучающихся к деятельности в условиях постиндустриального информационного общества, дать им представление о правовом регулировании отношений в сфере защиты информации, об основных организационных, инженерно-технических и иных мерах защиты.

Помимо прикладного аспекта введение таких компетенций имеет большое социально-воспитательное значение. Они должны быть направлены на формирование нравственных ориентиров в

общественной жизни, на воспитание правосознания граждан и в то же время на устранение препятствий в реализации их конституционных прав и свобод в области духовной жизни и информационной деятельности. Подобную новацию, реализуемую в современной отечественной практике подготовки специалистов, следует рассматривать как элемент государственной информационной политики, позволяющей реализовать гармоничное сочетание интересов личности, общества и государства в информационной сфере.

Основой для разработки конкретного содержания соответствующих дисциплин, формирующих необходимые компетенции, может послужить материал резолюции Генеральной Ассамблеи ООН [7], принятой в декабре 2002 года и утвердившей принципы формирования глобальной культуры кибербезопасности. Глобальная культура кибербезопасности в трактовке данной резолюции формируется на основе 9 взаимодополняющих элементов:

- *осведомленности* об угрозах и подходах к обеспечению безопасности информационных систем и сетей;
- *ответственности* пользователей за безопасность информационных систем и сетей сообразно с ролью каждого из них;
- *реагирования*, подразумевающего принятие своевременных и совместных мер по предупреждению инцидентов, затрагивающих безопасность;
- *этики* как учета законных интересов других сторон и признания каждым участником, что его действия или бездействие могут причинить вред другим;
- *демократии* как непременного следования ценностям демократического общества, включая свободу обмена мыслями и идеями и свободный доступ к информации;
- *оценки риска*, предполагающей обязательную оценку потенциального риска любых действий, выявление угроз и факторов уязвимости;
- *проектирования и внедрения средств обеспечения безопасности* как важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;
- *управления обеспечением безопасности* на основе комплексного подхода, охватывающего все уровни деятельности членов информационного общества и все аспекты их операций в информационной сфере;
- *переоценки* как своевременного внесения надлежащих изменений в политику, практику, меры и процедуры обеспечения безопасности.

Отметим еще раз, что сегодня компетентность в сфере информационных технологий и информационной безопасности становится необходимым условием успешной социализации личности в новой информационной среде общества.

4. Единая образовательная среда как средство реализации концепции массового обучения

Развитие российского образования в соответствии с политикой, определенной Законом «Об образовании в Российской Федерации», предполагает формирование углубленных интеграционных и междисциплинарных программ, соединение их с прорывными высокими технологиями, актуализацию и приведение в соответствие с современной проблематикой учебных программ по большинству преподаваемых дисциплин, связанных с информационными технологиями. Среди прочего такая модернизация предполагает первоочередное внедрение в сферу образования новых информационных технологий, позволяющих существенно повысить качество образовательных процессов, расширить доступность образования и упростить доступ к образовательным ресурсам.

Важным шагом на пути к достижению намеченных целей должно стать создание Единой образовательной информационной среды как принципиально нового механизма передачи, обработки и хранения информации в сфере образования, как средства распространения знаний и интеграции образовательных процессов. Вопрос о формировании такой среды с разной степенью интенсивности обсуждается на протяжении последних десяти лет как на разного рода конференциях и совещаниях, так и в научных и массовых публикациях. Задача эта оказывается непростой, так как

предполагает постановку и решение ряда важных экономических и научно-технических проблем. К последним можно отнести следующие проблемы:

- техническую реализацию Единой образовательной среды;
- содержательное наполнение;
- обеспечение информационной безопасности среды.

Первая из этих проблем – техническая реализация Единой образовательной информационной среды – предполагает использование самых современных информационных технологий: широкое внедрение средств вычислительной техники, построение информационно-телекоммуникационных систем, систем распределенной обработки и хранения данных. Методологической основой создания современных крупномасштабных компьютерных информационных систем является концепция открытых систем и распределенной обработки данных. На сегодняшний день концепция открытых систем, основанная на системе международных стандартов и иных нормативных документов международных организаций, является единственным общепризнанным и универсальным подходом к формированию высоко сложных распределенных систем обработки данных и информационных систем на их основе.

Вторая проблема – содержательное наполнение Единой образовательной информационной среды, очевидно, предполагает, что в ней не только размещаются образовательные ресурсы, но и циркулирует большое количество других видов информации, что связано с многообразием функций образовательной среды. Все это требует введения как составной части среды средств и сетей хранения больших массивов информации.

Исключительно большое значение имеет проблема обеспечения информационной безопасности Единой образовательной информационной среды, на которой необходимо остановиться более подробно. Сложность этой проблемы обусловлена не только тем, что сама по себе сфера образования относится к приоритетным областям государственных интересов, но и тем, что Единая образовательная информационная среда является сложным и многофункциональным организационно-техническим комплексом. Очевидно, что эта проблема не может решаться без учета современных методов организации и технической реализации информационных систем. С целью уточнения методов и путей решения этой проблемы необходим анализ научно-методической и нормативно-технической базы в области открытых систем, созданной международными организациями по стандартизации информационных технологий.

Попробуем сформулировать в общих чертах концепцию обеспечения информационной безопасности Единой образовательной информационной среды. Концепция включает два основных аспекта – технический и организационный. Понятно, что технически она должна опираться на общепринятые международным сообществом принципы формирования открытых информационных систем с применением технических средств хранения и обработки больших массивов информации. Применение научно-методического аппарата открытых информационных систем позволяет создать основу единства и доступности формирующейся среды. Разработка политик безопасности основных структурных элементов Единой образовательной среды позволяет подойти к решению задач обеспечения доступности и целостности информации. При этом необходимо учитывать присутствие в составе среды средств и сетей распределенной обработки и хранения больших массивов информации.

Организационная сторона концепции должна базироваться на действующем российском законодательстве. Таким образом, необходима разработка организационно-распорядительных документов, содержащих рекомендации по организации правоотношений в области охраны интеллектуальной собственности, а также устанавливающих механизмы распространения в среде сведений ограниченного распространения.

Детальный анализ особенностей рассматриваемой нами проблемы приводит к заключению о необходимости расширения самой предметной области обеспечения информационной безопасности в Единой образовательной информационной среде. Со всей очевидностью вскрываются новые существенные аспекты этой проблемы.

Во-первых, очевидно многообразие технических средств и решений, доступных сегодня на рынке информационных технологий. В этой связи весьма актуальной является задача оптимального выбора из этого обширного арсенала технических средств решений, необходимых для формирования Единой образовательной среды. Таким образом, необходима формулировка технической политики безопасности Единой образовательной информационной среды.

Вторая проблема связана с содержательным наполнением новой информационной среды, созданной на базе применения распределенных систем обработки и хранения информации. Развертывание и широкомасштабное применение Единой образовательной среды должно, по-видимому, сопровождаться определенной критической оценкой ценности и возможности применения обращающегося в ней контента.

Здесь, очевидно, необходимо особо отметить, что существует опасность превращения образовательной среды в своего рода «средство массовой дезинформации» и даже орудие ведения «информационных войн» и разрушения психики человека.

В этой связи необходима формулировка политики содержательного наполнения образовательной среды, где проблемы информационной безопасности приобретают особую актуальность. На первый план здесь выходит рассмотрение проблемы информационно-ценностного наполнения созданной новой среды обращения информации.

Третья важная проблема связана с необходимостью получения ответа на вопрос, каковы перспективы и прогнозы дальнейшего развития информационных технологий и средств их реализации. Без ответа на этот вопрос невозможно грамотно и точно сформулировать концепцию развития такой сложной организационно-технической системы, каковой является Единая образовательная информационная среда.

Достоверное прогнозирование будущего развития защищенных информационных технологий как основы цифровой экономики не может быть осуществлено без оценки нынешней роли информационных технологий в современном мире, с учетом как позитивных, так и негативных факторов, порождаемых этим явлением в жизни человеческого общества. Безусловно, появление информационных технологий стало одним из самых существенных этапов развития научно-технического прогресса, внесло коренные изменения во многие сферы деловой деятельности человека, в том числе и в сферу образования. Однако вместе со всеми позитивными тенденциями, которые вносят информационные технологии в развитие человеческого общества, с ними связан большой круг политических, психологических и духовно-нравственных проблем. Информационные технологии поднимают на новый уровень давно стоящую проблему – вместо естественного и гармонического взаимодействия научно-технический прогресс общества и его духовный прогресс становятся тормозом один для другого. Государственная система образования как сфера, ответственная за формирование личностных и гражданских качеств членов общества, особенно чувствительна к этой проблеме.

Четвертая существенная проблема – разработка методов построения прикладных программ и систем на базе Единой образовательной информационной среды, таких как системы защищенного электронного документооборота, системы дистанционного обучения и других систем.

С учетом, с одной стороны, сложности структуры и информационного наполнения среды, а с другой – ее многофункциональности и универсального характера для решения различных классов задач данная проблема также требует для своего решения определенной научно-методической основы. Необходимо проведение исследований, направленных на разработку методов обеспечения устойчивости функционирования и безопасности прикладных программ. Должны быть предусмотрены способы обеспечения доступа к информации даже в таких сложных условиях, когда происходит физическое или логическое прерывания доступа к части узлов распределенной системы. Такие события могут иметь место как в случае возникновения нештатных ситуаций, связанных с разрушением части системы, обрывом каналов связи, диверсионными акциями, так и в случае ошибок персонала, обслуживающего систему, технических сбоев и отказов аппаратуры или программного обеспечения.

Таким образом, анализ проблем информационной безопасности в Единой образовательной информационной среде указывает на то, что роль защиты самих информационных технологий и циркулирующей в них информации с течением времени может и должна возрастать. При этом очевидно, что информационные технологии как организационно-техническая основа формирования новой образовательной среды не имеют альтернативы в обозримом будущем. Следовательно, безопасность, в широком смысле, в перспективе должна превратиться в центральную качественную характеристику информационных технологий в сфере образования.

5. Государственное регулирование и закрепление кадров

В предыдущих разделах статьи уже неоднократно подчеркивалась ведущая роль государства в решении проблемы кадрового обеспечения информационной безопасности. Понятно, что это связано с ее решающей ролью в решении задач национальной безопасности в условиях развития глобального информационного общества.

Исторической иллюстрацией государственного регулирования сферы кадрового обеспечения ИБ является решение Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности от 22.06.1999 № 2.1 «Об основных направлениях совершенствования системы подготовки, повышения квалификации переподготовки кадров в области обеспечения информационной безопасности», сыгравшее ключевую роль в развитии всей системы подготовки кадров в этой области.

Основная тяжесть в выполнении данного решения легла на тогдашнее Министерство образования, а в методическом плане, соответственно, на УМО ИБ. И если в методическом плане на сегодняшний день достигнуты определенные результаты (разработаны новые стандарты, создана отдельная группа специальностей и направлений подготовки, разработаны примерные учебные планы и программы, подготовлен и готовится целый ряд учебно-научных и методических материалов и т.д.), то в направлении нормативного и организационного обеспечения подготовки кадров продолжают оставаться определенные проблемы.

Первое, что необходимо отметить, это несовершенный, на наш взгляд, механизм формирования государственного заказа на подготовку кадров в области информационной безопасности. Причиной здесь является несоответствие между потребностью и выпуском специалистов. Расчеты показывают (см. рис. 2), что в этой области имеют место иногда достаточно серьезные диспропорции.

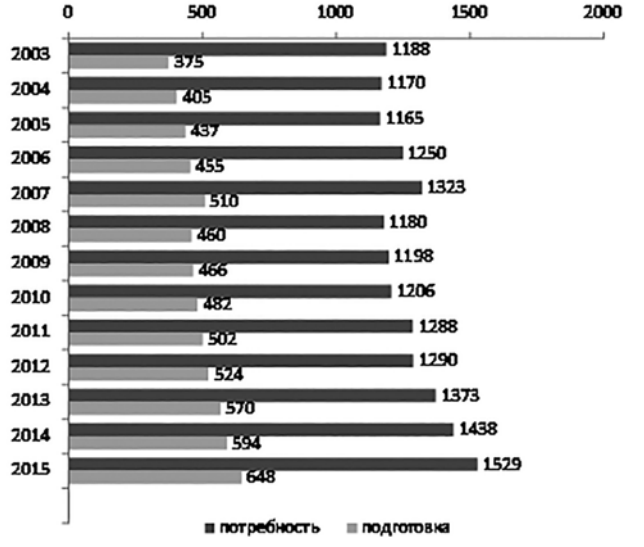


Рис. 2. Потребность и выпуск специалистов по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» (Fig. 2. Demand and graduation of specialists in the specialty «Complex provision of information security of automated systems»)

Объективными условиями возникновения этих диспропорций является неполное соответствие подготовки специалистов потребностям экономики страны. Не считаться с диспропорцией нельзя, поскольку она является причиной, с одной стороны, неполной обеспеченности кадрами, а с другой – роста безработицы или непрофильного использования специалистов. Все это в конечном счете отрицательно сказывается на эффективности развития отраслей экономики и приводит к потерям государственного бюджета. Для того чтобы избежать этих потерь, необходимо обеспечить соответствие между потребностями, подготовкой, трудоустройством и использованием специалистов.

Объективная возможность решения этой задачи заключается в прогнозировании возможных изменений в потребности в специалистах и учете их при формировании государственного заказа на подготовку контрольных цифр приема (КЦП). При этом важное значение имеет научное обоснование заявок на подготовку специалистов, что позволяет корректировать текущие и перспективные планы подготовки специалистов, осуществлять сокращение или расширение выпуска специалистов различных специальностей и направлений, воздействуя на миграцию специалистов, обеспечивая рациональное региональное размещение учебных заведений и т.д.

Причины существования этих да и ряда других проблем, по нашему мнению, заключаются в следующем:

• недостаточно проработаны концептуальные научные проблемы в сфере подготовки кадров в области информационной безопасности;

• отнесение нормативного и ресурсного обеспечения функционирования рассматриваемой системы подготовки кадров, а также вопросов закрепления специалистов в области информационной безопасности к компетенции различных федеральных органов исполнительной власти;

• недостаточное финансирование сферы образования и, как следствие, ограниченность финансовых средств, выделяемых со стороны Минобрнауки России, на проведение НИР по проблемам информационной безопасности, информационное и материально-техническое обеспечение рассматриваемой системы подготовки кадров;

• отставание нормативно-правового обеспечения деятельности в области ИБ.

Отметим еще и такое соображение. При непростой демографической ситуации, сложившейся в мире в целом, общем снижении интереса молодежи к сферам деятельности, связанным с решением инженерных проблем, задача кадрового сопровождения такой критической отрасли, как обеспечение ИБ, с опорой на национальные кадры приобретает первостепенное значение. Понятно, что ее решение требует существенных материальных и финансовых издержек. Вместе с тем в условиях рыночной экономики при решении вопросов развития профессионального образования весьма важной является проблема экономической эффективности затрат на образование. Кстати наиболее интересные результаты в этом направлении были получены в 60 – 70-х годах прошлого века советской экономической школой, возглавляемой академиками С.Г. Струмилиным и А.Г. Аганбегяном. С тех пор эта проблема практически выпала из внимания как отечественных, так и зарубежных экономистов.

Ориентируясь на пословицу, что «Новое – это хорошо забытое старое», попытаемся кратко проанализировать полученные в ту пору результаты и возможность их использования в современных условиях.

Прежде всего следует, на наш взгляд, отметить ошибочное и даже вредное (для обоснования затрат) отнесение образования к сфере услуг. При этом фактически забывается важнейшая социальная значимость образования и его роль в развитии научно-технического прогресса, формировании инновационной экономики.

Представляется, что затраты на образование в узко экономическом смысле аналогичны затратам на средства производства. Они также представляют собой издержки на создание необходимых предпосылок производства. Затраты на образование и на средства производства взаимно дополня-

ют друг друга. Они содействуют созданию материальных и интеллектуальных факторов повышения производительности труда и развития производства. Иначе говоря, затраты на средства производства и на образование есть составные части издержек, которое общество должно нести, чтобы придать живому труду способность производить большее количество потребительных стоимостей. Эта мысль подтверждается рядом публикаций рассматриваемого нами периода [8 - 12].

Таким образом, рассмотрение особенностей воздействия образования на производство позволяет выделить три возможных направления определения экономической эффективности затрат на образование в современных условиях.

Во-первых, затраты на образование работников должны учитываться наряду с другими издержками при определении эффективности капитальных вложений как в масштабе всей экономики, так и по отдельным отраслям и объектам.

Во-вторых, важнейшим обобщающим показателем соотношения между развитием производства и образованием является результат сопоставления объема выпускаемой продукции с суммой кумулятивных общественных издержек на все необходимое образование, которым обладают работники, вовлеченные в производство продукции. Этот показатель сходен с показателем капиталоемкости (фондоемкости), выражающим эффективность использования основных средств производства.

В-третьих, практическое определение экономической эффективности затрат на образование возможно также на основе исчисления потерь общества от недостаточной квалификации кадров в конкретных производственных звеньях экономики.

В этой связи сошлемся на работу [13], посвященную анализу взаимосвязи численности принимаемых на обучение по программам высшего образования УГСНП «Информационная безопасность» и социально-экономических показателей субъектов федерации. Исследование проведено на примере Центрального федерального округа. Оказалось, что численность принимаемых на обучение в большинстве случаев напрямую связана с таким показателем как доля регионального валового продукта субъекта, приходящаяся на душу населения.

Анализ изложенных выше соображений, а также выход проблемы информационной безопасности в ряд важнейших компонентов национальной безопасности, на наш взгляд, требует разработки и последовательной реализации специальной федеральной целевой программы развития системы подготовки кадров в области информационной безопасности в Российской Федерации.

Представляется, что для координации образовательной деятельности по повышению квалификации и переподготовке преподавательских кадров, реализующих программы в области ИБ, проведения научно-исследовательской работы в данной области было бы целесообразно преобразовать ФУМО ИБ в специальный федеральный учебно-методический комплекс. Это тем более целесообразно, когда одной из форм госрегулирования является мониторинг качества образования, даваемого вузами, который и мог бы взять на себя указанный комплекс.

Для практической реализации эффективной системы оценки качества образования в рамках специальностей и направлений по ИБ необходимо создание развитой нормативной базы как основания для построения оценочных средств и технологий мониторинга качества образования. В настоящее время такая нормативная база существует в виде совокупности федеральных государственных образовательных стандартов.

Для того чтобы ФГОС могли выполнять роль нормативной базы мониторинга в системе оценки качества образования, содержащиеся в них требования (в виде приобретаемых в процессе обучения компетенций) должны быть сформулированы с учетом принципа диагностики (проверяемости, контролируемости).

Необходимо отметить, что на сегодня в ФУМО ИБ реализован ряд положений с целью усиления такой диагностичности, хотя еще далеко не для всех требований. В них, в частности, заданы критерии сформированности умений и знаний у выпускника по уровням «иметь представление», «знать», «уметь», «владеть».

Подготовлены также комплекты контрольных заданий по основным дисциплинам каждого цикла дисциплин по ряду специальностей и направлений (опять же далеко не по всем). Разработаны примерные требования к образовательной среде и образовательному процессу, применяемые при лицензировании вузов. С целью получения оценки качества подготовки специалиста через год его практической деятельности разработана анкета-отзыв потребителя на выпускника.

Таким образом, можно говорить, что в целом нормативная база для мониторинга качества подготовки специалистов в первом приближении имеется.

В дальнейшем необходимо определить, кто и как будет осуществлять данный мониторинг. В соответствии с законодательством Российской Федерации государственный контроль возложен на государственные органы управления образованием (Рособрнадзор). Однако представляется, что наряду с этим необходимо усилить роль ФУМО в области контроля качества высшего образования. В частности, было бы полезно создать на базе ФУМО государственно-общественный центр сертификации качества высшего образования в области ИБ. Для усиления государственного регулирования вопросов подготовки специалистов в состав центра целесообразно включить помимо представителей высшей школы представителей от ФСБ, ФСТЭК и других структур – государственных регуляторов.

Качество высшего образования и качество специалистов в последнее время увязываются с требованиями профессиональных стандартов в области ИБ. Инструментами для оценки такой взаимосвязи должны стать внедряемые в настоящее время процедуры профессионально-общественной аккредитации образовательных программ и независимая оценка квалификаций специалистов.

И несколько слов о закреплении кадров. Очевидно, что какой бы эффективной система подготовки специалистов в области ИБ ни была, она не сможет обеспечить кадрами потребителей (прежде всего госструктуры), если в стране не будет создана эффективная система закрепления кадров. А пока системного решения этой проблемы нет.

Выводы

В целом с учетом всех современных задач кадрового обеспечения ИБ, как того требует формирование цифровой экономики и реализация положений Доктрины информационной безопасности Российской Федерации, основные направления дальнейшего совершенствования системы подготовки специалистов в области ИБ, на наш взгляд, должны включать следующее:

- поддержку функционирования и дальнейшее развитие группы специальностей и направлений в области ИБ;
- разработку государственных образовательных стандартов и образовательных программ, в том числе и новых, при активном участии министерств и ведомств, регулирующих данную сферу деятельности;
- определение и формирование государственного кадрового заказа, особенно в интересах силовых министерств и ведомств;
- мониторинг использования специалистов в области информационной безопасности;
- формирование при государственной поддержке системы массового обучения культуре информационной безопасности (своего рода «всеобуча», в том числе на основе использования Единой образовательной среды), повышение уровня культуры личной информационной безопасности граждан страны;
- финансовое и материально-техническое обеспечение подготовки специалистов со стороны государства и ведомств, в том числе на условиях кооперации;
- нормативное оформление порядка лицензирования и контроля образовательной деятельности в области информационной безопасности;
- издание и использование в образовательном процессе учебно-методической литературы (в том числе электронных изданий), прошедшей экспертизу в ФУМО и соответствующих ведомствах;
- аттестацию и подготовку педагогических кадров в области защиты информации.

И еще одно замечание. На наш взгляд, серьезно стоит проблема участия ФУМО ИБ в лицензировании вузов по специальностям и направлениям подготовки, не входящим в объединенную группу 2.10.00.00 ОКСО, но напрямую посвященным ИБ, что требует более тесного взаимодействия с УМО или УМС, «смежными» с этой группой.

СПИСОК ЛИТЕРАТУРЫ:

1. Малюк А.А. Формирование культуры информационной безопасности общества // М.: Педагогика. ISSN: 0869-561X. № 3, 2009. С. 33-39. (https://elibrary.ru/item.asp?id=12609790).
2. Павлова Е.Д. Медиаобразование как способ формирования национальной информационной культуры// Приоритетные национальные проекты: первые итоги и перспективы реализации (Отв. ред. Ю.С. Пивоваров). – М.: ИНИОН РАН, 2007.
3. Malyuk A., Tolstoy A. Personnel Training for Information Security Maintenance in Russia // First World Conference on Information Security Education, Sweden, Kista, 1999.
4. Malyuk A., Miloslavskaya N., Tolstoy A. The Russian Experience Information Security Education // Second World Conference on Information Security Education, Perth, Western Australia, 2001.
5. Malyuk A., Miloslavskaya N., Tolstoy A. Teaching undergraduate information assurance in Russia // Third annual World Conference on Information Security Education, Monterey, California, USA, 2003.
6. Малюк А.А. Анализ и прогнозирование потребности в специалистах по защите информации. – М.: Горячая линия – Телеком, 2014.
7. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Создание глобальной культуры кибербезопасности». https://undocs.org/ru/A/RES/57/239
8. Марцинкевич В.И. Образование в США: экономическое значение и эффективность. – М.: Наука, 1967.
9. Жамин В.А. Экономика образования (вопросы теории и практики). – М.: Просвещение, 1969.
10. Волков Ф.М. Воспроизводство квалифицированной рабочей силы в СССР. – М.: Соцэкгиз, 1961.
11. Толыпин Ю.М. Действие закона экономии времени и новая методология его математического анализа.– М.: изд-во МГУ, 1964.
12. Я. Гомберг. Редукция труда. – М.: Экономика, 1965.
13. Лось В.П., Тышук Е.Д. Анализ взаимосвязи численности принимаемых на обучение по программам высшего образования УГСНП «Информационная безопасность» и социально-экономических показателей субъектов федерации (на примере Центрального федерального округа) / «Информация и безопасность», 2017, Т.20, № 3 (4).

REFERENCES:

[1] Malyuk A. Forming culture of society's information security. M.: Pedagogika. ISSN: 0869-561X. № 3, 2009. P. 33-39. (https://elibrary.ru/item.asp?id=12609790). (in Russian).
[2] Pavlova E.D. Media education as a way of formation of national information culture. Prioritetnije nacionalnije projekti: pervije itogi i perspektivi pealizacii. (otv. red. Ju.S. Pivovarov. – M.: INION RAN, 2007. (in Russian).
[3] Malyuk A., Tolstoy A. Personnel Training for Information Security Maintenance in Russia. First World Conference on Information Security Education, Sweden, Kista, 1999.
[4] Malyuk A., Miloslavskaya N., Tolstoy A. The Russian Experience Information Security Education. Second World Conference on Information Security Education, Perth, Western Australia, 2001.
[5] Malyuk A., Miloslavskaya N., Tolstoy A. Teaching undergraduate information assurance in Russia. Third annual World Conference on Information Security Education, Monterey, California, USA, 2003.
[6] Malyuk A.A. Analysis and forecasting of the need for information security specialists. – M.: Goryachaja linija–Telekom, 2014. (in Russian).
[7] Resolution of the UN General Assembly A/RES/57/239 «Creating a global culture of cybersecurity». https://undocs.org/ru/A/RES/57/239. (in Russian).
[8] Marcinkevich V.I. Education in the USA: economic value and efficiency. – M.: Nauka, 1967. (in Russian).
[9] Zhamin V.A. Economics of education (theory and practice). – M.: Prosveschenije, 1969. (in Russian).
[10] Volkov F.M. The reproduction of skilled labor in the USSR. – M.: Socekgiz, 1961. (in Russian).
[11] Tolipin Ju.M. Effect of the law of time saving and new methodology of its mathematical analysis. – M.: Ekonomika, 1964. (in Russian).
[12] Ja. Gomberg. Reduction of labor. – M.: Ekonomika, 1965. (in Russian).

[13] Los V.P., Tischuk Je.D. Analysis of the relationship between the number of students enrolled in higher education programs of areas of education «Information security» and socio-economic indicators of the subjects of the Federation (for example, the Central Federal district). «Informacija i Bezopasnost», 2017, T.20, N 3(4). (in Russian).

Поступила в редакцию – 17 сентября 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – September 17, 2018. The final version – November 01, 2018.

Владимир И. Будзко, Дмитрий А. Мельников
Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, г. Москва, 119333, Россия
e-mail: vbudzko@ipiran.ru, https://orcid.org/ 0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

ИСТОРИЧЕСКИЙ РАКУРС ТЕХНОЛОГИИ «BLOCKCHAIN». «ВСЁ НОВОЕ – ХОРОШО ЗАБЫТОЕ СТАРОЕ»

DOI: http://dx.doi.org/10.26583/bit.2018.4.02

Аннотация. Блокчейн-технология (БЧ-технология) представляет неизменяемые распределённые системы цифровых реестров без центрального хранилища/репозитария, как правило, не имеющие единого центра управления. В настоящее время существует большой ажиотаж вокруг использования БЧ-технологии, хотя сама технология, с одной стороны, многим ещё не совсем понятна, а с другой (и это главное) – не нова. Поверхностное представление о БЧ-технологии как о феномене с «волшебными свойствами» приводит к многочисленным прогнозам о возможности революционных преобразований на основе её применения целых отраслей экономики и прежде всего в кредитно-финансовой сфере (КФС). В связи с этим в настоящей статье представлены систематизированный анализ, история возникновения БЧ-технологии, ведущая своё начало с международных стандартов ISO 7498-2 от 1989 года и ITU-T X.800 от 1991 года. Дано краткое неформальное определение БЧ-технологии, рассмотрены ее основные принципы и компоненты, среди которых криптографические однонаправленные функции (ОНФ), транзакции, адреса и их извлечение, реестры, блоки, операции с последовательностями блоков. Представление БЧ-технологии как последовательности блоков, связанных на основе известных способов обеспечения целостности данных с использованием ассиметричной криптографии, позволяет сделать вывод о возможности только эволюционного развития ее применений, хотя и быстрыми темпами в масштабе реального времени, что является характерной особенностью современного этапа становления и всех остальных разновидностей IT-технологий. В заключение обращено внимание на необходимость проведения дополнительных исследований оценки защищённости и надёжности БЧ-технологии в аспекте оценки перспектив её применения в конкретных бизнес-приложениях и системах критической информационной инфраструктуры.

Ключевые слова: блокчейн, цифровой реестр, криптовалюта, электронный кошелёк, электронная подпись, транзакция, целостность виртуального соединения, открытый ключ, однонаправленная функция, компендиум, сертификат, аутентификация, неотказуемость.

Для цитирования: БУДЗКО, Владимир И.; МЕЛЬНИКОВ, Дмитрий А. ИСТОРИЧЕСКИЙ РАКУРС ТЕХНОЛОГИИ «BLOCKCHAIN». «ВСЁ НОВОЕ – ХОРОШО ЗАБЫТОЕ СТАРОЕ». Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 23-33, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1158>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.02.

Vladimir I. Budzko, Dmitry A. Melnikov
Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Vavilov str., 44/2, Moscow, 119333, Russia
e-mail: vbudzko@ipiran.ru, https://orcid.org/0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

The Historical View Of The Blockchain Technology. The More Things Change, the More They Stay the Same

DOI: http://dx.doi.org/10.26583/bit.2018.4.02

Abstract. Blockchain technologies (BC) are immutable distributed systems of digital ledgers (i.e., without central repository) and, as rule, without central authority. Currently, there is a lot of excitement around the use of BC

technology, although the technology itself, on the one hand, is still not quite clear to many ones, and on the other (and this is the main thing) is not new. Superficial understanding of the BC as a phenomenon with «magical properties» leads to numerous predictions about the possibility of revolutionary transformations based on its application to entire sectors of the economy and, above all, in the credit and financial sphere. In this regard, this article presents a systematized analysis, the history of the BC emergence, leading from the international standards ISO 7498-2 of 1989 and ITU-T X.800 of 1991, as well as a brief informal definition of BC and considered are the basic principles and components of this technology, including cryptographic one-way functions (hashes), transactions, addresses and their retrieval, «digital wallets», ledgers, blocks, blockchain in operations. Representation of the BC as a sequence of blocks bounded base on known mechanisms of the data integrity with using asymmetric cryptography allows us to conclude that only its evolutionary development is possible, although at a rapid pace in real time. This is a characteristic feature of establishing modern stage of and all other IT types. In conclusion, attention is drawn to the need for additional research to assess the security and reliability of the BC in terms of assessing the prospects for its use in specific business applications and critical information infrastructure systems.
Keywords: blockchain; ledger; repository; cryptocurrency; digital wallet; digital signature; transaction; connection integrity; public key; one way function; compendium; certificate; authentication; non-repudiation.
For citation: BUDZKO, Vladimir I.; MELNIKOV, Dmitry A. The historical view of the blockchain technology. The more things change, the more they stay the same. IT Security (Russia), [S.l.], v. 25, n. 4, p. 23-33, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1158>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.02.

Введение

В настоящее время в связи с объявлением программы цифровизации экономики существует ажиотаж вокруг вопроса применения технологии «блокчейн» (БЧ, *blockchain*), хотя сама технология многим ещё не совсем понятна, а главное – не нова. Множество статей и видеоматериалов научно-популярного характера описывают «волшебные» свойства БЧ-технологии[1], хотя в ней нет ничего «магического», так как эта технология базируется на хорошо известных специалистам принципах и поэтому не способна решить все проблемы. Как и в случае со всеми «новыми» веяниями, существует тенденция, связанная со стремлением применить её в каждом секторе экономики (бизнес-проекте), причём самым невероятным образом. БЧ-технология – последовательность (цепочка) криптографически связанных блоков. Система БЧ (СБЧ) представляет собой совокупность неизменяемых цифровых реестров (хранилищ, *ledger*), объединённых в распределённую структуру (т.е. без центрального хранилища – репозитария, *central repository*) и, как правило, не имеющих единого центра управления. СБЧ позволяет сообществам пользователей регистрировать транзакции в хранилище, которое открыто для этого сообщества. После того как транзакция стала открытой, она не может быть изменена в дальнейшем. В 2008 году идея БЧ [1] была объединена инновационным образом с несколькими другими технологиями и вычислительными ресурсами, что обеспечило формирование современных криптовалют (*cryptocurrencies*), т.е. электронных денег, защищённых с помощью криптографических методов, без центрального репозитария. Первая криптовалюта, основанная на СБЧ, была «Биткоин» (*BTC*, «*Bitcoin*» [2]). Новизна таких валют на основе СБЧ заключается в том, что они якобы имеют стоимостное выражение (*value*), а не только информационный контент. Стоимость «привязывается» к «электронному кошельку» (*digital wallet*), представляющему собой комплекс программного обеспечения (КПО), который позволяет его владельцу осуществлять электронные торговые сделки (*transactions*). Кошельки используются для подписи торговых сделок, которые транслируются из одного кошелька в другой, и регистрируют доставленную стоимость открыто, что обеспечивает всем пользователям сети возможность проведения независимой проверки подлинности транзакций. Каждый пользователь (участник СБЧ) может хранить полную запись всех транзакций, что делает сеть устойчивой к попыткам модифицировать такую запись (или фальсифицировать транзакции) в дальнейшем. Как правило, каждая транзакция включает в себя один или несколько адресов

[1]Например, в Финансовом университете при Правительстве Российской Федерации проводятся платные курсы (16800 ₽) по изучению БЧ-технологии («Криптовалюты и технологии блокчейн. Смарт-контракты и коллективное инвестирование»), которые призваны показать слушателям её «безграничные» возможности (http://www.fa.ru/org/dpo/fintechschool/Pages/bc.aspx).

и запись того, что произошло, а также электронную подпись (ЭП). БЧ состоят из блоков, каждый блок представляет собой группу транзакций. Все транзакции в блоке группируются вместе и объединяются с результатом вычисления криптографической однонаправленной функции предыдущего блока (называемой *свёрткой (компендиумом) сообщения* (*message digest*) или просто *компендиумом*, *compendium*) [3]. Наконец вычисляется новый компендиум (C_m) для заголовка текущего блока с целью его размещения в самих данных блока, а также в следующем блоке. Далее каждый блок «привязывается» к предыдущему блоку в «цепочке» (последовательности) блоков путём добавления компендиума предыдущего блока в заголовок текущего блока (рис. 1).

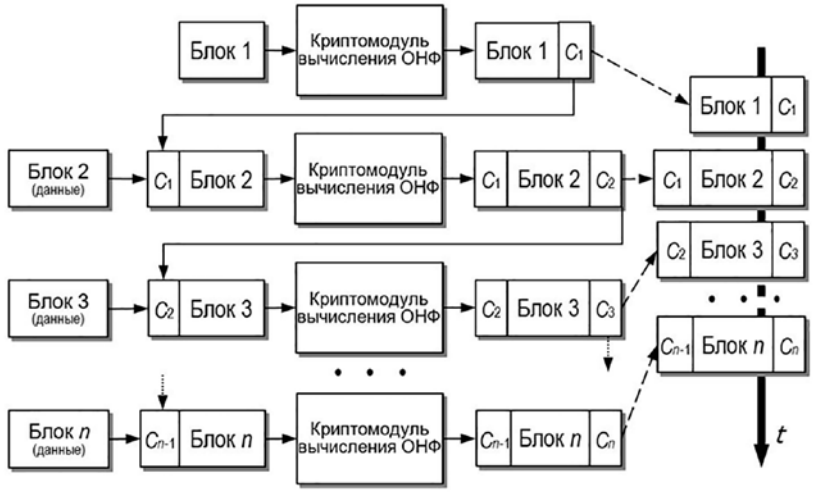


Рис. 1. Принцип формирования последовательности (цепочки) блоков данных
(Fig. 1. The sequence (chain) of data blocks creation principle)

В данной статье проанализирована ретроспектива появления и основные аспекты БЧ-технологии, а также сделан вывод о её дальнейшем применении.

1 Ретроспектива

Первое упоминание о «последовательности блоков», связанных с помощью криптографической функции (*binding*), появилось почти 30 лет назад в международном стандарте ISO 7498-2 от 1989 года [4], положившем начало развитию всей международной системы стандартизации в области информационной безопасности (ИБ). Полный аналог стандарта ISO 7498-2 – Рекомендация X.800 Международного союза электросвязи [5], вышедшая в 1991 году, в которой представлено понятие «*способ обеспечения целостности данных*» (*data integrity mechanism*) и, в частности, понятие «криптографическая связка».

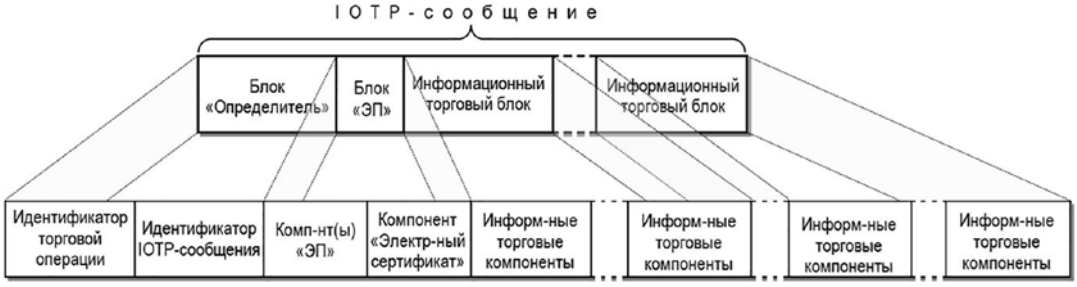


Рис. 2. Формат IOTP-сообщения
(Fig. 2. IOTP message structure)

Указанный способ обеспечения целостности широко применяется в электронной коммерции [6]. В интернет-сообществе принят стандарт RFC-2801 под названием «*Internet Open Trading*

Protocol» (IOTPv1) [7]. Формат IOTP-сообщения представлен на рис. 2, а структура торговой транзакции IOTP-протокола – на рис. 3 [8].

Оба рисунка показывают, что каждая из взаимодействующих сторон (покупатель и продавец) подписывает каждое своё IOTP-сообщение, при этом каждая из них прибавляет к полученному IOTP-сообщению новый информационный торговый блок (ИТБ). В итоге завершающее IOTP-сообщение представляет собой последовательность ИТБ, в начале которой располагается определитель последовательности и субпоследовательность, состоящая из электронных подписей (ЭП) и сертификатов открытых ключей (СЕРТ|ОК) каждой из сторон. Наличие СЕРТ|ОК (это принципиальное отличие от СБЧ) позволяет проверить подлинность транзакции путём проверки владельца закрытого ключа ЭП и того, что на момент подписания электронного документа пара ключей не была просрочена и/или скомпрометирована. А в дальнейшем ЭП обеспечивает неотказуемость любой из сторон электронной торговой сделки, т.е. обеспечивает невозможность отказа любой из сторон от участия в транзакции.

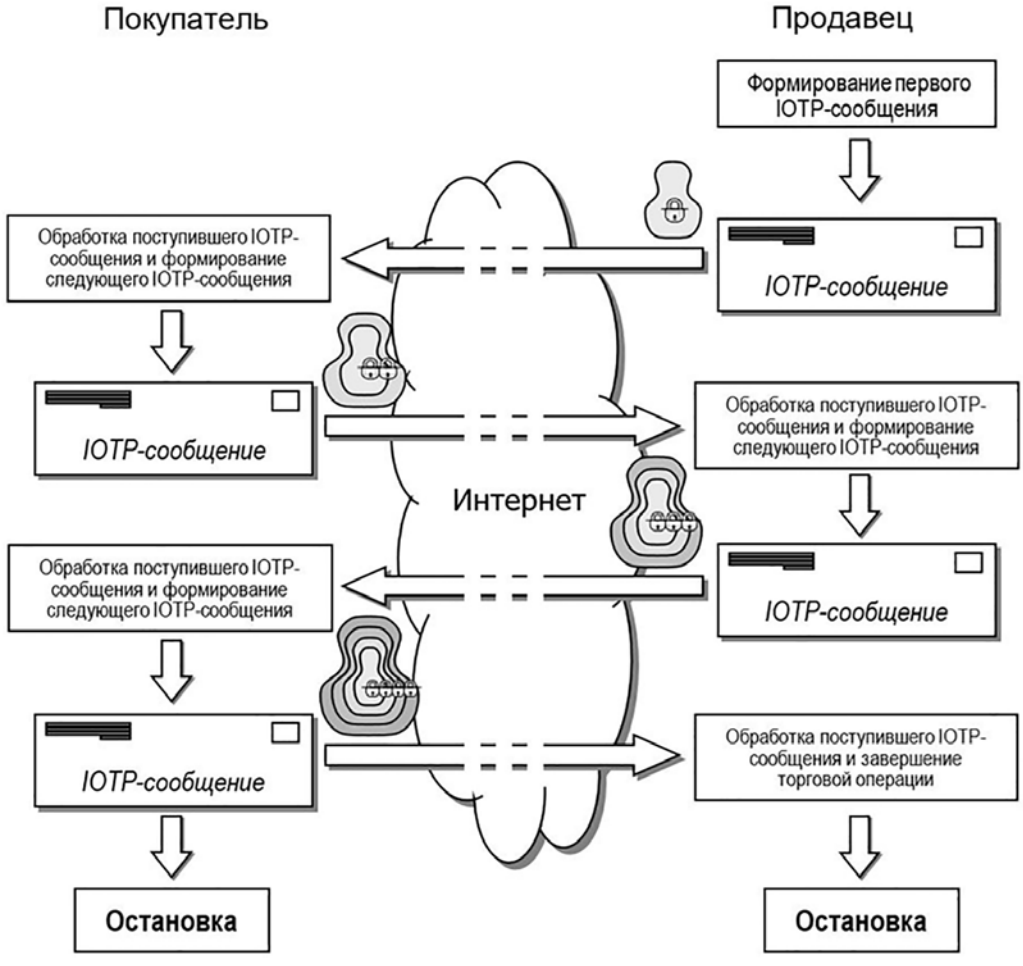


Рис. 3. Структура торговой операции (транзакции) IOTP-протокола
(Fig. 3. IOTP transaction)

В августе 2002 года был принят новый интернет-стандарт под названием «*Internet Open Trading Protocol Version 2 Requirements*» [9], в котором, в частности, содержатся два основных требования: отсутствие ограничений на число транзакций, включаемых в цепочку ИТБ (последовательность ИТБ может включать любое их число); наличие электронных кошельков в составе прикладных серверов (обязательное наличие КПО, реализующего функции электронного кошелька).

С прикладной точки зрения IOTP-протокол широко использует ассиметричные криптографические системы, а именно: ЭП, СЕРТ|ОК, инфраструктуру открытых ключей (*public key infrastructure*, PKI) [3] и соответствующие системы проверки ЭП и их авторов на основе подтверждения подлинности СЕРТ|ОК.

2 Основные принципы и компоненты СБЧ

СБЧ – это системы неизменяемых цифровых реестров, реализованные по распределенной структуре и, как правило, без центрального органа управления и контроля [10]. Они позволяют сообществу пользователей записывать транзакции в реестр, общедоступный для данного сообщества, и, как следствие, никакая транзакция после её опубликования не может быть изменена. Эта технология стала всемирно известной начиная с 2008 года (т.е. после IOTP-протокола), когда она была использована с целью создания условий появления и применения цифровых валют в распределённых финансовых системах, в которых осуществляется доставка электронных денег. Она способствовала развитию систем электронной коммерции, таких как «*Bitcoin*» (*BTC*) [2], «*Ethereum*» [11], «*Ripple*» [12] и «*Litecoin*» [13]. Из-за этого СБЧ очень часто рассматриваются как системы, связанные с *BTC* или, возможно, с электронными финансовыми системами в целом. Однако эта технология нашла более широкое применение и доступна для самых различных прикладных автоматизированных информационных систем (АИС).

С неформальной точки зрения, *БЧ-технологии* – это последовательности криптографически связанных блоков, которые представляют собой распределённые цифровые реестры, содержащие криптографически подписанные транзакции, сгруппированные в блоки. Каждый блок криптографически привязан к предыдущему блоку после подтверждения подлинности и принятия общего согласованного решения. Так как в последовательности криптографически связанных блоков постоянно добавляются новые блоки, модифицировать старые блоки становится всё значительно сложнее. Новые блоки дублируются во всех копиях реестров в сети, а любые конфликты разрешаются автоматически с использованием установленных правил.

2.1 Терминология

Для описания особенностей БЧ-компонентов используются термины «пользователь» (*user*) и «узел» (*node*). Термин «пользователь» может соотноситься с физическим лицом, организацией, объектом, бизнесом, ведомством и т.д., которые используют СБЧ. Термин «узел» означает систему внутри СБЧ и может означать «полнофункциональный узел» (*full node*, который хранит всю БЧ), «добывающий узел» (ДУ, *mining node*, полнофункциональный узел, который «публикует» новые блоки) или «усечённый узел» (УУ, *lightweight node*, узел, который не хранит всю БЧ).

2.2 Архитектура СБЧ

На самом верхнем уровне архитектура СБЧ использует стандартные компьютерные технологии («связанные» перечни (списки), распределённые вычислительные сети), а также криптографические алгоритмы и способы (ОНФ, ЭП, открытые/закрытые ключи), которые объединены с финансовыми концепциями (например, реестры).

2.2.1 ОНФ

Важный компонент БЧ-технологии – криптографическая ОНФ, которая применяется во многих процедурах, например, вычисление ОНФ по содержанию блока. Во многих БЧ-технологиях используется стандартный алгоритм вычисления ОНФ «*SHA*» (*Secure Hash Algorithm*) [14], который даёт выходную последовательность длиной 256 бит (SHA_{256}). Результат вычисления SHA_{256} – выходная последовательность, состоящая из 32 8-битовых субпоследовательностей. Из этого следует, что возможное число компендиумов составляет

$$2^{256} \approx 10^{77}, \text{ или}$$

1157920892373161954235709850086879078532699846656405640394575840079131296399 36.
SHA_{256}-алгоритм считается устойчивым к коллизиям, так как для нахождения коллизии необходимо повторить SHA_{256}-алгоритм примерно 2^{128} раз.

2.2.2 Транзакции

В СБЧ под транзакцией понимается запись доставленных активов между взаимодействующими сторонами. Каждый блок в СБЧ включает несколько транзакций. Отдельная транзакция, как минимум, включает следующие информационные поля: *сумму* (*amount*) – общую сумму цифровых активов, предназначенных для доставки; *входные данные* (*inputs*) – перечень цифровых активов, которые подлежат доставке (их общая стоимость равна сумме); *выходные данные* (*outputs*) – учётные записи, определяющие получателей цифровых активов; *идентификатор/компендиум транзакции* (*transaction ID*/*Hash*) – уникальный идентификатор каждой транзакции.

2.2.3 Адреса и извлечение адресов

Адрес пользователя представляет собой короткую буквенно-цифровую последовательность (C_{Kp}), извлекаемую из открытого ключа (K_p) пользователя с использованием ОНФ (F_H), которая дополняется некоторыми данными (используемыми для обнаружения ошибок). Адреса короче открытых ключей, они несекретные. Как правило, процедура формирования адреса означает получение открытого ключа, его преобразование с помощью ОНФ и преобразование полученного компендиума в текстовый формат:

$$\text{открытый ключ } (K_p) \rightarrow \text{ОНФ } (F_H(K_p)) \rightarrow \text{адрес } (C_{Kp})$$

Пользователи по своему желанию могут сформировать достаточно много пар ключей и, следовательно, много адресов, что позволяет им варьировать уровни псевдоанонимности. Адреса выступают в качестве открытых параметров подлинности пользователей в СБЧ, и часто адрес преобразуется в QR-код.

Когда СБЧ распределяет цифровые активы, она делает это путём присвоения им адресов. Чтобы потратить такой цифровой актив, пользователь должен доказать, что он (и только он) владелец закрытого ключа, соответствующего адресу.

2.2.4 Хранилище закрытых ключей

Большинство пользователей СБЧ не регистрируют свои закрытые ключи вручную, а, скорее всего, для их надёжного хранения будут использовать КПО, обычно именуемый как (электронный) *«кошелёк»*. Электронный кошелёк (ЭК) может хранить закрытые ключи, открытые ключи и связанные с ними адреса. Кроме того, программная реализация ЭК может рассчитывать общее количество активов, которое может иметь пользователь.

Хранилище закрытых ключей – чрезвычайно важный компонент БЧ-технологии. В большинстве случаев БЧ-данные не могут быть изменены, поэтому после компрометации закрытого ключа и публичного перемещения связанных с этим ключом финансовых средств на другой счёт такую незаконную транзакцию отменить уже нельзя.

2.2.5 Реестры (электронные журналы бухгалтерского учёта)

Реестр представляет собой совокупность зарегистрированных транзакций [15, 16]. В настоящее время книги бухгалтерского учёта хранятся в цифровом виде (реестры), как правило, в больших БД, которые принадлежат и обслуживаются исключительно централизованными доверенными третьими сторонами (ДТС) от имени сообщества пользователей (т.е. ДТС – владелец реестра).

Несомненно, что любой централизованный реестр заинтересован в создании резервных копий данных, подтверждении подлинности транзакций, включении всех подлинных транзакций и неизменении истории. Встроенный реестр, использующий БЧ-технологию, может снизить остро-

ту указанных проблем за счёт использования способа распределённого согласования (консенсуса). БЧ-реестр будет дублироваться и распределяться между всеми узлами в системе.

Всякий раз, когда новые пользователи присоединяются к системе, они получают полную БЧ-копию, что затрудняет потерю или модификацию реестра. Все транзакции хранятся в блоках внутри СБЧ.

2.2.6 Блоки

Пользователи могут направлять в реестр транзакции-претенденты путём передачи таких транзакций в некоторые узлы, которые участвуют в СБЧ. Отправленные транзакции распространяются по другим узлам сети, но это само по себе не обеспечивает включения транзакции в СБЧ. Распределённые транзакции после этого ожидают в очереди, до тех пор пока не будут добавлены ДУ в СБЧ.

ДУ представляют собой подмножество узлов, которые обслуживают СБЧ путём опубликования новых блоков. Транзакции добавляются в СБЧ, когда ДУ публикуют блок. Блок включает совокупность подтверждённых транзакций. «Подлинность» гарантируется путём проверки того, что поставщикам финансовых средств в каждой транзакции принадлежит каждая криптографически подписанная транзакция.

Другие ДУ будут проверять подлинность всех транзакций в опубликованном блоке, и если блок будет содержать какие-либо недействительные транзакции, то его отвергнут.

После своего формирования каждый блок проходит обработку в соответствии с ОНФ-алгоритмом. В результате формируется компендиум, отображающий блок. Все узлы получат копию компендиума блока и затем смогут убедиться в том, что блок не был модифицирован.

На рис. 4 показан примерный состав «поля» данных, входящего в блок. «Уникальное слово» (*nonce value*) – это число, контролируемое (формируемое) ДУ с целью решения ОНФ-задачи, которое даёт ему право опубликования блока.

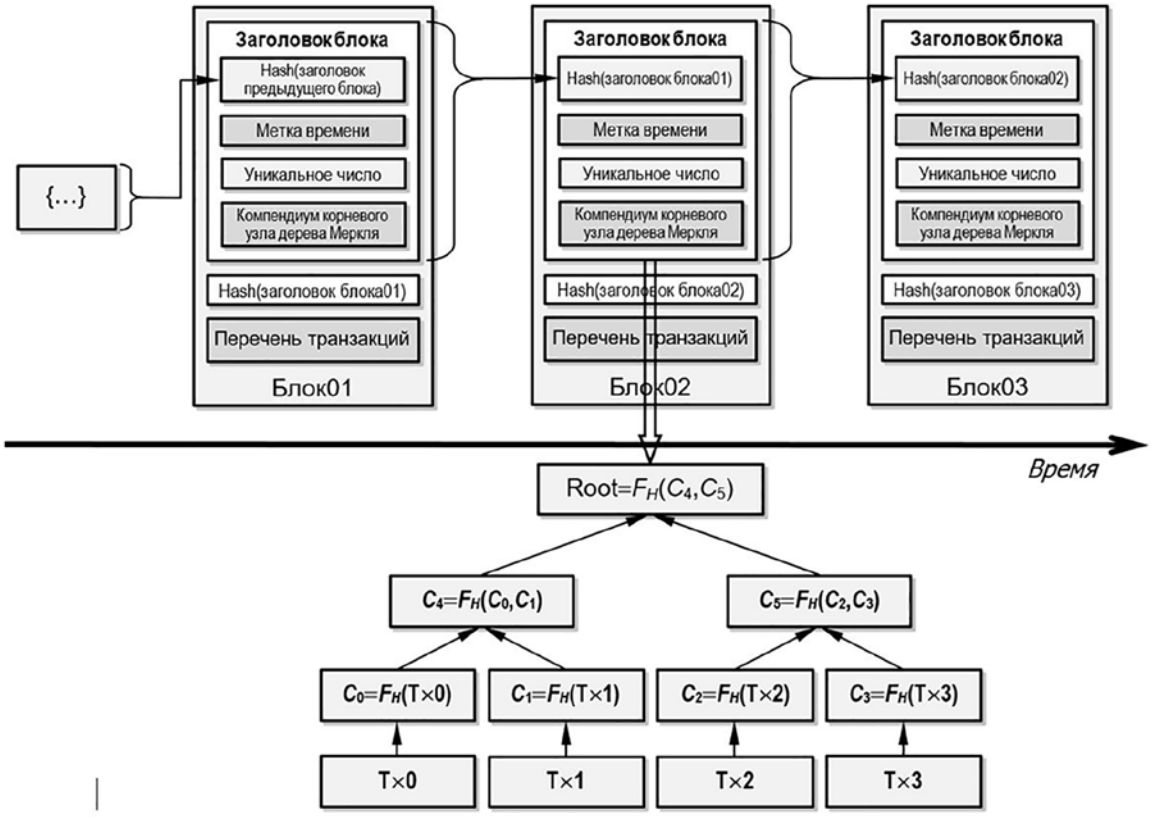


Рис. 4. БЧС на основе «дерева Меркли»
(Fig. 4. Blockchain with Merkle tree)

Вместо того чтобы хранить компендиум каждой транзакции в заголовке блока, используется структура данных, известная как «дерево Меркля» (ДМ, *Merkle tree* [1]). ДМ объединяет компендиумы данных до тех пор, пока существует единый корневой узел ДМ. Такой узел обеспечивает объединение транзакций в блоке и возможность проверки наличия транзакции в составе блока. Такая структура гарантирует, что данные, переданные по распределённой сети, достоверны, так как любое изменение исходных данных может быть обнаружено и такие данные могут быть отвергнуты. На рис. 5 представлен пример ДМ. Взаимосвязи между ДМ и блоком показаны на рис. 4.

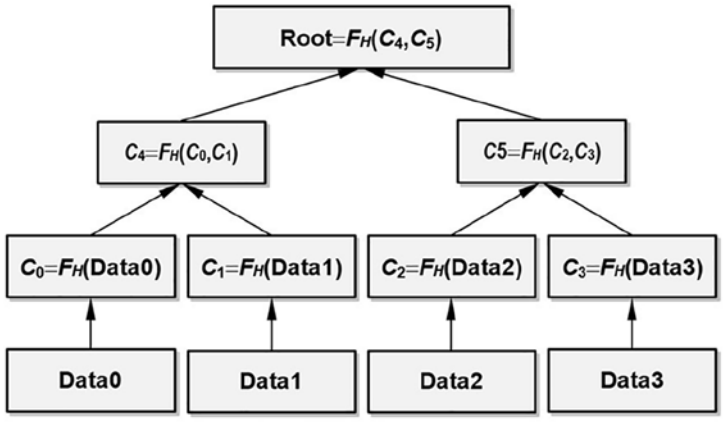


Рис. 5. Пример «дерева Меркля»
Fig. 5. Example Merkle Tree

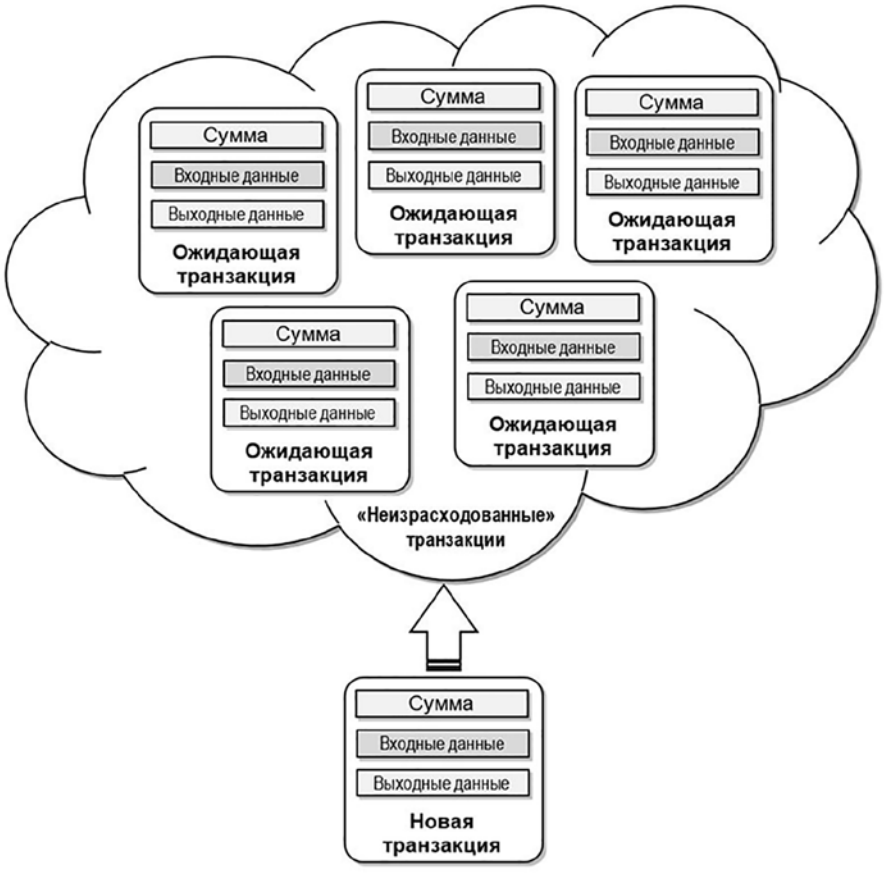


Рис. 6. Добавление транзакции в пул «неизрасходованных» транзакций
(Fig. 6. Transaction being added to unspent transaction pool)

3 Операции с последовательностями (цепочками) блоков

Рассмотрим процесс расширения СБЧ «без разрешения», который использует способ согласования (консенсуса) с доказательством «выполненной работы» (используется системой *BTC* и её аналогами). СБЧ функционируют на основании консенсуса (согласия) группы ДУ, использующих КПО БЧ. Каждый узел хранит копию БЧ и может предложить новый блок другим ДУ. Недействительные блоки будут выявляться и уничтожаться, так как весьма трудно вычислить действительный блок, но с вычислительной точки зрения его очень легко проверить. Добыча (*mining*, «майнинг») – это преднамеренно ресурсоёмкая задача, требующая больших объёмов вычислительной мощности, памяти или того и другого одновременно, что зависит от конкретной прикладной АИС с БЧ.

Функционирование ДУ заключается в хранении БЧ-данных, отправке данных другим узлам и обеспечении гарантий того, что вновь добавленные блоки действительные (подлинные). Подлинность обеспечивает гарантии того, что формат блока корректен, все компендиумы в новом блоке были вычислены правильно, новый блок содержит компендиум предыдущего блока, и каждая транзакция в блоке действительна и подписана соответствующими сторонами. ДУ могут формировать новые блоки. УУ не нужно хранить полные БЧ-копии, и очень часто они отправляют свои данные на обработку в полномасштабные узлы. УУ, как правило, встраиваются в смартфоны и устройства сети интернет-вещей. Такие устройства имеют ограниченные вычислительные ресурсы и/или объёмы памяти.

Предложенные транзакции в рамках СБЧ хранятся в ДУ в составе *пула «неизрасходованных» транзакций*, которые ожидают включения в блок (рис. 6).

Некоторые СБЧ требуют счёт об оплате за формирование нового блока, – например, за потраченное время и ресурсы или за предоставление привилегий. В системах, в которых требуются время и ресурсы, ДУ вычисляет несколько (достаточно много) значений случайных уникальных слов с целью попытки решить сложную с вычислительной точки зрения задачу («головоломку», *puzzle*).

ДУ-победитель получает право опубликовать следующий блок. Как правило, перед решением задачи ДУ опробуют много возможных значений уникальных слов. После того как задача будет решена, узел вычисляет компендиум данных блока и хранит его внутри самого блока. На рис. 7 представлена многоуровневая структура сформированного блока.

Рис. 7. Заключительный (обобщённый) блок
(Fig.7. Finalized (generalized) block)

Затем блок передаётся другим узлам для проверки. Если всё подтвердилось, то узлы принимают этот блок в качестве самого последнего (новейшего) и продолжают передавать его дальше по сети.

Заключение

Появление СБЧ было предопределено всеми предшествующими этапами развития информационных технологий, постоянно требующих их совершенствования с целью дальнейшего повышения уровня (качества) прежде всего государственного управления и/или бизнес-приложений. Поэтому, несмотря на применение в БЧ-технологии определенных инновационных решений, не стоит переоценивать ее «безграничные», революционные возможности применения во всех сферах цифровой экономики. Безусловно, СБЧ займут определенную нишу на рынке ИТ-технологий, в частности в сфере развития криптовалютных систем. Но, как и для всяких других прикладных АИС перспективы их практической реализации будут определяться возможностью выполнения основных принципов обеспечения информационной безопасности [17], среди которых: аутентификация (персонификация) и обеспечение неотказуемости для всех без исключения участников информационного взаимодействия, обеспечение надежности подсистемы обеспечения криптоключами. В настоящее время разработчики СБЧ просто игнорируют указанные принципы либо минимизируют их значимость. Другими словами, СБЧ пока что являются ненадёжными системами, которые не могут быть основой всеохватывающей инфраструктуры подтверждения подлинности (доверия), т.е. несут колоссальные риски. Отчасти это связано с принципиальной особенностью современных СБЧ, определенным преимуществом которых провозглашается принцип анонимности, обеспечивающий практически полное отсутствие централизованного (государственного) регулирования. С другой стороны, его реализация, очевидно, приведет к появлению новой сферы криминальной (и, возможно, террористической) деятельности. Таким образом, без решения указанной проблемы фундаментального характера давать какие-либо прогнозы о перспективах применения БЧ-технологий, особенно в сфере государственного управления, на объектах критической информационной инфраструктуры, пока что явно преждевременно.

СПИСОК ЛИТЕРАТУРЫ:

1. National Institute of Standards and Technology. «Blockchain Technology Overview». Draft NISTIR 8202, January 2018.
2. Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008. https://bitcoin.org/bitcoin.pdf
3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации: Учебник (в 2-х частях). — М.: Юрайт, 2016. ISBN 978-5-534-01741-0, ISBN 978-5-534-01740-3.
4. ISO, «Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture». ISO 7498 - 2: 1989.
5. ITU-T, X.800, «Security Architecture for Open Systems Interconnection for CCITT Applications», 03/1991.
6. D. Burdett, D.E. Eastlake III, and M. Goncalves, «Internet Open Trading Protocol», McGraw-Hill, 2000. ISBN 0-07-135501-4.
7. RFC 2801, «Internet Open Trading Protocol – IOTP Version 1.0», IETF, April 2000.
8. Мельников Д.А. «Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник». – М.: IDO Press. КДУ, 2015. ISBN 978-5-98227-960-6, 978-5-4243-0004-2.
9. RFC 3354, «Internet Open Trading Protocol Version 2 Requirements», IETF, August 2002.
10. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., «Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction», Princeton University Press, 2016.
11. Wong, J. and Kar, I., «Everything you need to know about the Ethereum 'hard fork'», *Quartz Media*, July 18, 2016. https://qz.com/730004/everything-you-needto-know-about-the-ethereum-hard-fork/.
12. «Introduction to Ripple for Bitcoiners», last modified December 10, 2013. https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners.
13. Hertig, A., «Litecoin's SegWit Activation: Why it Matters and What's Next», *CoinDesk*, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activationwhy-it-matters-and-whats-next/.
14. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, «Secure Hash Standard (SHS)», August 2015. https://doi.org/10.6028/NIST.FIPS.180-4.
15. Cachin, C., «Architecture of the Hyperledger blockchain fabric», in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, July 2016.
16. «Hyperledger Business Blockchain Technologies», The Linux Foundation. https://www.hyperledger.org/projects.

17. Будзко В.И., Мельников Д.А. «Информационная безопасность и блокчейн» // Системы высокой доступности. 2018. Т. 14. № 3. С. 5 – 11.

REFERENCES:

[1] National Institute of Standards and Technology. «Blockchain Technology Overview». Draft NISTIR 8202, January 2018.
[2] Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008. https://bitcoin.org/bitcoin.pdf
[3] Fomichev V.M., Melnikov D.A. Cryptographic methods of information protection: Textbook (Two Paths). — M.: Urait, 2016. ISBN 978-5-534-01741-0, ISBN 978-5-534-01740-3. (in Russian).
[4] ISO, «Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture». ISO 7498-2: 1989.
[5] ITU-T, X.800, «Security Architecture for Open Systems Interconnection for CCITT Applications», 03/1991.
[6] D. Burdett, D.E. Eastlake III, and M. Goncalves, «Internet Open Trading Protocol», McGraw-Hill, 2000. ISBN 0-07-135501-4.
[7] RFC 2801, «Internet Open Trading Protocol – IOTP Version 1.0», IETF, April 2000.
[8] Melnikov D.A. «Organization and security management of IT networks and systems: Textbook». – M.: IDO Press. KDU, 2015. ISBN 978-5-98227-960-6, 978-5-4243-0004-2. (in Russian).
[9] RFC 3354, «Internet Open Trading Protocol Version 2 Requirements», IETF, August 2002.
[10] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., «Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction», Princeton University Press, 2016.
[11] Wong, J. and Kar, I., «Everything you need to know about the Ethereum 'hard fork'», *Quartz Media*, July 18, 2016. https://qz.com/730004/everything-you-needto-know-about-the-ethereum-hard-fork/.
[12] «Introduction to Ripple for Bitcoiners», last modified December 10, 2013. https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners.
[13] Hertig, A., «Litecoin's SegWit Activation: Why it Matters and What's Next», *CoinDesk*, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activationwhy-it-matters-and-whats-next/.
[14] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, «Secure Hash Standard (SHS)», August 2015. https://doi.org/10.6028/NIST.FIPS.180-4.
[15] Cachin, C., «Architecture of the Hyperledger blockchain fabric», in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, July 2016.
[16] «Hyperledger Business Blockchain Technologies», The Linux Foundation. https://www.hyperledger.org/projects.
[17] Budzko V.I., Melnikov D.A. «Information security and blockchain» // Highly available systems. 2018. V.14. №3. p.p. 5 - 11. (in Russian).

Поступила в редакцию – 30 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 30, 2018. The final version – November 01, 2018.

Антон А. Конев[1], Татьяна Е. Минеева[1], Михаил Л. Соловьёв[2],
Александр А. Шелупанов[1], Мария П. Силич[1]
[1]Томский государственный университет систем управления и радиоэлектроники,
просп. Ленина, 40, г. Томск, 634050, Россия
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Сибирский государственный университет телекоммуникаций и информатики
ул. Кирова, 86, г. Новосибирск, 630102, Россия
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.03

Аннотация. При построении системы защиты информации одной из ключевых проблем становится создание комплекта нормативной документации. Регуляторы в сфере обеспечения информационной безопасности определяют перечень необходимой документации в основном применительно к механизмам защиты (аутентификация, антивирусная защита и т.п.) и практически не учитывают этапы жизненного цикла средств защиты информации и персонала организации. В статье предлагается подход к формализации составления перечня процессов управления информационной безопасностью, нуждающихся в регламентации. Данный подход позволяет при формировании политики информационной безопасности учитывать процессы управления персоналом и комплексом программно-аппаратных средств защиты информации, что необходимо для обеспечения высокого уровня защищенности объектов критической информационной инфраструктуры.
Ключевые слова: система защиты информации, жизненный цикл, процессы управления, объект критической информационной инфраструктуры.
Для цитирования: КОНЕВ, Антон А. et al. МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 34-41, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1159>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.03.

Anton A. Konev[1], Tatiana E. Mineeva[1], Mikhail L. Soloviev[2],
Aleksander A. Shelupanov[1], Mariya P. Silich[1]
[1]Tomsk state university of control systems and radioelectronics,
Lenina Av., 40, Tomsk, 634050, Russia
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Siberian state university of telecommunications and information sciences
Kirova St, 86, Novosibirsk, 630102, Russia
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

Model of the life cycle of the information security system

DOI: http://dx.doi.org/10.26583/bit.2018.4.03

Abstract. When building an information security system, one of the key problems is the creation of regulatory documents. Regulators in the field of information security determine the list of necessary documentation

mainly in relation to protection mechanisms (authentication, anti-virus protection, etc.) and practically do not take into account the stages of the life cycle of information security tools and personnel of the organization. The article proposes an approach to formalization of the list of information security management processes that need regulation. This approach allows the formation of information security policy to take into account the processes of personnel management and the complex of software and hardware information security, which is necessary to ensure a high level of security of critical information infrastructure.

Keywords: information protection system, life cycle, management processes, classification.

For citation: KONEV, Anton A. et al. Model of the life cycle of the information security system. IT Security (Russia), [S.l.], v. 25, n. 4, p. 33-41, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1159>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.03.

Введение

Вступление в силу Федерального Закона «О безопасности критической информационной инфраструктуры Российской Федерации» [1] с 01.01.2018 г. привело к необходимости разработки практических рекомендаций по обеспечению безопасности соответствующих объектов. В частности, статьей 11 предусматривается «планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры», а также «принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры». Это означает, что регламентация процессов управления самим объектом критической информационной структуры и комплексом средств защиты информации является крайне актуальной при обеспечении безопасности подобных объектов.

Для конкретизации требований ФЗ «О безопасности критической информационной инфраструктуры РФ» ФСТЭК России были разработаны требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры [2], включающие в том числе и требования по разработке различных нормативных документов, направленных на обеспечение информационной безопасности, на уровне организации. Указанный документ включает требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов.

На сегодняшний день существуют подходы, основанные на разработке эффективных политик безопасности, без которых создание системы защиты информации невозможно [3]. Данные политики безопасности учитывают основные принципы обеспечения информационной безопасности и поддерживаются на протяжении всего жизненного цикла. Но существенным недостатком таких подходов является то, что данной политикой информационной безопасности не учитываются все процессы управления системой защиты информации, следствием чего является низкий уровень защищенности информационной инфраструктуры.

Существует подход к построению системы защиты информации, который основывается на зависимости структуры системы от перечня угроз защищаемой системе. Тем самым модель угроз, на основе которой проектируется структура системы защиты информации, должна включать в себя следующие разделы:

–перечень угроз информации;

–перечень угроз носителям информации;

–перечень угроз элементам информационной системы;

–перечень угроз элементам системы защиты;

–перечень угроз, касающихся управления системой защиты [4].

Модель угроз информации и ее носителям, модель угроз, направленных на информационную систему, представлены в работах [5] и [6]. Необходимо рассмотреть и угрозы, направленные на процессы управления самой системой. Но для получения модели угроз необходимо формализованное описание самих процессов управления защищаемым объектом.

Построение модели жизненного цикла

Под моделью жизненного цикла понимается структурная основа процессов и действий, относящихся к жизненному циклу, которая служит в качестве общей ссылки для установления связей и взаимопонимания сторон [7].

Собственно, жизненный цикл системы — это непрерывный процесс с момента создания системы и до полного завершения ее работы. Процессы управления предназначены для реализации управляющих действий в отношении системы защиты информации [8].

Для построения модели жизненного цикла была проведена классификация процессов управления системой защиты информации и ее составляющих. Согласно Приказу ФСТЭК России № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, система защиты информации включает силы обеспечения безопасности значимых объектов (персонал) и средства обеспечения безопасности, к таковым относятся программно-аппаратные средства, а также организационную документацию, в соответствии с которой функционирует система безопасности [9].

Классификация процессов управления основывается на определении состояния, которое будет воздействовать на данный процесс на различных этапах жизненного цикла средств защиты информации и персонала организации [10]. Соответственно, были сформированы следующие классы процессов управления:

– процессы, связанные с приобретением/уничтожением;
– процессы, связанные с вводом/выводом из эксплуатации;
– процессы, связанные с эксплуатацией;
– процессы, связанные с проверкой/улучшением;
– процессы, связанные с контролем функционирования/доработкой.

В один класс были объединены противоположные процессы, так как они воздействуют на одни и те же состояния объекта критической информационной инфраструктуры.

На основе данной классификации были построены модели жизненного цикла программно-аппаратных средств защиты, персонала организации, а также нормативной документации.

Стоит пояснить, что процессы, связанные с вводом/выводом из эксплуатации, включают в себя процессы, связанные с правами на работу с конфиденциальной информацией. Например, процесс управления класса ввода/вывода из эксплуатации персонала- это допуск к конфиденциальной информации сотрудника или отбор прав на работу с данной информацией соответственно.

На рис. 1 представлена модель жизненного цикла программных средств защиты информации. Данная модель также подходит и для аппаратных средств защиты, так как состояния на различных этапах жизненного цикла, а также процессы управления данными средствами будут аналогичными.

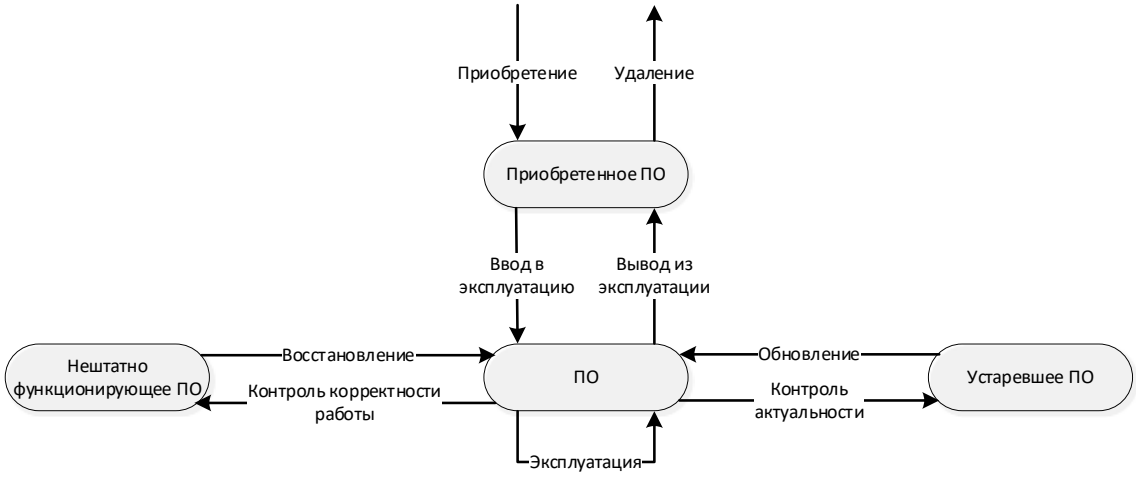


Рис. 1. Модель жизненного цикла программного и аппаратного обеспечения
(Fig. 1. Software and hardware lifecycle model)

Жизненный цикл программно-аппаратных средств защиты информации начинается с момента их приобретения. Основные задачи, выполняемые на этом этапе, – определение требований к продукту и определение потребности в нем [11].

Затем купленное или разработанное ПО вводится в эксплуатацию. В целях сопровождения программно-аппаратных средств защиты проводится контроль корректности работы. Контроль является одним из важных направлений работ по защите информации, его целью является выявление слабых мест, а также допущенных ошибок. Программное обеспечение не подвержено физическому износу, но в ходе его эксплуатации обнаруживаются неисправности, требующие исправления [12]. Неисправности могут также возникать при изменении условий использования программы.

При выявлении каких-либо ошибок в работе проводится восстановление работоспособности, исправление найденных ошибок [13].

При контроле актуальности выясняется степень устаревания продукта, за которым следует процесс обновления, если средство защиты устарело. Если было принято решение о приостановлении эксплуатации программного обеспечения, а именно прекращение доступа данного ПО на работу с конфиденциальной информацией, то происходит процесс вывода из эксплуатации [14] с последующей деактивацией программы (удалением).

Аналогичный жизненный цикл будет и у нормативной документации (рис. 2).

Функционирование нормативной документации является важным вопросом, так как именно ей определяются правила и требования, которые реализует персонал в совокупности с программно-аппаратным обеспечением. А от совокупности работы всех составляющих системы защиты информации и зависит надлежащий уровень информационной безопасности организации.

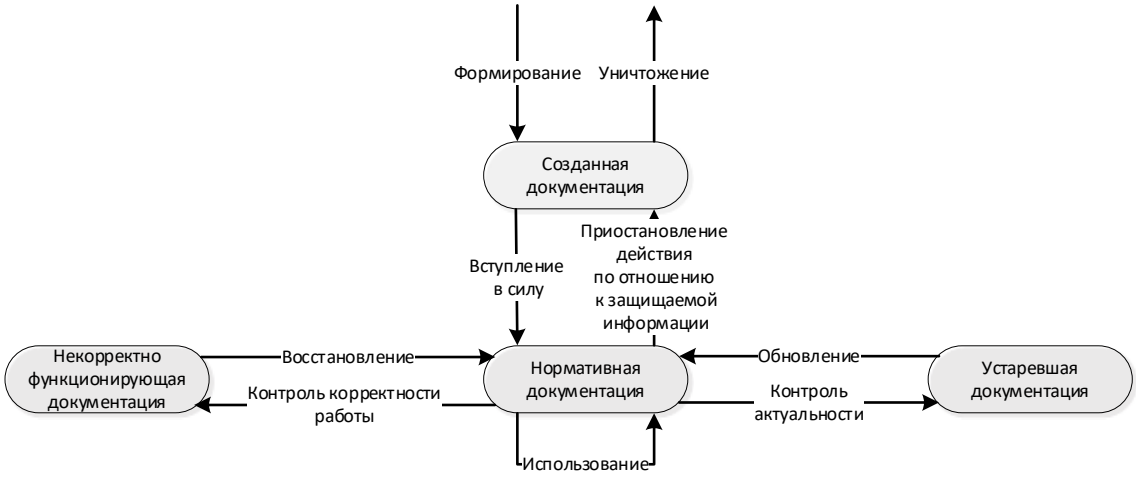


Рис. 2. Модель жизненного цикла нормативной документации
(Fig. 2. Life-cycle model of regulatory documents)

Сначала происходит решение о формировании конкретной документации, затем принимается решение о вступлении данной документации в силу. Далее происходят все те же процессы, что и с программно-аппаратными средствами защиты [15]. Процесс приостановления действия документации по отношению к защищаемой информации – это процесс, когда документация, относящаяся к конкретной защищаемой информации, становится недействующей по причине прекращения работы какого-либо продукта, функцией которого являлась защита информации, либо по причине прекращения потребности в защите определённого вида информации [16]. Затем по решению руководства данная документация полностью уничтожается.

Все аналогичные процессы управления относятся и к жизненному циклу сотрудников (рис. 3).

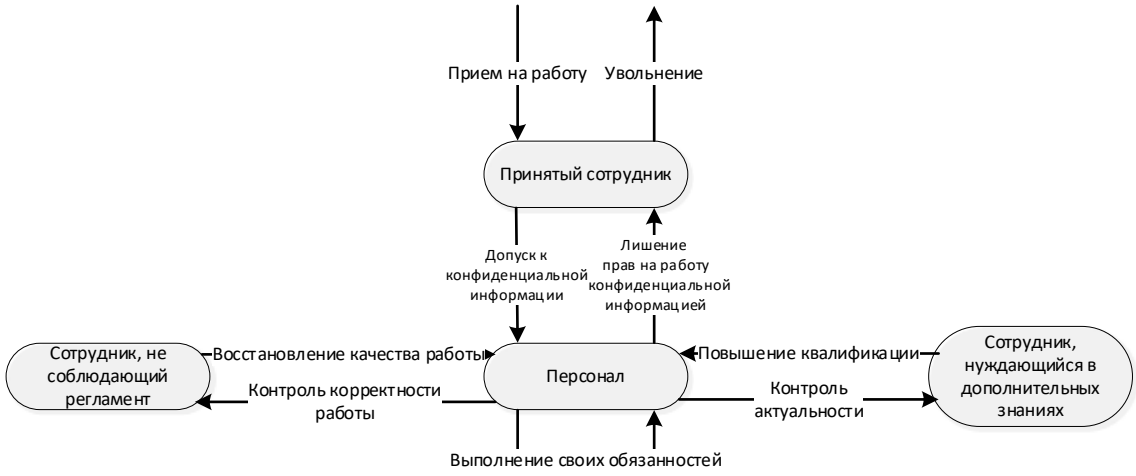


Рис. 3. Модель жизненного цикла сотрудников
(Fig. 3. Employee life cycle model)

Процессы управления сотрудниками это - целенаправленное воздействие на персонал, ориентированное на приведение в соответствие возможностей персонала и целей, стратегий и условий развития организации [17].

По данным моделям жизненного цикла программно-аппаратных средств защиты, нормативной документации и персонала была составлена типовая модель жизненного цикла системы защиты информации (рис. 4).

Были выделены основные этапы жизненного цикла [18]:

–планирование;

–ввод в эксплуатацию;

–эксплуатация;

–контроль за функционированием;

–улучшение;

–вывод из эксплуатации;

–уничтожение.

В рамках процесса планирования осуществляются разработка и утверждение плана мероприятий по обеспечению критической информационной инфраструктуры [19].

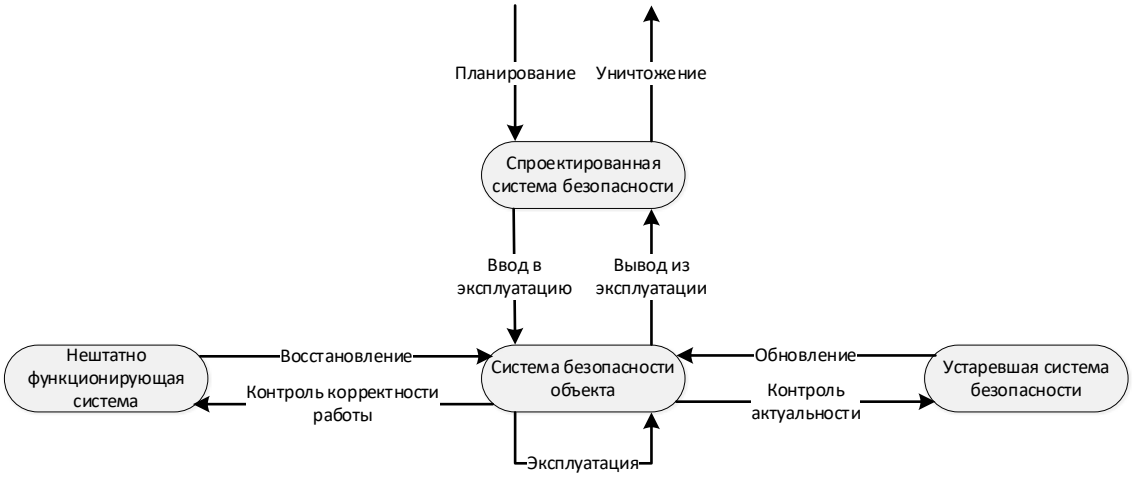


Рис. 4. Модель жизненного цикла системы защиты информации
(Fig. 4. Information security system life cycle model)

Модель жизненного цикла системы защиты информации отражает состояния и процессы управления ее составляющих, а именно: программно-аппаратных средств защиты, нормативной документации и персонала, также при ее построении были учтены основные этапы жизненного цикла системы.

Сравнивая данную модель с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, можно отметить, что все процессы управления системой перекрываются мерами обеспечения безопасности, содержащимися в рассматриваемом нормативном документе. Например, «выявление компьютерных инцидентов» проводится на этапе контроля корректности работы системы, а «разделение полномочий пользователей» подчинено процессу допуска к конфиденциальной информации. Данное соответствие говорит об актуальности данной модели и о том, что при формировании политики информационной безопасности в организации будут учтены процессы управления системой защиты информации, что позволит обеспечить высокий уровень защищенности информационной инфраструктуры.

Также стоит отметить, что разработанная модель учитывает следующие требования по обеспечению безопасности значимых объектов информационной инфраструктуры, которые не рассматриваются выше указанным нормативным документом:

1. Лишение прав сотрудника на работу с критической информацией.
2. Восстановление корректности работы значимого объекта.
3. Требования по обеспечению безопасности на этапе вывода из эксплуатации значимого объекта.
4. Требования по обеспечению безопасности на этапе уничтожения или удаления значимого объекта.

Тем самым можно дополнить перечень требований по обеспечению безопасности, содержащийся в нормативном документе ФСТЭК России требованиями разработанной модели жизненного цикла системы защиты информации.

Заключение

На основе классификации процессов управления системы защиты информации были построены модели жизненного цикла программно-аппаратных средств защиты, нормативной документации и персонала организации, а также модель жизненного цикла самой системы защиты информации. Были выделены этапы жизненного цикла, на основе которых и проведена классификация процессов управления системой защиты информации.

По результатам сравнения с требованиями по обеспечению безопасности значимых объектов было выявлено, что все выделенные процессы управления системой защиты информации перекрываются мерами обеспечения безопасности, которые приведены в рассматриваемом нормативном документе. Разработанная модель включает в себя все процессы управления системы защиты информации, а также учитывает несколько требований по обеспечению безопасности значимых объектов информационной инфраструктуры, которые не рассматриваются в документах ФСТЭК России, что является преимуществом перед уже существующими подходами решения данной проблемы.

Построенная модель позволит рассмотреть каждый из классов процессов управления более подробно и в дальнейшем раскрыть перечень угроз, направленных непосредственно на процессы управления информационной безопасностью, нуждающиеся в регламентации. Соответственно, рассмотрев перечень угроз, можно будет описать механизмы защиты, направленные на минимизацию этих угроз, что обеспечит безопасность критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // СПС КонсультантПлюс.
2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 // СПС КонсультантПлюс.

3. Зайцев С.Е. Политики информационной безопасности в системах информационной безопасности // Научный вестник Московского государственного технического университета гражданской авиации (137) 2008. С. 37 – 44.
4. Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУР. 2013. № 2 (28). С. 107 – 111.
5. Novokhrestov A., Konev A. Mathematical model of threats to information systems // AIP conference proceedings (Tomsk, 26 – 29 April 2016). Tomsk, 2016. Vol. 1772. P. 060015.
6. Новохрестов А.К., Конев А.А., Шелупанов А.А., Егошин Н.С. Модель угроз безопасности информации и ее носителей // Вестник Иркутского государственного технического университета. 2017. Т. 21. № 10. С. 93 – 104
7. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008. – 12 с.
8. Грибунин В.Г. Комплексная система защиты информации на предприятии [Текст]: учебное пособие для студентов высших учебных заведений / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
9. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 // СПС КонсультантПлюс.
10. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. М.: Стандартинформ, 2006. – 53 с.
11. И.А. Жуклинец, О.Н. Марков. Управление процессами ИБ в интересах бизнеса. Технологии безопасности № 1 (24) – 2013.
12. Доросинский Л. Г. Информационные технологии поддержки жизненного цикла изделия / Л.Г. Доросинский, О. М. Зверева. – Ульяновск: Издательство «Зебра», 2016. – 243 с. – ISBN 978-5-9908739-8-8.
13. Скопин И.Н. Понятия и модели жизненного цикла программного обеспечения: Учебное пособие Новосиб. гос. ун-т. – Новосибирск, 2012.
14. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности. Основные концепции. Вопросы кибербезопасности № 1(2) – 2014, С. 67 – 73.
15. ГОСТ Р ИСО/МЭК 27001 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. М.: Стандартинформ, 2008. –31с.
16. РС БР ИББС-2.6-2014. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/credit/gubzi_docs/rs-26-14.pdf (дата обращения 18.05.2018).
17. Гришина Н.В. Организация комплексной системы защиты информации. [Текст] / Н.В. Гришина – М.: Гелиос АРВ, 2007. – 256 с.
18. Бочков С.И. О ценности информации на различных этапах жизненного цикла. Правовая информатика № 3 – 2016, С. 35 – 40.
19. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: приказ Федеральной службы по техническому и экспортному контролю от 22.12.2017 г. № 236 // СПС КонсультантПлюс.

REFERENCES:

[1] On the Security of the Critical Information Infrastructure of the Russian Federation: Federal Law of July 26, 2017 No. 187-FZ. SPS ConsultantPlus.
[2] On approval of the Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation: Order FSTEC of Russia of 25.12.2017 No. 239. ATP ConsultantPlus.
[3] Zaitsev S.E. Information security policies in information security systems. Scientific Bulletin of Moscow State Technical University of Civil Aviation (137) 2008. P. 37 – 44.
[4] Konev A.A., Davydova E.M. Approach to structuring information security systems. Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki [Proceedings of Tomsk State University of Control Systems and Radioelectronics]. 2013, no. 2 (28), pp. 107 – 111.

[5] Novokhrestov A., Konev A. Mathematical model of threats to information systems. AIP conference proceedings (Tomsk, 26 – 29 April 2016). Tomsk, 2016, vol. 1772, pp. 060015.
[6] Novokhrestov A.K., Konev A.A., Shelupanov A.A., Egoshin N.S. Information and information carrier security threat model. Proceedings of Irkutsk State Technical University. 2017, vol. 21, no. 10, pp. 93–104.
[7] GOST R 50922-96. Data protection. Basic terms and definitions. Moscow: Standardinform, 2008. - 12 p.
[8] Gribunin V.G. Integrated system of information security at the enterprise [Text]: textbook for students of higher educational institutions. V.G. Gribunin, V.V. Chudovsky. - Moscow: Publishing Center "Academy", 2009. - 416 p.
[9] On approval of the Requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and ensuring their functioning: the order of the Federal Service for Technical and Export Control dated December 21, 2017 No. 235. SPS ConsultantPlus.
[10] GOST R ISO IEC 15288-2005. Information technology. System engineering. Processes of the life cycle of systems. Moscow: Standartinform, 2006. – 53 p.
[11] I.A. Zhukliniec, ON Markov. Management of IB processes in the interests of business. Security technologies №1 (24) – 2013.
[12] Dorosinsky LG Information technology to support the product life cycle. LG Dorosinsky, OM Zvereva. - Ulyanovsk: Zebra Publishing House, 2016. - 243 p. - ISBN 978-5-9908739-8-8.
[13] Skopin I.N. Concepts and models of the life cycle of software: Textbook Novosib. state. un-t. - Novosibirsk, 2012.
[14] Dorofeev AV, Markov AS Information Security Management. Basic concepts. Cybersecurity issues №1 (2) - 2014, pp. 67 – 73.
[15] GOST R ISO IEC 27001 - 2006. Information technology. Methods and means of ensuring security. Information security management systems. Moscow: Standardinform, 2008. - 31p.
[16] RS BR BRSI-2.6-2014. Ensuring information security at the stages of the life cycle of automated banking systems [Electronic resource]. - Access mode: http://www.cbr.ru/credit/gubzi_docs/rs-26-14.pdf (circulation date is May 18, 2018).
[17] Grishina N.V. Organization of a comprehensive information security system. [Text]. N.V. Grishina-M.: Helios ARV, 2007. – 256 p.
[18] Bochkov S.I. On the value of information at various stages of the life cycle. Legal Informatics № 3 - 2016, P. 35 – 40.
[19] On approval of the form for sending information on the results of assigning to the object a critical information infrastructure of one of the significance categories or about the absence of the need to assign to it one of such categories: the order of the Federal Service for Technical and Export Control dated December 22, 2017 No. 236. SPS ConsultantPlus.

Поступила в редакцию – 17 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 17, 2018. The final version – November 01, 2018.

Евгений А. Басыня[1, 2]
[1] Новосибирский государственный технический университет,
просп. К. Маркса, 20, г. Новосибирск, 630073, Россия
[2] Научно-исследовательский институт информационно-коммуникационных технологий,
ул. Депутатская, 48, г. Новосибирск, 630099, Россия
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА, ОБРАБОТКИ И АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

DOI: http://dx.doi.org/10.26583/bit.2018.4.04

Аннотация. Большинство сетевых инфраструктур государственных учреждений и частных предприятий функционируют на базе стека протоколов TCP/IP, обладающего существенными уязвимостями. В качестве примера стоит привести отсутствие проверки подлинности субъекта взаимодействия в базовых протоколах и технологиях данного стека. Часть уязвимостей можно устранить интеллектуальными функциями управляемого сетевого оборудования: от профилирования доступа до сегментации трафика. Немаловажным звеном защиты выступают комплексные межсетевые экраны, включающие системы обнаружения и предотвращения вторжений. Российскими и зарубежными учеными развиваются методы сигнатурного, эвристического, поведенческого, автомодельного, прогнозируемого и других способов анализа сетевого трафика и идентификации сетевых угроз. Однако предлагаемые решения не дают однозначного результата при использовании оверлейных технологий и криптографических протоколов. Также не уделяется надлежащее внимание обработке, анализу сетевого трафика и логов операционных систем Windows/Linux и приложений. Целью данной работы являлось исследование, разработка и программная реализация распределенной системы сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Ключевой задачей ставилось обеспечение объективного мониторинга сетевой информационной безопасности. Дополнительной задачей являлось обеспечение мониторинга работы пользователей персональных компьютеров под управлением операционных систем Windows и Linux. Для решения поставленной задачи была разработана концепция комплексной обработки трафика вычислительной сети и событий информационной безопасности как на стороне сервера, так и на стороне клиента. На обзор вынесен оригинальный сигнатурный и статистический метод составления базы знаний системы посредством тестирования и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации. Изложен подход к выполнению автоматизированного анализа коррелирующих событий с применением глубокого анализа содержимого пакетов и мониторинга локальной работы пользователей. Предложенное решение успешно апробировано и использовано в качестве одного из модулей обеспечения сетевой информационной безопасности системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором.

Ключевые слова: IDS, IPS, SIEM, анализ событий информационной безопасности, мониторинг работы сети и пользователей.

Для цитирования: БАСЫНЯ, Евгений А. РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА, ОБРАБОТКИ И АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 42-51, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1160>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.04.

Evgeny A. Basinya[1, 2]
[1]Novosibirsk State Technical University,
20 K. Marx Street, Novosibirsk, 630073, Russia
[2]Research Institute of Information and Communications Technologies,
48 Deputatskaya Street, Novosibirsk, 630073, Russia
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure

DOI: http://dx.doi.org/10.26583/bit.2018.4.04

Abstract. The majority of the network infrastructures of government agencies and private enterprises operate on the basis of a TCP/IP protocol stack, which has significant vulnerabilities. For illustrative purposes, it is worth mentioning the lack of verification of the interaction subject authenticity in the basic protocols and technologies of this stack. Some of the TCP/IP stack vulnerabilities can be eliminated by the intelligent functions of managed network devices: from access profiling to traffic segmentation. Complex firewalls, which include intrusion detection and prevention systems, are also an important element of the network protection. Methods of signature, heuristic, behavioral, self-similar, predictable and other approaches for analyzing network traffic and identifying network threats are further being developed by Russian and foreign scientists. However, the proposed solutions do not give an unambiguous result when using overlay technologies and cryptographic protocols. Also, due attention is not being paid to the processing, analysis of network traffic and logs of Windows/Linux operating systems and applications. The aim of this work was the research, development and software implementation of a distributed system for collecting, processing and analyzing security information events of an enterprise network infrastructure. The key task was to ensure objective monitoring of network information security. An additional task was to ensure the monitoring of the activity of users of personal computers running Windows and Linux operating systems. In order to address this challenge, a concept for complex processing of computer network traffic and security information events both on the server and on the client sides was developed. An original signature and statistical method of compiling the knowledge base system by testing and simulating known network and local attacks with tracking the response of operating systems and applications in a virtualization environment is reviewed. The approach to performing the automated analysis of correlating events with the use of deep packets inspection (DPI) and monitoring of users' local activity is described. The reviewed solution was successfully tested and used as one of the modules for providing network information security of the system for intelligent adaptive enterprise network infrastructure management, designed by author.

Keywords: IDS, IPS, SIEM, security information events analysis, user and network activity monitoring.
For citation: BASINYA, Evgeny A. Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure. IT Security (Russia), [S.l.], v. 25, n. 4, p. 42-51, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1160>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.04.

Введение

Одним из приоритетных направлений развития науки, технологий и техники в Российской Федерации выступают информационно-коммуникационные технологии, оказывающие существенное влияние на уровень национальной безопасности и экономической конкурентоспособности государства. Большинство сетевых инфраструктур государственных учреждений и частных предприятий функционируют на базе стека протоколов TCP/IP с использованием технологии канального уровня Ethernet, а также имеют доступ к глобальной вычислительной сети Интернет. С каждым годом возрастает количество и уровень изощренности кибернетических атак. Злоумышленники, мотивированные целью получения материальной выгоды, предпринимают попытки вывести из состояния доступности или получить несанкционированный доступ к информационным системам и вычислительным сетям, что потенциально может нанести существенный экономический ущерб

компании и (в худшем случае) ущерб суверенитету, территориальной целостности, политической и социальной стабильности страны.

Соответственно, возрастает актуальность задачи обеспечения информационной безопасности сетевых инфраструктур предприятий. Стоит отметить несовершенство стека протоколов TCP/IP: так в базовых протоколах и технологиях отсутствуют проверки подлинности субъекта взаимодействия (не введены процедуры идентификации, аутентификации и авторизации). В качестве примера стоит привести возможность использования ложных ARP-ответов (англ. Address Resolution Protocol — протокол определения адреса) и фальсифицированных сообщений протоколов маршрутизации и управления сетью. Часть уязвимостей стека можно устранить интеллектуальными функциями управляемого сетевого оборудования: от профилирования доступа до сегментации трафика. Но одним из ключевых звеньев защиты локальной вычислительной сети выступает комплексный межсетевой экран. Как правило, в его состав входит система обнаружения и предотвращения вторжений (англ. IDS/IPS, Intrusion detection system / Intrusion prevention system). Подобные системы могут функционировать на уровне приложения, хоста или сети. Сбор трафика зачастую осуществляется с каждого сегмента сети посредством агентов/датчиков, подключенных к коммутаторам/маршрутизаторам на зеркалируемый порт (англ. port mirroring). Российскими и зарубежными учеными развиваются методы сигнатурного, эвристического, поведенческого, автомодельного, прогнозируемого и других анализов сетевого трафика и идентификации сетевых угроз. Данными исследованиями занимаются: Ходашинский И.А., Мещеряков Р.В., Рубанов С.А., Тимонина А.А., Тимонина Е.Е., Половко И.Ю., Пескова О.Ю., Сычев М.П., Ефимов А.Ю., Бурлаков М. Е., Бондяков А.С. и многие другие ученые. [1 - 7]

Заслуживающими внимания положительными тенденциями являются: организация работы IDS/IPS на основе встраиваемых микропроцессорных систем и технологии data mining [8 - 9], а также консолидация IDS/IPS и систем управления безопасностью и событиями (англ. SIEM, Security information and event management) [10 - 15]. Импортозамещение иностранных технологий и продуктов в данной сфере является приоритетным направлением развития российской науки. [16]

Однако предлагаемые методики не дают однозначного результата при использовании оверлейных технологий и криптографических протоколов, а также не уделяют надлежащего внимания обработке, анализу сетевого трафика и логов операционных систем (ОС) семейства Windows/Linux и приложений.

Немаловажной функциональной проблемой комплексных межсетевых экранов выступает отсутствие возможности формирования объективных отчетов и статистики о деятельности пользователя, особенно при использовании средств анонимизации (например, сети TOR <англ. The Onion Router>). Существенным недостатком является отсутствие взаимодействия следующих решений: IDS/IPS, SIEM, систем контроля работы пользователей, систем поддержки принятия решений по вопросам администрирования и информационной безопасности, что приводит к нерентабельному избыточному потреблению вычислительных ресурсов сервера, дублированию ряда информационных блоков.

1. Постановка задачи

Целью данной работы являлось исследование, разработка и программная реализация распределенной системы сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Задачей ставилось обеспечение объективного мониторинга сетевой информационной безопасности и работы пользователей персональных компьютеров под управлением операционных систем Windows и Linux. Предложенное решение будет использовано в качестве модуля систем обеспечения сетевой информационной безопасности комплексного интеллектуально-адаптивного шлюза, разрабатываемого автором.

2. Теория и практика

На сегодняшний день широкое распространение получили средства сетевой анонимизации: прокси-серверы, виртуальные защищенные каналы связи и виртуальные частные сети (англ. Virtual Private Network), оверлейные сети на базе луковой и чесночной маршрутизации. Данные инструменты позволяют пользователям посещать любые информационные ресурсы в обход правил фильтрации межсетевых экранов, в том числе UTM-шлюзов безопасности (англ. Unified threat management) и NGFW (англ. Next generation firewall).

Используя оверлейную сеть TOR, пользователь может посетить целевой информационный ресурс через цепочку из трех и более случайных прокси-серверов/нодов (входного, промежуточных и выходного), с каждым из которых он обменивается ключами и шифрует исходную информацию последовательно ключами от выходного до входного нодов, оставляя открытой лишь полезную часть заголовка пакетов для выполнения следующей трансляции информационного потока. Осуществляется многослойное шифрование и продвижение трафика по цепочке нодов, именуемое луковой маршрутизацией. Соответственно, межсетевой экран способен установить факт взаимодействия пользователя с входной нодой сети TOR, но идентифицировать целевой (посещаемый) информационный ресурс и дешифровать/проанализировать трафик не может. Тем самым пользователь может успешно обойти правила фильтрации трафика.

Одним из методов противодействия выступает механизм цифровых подписей и сертификации всех процессов операционной системы и устанавливаемых приложений. Альтернативным методом является установка корневых сертификатов в систему и ввод дополнительных средств разграничения прав доступа. Описанные подходы позволят предотвратить установку нежелательного программного обеспечения пользователями, а также дешифровывать и анализировать сетевой трафик хостов на стороне шлюза/межсетевого экрана. Стоит отметить существенный недостаток использования данных методик в гражданской сфере: работа рядового пользователя за персональным компьютером утрачивает гибкость, простоту и удобство взаимодействия с операционной системой, ограничивается по функциональности и требует постоянного вмешательства квалифицированного специалиста. Подмена корневых сертификатов в ряде стран является неэтичной и трактуется как попытка внедрения тоталитарного контроля, посягающего на свободу слова.

Задача сбора и анализа логов операционных систем и приложений может представляться тривиальной и простой. Однако стоит привести простой пример. Пользователь хоста А подключается к хосту Б с использованием протокола удаленных рабочих столов RDP (англ. Remote Desktop Protocol). Оба узла функционируют на базе операционной системы семейства Windows (версии 7 и выше). Системному администратору ставится задача установления времени пребывания пользователя хоста А на узле Б. Разумеется, специалист обращается к логам журнала событий EVTX (англ. XML EventLog, новый формат журнала Microsoft). Во вкладке «безопасность» он обнаруживает 48 событий входа/выхода пользователя в систему с идентичными кодами событий. При этом фактически пользователь находился в системе лишь один час пятнадцать минут, был произведен лишь один вход и один выход из системы с использованием протокола RDP, локальных действий не производилось. Подобных примеров можно привести большое количество, что отражает трудоемкость процесса сбора и анализа объективной информации о событиях сетевой инфраструктуры, в том числе и о работе пользователей за персональными компьютерами на базе операционных систем семейства Windows/Linux при использовании.

Для решения данных проблем было решено разработать распределенную систему сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Данная система проектировалась как модуль системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором (рис. 1).

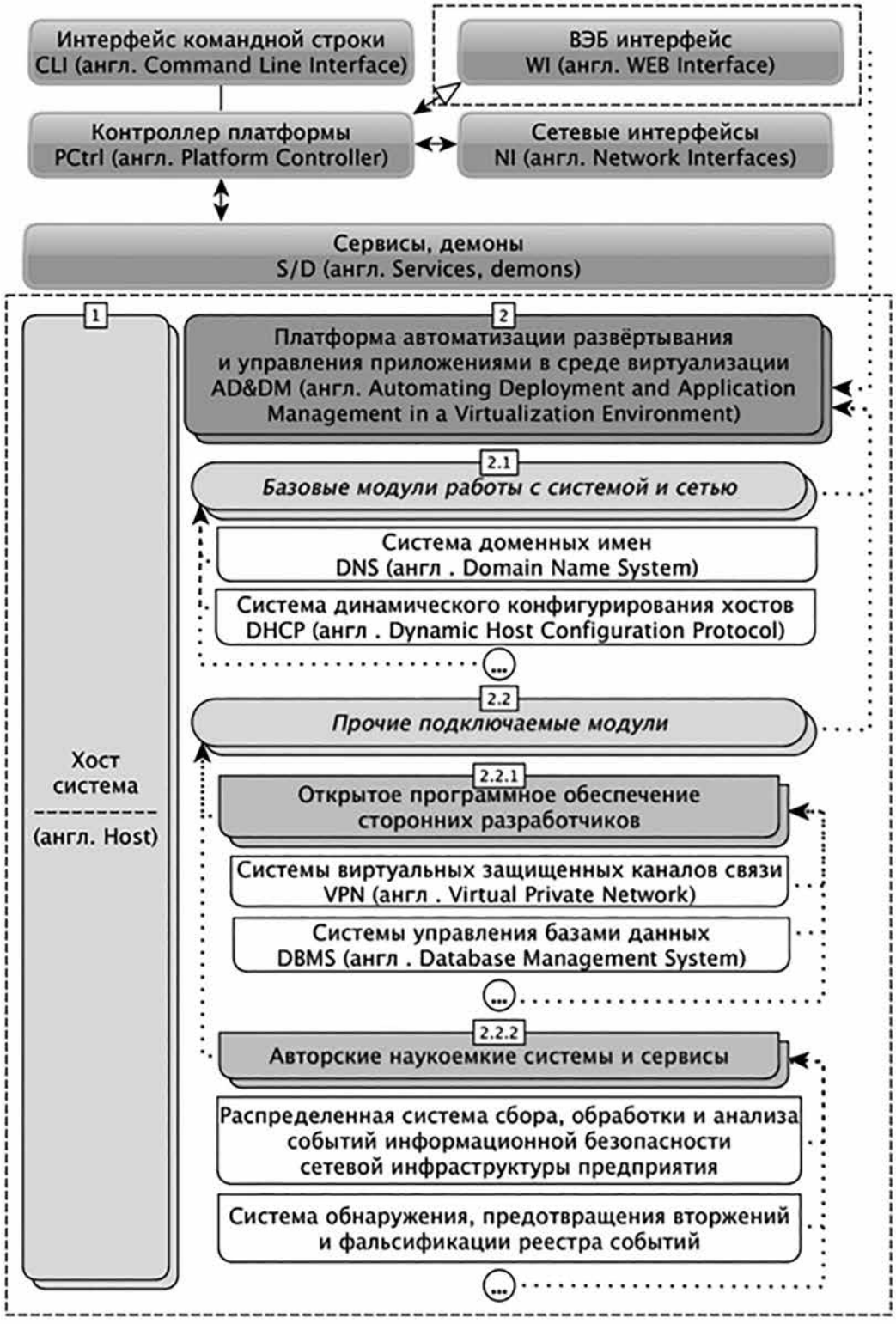


Рис. 1. Архитектура серверной части системы
(Fig. 1. Architecture of the server part of the system)

Архитектура серверной части выполнена с использованием платформы автоматизации развёртывания и управления приложениями в среде виртуализации, что обеспечивает дополнительную надежность и отказоустойчивость решения.

При проектировании функционала клиентской части приложения, устанавливаемой на персональные компьютеры пользователей было предложено совместить в едином продукте шесть оригинальных разработок, представленных на рис. 2.

Рис. 2. Диаграмма компонентов клиентского программного обеспечения комплексного интеллектуально-адаптивного шлюза
(Fig. 2. Diagram of the client software components of the integrated intelligent adaptive gateway)

Данная диаграмма иллюстрирует пересечение функционала систем. Приведем простой пример. Система интеллектуального контроля и управления доступом к информационным ресурсам ПК блокирует подключение сторонних USB-носителей, подключение к сетям не из списка доверенных, несанкционированную отправку информации через файлообменники или почтовые сервисы, проверяет наличие секретного устройства в зоне действия локальной вычислительной сети и Bluetooth-метки, анализирует клавиатурный почерк и задействует 2d-распознавание лица.

Система мониторинга работы пользователей персональных компьютеров отслеживает активность работы пользователя в различных приложениях, анализируя нажатия клавиш, движения мыши и идентифицируя системы фальсификации деятельности пользователя. Изучает интернет-серфинг пользователя, проверяя доступность HTTPS протокола (англ. HyperText Transfer Protocol Secure) посещаемых ресурсов (в том числе отдельных блоков сайтов) и рекомендуя его использовать.

Автоматизированная система сетевого и системного администрирования ОС семейства Windows организует систему заявок между пользователем и администратором, а также в автоматическом режиме решает широкий спектр проблем. Обрабатывает логи операционных систем и приложений, мониторит сетевую активность.

Соответственно, функционал обработки, анализа логов и сетевого трафика является неотъемлемой частью всех приведенных на рис. 2 компонентов, которые должны взаимодействовать с серверной частью системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, в том числе выполняющей функцию комплексного межсетевого экрана.

Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия выполняет следующие функции:

На стороне клиента:

1) сбор и локальную обработку логов операционной системы по сигнатурному методу;
2) сбор и локальную обработку логов установленного программного обеспечения по сигнатурному методу;
3) анализ всего трафика, обрабатываемого хостом, с использованием технологии глубокого анализа содержимого дейтаграмм DPI (англ. Deep Packet Inspection);
4) мониторинг работы пользователей в системе и различных приложениях;
5) идентификацию и блокировку приложений, фальсифицирующих активность пользователя;
6) мониторинг работы каждого запущенного процесса, изучение генерируемого им трафика;
7) составление модели поведения пользователей и процессов, задействование методов поведенческого принципа и идентификации аномалий;
8) корреляционный и статистический анализ всей собираемой информации;
9) предоставление функционала изолированной среды тестирования и изучения каждой единицы устанавливаемого программного обеспечения, так называемой песочницы;
10) работа с полученной базой знаний от сервера и формирование собственных знаний системы на основе получаемого опыта;
11) взаимодействие с серверной частью от отправки всей собранной информации до получения команд и обновления базы знаний/компонентов системы.

Под обработкой логов подразумевается не только парсинг, но и идентификация, структуризация, ранжирование и объединение событий. Так, в приведенном ранее примере удаленного подключения к хосту Б по протоколу RDP из 48 событий операционной системы было составлено 1 корректное.

Функционал «песочницы» позволяет отслеживать поведение программного обеспечения: к каким файлам, ресурсам, оборудованию и веткам реестра (в случае использования хостом ОС Windows) обращается источник, какой трафик генерирует, отправляет ли в скрытом режиме информацию, имеет ли не задекларированные правообладателем функции.

На стороне сервера выполняются следующие действия:

1) локальный сбор и обработка логов серверной операционной системы по сигнатурному методу;
2) локальный сбор и обработка логов установленного серверного программного обеспечения по сигнатурному методу;
3) анализ локального трафика, обрабатываемого сервером, с использованием технологии глубокого анализа содержимого дейтаграмм DPI;
4) сбор с клиентов обработанных логов операционной системы;
5) сбор с клиентов обработанных логов программного обеспечения;
6) сбор с клиентов информации об обработанном ими трафике;
7) сбор с клиентов выработанных знаний системы на основе полученного опыта;
8) формирование основной базы знаний системы на основе оригинального сигнатурного и статистического метода;
9) расширение базы знаний системы;

10) корреляционный и статистический анализ всей собираемой информации;

11) управление клиентами.

Полученные знания разными клиентами в штатном режиме работы вносятся в общую базу лишь при аналогичных результатах от 50 % клиентов с аналогичным установленным программным обеспечением, при этом минимальное количество хостов составляет десять единиц.

Для составления основной базы знаний системы был разработан оригинальный сигнатурный и статистический метод, реализован фреймворк, который в свою очередь использовался для написания программы «Researcher» по тестированию систем и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации на модельных объектах.

В базу знаний программы внесены официально известные уязвимости операционных систем семейства Windows/Linux, популярных программных продуктов и вычислительных сетей, а также добавлены существующие или написанные самостоятельно эксплойты (программные реализации осуществления атаки на объект, имеющий определенную уязвимость).

Для проведения исследований на выделенном сервере устанавливается и конфигурируется гипервизор, настраивается виртуальная сетевая инфраструктура. Далее создаются модельные объекты в виде виртуальных машин с различными операционными системами и набором программного обеспечения. Для автоматизации развертки и конфигурирования решений на базе Linux с введением дополнительного слоя изоляции задействуются Docker-контейнеры и Ansible скрипты, на базе Windows – система эталонного образа и контейнеризации программ, включая «песочницы». На модельные объекты производится установка разработанного клиентского программного обеспечения. Соответственно, моделируется полноценная сетевая инфраструктура предприятия. Для восстановления начального, эталонного состояния виртуальной машины используется технология снапшотов (снимков системы).

Далее запускается программа «Researcher». Сначала со стороны виртуальной локальной сети, затем снаружи, за виртуальным межсетевым экраном. Итерационно задействуются механизмы активного и пассивного анализа трафика вычислительной сети и информационных ресурсов (сканирование, зондирование, пентестинг) по отношению к каждому модельному объекту. Клиенты модельных объектов «снимают показания» в виде логов и трафика, передают их серверу, где математический аппарат выявляет корреляцию событий по каждой атаке, составляет «слепок» поведения операционной системы и программного обеспечения в зависимости от проведенного внешнего возмущения. Количество итераций по выполнению одной процедуры (например, выполнению эксплойта) на чистый модельный объект составляет не менее 10 и может вручную задаваться администратором. Таким образом формируется основная база знаний системы.

Программная реализация серверной части была выполнена с использованием Python, Flask, C++, Bash, Docker, Ansible на ОС Alpine Linux. Клиентский модуль под ОС Windows написан на языке программирования C# с использованием native controls из .NET библиотеки Windows Forms, а под Linux использовался Python и Qt-фреймворк.

Для проверки работоспособности было выполнено ручное и автоматизированное тестирование разработанного программного продукта (клиентской и серверной части, а также их взаимодействия).

Далее был проведен эксперимент по определению эффективности предложенного подхода, объективно предоставляющего информацию даже при использовании пользователями средств анонимизации: на сотне компьютеров сотрудниками компании, принявшей участие в эксперименте, в ручном режиме были установлены и запущены: Tor и I2P браузеры, OpenVPN клиент с подключением к коммерческому VPN сервису. С использованием этих инструментов пользователи посещали различные информационные ресурсы, каждое посещение было зафиксировано разработанным клиентским программным обеспечением, информация успешно отправлялась на серверную часть. При этом сторонние комплексные межсетевые экраны с задачей не справились, т.к. не были установлены корневые сертификаты и дополнительные средства разграничения прав доступа.

Затем в рамках этой же сетевой инфраструктуры была исследована загрузка каналов связи предложенной системы в сравнении со стандартным методом сбора логов системами обнаружения и предотвращения вторжений, системами управления безопасностью (Snort, Suricata, Bro, OSSEC, ELK, LightSIEM и др.). Длительность эксперимента составила два месяца. Уменьшение загрузки каналов связи трафиком рассматриваемых продуктов при прочих условиях составило 12–47 % при использовании разработанной системы (при этом информативность была улучшена). Однако существенным недостатком выступило использование больших вычислительных мощностей: от 16 до 39 %. При этом важно отметить, что функционал системы значительно шире в сравнении с существующими решениями в комплексе. Работа по оптимизации системы продолжается.

Заключение

В рамках данного исследования была разработана и программно реализована система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия, функционирующая на основе оригинального сигнатурного и статистического метода по составлению базы знаний системы посредством тестирования и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации на модельных объектах. Изложен подход к выполнению автоматизированного анализа коррелирующих событий в совокупности с модулями глубокого анализа содержимого пакетов DPI (англ. Deep Packet Inspection) и мониторинга локальной работы пользователей. Предложена концепция комплексной обработки трафика вычислительной сети и событий информационной безопасности как на стороне сервера, так и на стороне клиента. Недостатком программной реализации предложенного решения является потребление вычислительных мощностей на стороне клиента на 16–39 % больше в сравнении с альтернативными продуктами. Что выступает ценой за расширенный функционал и использование языка программирования Python. Предложенное решение использовано в качестве одного из модулей обеспечения сетевой информационной безопасности системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором.

СПИСОК ЛИТЕРАТУРЫ:

1. Ходашинский И.А., Мещеряков Р.В., Рубанов С. А. Гибридная система обнаружения вторжений на базе нечеткого классификатора с использованием жадного и генетического алгоритмов // Вопросы защиты информации. 2013. № 4(102). С. 67 – 72.
2. Тимонина А.А., Тимонина Е.Е. Атаки на централизованные системы обнаружения вторжений // Системы и средства информатики. 2013. Т. 23. № 1. С. 33 – 42.
3. Половко И.Ю., Пескова О.Ю. Анализ функциональных требований к системам обнаружения вторжений // Известия ЮФУ. Технические науки. 2014. № 2(151). С. 86 – 92.
4. Обоснование архитектуры перспективной системы обнаружения и предотвращения вторжений / М.П. Сычев [и др.] // Инженерный журнал: Наука и инновации. 2013. № 2 (14). С. 23.
5. Ефимов А.Ю. Проблемы обработки статистики сетевого трафика для обнаружения вторжений в существующих информационных системах // Программные продукты и системы. 2016. № 1. С. 17 – 21.
6. Бурлаков М. Е. Модель многослойной универсальной системы обнаружения вторжений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2(32). С. 214–218.
7. Бондяков А. С. Основные режимы работы системы предотвращения вторжений (IDS/IPS SURICATA) для вычислительного кластера // Современные информационные технологии и ИТ-образование. 2017. Т. 13. № 3. С. 31 – 37.
8. Булдакова Т. И., Джалолов А. Ш. Выбор технологий DATA MINING для систем обнаружения вторжений в корпоративную сеть // Инженерный журнал: Наука и инновации. 2013. № 11(23). С. 36.
9. Доценко С.М., Владыко А.Г., Летенко И.Д. Системы обнаружения вторжений на основе встраиваемых микропроцессорных систем // Телекоммуникации. 2013. № S7. С. 15 – 18.
10. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2(25). С. 113 – 134.

11. Lavrova D.S. An approach to developing the SIEM system for the internet of things // Automatic control and computer sciences. 2016. Vol.50. №8. P. 673 – 681.
12. Анализ методов корреляции событий безопасности в SIEM-системах часть 1 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН. 2016. № 4(47). С. 5 – 27.
13. Грани SIEM / С. А. Графов, А. Ю. Белявцев, Д. А. Воронов, А. А. Трофимов // Защита информации. Инсайд. 2017. № 1(73). С. 56 – 62.
14. Графов А.Ф. Развитие российских SIEM-систем: Security Capsule // Защита информации. Инсайд. 2013. № 5(53). С. 84 – 86.
15. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-Системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2016. № 19. С. 111–124.
16. Петренко С.А., Цирлов В. Л. Импортозамещение решений IDS и SIEM // Защита информации. Инсайд. 2017. № 5(77). С. 46 – 51.

REFERENCES:

[1] Xodashinskij I.A., Meshheryakov R.V., Rubanov S. A. The construction of fuzzy intrusion detection classifiers based greedy and genetic algorithms. Voprosy` zashhity` informacii. 2013. № 4(102). pp. 67 – 72. (in Russian).
[2] Timonina A.A., Timonina E.E. Attacks on the centralized systems of intrusion detection. Sistemy` i sredstva informatiki. 2013. V. 23. № 1. pp. 33 – 42. (in Russian).
[3] Polovko I.Yu., Peskova O.Yu. Analysis of the functional requirements for intrusion detection systems. Izvestiya YuFU. Texnicheskie nauki. 2014. № 2(151). pp. 86 – 92. (in Russian).
[4] Proposal of perspective architectural intrusion detection and prevention system M.P. Sy`chev [i dr.]. Inzhenerny`j zhurnal: Nauka i innovacii. 2013. № 2(14). pp. 23. (in Russian).
[5] Efimov A.Yu. Problems of collecting and analyzing network traffic statistics to detect intrusion in information systems. Programmny`e produkty` i sistemy`. 2016. № 1. pp. 17 – 21. (in Russian).
[6] Burlakov M. E. The common model of intrusion detection syste. Doklady` Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioe`lektroniki. 2014. № 2(32). pp. 214 – 218. (in Russian).
[7] Bondyakov A. S. The basic modes of the intrusion prevention system (ids/ips suricata) for the computing cluster. Sovremenny`e informacionny`e texnologii i IT-obrazovanie. 2017. V. 13. № 3. pp. 31 – 37. (in Russian).
[8] Buldakova T. I., Dzhalolov A. Sh. Choice of the Data Mining technologies for intrusion detection systems into a corporate network. Inzhenerny`j zhurnal: Nauka i innovacii. 2013. № 11(23). pp. 36. (in Russian).
[9] Docenko S.M., Vlady`ko A.G., Letenko I.D. Intrusion detection systems based on embedded microprocessor systems. Telekommunikacii. 2013. № S7. pp. 15 – 18. (in Russian).
[10] Kotenko I.V., Saenko I.B., Polubelova O.V. Perspective data storage systems for security information monitoring and management. Trudy` SPIIRAN. 2013. № 2(25). pp. 113 – 134. (in Russian).
[11] Lavrova D.S. An approach to developing the SIEM system for the internet of things. Automatic control and computer sciences. 2016. Vol.50. №8. pp. 673 – 681. (in Russian).
[12] An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. A.V. Fedorchenko, D.S. Levshun, A.A. Chechulin, I.V. Kotenko. Trudy` SPIIRAN. 2016. № 4(47). pp. 5 – 27. (in Russian).
[13] SIEM-profile. S. A. Grafov, A. Yu. Belyavcev, D. A. Voronov, A. A. Trofimov. Zashhita informacii. Insajd. 2017. № 1(73). pp. 56 – 62. (in Russian).
[14] Grafov A.F. Development of Russian SIEM-systems: Security Capsule. Zashhita informacii. Insajd. 2013. № 5(53). pp. 84 – 86. (in Russian).
[15] Shaburov A.S., Borisov V.I. developing model information protection corporate network based on the implementation of siem-system. Vestnik Permskogo nacional`nogo issledovatel`skogo politexnicheskogo universiteta. E`lektrotexnika, informacionny`e texnologii, sistemy` upravleniya. 2016. № 19. pp. 111 – 124. (in Russian).
[16] Petrenko S.A., Cirlov V. L. Import Substitution Solutions IDS and SIEM. Zashhita informacii. Insajd. 2017. № 5(77). pp. 46 – 51. (in Russian).

Поступила в редакцию – 30 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 30, 2018. The final version – November 01, 2018.

Анатолий М. Тарасов
Академия управления МВД России,
ул. Зои и Александра Космодемьянских, 8, г. Москва, 125993, Россия
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

СТРУКТУРА И СОДЕРЖАНИЕ КОНВЕНЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

DOI: http://dx.doi.org/10.26583/bit.2018.4.05

Аннотация. В статье актуализируется проблема противодействия киберпреступлениям на основе консолидации международных усилий в данном направлении наряду с противодействиями терроризму, обороту наркотиков и другими правонарушениями, имеющими трансграничный характер. Приводятся результаты критического анализа структуры и содержания основных положений соответствующей Будапештской конвенции, принятой Советом Европы 23 ноября 2001 г. (ETS № 185). Анализ отражения в Конвенции вопросов организационно-правового регулирования борьбы с компьютерной преступностью проведен в сравнении с соответствующими нормами российского законодательства, в частности по терминологическим аспектам уголовного и уголовно-процессуального права в области компьютерной информации. Особое внимание обращается на критическое рассмотрение вопросов международного сотрудничества в свете новых вызовов и угроз в условиях все возрастающей конфронтации межгосударственных отношений. В заключение обосновывается необходимость принятия соответствующей конвенции Организацией Объединенных Наций с предложениями по содержанию ее основных направлений.
Ключевые слова: Конвенция Совета Европы, правоохранительные и судебные органы, правоохранительная деятельность, киберпреступность, международное сотрудничество, конфиденциальность, компьютерная техника, расследование, программное обеспечение, пароли и коды доступа, детская порнография, авторское право.
Для цитирования: ТАРАСОВ, Анатолий М. СТРУКТУРА И СОДЕРЖАНИЕ КОНВЕНЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 52-62, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1167>. Дата доступа: 19 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.05.

Anatoly M. Tarasov
Management Academy of the Ministry of the Interior of Russia,
Zoi and Alexandra Kosmodemianskikh str., 8, Moscow, 125993, Russia
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

The structure and content of the convention on combating cybercrime

DOI: http://dx.doi.org/10.26583/bit.2018.4.05

Abstract. Consolidation of international efforts plays a crucial role in combating cybercrime the same way as in counteracting to terrorism, drug trafficking and other offenses of cross-border nature. The results of a critical analysis of the structure and content of the major provisions of the Budapest European Convention of 23 November 2001 (ETS No. 185) are presented. The paper provides a comparative analysis of the Convention and the Russian legislation from the point of view of organizational and legal regulation of fight against computer crime. The accent is made on terminological aspects of criminal and criminal procedure law in the field of computer information. Particular attention is drawn to the critical consideration of issues of international cooperation in the light of new challenges and threats of an increasingly confrontational inter-state relations. The conclusion substantiates the need for the adoption of the relevant United Nations Convention with proposals on the content of its main statements.
Keywords: Council of Europe Convention, law enforcement and judicial authorities, law enforcement,

cybercrime, international cooperation, privacy, computer technology, investigation, software, passwords and access codes, child pornography, copyright.
For citation: TARASOV, Anatoly M. The structure and content of the convention on combating cybercrime. IT Security (Russia), [S.l.], v. 25, n. 4, p. 52-62, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1167>. Date accessed: 19 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.05.

Введение

Актуальность и важность рассмотрения данной темы связана с тем, что сегодня международное взаимодействие по противодействию киберпреступности ослабевает, все большее количество государств предпринимают шаги для получения господства в информационном пространстве. Во многих странах созданы и активно действуют кибервойска. Милитаризация киберпространства усиливает масштабы проявлений информационных войн, направленных против мира и безопасности. При этом основные угрозы нацелены на подрыв политической, экономической и социальной систем других государств, массированную психологическую обработку населения, сфокусированную на дестабилизации работы государственных и общественных институтов, в том числе с целью проведения так называемых «цветных революций» [1].

Постоянно увеличивается количество кибератак на сайты органов государственной власти других государств, все чаще атакуются критически важные объекты экономической и военной инфраструктуры, бизнеса, особенно банковского сектора [2].

Человечество сегодня столкнулось с серьезными рисками и вызовами, связанными с растущей латентностью киберпреступлений, их организованностью и глобализацией. Среди наиболее распространенных видов киберпреступлений в международном плане можно выделить создание, распространение и использование вредоносных программ, взлом паролей, кражу банковских реквизитов для совершения различных преступлений, распространение противоправной информации (клеветы, порнографических материалов и т.д.). Большую распространенность получили DdoS-атаки и финансовые киберпреступления, нацеленные на похищение платежных данных пользователей интернет-банкинга, платежных карт, а также непосредственно денег со счетов компаний и отдельных пользователей [3]. Одна из первых таких проб пера началась с троянца Ibank, в его развитие были созданы ZeuS и SpyEye, затем эту группу пополнили Carberp и Carbanak. Злоумышленники международной группы Carbanak, в которую входили граждане России, Украины, стран Европы и Китая, были установлены при непосредственном участии специалистов Лаборатории Касперского. По имеющимся данным, в 30 странах мира ими было похищено со счетов порядка 100 банков около 1 миллиарда долларов США. Кстати, о значительном росте киберугроз свидетельствуют следующие данные. Еще четыре-пять лет назад антивирусные ресурсы Лаборатории Касперского обнаруживали в течение суток порядке 125 – 150 тыс. вредоносных объектов, а в настоящее время – порядка 300 тыс. (рост в два раза).

Все более серьезную опасность представляют так называемые «умные дома», «умные квартиры», оборудованные «умными вещами» (телевизорами, стиральными машинами, кофеварками и другими бытовыми приборами, а также автомототранспортом). Такие вещи, подключенные к Интернету, программы которых требуют периодической прошивки, обновления, фиксируют и могут передавать информацию о наших привычках, интересах, с кем общаемся, интимных особенностях, то есть персональные качества. Принцип приватности все больше девальвируется.

Таким образом, можно сделать вывод, что борьба с киберпреступностью и новыми кибервызовами в международном формате наряду с проблемами борьбы с терроризмом, незаконным оборотом наркотиков, оружия, коррупцией является одной из наиболее сложных и требующих особого и постоянного внимания международного сообщества.

Масштабность киберугроз по логике вещей должна нацеливать различные государства на объединение усилий по созданию эффективных международных организационно-правовых механизмов по противодействию киберправонарушениям, однако, к сожалению, особенно в последние годы международные связи в этом направлении ослабли, эффективность противодействия киберпреступности существенно не возрастает. Вместе с тем именно нарастание в 90-е годы киберугроз

способствовало принятию Советом Европы 23 ноября 2001 г. в Будапеште Европейской конвенции по противодействию киберпреступлениям (ETS № 185) [4][1] (далее – Конвенция).

Анализ основных положений Конвенции

Сегодня все большее количество государств видят решение проблемы повышения эффективности противодействия киберпреступности в реализации принципа «неделимости безопасности кибепространства», то есть в применении правила-запрета отдельному государству добиваться господства в информационном пространстве над другими государствами. При этом учитывается, что решение этой проблемы заключается в совершенствовании механизмов сотрудничества, организационного, правового, финансового, кадрового, технического, информационного, научно-методического обеспечения деятельности правоохранительных и судебных органов власти.

На решение многих из указанных выше проблем нацелены положения Конвенции по противодействию киберпреступлениям, необходимость их реализации актуальна и востребована по сей день.

Слово и понятие «киберпреступность» используется в различных значениях, в том числе как компьютерная преступность[2] [5], преступность в сфере компьютерных технологий, компьютерной информации [6]. Эти понятия, как правило, воспринимаются как тождественные.

Под киберпреступлениями, как правило, понимаются преступные деяния, посягающие на информационную безопасность и совершенные в виртуальном пространстве с применением компьютерных технологий. Предметом их являются информация и компьютерные средства. При этом компьютер, его программное обеспечение являются либо орудием, либо предметом, либо средством посягательств.

Анализ положений Конвенции показывает, что их содержательная часть нацелена на создание эффективного организационно-правового механизма сотрудничества между государствами – членами Конвенции, а также организациями и частными лицами. Основной идеей данного документа стало установление единообразного международного подхода к составам компьютерных преступлений, которые государства должны включить в свое национальное законодательство, а также разработка мер по предотвращению правонарушений, направленных против целостности, доступности, конфиденциальности информации, компьютерных систем, сетей, данных, а также неправомерного их использования. Целью принятия Конвенции также является установление путей применения властных полномочий, способствующих обнаружению, расследованию и судебному преследованию за совершение кибердеяний с учетом соблюдения прав человека. Отметим при этом, что для государств, подписавших Конвенцию, большинство её положений несут не обязательный, а рекомендательный характер.

Анализ структуры и содержания показывает, что Конвенция охватывает три основных направления:

- согласование национальных правовых норм, определяющих составы соответствующих преступлений;
- формирование процедуры расследования киберпреступлений;
- создание действенной системы межгосударственного сотрудничества в сфере противодействия киберпреступности.

Структура и содержание Конвенции

Рассмотрим подробнее содержание и структуру Конвенции.

[1] Текст Конвенции размещен на ресурсе СПС «Гарант»: http://base.garant.ru/4089723/#ixzz5WwK9w8it. Российская Федерация к Конвенции не присоединилась, поскольку Россию, как и ряд других стран, не устраивает установленное в ст. 32 Конвенции право спецслужб одних стран проникать в киберпространство других стран и проводить там операции, не ставя в известность местные власти. За прошедший период к Конвенции присоединились или её подписали порядка 50 стран.

[2] См.: например: А.Я. Минин О специфике противодействия киберпреступности // Российский следователь. 2013. № 8; Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. №24.

В главе 1 Конвенции дается толкование терминов, связанных с содержанием данного международного документа. Например, дефиниция «компьютерная система» означает любое устройство или совокупность соединенных между собой или связанных устройств, одно либо более из которых осуществляет автоматическую обработку данных в соответствии с программой.

При этом отметим, что в российском законодательстве используется такой сходный термин, как «информационная система» [7]. Под ней в соответствии со статьей 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понимается «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

В Конвенции дается понятие термина «компьютерные данные» – это любое представление фактов, информации или концепций в форме, подходящей для обработки в компьютерной системе, в том числе это программы, предназначенные для выполнения компьютерной системой определенных действий. Следует сказать, что в примечании 1 к статье 272 УК РФ используется термин «компьютерная информация». Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В свою очередь под «данными трафика» (передвижения) в Конвенции понимаются любые компьютерные данные, связанные с операциями по их передаче посредством компьютерной системы, которые созданы компьютерной системой, являющейся звеном в цепочке передачи данных, и указывают на источник сообщения, его назначение, маршрут, время, дату, размер, длительность или тип лежащей в его основе услуги. Кроме того, в Конвенции дается определение «сервис-провайдера» или «поставщика услуг» – это любая государственная или частная организация (юридическое лицо), предоставляющая своим пользователям возможность обмениваться данными (коммуникационные услуги) посредством компьютерной системы, а также любая иная организация, которая обрабатывает или хранит компьютерные данные по поручению организации, предоставляющей коммуникационные услуги, либо пользователей таких услуг.

В разделе 2 главы 1 Конвенции перечисляются меры в области материального уголовного права, которые следует принять государствам в целях реализации положений Конвенции на национальном уровне.

Согласно Конвенции, к *объектам киберпреступлений относятся* охраняемые нормами права общественные отношения, связанные с информационно-коммуникационными процессами по поводу поиска, сбора, обработки, производства, накопления, хранения, передачи, распространения, потребления компьютерной информации. Для совершения киберпреступления в технико-технологическом плане необходимо наличие компьютерного устройства, компьютерных систем, соответствующего программного обеспечения, сети.

Анализ положений второй главы показывает, что структура киберпреступлений в Конвенции представлена четырьмя группами *общественно опасных деяний*.

В части 1 главы 2 Конвенции рассматриваются преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. В частности, в **статье 2** названо такое правонарушение, как «незаконный доступ», **в статье 3 «незаконный перехват», в статье 4 «вмешательство в данные», в статье 5 «вмешательство в систему, в статье 6 «ненадлежащее использование устройств».**

В части 2 главы 2 Конвенции рассматриваются преступления, связанные с компьютерами, такие как: **«подлог компьютерных данных» (ст. 7), «компьютерное мошенничество» (ст. 8). Статья 9 части 3** посвящена деяниям, связанным с содержанием контента, в частности **с детской порнографией. В статье 10 части 4** Конвенции рассматриваются преступления, связанные с нарушениями авторского права и смежных прав.

Статья 11 части 5 главы 2 посвящена вопросам, связанным с дополнительной ответственностью и санкциями, в частности, в связи **с покушением, пособничеством и подстрекательством**

в совершении киберпреступления. Кроме того, в статье 12 части 5 рассматриваются вопросы коллективной ответственности. Следует отметить, что статья 13 части 5 посвящена санкциям и мерам за совершение киберпреступлений. В ней акцент делается на то, что стороны Конвенции должны принять меры законодательного и иного характера, которые бы гарантировали, что лица, совершившие киберпреступления, будут наказаны действенными, соразмерными и убедительными санкциями, включающими в себя лишение свободы.

Таким образом, в Конвенции установлен перечень мер, которые должны принимать страны в отношении совершенных кибердеяний против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушений, связанных с компьютерами; правонарушений, относящихся к детской порнографии, а также связанных с нарушением авторских и смежных прав.

В Конвенции также установлено, что состав уголовно наказуемого правонарушения определяется наличием следующих условий:

а) совершенное деяние должно повлечь за собой ответственность;

б) при этом деяние должно быть совершено умышленно и противоправно.

Таким образом, для установления наличия состава преступления необходимо, чтобы в уголовном законодательстве соответствующего государства было предусмотрена ответственность за такое деяние, только тогда деяние становится противоправным, а также необходимо, чтобы преступление было совершено умышленно. Итак, в Конвенции определено, что преступной является деятельность, если её осуществление не санкционировано государством в установленном законном порядке.

Кстати, в российском уголовном законодательстве данное положение Конвенции нашло прямое отражение, в том числе в главе 28 УК РФ, именуемой «Преступления в сфере компьютерной информации», и других нормах. Так, в статье 272 УК РФ уголовное наказание предусмотрено за неправомерный доступ к охраняемой законом компьютерной информации, в статье 273 – за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, в статье 274 – за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации …».

Анализ содержания второй главы Конвенции позволяет сделать вывод о том, что компьютеры, компьютерные сети, программное обеспечение, человеческий ресурс могут быть использованы как в декларированном законом порядке, так и для достижения криминальных целей. В этой связи компьютерные программы в зависимости от субъективных целей фактически могут иметь двойное назначение: позитивное и криминальное – зависит от наличия или отсутствия соответствующего умысла, то есть от субъективного фактора.

Поэтому положения Конвенции, имеющие рекомендательный и дифференцированный характер, считаем вполне оправданными. При внесении изменений в национальные законодательства государства могут руководствоваться национальными факторами (особенностями). Причем Конвенция нацеливает государства на то, что в действиях лица, использующего технические возможности компьютера, его программное обеспечение, а также сети связи, необходимо устанавливать не только наличие или отсутствие преступного замысла, но и достижение его реализации. Ведь цель может быть не достигнута, например, по причинам отказа от доведения криминальной цели до результата в связи с отказом злоумышленника, либо по причине того, что не сработало программно-техническое обеспечение (покушение на преступление).

Отметим при этом, что компьютерные программы, состоящие из различных элементов, а также каждый элемент по отдельности могут быть задекларированы, но тем не менее программа может быть использована для совершения, например, неправомерного удаленного доступа к охраняемой законом компьютерной информации. Или наоборот, некоторые включенные в программу элементы, их функции могут быть не задекларированы и использованы для достижения преступных це-

лей, однако программа в целом, считается, не предоставляет таких технологических возможностей. Подход в таких случаях должен быть дифференцированным, и в законодательствах должны быть учтены и такие обстоятельства.

В этой связи в статье 273 УК РФ речь, очевидно, должна идти и об уголовной ответственности за создание отдельных элементов, которые могут быть использованы либо используются для создания программ, позволяющих применять их в преступных целях, причем как создателями, так и другими лицами. То есть важно учитывать, что одни лица создают элементы (составные части) или целые криминальные программы, другие их перепродают, не всегда зная об их криминальных ресурсах, а третьи их применяют в различных целях.

Понятно, что установить злоумышленников, обнаружить недекларируемые технологические элементы и их следы в программно-техническом обеспечении компьютера непросто[8], а доказать их преступную направленность, тем более до совершения криминального деяния, вообще крайне сложно. Нужны высокопрофессиональные специалисты и передовые технологии. Их отсутствие напрямую способствует высокой латентности совершенных киберпреступлений.

В этой связи и в целях повышения эффективности деятельности по профилактике киберпреступлений в уголовном законодательстве важно предусматривать различные аспекты, в том числе цели, признаки, стадии производства и использования программно-технического потенциала.

Перейдем к рассмотрению второго раздела второй главы Конвенции, именуемого «Процессуальные нормы». В нем установлены нормы, определяющие процедуру расследования компьютерных преступлений, то есть процессуальные вопросы борьбы с киберпреступностью. В частности, прописаны следующие аспекты, связанные с киберпреступностью:

– защита хранящихся в компьютерах данных;
– обеспечение безопасности хранения и оперативного представления данных о трафике;
– поиск и арест электронных систем;
– фиксация трафика, перехват сетевого контента.

При этом отметим, что статья 14 Конвенции содержит положение, относящееся к государствам – членам Конвенции, о необходимости нормативного правового обеспечения использования компьютерных систем и сбора доказательств в электронной форме при расследовании киберпреступлений, а статья 19 предусматривает расширение полномочий правоохранительных органов в первую очередь в части правовой регламентации их деятельности, касающихся осуществления оперативно-розыскных мероприятий в отношении компьютерных систем и носителей компьютерных данных. В этом связи можно сделать вывод о том, что Конвенция не просто рекомендует, а и обязывает государства – члены Конвенции создавать правовые возможности для ведения активного противодействия киберпреступности, включая наделение, например, субъектов оперативно-розыскной деятельности правом:

– выемки компьютерной системы, ее частей или носителей;
– конфискации копий компьютерных данных;
– уничтожения или блокировки компьютерных данных, находящихся в компьютерной системе;
– обеспечения целостности и сохранности хранящихся компьютерных данных, относящихся к конкретному делу[3].

При этом следует отметить, что основные задачи оперативно-розыскной деятельности (ОРД) согласно статье 2 Закона об ОРД состоят в выявлении, предупреждении, пресечении и раскрытии преступлений, а также в установлении лиц, их подготавливающих, совершающих или совершивших, скрывающихся от органов дознания, следствия и суда. Перечень допустимых оперативно-розыскных мероприятий указан в статье 6 этого Закона. К ним, в частности, относятся: исследование

[3] В России подобными правами в соответствии со ст. 13 Федерального закона от 12 августа 1995 г. «Об оперативно-розыскной деятельности» наделены, например, специальные подразделения МВД России, ФСБ России), ФСО России, СВР России, ФСИН России, ФТС России, Главного управления (ГРУ) Минобороны России.

предметов, … снятие информации с технических каналов связи[4] [9].

При решении задач ОРД субъекты оперативно-розыскной деятельности правоохранительных органов имеют право (статья 15 Закона об ОРД) производить изъятие документов, предметов, материалов и сообщений, прерывать предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Поясним, что при копировании документов и (или) информации, содержащейся на изымаемых электронных носителях информации, должны обеспечиваться условия, исключающие возможность утраты или изменения документов и (или) информации.

В соответствии с требованиями статьи 8 Закона Об ОРД проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, сообщений, передаваемых по сетям электрической связи, допускается на основании судебного решения и при наличии у субъектов ОРД установленной в Законе соответствующей информации.

Вместе с тем нужно сказать, что нормы Конвенции, касающиеся процессуальных решений и действий, как показывает их анализ, не обеспечивают в полном объеме унификацию процедуры раскрытия и расследования компьютерных преступлений, а также судебного преследования за их совершение, по которым сбор доказательств проводится с применением электронных средств и способов. Конвенция в этой части, на наш взгляд, регулирует только содержание отдельных розыскных, следственных и судебных действий.

При этом целый ряд достаточно важных процессуальных вопросов оставлен на усмотрение государств (сторон), её подписавших. Например, какие органы могут быть наделены полномочиями давать указания о сохранности электронных данных, об их предъявлении, блокировке и т. п. И такой подход является оправданным, поскольку на практике возникают проблемы, связанные с наличием/отсутствием соответствующей компетенции у тех или иных правоохранительных и судебных органов конкретного государства. Кстати, в различных государствах такими полномочиями наделены либо следственные, либо судебные органы, либо те и другие. В этой связи различается по своей процедуре и проведение процессуальных мероприятий.

Отметим также, что в Конвенции установлено, что государства-участники должны принять такие законодательные и иные меры, какие будут необходимы, чтобы обязать определенную структуру, лицо хранить компьютерные данные и обеспечивать их сохранность в течение адекватного периода времени. В этой связи возникает вопрос о длительности «адекватного» периода времени, а также о том, какие субъекты будут это устанавливать (государство в своём законодательстве или уполномоченные государственные органы в каждом конкретном случае).

Важное значение в Конвенции для ее ратификации имеет статья 20 «Сбор данных трафика в режиме реального времени» и статья 21 «Перехват данных содержания». В них установлены нормы, определяющие необходимость формирования национальной нормативной базы, обязывающей сервис-провайдеров проводить сбор, фиксацию, перехват необходимой информации с помощью имеющихся у них технических средств. Причем речь идет о сборе компьютерных данных в режиме реального времени. В решении таких вопросов сервис-провайдеры обязываются при сохранении полной конфиденциальности о фактах сотрудничества с правоохранительными органами способствовать их деятельности.

Принятый в России так называемый «Закон Яровой» (Федеральный закон от 6 июля 2016 года № 374-ФЗ, вносящий изменения в п.1 ст. 64 Федерального закона «О связи») предписывает операторам связи и организаторам распространения информации в сети «Интернет» хранить записи звонков и переписку своих абонентов и пользователей до шести месяцев, а информацию о фактах коммуникаций – до трех лет.

[4] Н.В. Павличенко Правовые и теоретические проблемы обеспечения негласности в оперативно-розыскной деятельности. Монография. М: 2016. 185 с.

Раздел III Конвенции именуется «Международное сотрудничество».

Этот раздел посвящен в основном вопросам экстрадиции и совместной деятельности государств – участников Конвенции по противодействию киберпреступлениям, достижения согласованности при сборе доказательств в электронной форме. Кроме того, в разделе определены общие для всех интернет-провайдеров международные правила хранения личной информации клиентов на случай, если такая или подобная информация будет затребована, например, правоохранительными органами в ходе расследования киберпреступлений.

Вопросы, связанные с экстрадицией, нашли непосредственное отражение в статье 24 Конвенции, где указывается, что экстрадиция применима, если совершены преступления, установленные в статьях 2 – 11 Конвенции и, если за эти преступления в законодательствах государств предусмотрена ответственность в виде лишения свободы на один год или более строгая мера ответственности. Важно отметить, что для государств, между которыми отсутствуют соглашения о выдаче преступников, но они являются сторонами Конвенции, данная норма является юридическим основанием для экстрадиции лиц, совершивших преступления, указанные в статьях 2 – 11 Конвенции.

В статье 25 Конвенции сформулированы общие принципы взаимной помощи государств – участников Конвенции, в статье 26 – порядок добровольного предоставления информации, в статье 27 определены принципы направления и выполнения запросов о содействии в случае отсутствия соответствующих международных соглашений, в статье 28 – принципы конфиденциальности и ограниченного использования информации. Перечисленные статьи (принципы) Конвенции нацелены в том числе на защиту прав и свобод человека и гражданина. Так, в статье 28 установлено, что государства обязаны соблюдать требования о конфиденциальности запросов об экстрадиции и не использовать полученную информацию в целях, не указанных в запросе. Адреса организаций соответствующего государства – стороны Конвенции, ответственной за подготовку запросов об экстрадиции или организации арестов, вносятся в регистр Генерального секретаря Совета Европы.

Помимо традиционных форм международного сотрудничества, регулируемого такими документами, как Европейская конвенция о выдаче (экстрадиции) от 13.12.1957 г. (ETS № 24)[5] и Европейская конвенция о взаимной правовой помощи по уголовным делам[6], принятой в Страсбурге 20 апреля 1959 г., в Конвенции по противодействию киберпреступлениям предусматривается осуществление международного сотрудничества, благодаря которому правоохранительные органы одних государств могут собирать хранимую на электронных носителях (компьютерах) информацию и улики, не проводя при этом трансграничных расследований и розыска [10].

К формам оказания правовой помощи по уголовным делам относится и установленная в Конвенции возможность применения электронных и факсимильных средств и способов связи, включая шифрование, в виртуальном пространстве, в частности, при направлении запросов и получении на них ответов (ст. 25 Конвенции).

Как показывает анализ содержания Конвенции, принципиальное значение для её подписания имеет статья 32, именуемая «Трансграничный доступ к компьютерным данным, находящимся в системах общего доступа, либо при получении соответствующего разрешения». В пункте b) статьи 32 установлено право любой из сторон без согласия другой стороны посредством компьютерной системы на своей территории получать трансграничный доступ к данным, которыми располагает другая сторона, без уведомления властей данного государства, располагающего соответствующей информацией, и в первую очередь это касается персональных (личных) данных. Такой правовой механизм позволяет нарушать фундаментальные гражданские права человека и гражданина. Получается, что каждое государство, подписавшее Конвенцию, с помощью действующих на его территории провайдеров может контролировать

[5] Собрание законодательства РФ. 25.10.1999. № 43. Ст. 5129. Конвенция ратифицирована.

[6] Собрание законодательства РФ. 05.06.2000. № 23. Ст. 2349. Конвенция ратифицирована с оговорками Федеральным законом от 25.10.1999 г. № 193-ФЗ.

информационный обмен в Сети. Как известно, основные провайдеры и их электронные ресурсы находятся на территории США, и у этой страны на этот счет имеются огромные преимущества. В то же время многие государства – стороны Конвенции не имеют такой технологической возможности, и данная норма для них является в основном декларативной, но обязательной для исполнения.

Кстати, отметим, что одним из противоречивых мест Конвенции является то, что, с одной стороны, в ней в качестве преступных деяний конкретно не указываются различные посягательства на конфиденциальность личных данных, с другой, согласно статье 10 Конвенции «О защите физических лиц в отношении автоматизированной обработки данных личного характера», государства – стороны Конвенции обязываются ввести в свое законодательство санкции за нарушение конфиденциальности личных данных.

Подчеркнем, что относиться к содержанию статьи 32 Конвенции можно по-разному. Положительная её направленность, в частности, проявляется в том, что эта норма позволяет получать трансграничный доступ к информации без бюрократических запросов, например, в ситуации, когда преступник и жертва находятся на территориях различных стран и в различной юрисдикции. Вместе с тем данной нормой создан общий механизм, позволяющий бесконтрольно правоохранительным органам одного государства непосредственно действовать в сфере юрисдикции другого государства, не прибегая к получению разрешения этого государства.

В этой связи отметим, что в основном именно из-за этой нормы целый ряд государств, в том числе Россия, не принимают решения о присоединении к Конвенции. Кстати, сам механизм присоединения к Конвенции определен в статьях 36 и 37. Так, в статье 36 установлено, что Конвенция открыта для подписания государствами – членами Совета Европы и государствами, не являющимися его членами, но участвовавшими в ее разработке, как, например, Россия.

Согласно статье 37 к Конвенции может присоединиться любое государство и вне Европы, но для этого необходимо согласие большинства государств – участников Конвенции. В этой гибкой процедуре проявляется значительный международный потенциал присоединения к Конвенции. Такой порядок, считаем, обоснован тем, что мировое сообщество крайне обеспокоено растущей опасностью, исходящей от киберугроз и стремится обеспечить международную безопасность киберпространства на основе глобального сотрудничества.

Заключение

В заключение отметим, что несмотря на некоторую противоречивость, Конвенция на сегодняшний день является одним из основных международных актов для развития национальных законодательств по противодействию киберпреступности, создания механизма государственного контроля за обращением компьютерных данных в связи с совершением киберправонарушений. Указанные в Конвенции разнообразные процессуальные действия позволяют сохранять, собирать, перехватывать и изымать информацию, являющуюся объектом и/или средством преступного посягательства.

При этом подчеркнем, что современные тенденции масштабного и трансграничного распространения киберпреступности, активно расширяющийся её глобальный характер обуславливают необходимость дальнейшего развития международного сотрудничества по противодействию киберугрозам в более широком формате – в рамках Организации Объединенных Наций (ООН). В этой связи на сегодняшний день важной задачей является принятие Конвенции ООН по кибербезопасности.

В проект данной Конвенции представляется необходимым включить следующие обязывающие государства принципы:

– невмешательства в информационное пространство друг друга, то есть неиспользования IT-технологий для вмешательства в дела, относящиеся к внутренней компетенции другого государства;

– неделимости обеспечения безопасности кибепространства;

– несовершения шагов, которые могли бы привести к усилению киберугроз;

– невмешательства во внутренние дела других государств, в частности для организации так называемых «цветных революций»;

– невключения в национальные нормативные правовые акты норм реагирования на кибератаки посредством применения ядерного оружия;

– неограничения доступа граждан в информационное пространство, за исключением случаев обеспечения национальной безопасности;

– сотрудничества при расследовании трансграничных кибератак (киберпреступлений).

СПИСОК ЛИТЕРАТУРЫ:

1. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с. (URL - http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf. (Дата доступа 14.10.2018).
2. Угрозы информационной безопасности в кризисах и конфликтах XXI века/Под редакцией А.В. Загорского, Н.П. Ромашкиной. – М: ИМЭМО РАН, 2015. – 151 с. (URL - https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf, дата доступа 14.10.2018).
3. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности. Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1 (3). С. 54 – 72.
4. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001) URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (Дата доступа: 10.10.2018).
5. Минин А. Я. О специфике противодействия киберпреступности // Российский следователь. 2013. № 8. С. 37 – 39.
6. Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. Издательство: Московский институт государственного управления и права (Москва). 2012. № 3. С. 178 – 186. URL: https://elibrary.ru/item.asp?id=21944441 (Дата доступа: 10.10.2018).
7. Тарасов А.М. Электронное правительство и информационная безопасность. Учебное пособие. М: Галарт, 2011. – 648 с.
8. Durakovsky, A. P., Melnikov, D. A., Gorbatov, V. S., Ivanenko, V. G. and Modestov, A. A., "Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)(FICLOUD), Vienna, Austria, 2016, pp. 123 – 130. doi:10.1109/FiCloud.2016.
9. Павличенко Н.В. Правовые и теоретические проблемы обеспечения негласности в оперативно-розыскной деятельности. Монография. М: 2016. – 185 с.
10. Hannigan R. The web is a terrorist's command-and-control network of choice // The Financial Times [Электронный ресурс]. URL: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I2F0l6FM (Дата доступа: 17.10.2018).

REFERENCES:

[1] Makarenko S.I. Information warfare and electronic warfare in the network-centric wars of the early XXI century. Monograph. — SPb.: Naukoemrie texnologii, 2017. — 546p. (URL - http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf (Access date: 14.10.2018)]. (in Russian).
[2] Informational Security Threats in Crises and Conflicts of XXI Century/ a.v. Zagorskii, N.P. Romashkina, eds. – Moscow, 2015. – 151p. (in Russian).
[3] Kazarin, O.V., eds. New types of threats to international information security. Vestnik RGGU. Seriya: Dokumentovedenie i arhivovedenie. Informatika. Zashchita informacii i informacionnaya bezopasnost'. 2016. № 1 (3). p. 54 – 72. (in Russian).
[4] Convention on crime in the sphere of computer information ETS N 185 (Budapest, November 23, 2001) URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (Access date: 10.10.2018).
[5] Minin, A.Ya. On the specifics of combating cybercrime. Rossijskij sledovatel'. 2013. №8. p. 37 – 39. (in Russian).

[6] Chekunov, I. G. Cybercrime: concept, classification, modern challenges and threats. Molodye uchenye. Publisher: Moscow Institute of public administration and law (Moscow). 2012. № 3. С. 178 – 186. URL: https://elibrary.ru/item.asp?id=21944441 (Access date: 10.10.2018) (in Russian).
[7] Tarasov, A.M. E - government and information security. Textbook. M: Galart, 2011. – 648 p. (in Russian).
[8] Durakovsky, A.P., Melnikov, D.A., Gorbatov, V.S., Ivanenko, V.G. and Modestov, A.A., "Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)(FICLOUD), Vienna, Austria, 2016, pp. 123 - 130. doi:10.1109/FiCloud.2016.
[9] Pavlichenko, N.V. Legal and theoretical problems of ensuring secrecy in operational-search activity. Monograph. M: 2016. – 185 p. (in Russian).
[10] Hannigan R. The web is a terrorist's command-and-control network of choice // The Financial Times [Электронный ресурс]. URL: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I2F0l6FM (Access date: 17.10.2018).

Поступила в редакцию – 14 октября 2018 г. Окончательный вариант – 15 ноября2018 г.
Received – October 14, 2018. The final version – November 15, 2018.

Александр Б. Саттаров, Наталья Г. Милославская
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ИЗУЧЕНИЮ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ» И СПОСОБОВ ЗАЩИТЫ ОТ НИХ

DOI: http://dx.doi.org/10.26583/bit.2018.4.06

Аннотация. Для реализации образовательной программы подготовки магистров по направлению 10.04.01 «Информационная безопасность» под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в НИЯУ МИФИ разработана программная оболочка учебно-лабораторного комплекса (УЛК), предназначенная для изучения сетевых атак типа «Человек посередине». В УЛК смоделированы четыре основные атаки данного типа: UDP Hijacking, Session Hijacking, TCP Hijacking и Bucket brigade attack. В статье представлены два приложения УЛК: приложение преподавателя и приложение студента. Для оценки знаний студентов после выполнения лабораторной работы создан модуль оценки знаний «Тестирование», который включает в себя вопросы для проведения тестирования с помощью программной оболочки УЛК. Составлены методические указания по выполнению лабораторной работы. В рамках дисциплины «Защищенные информационные системы» кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ, реализующих выше указанную программу подготовки магистров, проведена успешная апробация разработанного УЛК. В заключении статьи указаны пути дальнейшего совершенствования УЛК.
Ключевые слова: учебно-лабораторный комплекс, атака типа «Человек посередине», UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.
Для цитирования: САТТАРОВ, Александр Б.; МИЛОСЛАВСКАЯ, Наталья Г. УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ИЗУЧЕНИЮ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ» И СПОСОБОВ ЗАЩИТЫ ОТ НИХ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 63-74, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1162>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.06.

Alexander B. Sattarov, Natalia G. Miloslavskaya
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them

DOI: http://dx.doi.org/10.26583/bit.2018.4.06

Abstract. For the implementation of the Master's program "Business Continuity and Information Security Maintenance" in the field of specialty 10.04.01 "Information Security", a software shell of the educational laboratory complex (ELC) designed to study the "Man in the middle" network attacks has been developed in the NRNU MEPhI. In the framework of the ELC four basic attacks of this type are modeled: UDP Hijacking, Session Hijacking, TCP Hijacking and Bucket brigade attack. The paper presents two ELC applications: the instructor's application and the student's application. To assess the students' knowledge after performing laboratory work, the "Testing" module for assessing progress testing has been created, which includes questions for testing using the ELC software shell. Methodical instructions on performance of laboratory work have been written. Within the framework of the "Protected Information Systems" discipline of the

Information Security of Banking Systems Department of the NNIU MEPhI, implementing the above-mentioned Mastre's program, a successful approbation of the developed ELC has been carried out. In conclusion the ways to further improvement of the ELC are suggested.

Keywords: Educational and Laboratory System, Man-in-the-middle attack, MITM, UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.

For citation: SATTAROV, Alexander B.; MILOSLAVSKAYA, Natalia G. Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them. IT Security (Russia), [S.l.], v. 25, n. 4, p. 63-74, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1162>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.06.

Введение

Современный мир предъявляет к грамотному специалисту повышенные требования, которые не существовали в старых образовательных программах. Эти требования отличает большая универсальность, и согласно компетентностному подходу, впервые зародившемуся в начале 80-х годов XX века, они называются базовыми профессиональными компетенциями, включающими знания, умения и навыки. Компетентностный подход, реализуемый в современных российских образовательных стандартах, предполагает создание фондов оценочных средств, предназначенных для объективного контроля появления, развития и совершенствования заданного набора компетенций у выпускников вузов. При этом оценивание сформированности каждой компетенции как способности успешно применять знания, умения, навыки при решении задач профессиональной деятельности является важной задачей. Нередко для решения подобных задач в учебном процессе применяются электронные информационно-образовательные системы и среды, которые позволяют организовать и проводить мониторинг, контроль и управление процессом обучения.

В рамках образовательной программы «Обеспечение непрерывности и информационной безопасности бизнеса» подготовки магистров по направлению 10.04.01 «Информационная безопасность» кафедра «Информационная безопасность банковских систем» НИЯУ МИФИ реализует дисциплину «Защищенные информационные системы». Эта дисциплина формирует следующие общекультурные (ОК), общепрофессиональные (ОПК) и профессиональные компетенции (ПК) выпускников [1]:

- «способность к саморазвитию, самореализации, использованию творческого потенциала» (ОК-2);
- «способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой профессиональной деятельности» (ОК-3);
- «способность к самостоятельному обучению и применению новых методов исследования» (ОПК-2);
- «способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты в соответствии со стратегией развития информационных систем» (ПК-1);
- «способность проектировать и разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности» (ПК-2);
- «способность проводить обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов» (ПК-3);
- «способность разрабатывать программы и методики испытаний программных, программно-аппаратных и технических средств и систем обеспечения информационной безопасности» (ПК-4);

- «способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента» (ПК-7);
- «способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи» (ПК-8);
- «способность организовать выполнение работ по созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности» (ПК-15).

Для формирования компетенций ОК-3, ОПК-2 и ПК-1 разработан учебно-лабораторный комплекс (УЛК) по моделированию атак типа «Человек посередине» (англ. Man-in-the-Middle), который состоит из программной оболочки (включает приложение преподавателя и приложение студента), самих лабораторных модулей, модуля оценки знаний и методических указаний по выполнению лабораторных работ. В результате успешного прохождения лабораторных работ, реализованных в качестве модулей УЛК, студенты будут:

знать:

- основные методы и средства реализации атак типа «Человек посередине»;
- протоколы передачи данных TCP и UDP;

уметь:

- определять наличие уязвимостей информационных систем (ИС), подверженных атакам типа «Человек посередине»;

владеть:

- навыками распознавания атак типа «Человек посередине» на ИС для выбора адекватной защиты от них.

Суть атак типа «Человек посередине» широко освещена в англоязычных источниках, однако в русскоязычных практически не встречается. Проведение интерактивных лабораторных работ по данной теме возможно двумя способами: изучая реальные атаки в изолированной среде – песочнице (примеры учебных заведений, выбравших этот способ – Университет Тренто [https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:netsec:2016:network_security_lab_report_-_group_1.pdf], Мичиганский технологический университет [http://pages.mtu.edu/~xinlwang/itseed/labs/Spoof_MiTM.pdf], Исламский университет Газы [http://site.iugaza.edu.ps/nour/files/lab4-MITM1.pdf], Университет Петры [http://lms.uop.edu.jo/lms/pluginfile.php/401/mod_resource/content/0/Lab-MITM.pdf] и другие университеты) или полностью эмулируя их. Мы выбрали второй путь. Ни одного описания аналогичных лабораторных работ для данной атаки в открытой печати не найдено.

Целью данной статьи является описание разработанного УЛК по изучению атак типа «Человек посередине» и опыта его использования в рамках учебного процесса НИЯУ МИФИ.

Общие сведения об атаке «Человек посередине»

Атака типа «Человек посередине» впервые была применена еще задолго до появления современных компьютеров в 1586 г. в заговоре Боббингтона, в котором шифровки передавались на бумаге, а также позднее – во время Второй мировой войны, для чего использовался радиопередатчик «Aspidistra». При данной атаке возникает ситуация, в которой атакующий способен читать и изменять сообщения, передающиеся между атакуемыми [2, 3]. Такой метод компрометации канала позволяет злоумышленнику незаметно для атакуемых осуществлять активное вмешательство в протокол передачи данных, удаляя, искажая, навязывая ложную информацию или создавая сообщения от имени атакуемых. Очевидно, что такое вмешательство в канал связи открывает широкие возможности для атакующего и позволяет влиять на ситуацию, оставаясь незамеченным.

Первое упоминание атаки в сфере информационной безопасности (ИБ) появилось в 1981 г. в труде «Password authentication with insecure communication» автора Лесли Лампорта (Leslie Lamport)

[4]. С тех пор сетевые технологии значительно шагнули вперед, а атака приобрела более отчетливые черты и стала использоваться во множестве случаев. Атака активно применяется до сих пор и будет применяться до тех пор, пока компьютеры будут передавать информацию между собой незащищенным образом. Поэтому этой теме посвящено много работ современных исследователей: уязвимости анализируются, например, в [5], новые разновидности, особенно связанные с беспроводным доступом и протоколом IPv6, - в [6 - 8]. Вопросам защиты от этих атак посвящены, например, работы [9, 10].

В настоящее время известны четыре основные реализации названной атаки.

1. Bucket brigade attack – это разновидность атаки «Человек посередине», в которой атакующий перехватывает сообщения атакуемых при обмене ключами, используемыми для создания защищенного канала. Атакующий встает посередине между ними при обмене сообщениями (рис. 1). Свое название разновидность атаки получила из-за сходства с пожарными бригадами во время тушения пожара – они передавали ведро с водой от человека к человеку, чтобы доставить его до конца цепочки из людей и обратно. В сетевой атаке цепочка состоит из трех участников, где посередине находится атакующий, а по краям – атакуемые [11].

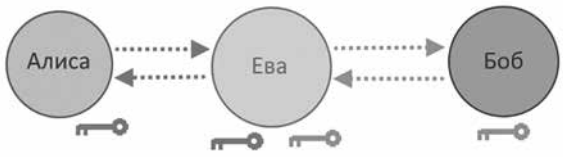


Рис. 1. Bucket brigade attack
(Fig. 1. Bucket brigade attack)

2. Session Hijacking (перехват сессии). В эпоху цифровых технологий люди активно используют поисковые системы, социальные сети и другие возможности Интернета. Но часто доступ к некоторой информации требуется разрешить только определенному кругу лиц. Многие сайты предоставляют возможность оставлять комментарии к новостям и общаться с другими пользователями. Для того чтобы наделить пользователя правом представляться тем, за кого он себя выдает, интернет-ресурсы ввели систему аутентификации: требуется ввести имя и пароль пользователя. Но время показало, что это удобно и необременительно не для всех пользователей. Сохранять же аутентификационные данные в браузере – небезопасно, поскольку при получении физического доступа к компьютеру они попадают в руки злоумышленника. Так появились сессии пользователя: при успешном прохождении процедуры аутентификации браузер пользователя сохраняет не введенные пользователем данные, а уникальную строку (характеризующую текущую сессию пользователя), которую ему сообщает посещаемый сайт. В будущем при каждом обращении к сайту браузер сообщает сайту ранее сохраненную сессионную строку, что подтверждает подлинность пользователя. Строка является уникальной для каждой сессии и исчезает необходимость сохранять пароль в браузере – требуется ввести его единожды при входе на сайт. Но и это открывает возможность без знания аутентификационных данных получить авторизованный доступ к интернет-ресурсу, если каким-либо образом узнать уникальную сессионную строку. Именно поэтому данная разновидность атаки и получила название Session Hijacking.

Если в момент запроса к сайту атакующий перехватит сессию, которую браузер атакуемого автоматически добавляет в запрос к сайту, то он сможет подставить ее в свой браузер. В таком случае атакующий без знания аутентификационных данных получает авторизованный доступ к сайту от лица атакуемого [12], что проиллюстрировано на рис. 2.

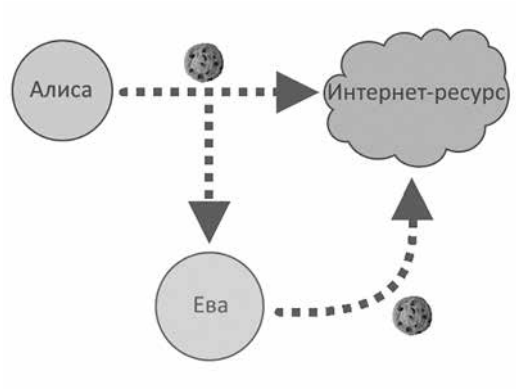
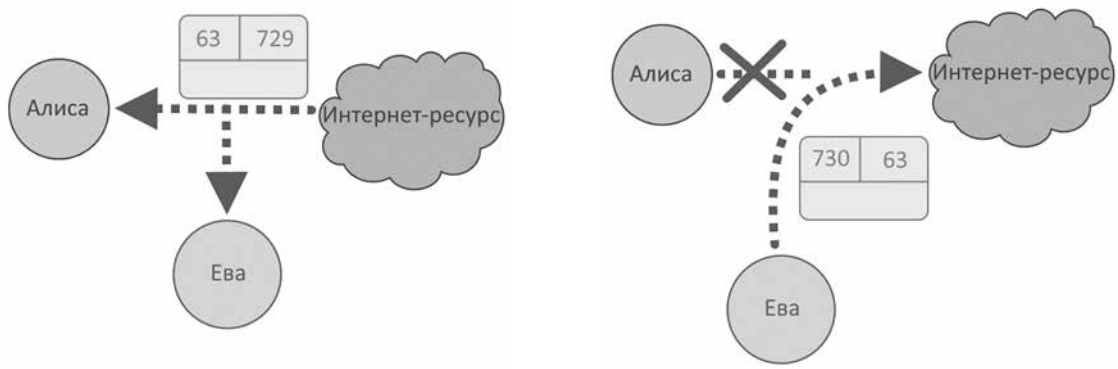


Рис. 2. Session Hijacking
(Fig. 2. Session Hijacking)

3. TCP Hijacking. С развитием технологий и появлением новых протоколов передачи данных существует вероятность возникновения и новых возможностей для проведения атак. Так произошло и с протоколом транспортного уровня TCP [13], который используется для гарантированной доставки информации от одного узла сети к другому. Известно, что для контроля обмена пакетами при TCP-соединении в пакетах предусмотрено два поля (Sequence number и Acknowledge number) по 32 бита каждое. Эти два поля являются единственными идентификаторами, с помощью которых сервер различает TCP-соединения и TCP-абонентов. С их помощью при обмене пакетами клиент с сервером ведут учет пакетов. Если атакующий сможет узнать эти поля, то у него появится возможность составить ложный TCP-пакет, который будет обработан сервером или клиентом [14]. Более того, будет возможно и дальше продолжать обмен ложными TCP-пакетами. Однако следует обратить внимание на очевидную закономерность при внедрении ложного TCP-пакета – получатель пакета при ответе будет использовать Acknowledge number, отличный от того, что ожидает его TCP-собеседник. Произойдет десинхронизация, и соединение между сервером и клиентом в рамках текущей TCP-сессии будет невозможно, но оно останется открытым для атакующего. И эта проблема решаема, если атакующий полностью контролирует все пакеты между клиентом и сервером – он может самостоятельно изменять значения идентификационных полей на корректные и пропускать модифицированный пакет дальше.

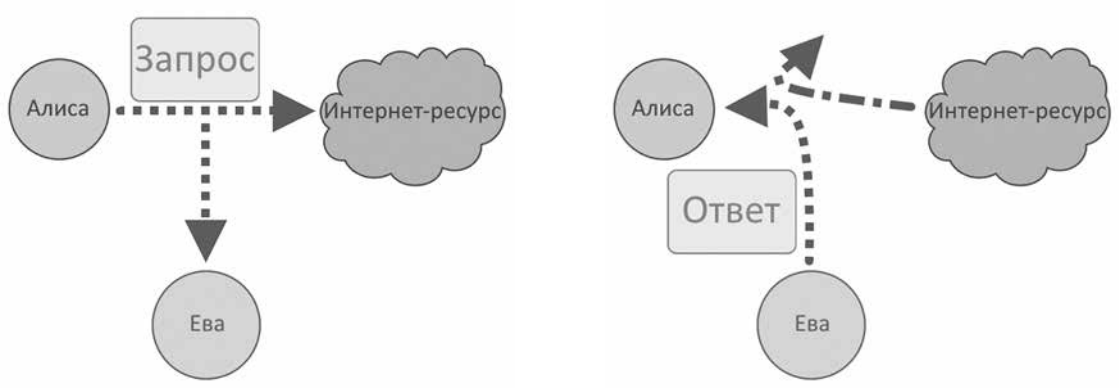
Для проведения рассматриваемой атаки злоумышленнику требуется узнать Sequence number. После он должен составить ложный пакет, который в поле Acknowledge number будет содержать Sequence number, увеличенное на единицу. В таком случае отправленный пакет будет корректно обработан (рис. 3).



А) *Б)*

Рис. 3. TCP Hijacking: А) перехват TCP-пакета; Б) захват соединения атакующим
(Fig. 3. TCP Hijacking: A) TCP packet interception; Б) connection capturing by attacker)

4. UDP Hijacking. Многие приложения (например, при передаче голоса или в играх реального времени с несколькими игроками по сети) используют протокол UDP из-за его легковесности. Потеря пакетов при доставке их клиенту или на сервер в таких случаях не существенна, ведь следом за ним придет пакет с актуальной информацией, а потерянный пакет уже будет не нужен. Это и является отличным условием для передачи атакующим атакуемому своего собственного ложного пакета. При этом пакет, который придет от сервера, уже будет не нужен – он считается устаревшим. На этом и основана атака UDP Hijacking (рис. 4). Атакующий, просматривая информацию, которой обмениваются атакуемый и сервер, ждет, когда атакуемый запросит у сервера некоторые данные по протоколу UDP. Если в этот момент отправить атакуемому ложный пакет в ответ на его запрос до того, как он получит ответ от сервера, то он его примет как действительный ответ на свой запрос [15]. С помощью этого можно скомпрометировать поведение атакуемого.



А) Б)

Рис. 4. UDP Hijacking: А) перехват запроса; Б) отправка ответа атакующим
(Fig. 4. UDP Hijacking: A) request interception; Б) sending of response by attacker)

Программная оболочка учебно-лабораторного комплекса

На основе рассмотренных выше видов атак составлены требования к УЛК, а также детально описаны его особенности. Описание было формализовано в виде технического задания. Для возможности расширения набора лабораторных модулей архитектура УЛК спроектирована таким образом, чтобы при написании кода сторонние разработчики могли использовать наработки УЛК с максимальным удобством и минимальными временными затратами.

В составе УЛК разработана программная оболочка, состоящая из двух приложений – преподавателя и студента.

Графический интерфейс приложения студента представлен на рис. 5 – 7. Это аутентификация студента, выбор им лабораторной работы и ее выполнение соответственно.

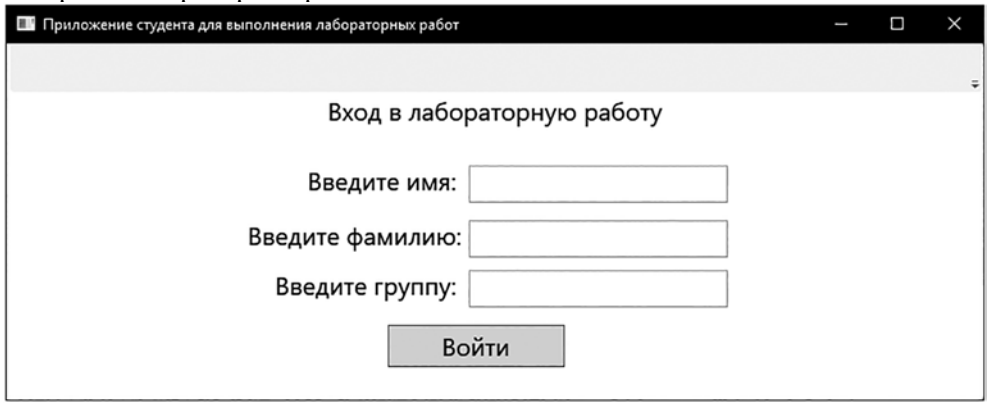


Рис. 5. Экран приложения студента для входа в лабораторную работу
(Fig. 5. The student application screen for entering the laboratory work)

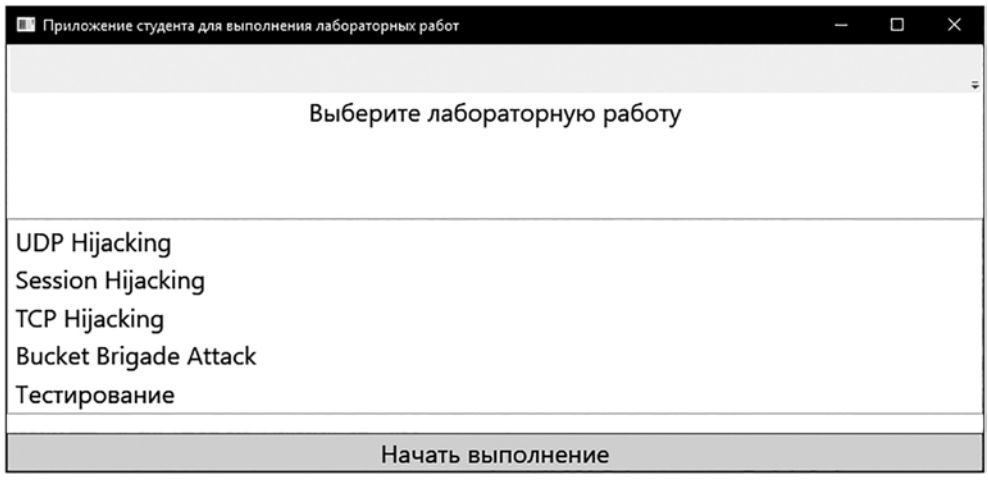


Рис. 6. Экран выбора лабораторной работы
(Fig. 6. Screen for selecting laboratory work)

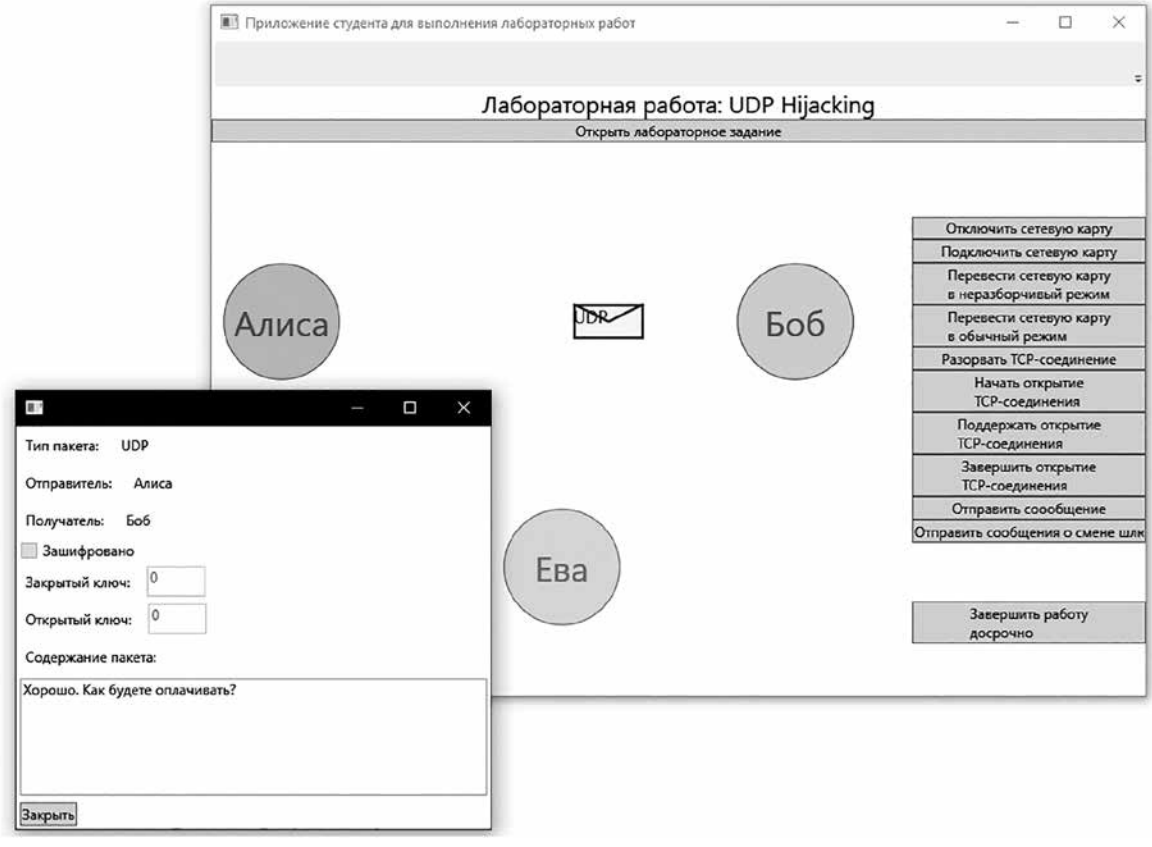


Рис. 7. Экран выполнения лабораторной работы
(Fig. 7. The screen of laboratory work implementation)

Если студент случайно закрывает свое приложение, то ему следует ввести те же самые идентификационные данные, так как встроенная система их контроля не позволит перейти к этапу выбора лабораторной работы, если они не совпадут с введенными в первый раз. Это сделано для предупреждения аутентификации студентов под чужими именами для «пробных» попыток прохождения лабораторных работ.

По завершении лабораторной работы в дополнительном окне отображается результат ее выполнения, выраженный целым числом по пятибалльной шкале.

Графический интерфейс приложения преподавателя отображает аутентифицировавшихся студентов (фамилию, имя, группу) и элементы управления для допуска к лабораторным работам, просмотра результатов их выполнения, а также сохранения в виде «*.CSV»-файла статистики выполнения четырех модулей лабораторной работы по каждому студенту в отдельности или статистики по всем студентам и всем модулям (рис. 8).

Если студент закроет свое приложение, то строка с его идентификационными данными станет серой, а при повторной аутентификации – снова зеленой.

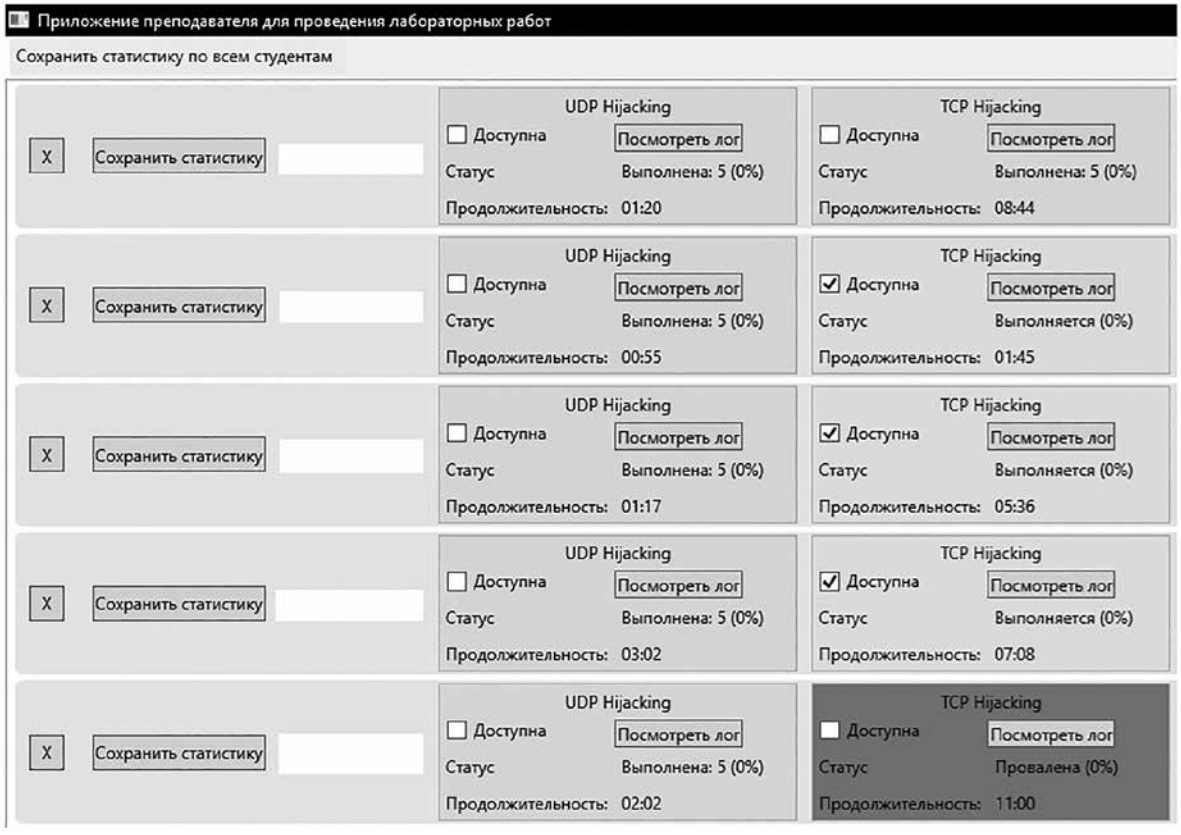


Рис. 8. Графический интерфейс приложения преподавателя
(Fig. 8. The graphical interface of the instructor's application)

В каждом блоке, соответствующем четырем модулям лабораторной работы, доступен элемент типа «CheckBox» с текстом «Доступна». При установке его в состояние «выбран» модуль лабораторной работы по сети передается в приложение соответствующего студента, а при установке в состояние «недоступна» – отзывается из приложения соответствующего студента. Таким образом, студент не сможет при получении несанкционированного доступа к лабораторным компьютерам (так называемым автоматизированным рабочим местам (АРМ) студента) получить модули для подготовки дома или заменить их на скомпрометированные. Также для предотвращения перехвата модулей по сети приложения преподавателя и студента используют протокол TCP с TLS 1.2 (Transport Layer Security). TLS-сертификат должен располагаться в папке «Certificate», а модули лабораторных работ в папке «Labs». Папки «Certificate» и «Labs» расположены в директории, в которую установлено приложение преподавателя.

Также в программной оболочке присутствует подсистема журналирования. Журналы индивидуальны для каждого модуля у каждого студента и позволяют вести журналирование при помощи

метода Log (string message) объекта radio, которые передаются в конструктор лабораторного модуля при создании. Для просмотра журналов предназначена кнопка «Посмотреть лог» в блоке модуля, после нажатия на которую содержимое журнала появится в отдельном окне. Также сами блоки окрашиваются в салатовый цвет, если студент успешно завершил выполнение модуля, в светло-красный, если завершил, но не успешно, и в светло-голубой на сером фоне, если студент находится в процессе выполнения лабораторной работы. В последнем случае в блоке присутствует секундомер, показывающий длительность выполнения студентом лабораторной работы. По завершении выполнения лабораторной работы в соответствующем блоке будет отображен результат выполнения: «Выполнена» с оценкой выполнения по пятибалльной шкале, если она успешно завершена, и «Провалена», если нет.

Представленная программная оболочка разработана на языке программирования C# с использованием платформы «.NET Framework», так как она является предустановленной на компьютерах с ОС «Windows» версий 7, 8.1 и 10, которые используются на компьютерах лаборатории кафедры. Разработка велась с использованием графической подсистемы Windows Presentation Foundation (WFP), входящей в состав «.NET Framework», что в случае необходимости расширения ее функционала позволяет гибко модифицировать исходный код программной оболочки. Также WPF позволяет использовать для этого не только элементы WFP, но и интегрировать распространенные до сих пор «Windows Forms» элементы, если разработчик не будет владеть WPF в достаточной мере.

Суммарное количество строк кода УЛК составляет порядка 11 тыс.

Шаблон «LabTemplate» и модули лабораторной работы

На платформе «.NET Framework» версии 4.0 был разработан шаблон «LabTemplate» в виде динамической библиотеки, содержащей одноименный класс в пространстве имен «LabTemplateNamespace», который необходимо использовать для реализации модуля лабораторной работы и переопределить методы, создающие графические элементы с заданием лабораторной работы и самой лабораторной работой.

Результатом компиляции модуля лабораторной работы является динамическая библиотека, исходный код которой также написан с использованием платформы «.NET Framework» версии 4.0.

Для переопределения доступны следующие методы:

- getUIControl: графический элемент, предназначенный для взаимодействия с пользователем, он будет отображен в центре приложения студента для выполнения лабораторных работ;
- getName: наименование лабораторной работы, которое будет отображено в заголовке лабораторной работы;
- getMission: графический элемент, предназначенный для отображения в отдельном окне лабораторного задания.

На языке программирования C# были разработаны пять модулей лабораторной работы, представляющие собой динамические библиотеки: модули «UDP Hijacking», «Session Hijacking», «TCP Hijacking» и «Bucket brigade attack» и модуль «Тестирование».

Апробация разработанного УЛК в учебном процессе НИЯУ МИФИ

Вышеописанный УЛК был установлен в двух учебно-лабораторных кабинетах на лабораторных компьютерах кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ. Его апробация происходила на 63 магистрантах трех групп первого года обучения в рамках дисциплины «Защищенные информационные системы».

Для подготовки студентов к лабораторным работам были составлены методические указания, включающие в себя как информацию о самих лабораторных работах, так и теоретическую справочную информацию в виде описания протоколов TCP и UDP, трехэтапного установления соединения по протоколу TCP, протокола Диффи-Хеллмана, шифра Цезаря, режимов работы сетевой карты и информации об ARP-таблице. Также в методических указаниях приведены способы защиты от моделируемых студентами атак типа «Человек посередине».

Условия выполнения лабораторных работ были следующие: количество попыток и время прохождения модулей не ограничены, допуск к модулям происходит последовательно – доступ к следующему модулю открывается при прохождении предыдущего, модули выполняются в следующей последовательности: «UDP Hijacking»; «Session Hijacking»; «TCP Hijacking»; «Bucket brigade attack»; «Тестирование».

Модуль «Тестирование» содержит список вопросов, из которых выбираются случайные 20. Каждый вопрос представлен в виде текста и нескольких вариантов ответа, среди которых можно выбрать один и более.

В табл. 1 указано среднее время прохождения каждого модуля и среднее количество попыток, совершенное студентами для его прохождения. Собрана следующая статистика: в среднем на прохождение модуля «UDP Hijacking» требуется 3 попытки по 4.1 мин каждая, модуля «Session Hijacking» – 2 попытки по 3.8 мин каждая, модуля «TCP Hijacking» – 3 попытки по 8.9 мин каждая, модуля «Bucket brigade attack» – 3 попытки по 21.4 мин каждая, модуля «Тестирование» – 1 попытка длительностью 17.1 мин.

Таблица 1. Средние показатели прохождения каждого модуля УЛК

	UDP Hijacking	Session Hijacking	TCP Hijacking	Bucket Brigade Attack	Тестирование
Среднее время прохождения модуля, мин	4.1	3.8	8.9	21.4	17.1
Среднее количество попыток прохождения модуля	3	2	3	3	1

Согласно этим данным, в среднем на проведение лабораторной работы требуется 127.9 минуты (чуть меньше трех академических часов). Однако показатель – средний, а значит будут присутствовать студенты, выполняющие лабораторную работу несколько дольше.

На рис. 8 представлен скриншот с графическим интерфейсом приложения преподавателя во время проведения лабораторной работы у одной из групп (идентификационные данные студентов искажены умышленно). Он показывает, что первый студент успешно выполнил три лабораторные работы, последний студент успешно выполнил первые две работы, но не смог выполнить третью, а остальные студенты успешно выполнили первые две работы и находятся в процессе выполнения третьей.

Заключение

Использование информационных технологий в сфере образования значительно ускоряет процесс передачи знаний за счет их более наглядного и динамического представления. Однако эта сфера настолько обширна, что создать для каждой учебной дисциплины поддержку в виде преобразования знаний в цифровой формат до сих пор является проблемой. Целью данной работы было оптимизировать процесс проведения лабораторных работ с помощью разработанного УЛК. В рамках представленной работы разработан и апробирован УЛК, состоящий из шаблона «LabTemplate» модуля лабораторной работы, программной оболочки (приложение преподавателя и приложение студента для проведения лабораторных работ), четырех модулей лабораторных работ («UDP Hijacking», «Session Hijacking», «TCP Hijacking», «Bucket brigade attack»), модуля оценки знаний «Тестирование» и методических указаний к лабораторной работе.

Апробация разработанного УЛК прошла успешно, что показало его работоспособность и соответствие поставленным целям, а также позволило собрать статистику прохождения студентами отдельных лабораторных модулей. В среднем студенту требуется 127.9 минут для того, чтобы пройти четыре модуля УЛК и протестировать полученные теоретические знания и практические навыки.

В текущей работе смоделированы вышеописанные атаки, однако в рамках работы отсутствуют реализации наглядных демонстраций способов защиты от них. Таким образом, продолжение

работы будет заключаться в расширении списка лабораторных работ, в которых будет реализовано моделирование способов защиты от вышеописанных атак.

СПИСОК ЛИТЕРАТУРЫ:

1. Образовательный стандарт высшего образования Национального исследовательского ядерного университета «МИФИ». 10.04.01 «Информационная безопасность». 2017.
2. Лапонина О. Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие. 2014. 16 с.
3. Müller L. Man in the Middle Attack. 2010. URL: http://jusit.eu/wp-content/uploads/2011/08/mitm.pdf (дата обращения 03.05.2018)
4. Lamport L. Password authentication with insecure communication. Communications of the ACM. ACM New York, NY, USA. Volume 24 Issue 11, Nov. 1981. Pages 770-772.
5. Kaka S., Sastry, V.N., Maiti, R.R. On the MitM vulnerability in mobile banking applications for android devices. 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016. DOI: 10.1109/ANTS.2016.7947811.
6. Gelernter N., Kalma S., Magnezi B., Porcilan H. The Password Reset MitM Attack. 2017 IEEE Symposium on Security and Privacy, SP 2017. San Jose; United States. Pages 251-267. DOI: 10.1109/SP.2017.9.
7. Vondráček M., Pluskal J., Ryšavý O. Automation of MitM attack on Wi-Fi networks. Proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2017. Prague, Czech Republic. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Volume 216, 2018, Pages 207-220. DOI: 10.1007/978-3-319-73697-6_16.
8. Huang Y., Jin L., Wei H., Lou Y., Kang X. Pilot Contamination with MITM Attack. Proceedings of the 5th IEEE Vehicular Technology Conference, VTC Spring 2017. Sydney, Australia. DOI:10.1109/VTCSpring.2017.8108523.
9. Ouseph C., Chandavarkar, B.R. Prevention of MITM attack caused by rogue router advertisements in IPv6. Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, Pages 952-956. DOI: 10.1109/RTEICT.2016.7807969.
10. Al Abri D. Detection of MITM attack in LAN environment using payload matching. Proceedings of the 2015 IEEE International Conference on Industrial Technology, ICIT 2015. Seville; Spain. Pages 1857-1862. DOI: 10.1109/ICIT.2015.7125367.
11. Bucket Brigade. SearchSecurity. URL: http://searchsecurity.techtarget.com/tip/Bucket-Brigade (дата обращения: 03.05.2018).
12. Study And Analysis On Session Hijacking Computer Science Essay. UK Essays. URL: https://www.ukessays.com/essays/computer-science/study-and-analysis-on-session-hijacking-computer-science-essay.php?utm_expid=309629-38._Nb6m1ixT_aGX1K3CVQTDw.0 (дата обращения: 03.05.2018).
13. RFC 793, Transmission Control Protocol. URL: https://tools.ietf.org/html/rfc793 (дата обращения: 03.05.2018).
14. Wegener C., Dolle W. Hijack Prevention – Understanding and preventing TCP attacks. Linux-Magazine, 09/2005; pages 66-71; ISSN 14715678.
15. Basta A., Basta N., Brown M. Computer Security and Penetration Testing. Cengage Learning. 2013. 400 p.

REFERENCES:

[1] Obrazovatel'nyj standart vysshego obrazovanija National Research Nuclear University «MEPhI». 10.04.01 «Information security». 2017.
[2] Laponina O. R. Fundamentals of network security. Part 1. Mezhsetevye jekrany: Uchebnoe posobie. 2014 (in Russian).
[3] Müller L. Man in the Middle Attack. 2010. Available at: http://jusit.eu/wp-content/uploads/2011/08/mitm.pdf (accessed 15.05.2018)
[4] Lamport L. Password authentication with insecure communication. Communications of the ACM. ACM New York, NY, USA. Volume 24 Issue 11, Nov. 1981. Pages 770 - 772.
[5] Kaka S., Sastry, V.N., Maiti, R.R. On the MitM vulnerability in mobile banking applications for android devices. 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016. DOI: 10.1109/ANTS.2016.7947811.
[6] Gelernter N., Kalma S., Magnezi B., Porcilan H. The Password Reset MitM Attack. 2017 IEEE Symposium on Security and Privacy, SP 2017. San Jose; United States. Pages 251 - 267. DOI: 10.1109/SP.2017.9.

[7] Vondráček M., Pluskal J., Ryšavý O. Automation of MitM attack on Wi-Fi networks. Proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2017. Prague, Czech Republic. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Volume 216, 2018, Pages 207 - 220. DOI: 10.1007/978-3-319-73697-6_16.

[8] Huang Y., Jin L., Wei H., Lou Y., Kang X. Pilot Contamination with MITM Attack. Proceedings of the 5th IEEE Vehicular Technology Conference, VTC Spring 2017. Sydney, Australia. DOI:10.1109/VTCSpring.2017.8108523.

[9] Ouseph C., Chandavarkar, B.R. Prevention of MITM attack caused by rogue router advertisements in IPv6. Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, Pages 952-956. DOI: 10.1109/RTEICT.2016.7807969.

[10] Al Abri D. Detection of MITM attack in LAN environment using payload matching. Proceedings of the 2015 IEEE International Conference on Industrial Technology, ICIT 2015. Seville; Spain. Pages 1857-1862. DOI: 10.1109/ICIT.2015.7125367.

[11] Bucket Brigade. SearchSecurity. No Author Available at: http://searchsecurity.techtarget.com/tip/Bucket-Brigade (accessed: 03.05.2018).

[12] Study And Analysis On Session Hijacking Computer Science Essay. UK Essays. Available at: https://www.ukessays.com/essays/computer-science/study-and-analysis-on-session-hijacking-computer-science-essay.php?utm_expid=309629-38._Nb6m1ixT_aGX1K3CVQTDw.0 (accessed: 03.05.2018).

[13] RFC 793, Transmission Control Protocol. Available at: https://tools.ietf.org/html/rfc793 (accessed: 03.05.2018).

[14] Wegener C., Dolle W. Hijack Prevention – Understanding and preventing TCP attacks. Linux-Magazine, 09/2005; pages 66-71; ISSN 14715678.

[15] Basta A., Basta N., Brown M. Computer Security and Penetration Testing. Cengage Learning. 2013. 400 p.

Поступила в редакцию – 06 мая 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – May 06, 2018. The final version – November 01, 2018.

Елена С. Басан, Александр С. Басан, Олег Б. Макаревич
Южный федеральный университет «ЮФУ»,
Институт компьютерных технологий и информационной безопасности,
ул. Чехова, 2, г. Таганрог, 347922, Россия
e-mail: ebasan@sfedu.ru, http://orcid.org/0000-0001-6127-4484
e-mail: asbasan@sfedu.ru, http://orcid.org/0000-0002-2973-2737
e-mail: obmakarevich@sfedu.ru, http://orcid.org/0000-0003-0066-8564

РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ УЗЛОВ В ГРУППЕ РОБОТОВ*

DOI: http://dx.doi.org/10.26583/bit.2018.4.07

Аннотация. Данная статья посвящена вопросам обеспечения безопасности в группе мобильных роботов при реализации злоумышленником атак, направленных на свойство доступности информации. Проанализированы основные методы и подходы к обнаружению атак и аномалий для мобильных роботов, выделены основные достоинства и недостатки существующих подходов. Основной целью является разработка метода обнаружения аномального поведения, который позволил бы избежать создания эталонного распределения, либо базы сигнатур, либо правил для группы мобильных роботов. Метод должен в текущих условиях при динамически изменяющейся структуре сети выявлять аномалии. В статье представлен метод обнаружения аномального поведения узла сети на основе анализа параметров: остаточной энергии и сетевой загруженности узлов сети. Проводится анализ поведения отдельных роботов группы относительно отклонения от общего поведения с использованием вероятностных методов. Разрабатываемый метод обнаружения аномального поведения основан на использовании вероятностной оценки событий. Определяются три типа состояний узлов сети, построен граф переходов узла в каждое из состояний, а также определены параметры, влияющие на данные переходы. Разработанный метод демонстрирует высокий показатель обнаружения атаки «отказ в обслуживании» распределенной атаки «отказ в обслуживании» при количестве злоумышленных узлов, не превышающем или незначительно превышающем количество доверенных узлов. А также обеспечивает обнаружение атаки Сивиллы. Проведено экспериментальное исследование, включающее в себя разработку модели, имитирующей группу мобильных роботов, в частности сетевое взаимодействие между роботами. Разработаны, реализованы сценарии атак для группы мобильных роботов, позволяющие оценить эффективность разработанного метода обнаружения аномального поведения. Для определения эффективности разработанного метода использовались показатели: время обнаружения атакующих узлов; количество узлов злоумышленника, которое позволяет обнаружить разработанный метод.

Ключевые слова: мобильные роботы, аномальное поведение, вероятностные методы, групповое управление, атака, обнаружение.

Для цитирования: БАСАН, Елена С.; БАСАН, Александр С.; МАКАРЕВИЧ, Олег Б. РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ УЗЛОВ В ГРУППЕ РОБОТОВ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 75-85, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1163>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.07.

***Благодарности.** Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (Инициативные научные проекты № 2.6244.2017/8.9).

Elena S. Basan, Alexander S. Basan, Oleg B. Makarevich
Southern Federal University "SFedU", Institute of Computer Technologies and Information Security,
str. Chekhov, 2, Taganrog, 347922, Russia
e-mail: ebasan@sfedu.ru, http://orcid.org/0000-0001-6127-4484
e-mail: asbasan@sfedu.ru, http://orcid.org/0000-0002-2973-2737
e-mail: obmakarevich@sfedu.ru, http://orcid.org/0000-0003-0066-8564

Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots*

DOI: http://dx.doi.org/10.26583/bit.2018.4.07

Abstract. The present paper examines the issues of security in a group of mobile robots in the implementation of malicious attacks aimed at the availability of information. The main methods and approaches for detecting attacks and mobile robots anomalies were analyzed. The major advantages and disadvantages of existing approaches were identified. The aim is to develop an attack detection method that allows avoiding a creation of either a reference distribution, or a signature database, or rules for a group of mobile robots. The method should detect anomalies within the current conditions with a dynamically changing network structure. The paper presents a method for detecting abnormal behavior of a network node based on analysis of parameters: the residual energy and network load. The behavior of individual robots of the group is analyzed with respect to the deviation from the general behavior using probabilistic methods, which avoids creating a reference distribution for describing the behavior of the node, as well as the creating of a signature database for detecting anomalies. The developed method of detecting abnormal behavior based on the probabilistic evaluation of events. Three types of a network node state were defined, a graph of node transitions to each state was constructed, and parameters that affect these transitions were determined. The developed method demonstrates a high detection rate of denial of service attacks and distributed denial of service attacks when the number of malicious nodes is not greater than or slightly greater than the amount trusted nodes. It also provides detection of the Sybil attack. An experimental study was carried out. It includes the development of a model to simulate a group of mobile robots, in particular a robot network. Scenarios of attacks were developed, implemented for a group of mobile robots. It allows evaluating the effectiveness of this method of anomalous behavior detection. To determine the effectiveness of the developed method, the following indicators were used: time of detection of attackers and the number of nodes of the attacker that can be detected.
Keywords: mobile robots, abnormal behavior, probabilistic methods, group control, attack, detection.
For citation: BASAN, Elena S.; BASAN, Alexander S.; MAKAREVICH, Oleg B. Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots. IT Security (Russia), [S.l.], v. 25, n. 4, p. 75-85, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1163>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.07.

***Acknowledgement.** The work was supported by the Ministry of Education and Science of the Russian Federation (Initiative Science Projects No. 2.6244.2017 / 8.9).

Введение

Сети мобильных роботов являются достаточно уязвимыми к атакам злоумышленника. В статье [1] была представлена модель угроз для сети мобильных роботов. Также авторами был проведен анализ атак для группы мобильных роботов. На основании проведенного анализа было выявлено, что основной набор атак, которые злоумышленник может реализовать для группы мобильных роботов, представляет собой: «отказ в обслуживании» (DoS) [2], распределенная атака «отказ в обслуживании» (DDoS) [3], человек посередине (MITM) и атака Сивиллы, а также исчерпание ресурсов [4]. Обнаружение этих атак с минимальной затратой ресурсов мобильных роботов является основной задачей данного исследования [5].

Обнаружение аномального поведения для группы мобильных роботов возможно при контроле и анализе изменения параметров узла сети. При активной атаке злоумышленник может влиять на какой-либо физический параметр мобильного робота путем сетевого или физического воздействия [6]. Данное исследование ограничено спектром атак, которые направлены на свойство доступности информации или узла сети.

Рассмотрим некоторые работы авторов, посвященные проблеме обнаружения аномального поведения для одиночных мобильных роботов или групп роботов с централизованным управлением.

В статье [7] авторами рассмотрена система обнаружения атак на основе дерева принятия решений, с использованием алгоритма C5.0 для группы роботизированных автомобилей. Достоинством представленного подхода является то, что для обнаружения кибератак авторы наряду с четырьмя признаками для анализа процесса коммуникации и обработки информации, которые называют киберфункциями ввода, используют четыре параметра для анализа физических свойств робота, которые авторы называют физическими характеристиками входного сигнала. Далее авторы проводят 5 типов деструктивного воздействия на робота и получают набор правил для построения дерева принятия решений. Недостатком подхода является то, что в данной работе рассмотрены атаки только на одного робота, а не на сеть роботов. Кроме того, в подобных системах имеется необходимость постоянного добавления правил для обнаружения новых атак.

В работе авторов [8] рассмотрена система обнаружения вторжений на основе сигнатурного анализа. Авторами проведен ряд экспериментов для создания эталонного шаблона, описывающего нормальное поведение робота при отсутствии внешнего воздействия, а также случайных аномалий поведения. Затем был промоделирован ряд ситуаций, при которых имело место аномальное поведение, вызванное условиями окружающей среды. На основании собранных данных строился шаблон нормального поведения робота с учетом весовых коэффициентов, рассчитанных на основании частоты возникновения того или иного типа аномального поведения. Авторами проведен ряд атак, которые влияют на определённый набор физических параметров узла. Данный подход демонстрирует большую эффективность при обнаружении злоумышленного узла, чем простой сигнатурный анализ, тем не менее имеются некоторые недостатки: например, необходимость постоянного обновления и пополнения базы данных сигнатур для контроля данных с неучтённых датчиков мобильного робота.

В статье [9] рассматривается система обнаружения атак на беспилотные летательные аппараты. При разработке данной системы использовался подход на основе создания базы данных сигнатур. Система работает следующим образом. Каждый узел сети имеет узел-монитор, которым может являться соседний беспилотный аппарат, фиксирующий поведение доверенного узла и записывающий его в матрицу. Узел-монитор постоянно наблюдает за поведением подопечного узла и выставляет ему оценки. Данные оценки зависят от того насколько поведение подопечного узла отклоняется от нормального шаблона поведения. Затем создается база данных правил и оценивается поведение узла. При этом оценка производится по 7 параметрам. К недостатку системы можно отнести необходимость постоянного контроля узлов друг за другом и анализа их поведения, что задействует вычислительную нагрузку и пропускную способность сети.

Таким образом, в результате рассмотрения работ, посвященных тематике обнаружения атак на мобильных роботов, можно выделить три основных недостатка существующих подходов:

1. Большинство систем основано на сигнатурном анализе либо на системе правил. В связи с этим имеются следующие ограничения: сложность обнаружения новых атак, не связанных с фиксируемыми шаблонами поведения злоумышленника, а также необходимость поддержания в актуальном состоянии базы правил или наборов сигнатур.

2. Системы, основанные на полностью распределенных методах обнаружения, требуют от узлов дополнительных затрат энергии, затрат вычислительной мощности и увеличивают пропускную способность.

3. При использовании централизованных методов узел, выполняющий основные функции по обнаружению аномального поведения является наиболее уязвимым местом системы. При выведении его из строя нарушается работа сети полностью [10].

В данной статье предлагается разработка метода обнаружения аномального поведения злоумышленника или нескольких злоумышленников в рамках группы мобильных роботов на основе вероятностных методов [11]. При этом основное отличие данного метода состоит в том, что он не требует построения эталонного вероятностного распределения, как другие вероятностные методы. Отсутствие необходимости построения эталонного распределения обусловлено тем, что для выявления аномального поведения берутся текущие показания узлов группы, далее строится функ-

ция нормального распределения и вычисляется доверительный интервал значений. Таким образом, появляется возможность оценивать вероятность отклонения поведения узла от общего поведения узлов группы.

Разработка и реализация метода обнаружения аномального поведения

В данной работе предлагается метод, разработанный для группы мобильных роботов. Особенность разработки метода для группы мобильных роботов заключается в том, что для формирования функции нормального распределения необходимо получение данных от нескольких узлов, выполняющих схожие функции. Для более точного определения степени отклонения текущих показаний узла от группы узлов необходимо, чтобы показатели группы узлов находились в одном диапазоне. В таблице 1 представлены параметры, по изменению которых можно судить о наличие аномальной активности в сети.

Таблица 1. Соотношение параметров сети и влияющих на них атак

Параметры сети	Атака злоумышленника
Пакеты с данными	Блокировка узла, блокировка узла с наличием условий, переадресация, отказ в обслуживании, задержка пакетов
Заряд батареи	Отказ в обслуживании, истощение ресурсов
Загруженность	Отказ в обслуживании, истощение ресурсов, атака Сивиллы, Flood-атаки, тунелирование

Под параметром «пакеты с данными» понимается факт передачи или перенаправления пакета, то есть оценивается доступность передаваемой информации. Если на сеть оказывается какое-либо воздействие со стороны злоумышленника, то могут возникать ситуации, когда пакеты отбрасываются, дублируются и т.п.

Под параметром «заряд батареи» может пониматься следующее: текущее потребление заряда аккумулятора (или потребляемая мощность), а также оставшийся в аккумуляторной батарее запас энергии, позволяющий устройству функционировать в сети.

Под параметром «загруженность» понимается общее количество пакетов, передаваемых в сети. Либо количество пакетов, передаваемых через один из узлов сети.

В случае реализации злоумышленником атаки «отказ в обслуживании» изменяется уровень трафика, передаваемый злоумышленным узлом сети, и уровень трафика, принимаемый жертвами атаки. Следовательно, целесообразным является оценивание изменений показателя «загруженность», который представляет собой общее количество принимаемых, отправляемых, перенаправляемых пакетов узла сети. При реализации атаки Сивиллы или атаки перенаправления влияния на себя, основной целью злоумышленника является изменение процессов и путей обмена данными в сети. Другими словами, злоумышленник добивается такой ситуации, что весь или большая часть трафика соседних узлов проходит через него.

В предыдущей работе авторов [12] помимо параметров «загруженность» и «остаточная энергия» рассматривался параметр «количество отброшенных пакетов» (P1). В данном исследовании он рассматриваться не будет, так как существенно не влияет на обнаружение перечисленных выше атак. Таким образом, рассмотрим два параметра: загруженность (P2) и остаточная энергия (P3). Изменение данных параметров влияет на состояние как узлов сети так и всей группы роботов в целом. Состояние узлов сети можно описать следующим образом: S1 – состояние, когда узел не подвержен атаке и сам не проводит атаку, т.е. является подлинным на текущий момент времени; S2 – состояние, когда поведение мобильного робота отклонилось от поведения большей части группы роботов, может наблюдаться при условии, что узел стал жертвой атаки, т.е. узел является неопределенным; S3 – когда поведение мобильного робота значительно отличается от узлов группы, т.е. вероятнее всего

узел является злоумышленным. На рис. 1 представлен граф переходов из одного состояния в другое, а также отражено влияние параметров и атрибутов друг на друга.

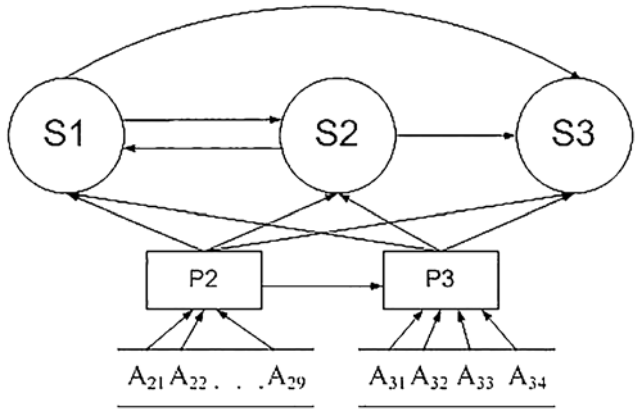


Рис. 1. Граф состояний узлов группы мобильных роботов, используемый при выявлении аномального поведения
(Fig. 1. The graph states of nodes a group of mobile robots, used for detecting anomalous behavior)

На параметр *P2 = L* оказывают влияние следующие атрибуты узла: A_{21} – общее количество отправленных узлом пакетов, содержащих данные. A_{22} – общее количество пакетов управления, или beacon - пакетов, предназначенных для проверки соединения. A_{23} – общее количество пакетов, отправленных по протоколу маршрутизации. A_{24} – общее количество принятых пакетов данными. A_{25} – общее количество принятых управляющих пакетов. A_{26} – общее количество принятых пакетов маршрутизации. A_{27} – общее количество отброшенных пакетов с данными. A_{28} – общее количество отброшенных управляющих пакетов. A_{29} – общее количество отброшенных пакетов маршрутизации.

Таким образом, параметр *L* может быть представлен следующим выражением:

$$L=A_{21}+A_{22}+A_{23}+A_{24}+A_{25}+A_{26}+A_{27}+A_{28}+A_{29} \quad (1)$$

Параметр *P3=e* можно характеризовать конечным множеством атрибутов $A_{3j.}$ Представленные ниже атрибуты влияют на количество остаточной энергии узла, но кроме описанных ниже атрибутов на количество остаточной энергии влияет уровень загруженности узла, т.е. параметр *P2*: A_{31} – начальный запас энергии узла сети. A_{31}=*initialEnergy*; A_{32} – мощность передаваемого сигнала. A_{32}=*rxPower*; A_{33} – мощность приема сигнала, A_{33}=*txPower*; A_{34} – скорость перемещения узла. A_{34}=*speed*.

Остаточная энергия вычисляется путем уменьшения уровня начальной энергии A_{31} для каждого переданного и каждого полученного пакета в единицу времени:

$$e_{tx}=A_{31}-(A_{31}*txTime), e_{rx}=A_{31}-(A_{32}*rcvTime), \quad (2)$$

где e_{tx} и e_{rx} - уровень остаточной энергии после приема пакета и после передачи первого пакета; *rcvTime* - время передачи пакета; *txTime* - время приема пакета.

Процедура вычисления доверия работает по следующему алгоритму.

1. Расчет доверительных интервалов загруженности узлов, загруженности на временном интервале и энергии [13].

1.1. Вычисление дисперсии и среднеквадратического отклонения:

$$D_{Li}=\left(\sum_{i}^{N}(L_i-\overline{L})^2\right)/n,\ D_{ei}=\left(\sum_{i}^{N}(e_i-\overline{e})^2\right)/n, \quad (3)$$

где D_{Li}, D_{ei} - дисперсия параметров *L* и *e* группы узлов в текущий интервал времени.

Вычисление среднеквадратического отклонения:

$$\sigma_{ei} = \sqrt{D}_{ei},\ \sigma_{Li} = \sqrt{D}_{Li}, \tag{4}$$

σ_{ei}, σ_{Li} - среднеквадратическое отклонение параметров *L* и *e* группы узлов в текущий интервал времени.

1.2. Вычисление верхних и нижних границ доверительных интервалов.

Верхняя граница доверительного интервала параметра *e* всегда равна максимально допустимому значению энергии, то есть a_{max} = *initialEnergy*. Это связано с тем, что узлы могут мигрировать из одной группы в другую, могут появляться новые узлы со значением остаточной энергии, равной начальному значению.

Вычисление нижней границы доверительного интервала производится только для значения остаточной энергии. Так как нижняя граница показателя *L* узла равна минимально необходимому количеству пакетов, прошедших через узел за один интервал времени L_{min}. Данные меры приняты по той причине, что мобильный робот может проявлять эгоистичное поведение, то есть отказаться принимать участие в работе сети для сбережения энергии, что может искусственно «занизить» границы интервала.

Далее представлены формулы для вычисления границ доверительного интервала.

$$a_{\min} = \bar{e} - t \cdot \sigma_e / \sqrt{n},\ a_{max} = A_{31},\ a_{max} = A_{31},\ a_{min} < a_{max}, \tag{5}$$

$$b_{min} = L_{min},\ b_{min} = L_{min},\ b_{max} = \overline{L} + t \cdot \sigma_L / \sqrt{n}, \tag{6}$$

где t*σ/√n - точность оценки; *t* – аргумент функции Лапласа, где $\Phi(t) = \frac{\alpha}{2}$ - функция Лапласа; α – заданная надежность, в данном исследовании значение коэффициента α = 0.98, значит аргумент *t = 2.34; n* – общее количество узлов.

2. Выполнение подпунктов 2.1, 2.2 для каждого узла.

2.1. Определение вероятности аномального поведения мобильного робота на основе рассчитанных границ доверительных интервалов. Для того чтобы вычислить значение среднеквадратического отклонения и математического ожидания необходимо сократить интервал, для которого вычисляется значение, и учитывать только показатели узла в предыдущий временной интервал L_{i-1}, e_{i-1} и L_i, e_i показатели узла для текущего интервала.

$$P_e(a_{\min} < e_i < a_{\max}) = \Phi\left(\frac{a_{\max} - \overline{e_в}}{\sigma_{e_в}}\right) - \Phi\left(\frac{a_{\min} - \overline{e_в}}{\sigma_{e_в}}\right), \tag{7}$$

$$P_L(b_{\min} < L_i < b_{\max}) = \Phi\left(\frac{b_{\max} - \overline{L}_в}{\sigma_{L_в}}\right) - \Phi\left(\frac{b_{\min} - \overline{L_в}}{\sigma_{Lв}}\right), \tag{8}$$

где Ф - функция Лапласа; $P_{Q(E)}$, P_L – вероятность попадания остаточной энергии узла и уровня загруженности узла в пределы доверительного интервала.

$\overline{e_в} = (e_{i-1} + e_i)/2$; $\overline{L_в} = (L_{i-1} + L_i)/2$ – математическое ожидание величин *e* и *L* для выборочного интервала. $D_{e_в} = \left(\sum_i^N (e_i - \overline{e_в})^2\right)/n$ - дисперсия для выборочного интервала для *e*; $D_{L_в} = \left(\sum_i^N (L_i - \overline{L_в})^2\right)/n$ - дисперсия для выборочного интервала для значения загруженности узла; $\sigma_{e_в} = \sqrt{D}_{e_в}$ – среднеква-

дратическое отклонение для выборочного интервала для остаточной энергии. $\sigma_{L_в} = \sqrt{D}_{L_в}$ – среднеквадратическое отклонение для выборочного интервала L.

2.2. Вывод результатов в журнал трассировки.

3. Выполнение подпункта 3.1 для каждого узла.

3.1. Обновление следующих значений для каждого узла: загруженность на предыдущем временном интервале, остаточная энергия в предыдущий момент времени.

4. Блокирование злоумышленных узлов.

4.1. Примем пороговое значение вероятности того, что узел является аномальным, равное 0,5.

4.2. Когда узел достигает значение, равное 0,5 необходимо уменьшить уровень его остаточной энергии в два раза, тогда узел считается в неопределенном состоянии.

4.3. Далее если значение уровня доверия достигает уровня 0,4, то необходимо считать узел злоумышленным и уменьшить его уровень энергии до нуля, таким образом, узел исключается из работы сети [14].

Проведение экспериментального исследования, оценка эффективности разработанного метода

Для проведения экспериментального исследования была разработана модель группы роботов в среде моделирования NS-2.35. На рис. 2 изображена группа мобильных роботов в системе моделирования, включающая в себя 10 узлов. Из них один узел N4 является базовой станцией или центральным сервером. Узел N0 является лидером группы и выполняет функции сбора информации от роботов группы и перенаправляет ее центральному серверу. Узлы группы обмениваются информацией друг с другом и с лидером группы [15]. При этом узлы *N6, N7, N8, N9,* начиная с 50-й секунды работы сети, будут проводить DDoS атаку.

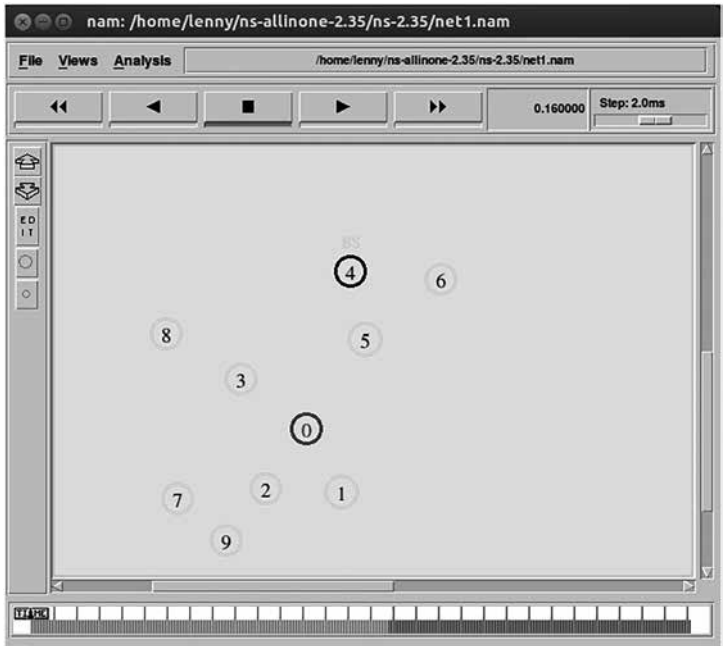


Рис. 2. Группа роботов в системе моделирования NS-2.35
(Fig. 2. Group of robots in the simulation system NS-2.35)

Реализация и обнаружение DoS атаки

Проводя атаку «отказ в обслуживании», злоумышленник создает такую ситуацию, когда узел сети становится недоступным для других узлов и не может отвечать на их запросы и работать в штатном режиме. Было проведено моделирование трех типов ситуаций. В первом случае проведена

оценка расходуемой энергии узлами сети при отсутствии атаки. На рис. 3 данная ситуация представлена графиком синего цвета, помеченным ромбами.

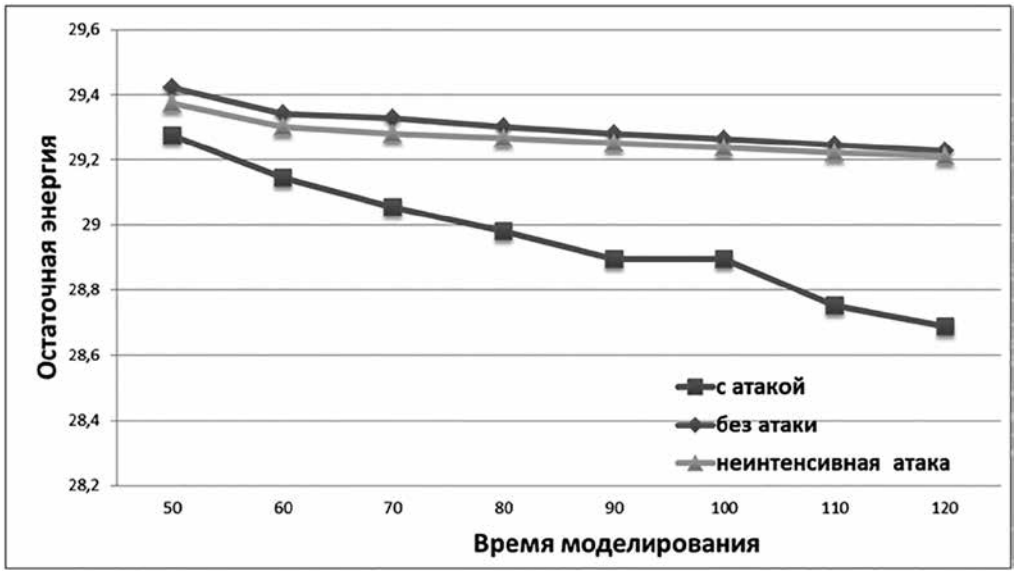
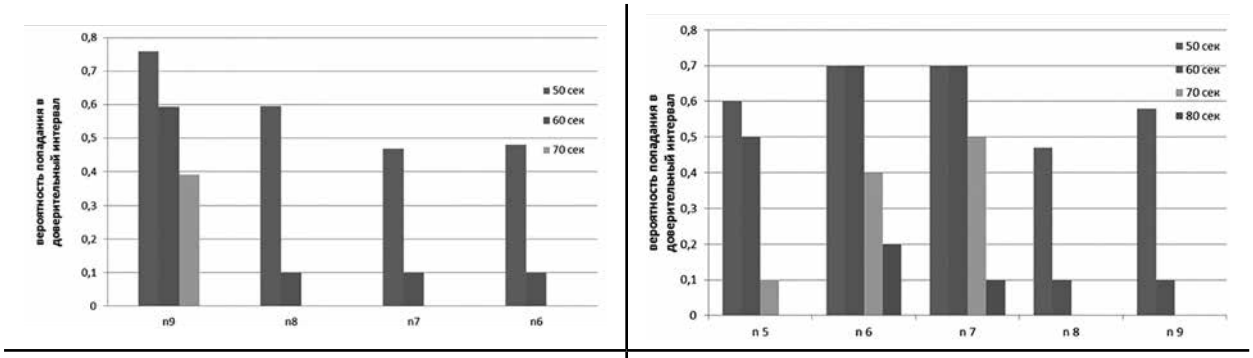


Рис. 3. Изменение уровня остаточной энергии в зависимости от интенсивности трафика узлов сети.
(Fig. 3. The residual energy level changes depending on the intensity of traffic nodes)

Во втором случае на сеть проводилась атака, при этом интенсивность трафика злоумышленного узла $I_t \le I_m \le 2I_t$, где I_m – трафик злоумышленного узла, I_t – трафик подлинного узла, т.е. низкоинтенсивная атака. Третий график представляет собой ситуацию, когда атака проводится интенсивно и $I_m > 2I_t$. Из рис. 3 видно, что во время проведения низкоинтенсивной атаки уровень энергии узлов останется практически таким же, как и для случая, когда атака не проводится. То есть в данном случае атаку можно считать не эффективной, т.к. она существенным образом не влияет на исчерпание ресурсов узла. На графике, отражающем изменение уровня энергии во время проведения интенсивной атаки, видно резкое падение уровня энергии, что подтверждает эффективность атаки. В случае, когда атака является интенсивной, разработанный метод позволяет обнаружить злоумышленника через 10 секунд.

Реализация и обнаружение DDoS атаки

Обнаружение распределенной атаки «отказ в обслуживании» является более сложной задачей [16]. Это связано с тем, что когда количество злоумышленных узлов преобладает над количеством подлинных узлов, границы доверительного интервала значительно расширяются. Когда количество злоумышленных узлов составляет 45 %, метод позволяет сразу обнаружить все злоумышленные узлы и заблокировать их уже на втором интервале времени, т.е. через 20 секунд от начала проведения атаки. На рис. 4 (а) представлена гистограмма, демонстрирующая уровень попадания текущих показателей *e* и *L* злоумышленных узлов в доверительный интервал. На рис. 4 (б) представлена гистограмма, демонстрирующая уровень обнаружения злоумышленных узлов, когда количество злоумышленных узлов составляет 50 %. Узлы N_9 и N_8 выявлены на втором интервале, узлы N_5 и N_6 обнаружены на третьем интервале и узел N_7 на четвертом интервале времени начиная с того момента, когда началась атака. При этом в первом случае необходимо 30 секунд для обнаружения злоумышленника, а во втором 40 секунд. Когда количество злоумышленных узлов составляет 60 %, то злоумышленные узлы полностью обнаруживаются через 60 секунд.



(а) *(б)*

Рис. 4. Уровень обнаружения узлов при распределенной атаке «отказ в обслуживании» для (а) 40 % злоумышленных узлов (б) для 50 % злоумышленных узлов и пяти подлинных узлов сети
(Fig. 4. Nodes detection level for distributed denial of service attack for (a) 40 % malicious nodes (b) for 50 % malicious nodes and five authentic network nodes)

Реализация и обнаружение атаки Сивиллы

Атака Сивиллы заключается в том, что злоумышленник представляется несколькими узлами (сущностями) в сети и пытается перенаправить большую часть трафика на себя [17]. В работах авторов [18], как правило, встречаются методы с применением жесткой защиты: парольной защиты, криптографической защиты, а также сигнатурного анализа и группового обнаружения. Данные методы применяются в сетях MANET, IoF, P2P [19]. Разработанный метод обнаружения аномального поведения показывает эффективность обнаружения атаки Сивиллы даже при условии, что злоумышленник перенаправил трафик на себя и больше не предпринимает никаких действий [20]. В данном случае обнаружение возможно за счет изменения уровня загруженности узлов, которые проводят атаку на соседние узлы. Метод позволяет выявить 100 % злоумышленных узлов, когда их количество в сети составляет 45 %. При этом для обнаружения всех узлов злоумышленника необходимо 60 секунд.

Заключение

Вопросы, связанные с обеспечением безопасности мобильных роботов, достаточно актуальны в связи с широким распространением самих робототехнических систем. Разработанный метод позволяет выявлять аномальное поведение в группе узлов, когда имеется возможность проводить анализ поведения большинства узлов и выявлять единичные или массовые отклонения от общего поведения. Имеется возможность наращивания количества анализируемых параметров для расширения спектра атак. Метод позволяет обнаруживать все злоумышленные узлы в пределах 30 – 60 секунд. Ограничения метода заключаются в количестве злоумышленных узлов, которые проводят атаку на сеть, их количество не должно превышать 60 % по сравнению с количеством доверенных.

В отличие от существующих методов обнаружения аномального поведения, где приходится составлять базы данных сигнатур или банки данных правил, хранить их, а затем обновлять, разработанный метод позволяет выявлять аномалии в текущий момент времени и в зависимости от текущей ситуации. Данное достоинство является достаточно важным, так как мобильные роботы могут быть использованы в разных средах и для выполнения различных задач, при этом помимо протоколов сетевого взаимодействия между мобильными роботами могут меняться и условия среды. Данный метод учитывает пороговые значения, то есть допустимый уровень аномалий, что уменьшает количество ложных срабатываний.

СПИСОК ЛИТЕРАТУРЫ:

1. Басан А.С., Басан Е.С. Модель угроз для систем группового управления мобильными роботами // Системный синтез и прикладная синергетика. Сборник научных трудов VIII Всероссийской научной кон-

ференции. Ростов-на-Дону: Южный федеральный университет. 2017. С. 205 – 212. URL: https://elibrary.ru/item.asp?id=29989970
2. H.S. Kim, S.W. Lee. Enhanced novel access control protocol over wireless sensor networks // IEEE Transactions on Consumer Electronics. 2009. № 55 (2). pp. 492 - 498. DOI: 10.1109/TCE.2009.5174412
3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Информационная безопасность. Труды СПИИРАН. 2016. № 2(45). С. 207 – 244. URL: http://proceedings.spiiras.nw.ru/ojs/index.php/sp/article/view/3267/1883
4. Petrovsky O. Attack on the drones // Proceedings of Virus bulletin conference. 2015. pp. 16 – 24. URL: https://www.virusbulletin.com/uploads/pdf/conference/vb2015/Petrovsky-VB2015.pdf
5. Garber L. Robot OS: A New Day for Robot Design // Computer. № 46 (12). 2013. pp. 16 – 20. DOI: 10.1109/MC.2013.434
6. Кожемякин И.В., Путинцев И.А., Семенов Н.Н., Чемоданов М.Н. Разработка подводного робототехнического комплекса, с использованием открытых средств моделирования движения, дополненных моделью гидроакустического взаимодействия // Известия ЮФУ. Технические науки. Раздел II. Морская робототехника. 2016. № 1 (174). С. 88 – 99. URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2016/1/7.pdf
7. Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles // Proceedings of 2015 IEEE International Workshop on Information Forensics and Security (WIFS). 2015. pp. 1 - 6. DOI: 10.1109/WIFS.2015.7368559.
8. Bezemskij A., Loukas G., Richard J. Gan D. Behavior-based anomaly detection of cyber-physical attacks on a robotic vehicle // Proceedings of 15th International Conference on Ubiquitous Computing and Communications and 2016. 8th International Symposium on Cyberspace and Security. 2016. pp. 61 - 68. DOI: 10.1109/IUCC-CSS.2016.017.
9. Mitchell R., Chen I.R. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications // IEEE Transactions on Systems, Man, and Cybernetics: Systems. №44 (5). 2014. pp. 593 - 599. DOI: 10.1109/TSMC.2013.2265083.
10. Monshizadeh M., Khatri V., Kantola R., Yan Z. An Orchestrated Security Platform for Internet of Robots // Proceedings of Springer International International Conference on Green, Pervasive, and Cloud Computing. 2017. pp. 298 – 312. https://doi.org/10.1007/978-3-319-57186-7_59
11. Басан А.С., Басан Е.С., Макаревич О.Б. Метод противодействия активным атакам злоумышленника в беспроводных сенсорных сетях // Известия ЮФУ. Технические науки. №5 (190).2017. С 16 – 25. DOI 10.23683/2311-3103-2017-5-16-25
12. Basan A., Basan E., Makarevich O. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust // Proceedings of 8th International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). Chengdu, China. 2016. pp.409 – 412. DOI: 10.1109/CyberC.2016.85
13. He W., Yang S., Teng D., Hu Y. A Link Level Load-Aware Queue Scheduling algorithm on MAC layer for wireless mesh networks // Proceedings of International Conference on Wireless Communications & Signal Processing.2009. Nanjing, China. pp. 1 – 16.
14. Basan A.S., Basan E.S., Makarevich O.B. Development of the Hierarchal Trust management System for Mobile Cluster–based Wireless Sensor Network // Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. 2016. pp. 116 – 122.
15. Абрамов Е.С., Басан Е.С. Разработка модели защищенной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. 2013. № 12(149). С. 48 – 56.
16. Пшихопов В.Х., Соловьев В.В., Титов А.Е., Финаев В.И., Шаповалов И.О. Групповое управление подвижными объектами в неопределенных средах // Под ред. В.Х. Пшихопова. М.: ФИЗМАТЛИТ. 2015. – С. 233 – 270.
17. Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. pp. 122 – 128.
18. Abbas S., Merabti M., D. Llewellyn-Jones, K. Kifayat. Lightweight Sybil Attack Detection in MANETs // IEEE system journal, №. 7, (2). 2013. pp 236 – 248.
19. Patel S.T., Mistry N.H. A review: Sybil attack detection techniques in WSN // Proceedings of 4th International Conference on Electronics and Communication Systems (ICECS). 2017. pp. 184 – 188.
20. Wang G., Musau F., Guo S., Abdullahi M. B. Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce // IEEE transactions on parallel and distributed systems. № 26 (3). 2015. pp. 824 – 833.

REFERENCES:

[1] Basan A.S., Basan E.S. [Threat model for mobile robot group management systems]. System synthesis and applied synergetics. Collection of proceedings of the VIII All-Russian Scientific Conference. - Sistemnyy sintez i prikladnaya sinergetika. Sbornik nauchnykh trudov VIII Vserossiyskoy nauchnoy konferentsii. Rostov-on-Don: Southern Federal University. 2017. C. 205 – 212. (in Russian).

[2] H.S. Kim, S.W. Lee. Enhanced novel access control protocol over wireless sensor networks]. IEEE Transactions on Consumer Electronics. 2009. № 55 (2). pp. 492 – 498.

[3] Branitsky A.A., Kotenko I.V. [Analysis and classification of methods for detecting network attacks] Information security. Proceedings of SPIIRAN - Informatsionnaya bezopasnost'. Trudy SPIIRAN.2016. №2(45). pp. 207 – 244. (in Russian).

[4] Petrovsky O. Attack on the drones. Virus bulletin conference. 2015. pp. 16 – 24.

[5] Garber L. Robot OS: A New Day for Robot Design. Computer. № 46 (12). 2013. pp. 16 – 20.

[6] Kozhemyakin I.V., Putintsev I.A., Semenov N.N., Chemodanov M.N. [Development of an underwater robotic complex, using open simulation tools, supplemented with a model of hydroacoustic interaction]. News of SFedU. Technical science. Section II. Marine robotics. - Izvestiya YUFU. Tekhnicheskiye nauki. Razdel II. Morskaya robototekhnika. 2016. № 1 (174). pp. 88 – 99. (in Russian).

[7] Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. 2015 IEEE International Workshop on Information Forensics and Security (WIFS) 2015. pp. 1 – 6.

[8] Bezemskij A., Loukas G., Richard J. Gan D. Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. 15th International Conference on Ubiquitous Computing and Communications and 2016 8th International Symposium on Cyberspace and Security. 2016. pp. 61 – 68.

[9] Mitchell R., Chen I.R. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications. IEEE Transactions on Systems, Man, and Cybernetics: Systems. №44 (5). 2014. pp. 593 – 599.

[10] Monshizadeh M., Khatri V., Kantola R., Yan Z. An Orchestrated Security Platform for Internet of Robots. Springer International International Conference on Green, Pervasive, and Cloud Computing. 2017. pp. 298 – 312.

[11] Basan A.S., Basan E.S., Makarevich O.B. [Method of counteracting active attacks of an attacker in wireless sensor networks]. Известия ЮФУ. Технические науки. №5 (190).2017. pp. 16 – 25. (in Russian).

[12] Basan A., Basan E., Makarevich O. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. 8th International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).Chengdu. 2016. pp. 409 – 412.

[13] He W., Yang S., Teng D., Hu Y. A Link Level Load-Aware Queue Scheduling algorithm on MAC layer for wireless mesh networks // Proceedings of International Conference on Wireless Communications & Signal Processing.2009. Nanjing, China. pp. 1 – 16.

[14] Basan A.S., Basan E.S., Makarevich O.B. Development of the Hierarchal Trust management System for Mobile Cluster–based Wireless Sensor Network // Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. 2016. pp. 116 – 122.

[15] Abramov E.S., Basan E.S. Development of a model of a secure cluster wireless sensor network. Izvestia SFU. Technical science. 2013. No. 12 (149). pp. 48 – 56. (in Russian).

[16] Pshikhopov V.Kh., Soloviev V.V., Titov A.E., Finaev V.I., Shapovalov I.O. [Group management of mobile objects in uncertain environments]. Ed. V.H. Pshihopova. M.: FIZMATLIT. - Pod red. V.KH. Pshikhopova. M.: FIZMATLIюT 2015. – pp. 233 – 270. (in Russian.).

[17] Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. pp. 122 – 128.

[18] Abbas S., Merabti M., D. Llewellyn-Jones, K. Kifayat. Lightweight Sybil Attack Detection in MANETs // IEEE system journal, №. 7, (2). 2013. pp 236 – 248.

[19] Patel S.T., Mistry N.H. A review: Sybil attack detection techniques in WSN // Proceedings of 4th International Conference on Electronics and Communication Systems (ICECS). 2017. pp. 184 – 188.

[20] Wang G., Musau F., Guo S., Abdullahi M. B. Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce // IEEE transactions on parallel and distributed systems. № 26 (3). 2015. pp. 824 – 833.

Поступила в редакцию – 01 октября 2019 г. Окончательный вариант – 01 ноября 2018 г.
Received – October 01, 2018. The final version – November 01, 2018.

Алексей С. Гераськин, София Ю. Стрельникова, Максим П. Завенягин
Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского
ул. Астраханская, 83, г. Саратов, 410012, Россия
e-mail: gerascinas@mail.ru, http://orcid.org/0000-0002-3118-1022
e-mail: sofia_strelnikova@mail.ru, http://orcid.org/0000-0001-7200-0577
e-mail: maximzombi@yandex.ru, http://orcid.org/0000-0002-8749-487X

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ УЛУЧШЕНИЯ РЕАЛИЗАЦИИ АЛГОРИТМА МЕТОДА КОЧА ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ИЗОБРАЖЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2018.4.08

Аннотация. В современном информационном обществе проблема контроля использования прав собственности на цифровые информационные ресурсы становится все более актуальной. Одним из наиболее эффективных способов решения этой проблемы является использование цифровых водяных знаков – цифровых меток, не видимых без специального программного обеспечения и секретного ключа. Цифровой водяной знак – технология, созданная для защиты авторских прав на мультимедийные файлы. Это может быть текст или логотип, однозначно идентифицирующий автора файла. Цифровые водяные знаки применяются в кодировании и декодировании акустической информации, в технологиях поиска и определения незаконных копий аудиоматериалов. В данной работе проводилось исследование алгоритмов встраивания цифровых водяных знаков именно в изображения. На практике чаще остальных для встраивания цифровых водяных знаков в изображения используют алгоритмы, основанные на дискретном косинусном преобразовании. В статье приводится исследование, которое позволяет заключить, что метод Кочa (Koch) является наиболее эффективным для защиты авторских прав путем внедрения цифрового водяного знака в изображение. Проводится анализ недостатков метода. Вследствие двукратного применения дискретного косинусного преобразования к изображению при внедрении и извлечении цифрового водяного знака, а также применения обратного дискретного косинусного преобразования для возврата к целочисленным матрицам пикселей после внедрения соотношение коэффициентов частотной матрицы может нарушиться, а это недопустимо, так как от этого напрямую зависит результат работы алгоритма. Во избежание возникновения данной проблемы во время встраивания бита цифрового водяного знака предлагается проводить корректировку значений коэффициентов частотной матрицы. Приводится алгоритм реализации метода Кочa и обосновывается его модернизация для встраивания цифровых водяных знаков. Описывается способ и алгоритм обратного преобразования. Приводятся результаты исследования на предмет зависимости значения коэффициента силы встраивания от яркости изображения-контейнера и размера встраиваемого цифрового водяного знака.

Ключевые слова: цифровой водяной знак, дискретное косинусное преобразование, метод Кочa.
Для цитирования: ГЕРАСЬКИН, Алексей С.; СТРЕЛЬНИКОВА, София Ю.; ЗАВЕНЯГИН, Максим П. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ УЛУЧШЕНИЯ РЕАЛИЗАЦИИ АЛГОРИТМА МЕТОДА КОЧА ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ИЗОБРАЖЕНИЯ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 86-94, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1166>. Дата доступа: 22 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.08.

Aleksey S. Geraskin, Sofiia Yu. Strelnikova, Maxim P. Zavenyagin
Saratov National Research State University named after N.G. Chernyshevsky
ul. Astrahanskaja, 83, g. Saratov, 410012, Russia
e-mail: gerascinas@mail.ru, http://orcid.org/0000-0002-3118-1022
e-mail: sofia_strelnikova@mail.ru, http://orcid.org/0000-0001-7200-0577
e-mail: maximzombi@yandex.ru, http://orcid.org/0000-0002-8749-487X

Research of possibility of improvement of realization of algorithm of method of koch for embedding of digital watermarks in images

DOI: http://dx.doi.org/10.26583/bit.2018.4.08

Abstract. In a modern information society the problem of the control of use of the property rights to digital information resources becomes more and more actual. One of the most effective ways of the decision of this problem is use of digital watermarks - digital labels, not visible without the special software and a confidential key. A digital watermark - the technology created for protection of copyrights to multimedia files. It can be the text or a logo unequivocally identifying the author of a file. Digital watermarks are applied in coding and decoding of the acoustic information, in technologies of search and definition of illegal copies of audio materials. In the given work research of algorithms of embedding of digital watermarks in images was conducted. In practice more often the others for embedding of digital watermarks in images are used by the algorithms based on discrete cosine transformation. In article research which allows to conclude is resulted that the method of Koch is the most effective for protection of copyrights by introduction digital watermarks in the image. The analysis of lacks of a method is carried out. Owing to double application discrete cosine transformation to the image at introduction and extraction digital watermarks, and also applications of the return discrete cosine transformation for return to integer matrixes of pixels after introduction the parity of factors of a frequency matrix can be broken, and it is inadmissible, as the result of work of algorithm directly depends on it. Avoid occurrence of the given problem during embedding of bit digital watermarks it is offered to spend correction of values of factors of a frequency matrix. The algorithm of realization of a method of Koch is resulted and its modernization for embedding of digital watermarks is proved. The way and algorithm of return transformation is described. Results of research about dependence of value of factor of force of embedding ε from brightness of the image-container and built in digital watermark are resulted the size.

Keywords: digital watermark, discrete cosine transformation, a method of Koch.

For citation: GERASKIN, Aleksey S.; STRELNIKOVA, Sofiia Yu.; ZAVENYAGIN, Maxim P. Research of possibility of improvement of realization of algorithm of method of koch for embedding of digital watermarks in images. IT Security (Russia), [S.l.], v. 25, n. 4, p. 86-94, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1166>. Date accessed: 22 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.08.

Введение

В современном информационном обществе проблема контроля использования прав собственности на цифровые ресурсы становится все более актуальной, поскольку использование цифровых форматов мультимедиа стало повсеместным. Одним из наиболее эффективных способов решения этой проблемы является использование методов стеганографии, т.е. встраивания в мультимедийные данные так называемых цифровых водяных знаков (ЦВЗ) – цифровых меток, не видимых без специального программного обеспечения и секретного ключа. Цифровой водяной знак – технология, созданная для защиты авторских прав на мультимедийные файлы. Это может быть текст или логотип, однозначно идентифицирующий автора файла [1].

ЦВЗ применяется в кодировании, декодировании акустической информации, в уникализации и индивидуализации звуковых треков, в технологиях поиска и определения незаконных копий аудиоматериалов. В данной работе проводилось исследование алгоритмов встраивания цифровых водяных знаков в изображения. На практике чаще остальных используются алгоритмы встраивания ЦВЗ в изображения, основанные на тех же видах преобразований, что и алгоритмы сжатия.

Существует множество различных методов встраивания ЦВЗ в изображение, таких как:

- метод замены наименее значащего бита (LSB (Last Significant Bit) [2];
- метод случайного интервала [3];
- метод псевдослучайной перестановки (выбора) [4];
- метод блочного скрытия [5];
- методы встраивания в коэффициенты дискретного косинусного преобразования (ДКП) [6].

Следует отметить, что методы встраивания ЦВЗ, которые осуществляют изменение изображения, подчиняются Гауссовому закону распределения [7, 8]. Такие преобразования обнаружить достаточно сложно, так как в изображении присутствует множество независимых источников Гауссового шума с различными амплитудами, отделение которых затрудняется с увеличением количества изменений. К данной группе относятся методы, использующие дискретное косинусное преобразование [9].

ДКП используется в алгоритмах сжатия формата JPEG, а вейвлет-преобразование в алгоритмах сжатия формата JPEG 2000, который является улучшенной версией формата JPEG. Но так как формат JPEG является более распространенным, то и алгоритмы встраивания ЦВЗ, основанные на ДКП, на практике применяются чаще [10].

Методы встраивания в коэффициенты ДКП

Встраивание данных в коэффициенты дискретного косинусного преобразования (ДКП, англ. Discrete Cosine Transform (DCT)) – одно из ортогональных преобразований. Это преобразование тесно связано с дискретным преобразованием Фурье. Дискретное косинусное преобразование применяется в алгоритмах сжатия с потерями. В результате применения ДКП к файлу, например формата JPEG, производится сокращение избыточной информации, за счет чего и происходит сжатие [11].

Белобоковой Ю.С. был проведен анализ методов встраивания, основанных на дискретном косинусном преобразовании по критериям: тип ДКП (поблочное или всего изображения), тип ЦВЗ, допустимого для внедрения (последовательность бит или бинарное изображение), схема извлечения ЦВЗ (слепая или с использованием исходного изображения), использование детектора или декодера при поиске/извлечении ЦВЗ в изображении [6].

Согласно данным, представленным в данном исследовании, можно сделать вывод о том, что метод Коча (Koch) является наиболее эффективным для защиты авторских прав путем внедрения ЦВЗ в изображение, так как он единственный сочетает в себе все следующие свойства:

- производится поблочное (8×8 пикселей) ДКП изображения, как и в алгоритмах сжатия JPEG, причем внедрение производится во все блоки, а не только в пригодные, как в алгоритме Бенхама (Benham) [12]. То есть можно внедрить ЦВЗ размером $\frac{3}{64}$ от размера изображения контейнера (в случае внедрения по биту в матрицы частот для R (red), G (green) и B (blue));
- возможность внедрения как битовой последовательности, так и бинарного изображения;
- слепая схема извлечения ЦВЗ (без исходного изображения), что делает обнаружение ЦВЗ практически невозможным;
- использование декодера при поиске ЦВЗ в изображении, то есть можно не просто сказать, что в данном изображении присутствует ЦВЗ, но и извлечь его [2].

Метод Коча (Koch)

Данный метод подразумевает встраивание бита ЦВЗ в блоки размером 8×8 пикселей. По определению ДКП для его реализации требуется два вложенных цикла. Значительно более эффективный вариант вычисления коэффициентов ДКП реализуется через перемножение матриц. Тогда для каждого блока производится дискретное косинусное преобразование по формуле:

$$DCT(i,j) = \begin{cases} \sqrt{\frac{1}{n}}, i = 0 \\ \sqrt{\frac{2}{n}} * \cos\left(\frac{(2j+1)i\pi}{2n}\right), i > 0 \end{cases}, \quad (1)$$

где *DCT*(*i,j*) – значения элементов матрицы частотных коэффициентов, (*i,j*) – количество столбцов/строк матрицы пикселей, – позиция текущего элемента матрицы пикселей [13].

Для этого пиксели каждого блока можно раскладывать на компоненты R (red – красный), G

(green – зеленый) и B (blue – синий), после чего матрица каждой из этих компонент умножается справа на транспонированную матрицу ДКП, а затем полученное значение умножается слева на матрицу ДКП. В итоге для каждого блока 8×8 пикселей исходного изображения получаются три матрицы частотных коэффициентов, в каждую из которых можно встроить один бит ЦВЗ [6].

Затем в матрице частотных коэффициентов псевдослучайно выбираются два коэффициента. Для передачи бита «0» разность абсолютных значений коэффициентов частотной матрицы должна быть больше некоторой положительной величины, а для передачи «1» меньше:

$$\begin{aligned} \left|c_b\left(j_{i,1},k_{i,1}\right)\right| - \left|c_b\left(j_{i,2},k_{i,2}\right)\right| &> \varepsilon,\ if\ s_i = 0, \\ \left|c_b\left(j_{i,1},k_{i,1}\right)\right| - \left|c_b\left(j_{i,2},k_{i,2}\right)\right| &< -\varepsilon,\ if\ s_i = 1, \end{aligned} \quad (2)$$

где $c_b(j,k)$ – значения коэффициентов, b – номер блока, (j,k) – позиция коэффициента внутри блока, s_i – встраиваемый бит ЦВЗ. Для простоты можно обозначить коэффициенты $c_b(j,k)$ за $K1$ и $K2$.Позиции коэффициентов $K1$ и $K2$ и одинаковы для всех частотных матриц и сохраняются для последующего изъятия ЦВЗ [14].

Встраивание производится в область средних частот. Схему внедрения можно увидеть на рис. 1.

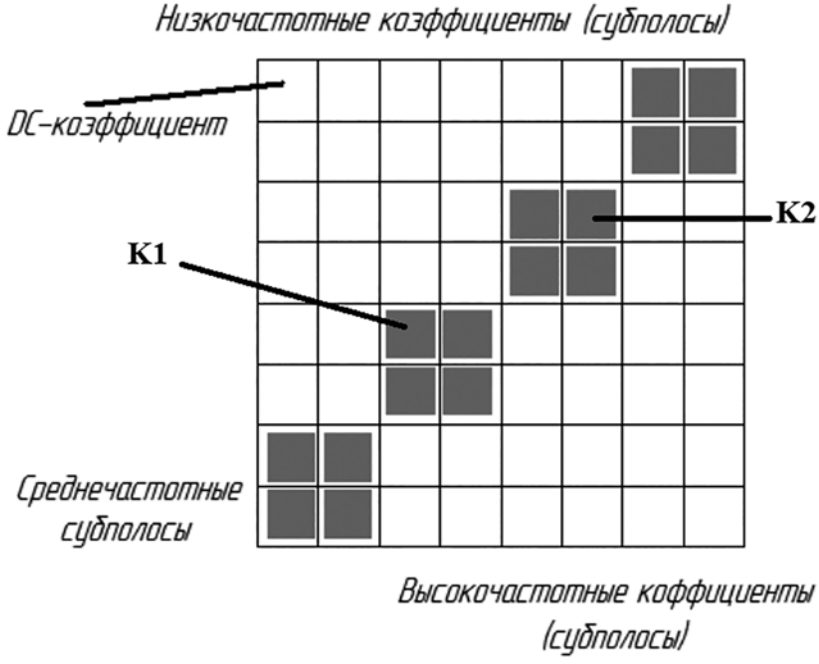


Рис. 1. Схема внедрения бита ЦВЗ в блок 8×8
(Fig. 1. The scheme of introduction of bit of a digital watermark in the block 8×8)

Как уже было сказано ранее, для внедрения нулевого бита ЦВЗ разность модулей коэффициентов частотной матрицы должна быть больше некоторой константы ε, а для внедрения единицы – меньше - ε. Очевидно, что после встраивания бита ЦВЗ произойдет визуальное изменение изображения-контейнера. При чем чем больше значение ε, тем более заметным будет это изменение. В работе Земцова А.Н. «Робастный метод цифровой стеганографии на основе дискретного косинусного преобразования» описано влияние данного метода встраивания на искажение изображения-контейнера. В этой работе был сделан вывод о том, что для того, чтобы искажение изображения было наименее заметным, значение константы ε должно быть ≤ 5 [15].

После внедрения ЦВЗ для возврата к целочисленным матрицам пикселей применяется обратное дискретное косинусное преобразование посредством умножения матриц частотных коэффициентов справа на матрицу ДКП, а затем умножения полученных результатов слева на траспони-

рованную матрицу ДКП. Далее производится переход от матриц интенсивностей R, G, B к матрице пиксейлей.

Для изъятия ЦВЗ к матрицам компонетнов пикселей (R, G, B) каждого блока изображения повторно примененяется прямое ДКП, после чего выявляемый бит равен «0», если $|K1'| > |K2'|$, а «1», если $|K1'| < |K2'|$, (позиции $K1$ и $K2$ известны), то есть функция изъятия является обратной к функции внедрения [2].

Модификация алгоритма

В алгоритме Коча (Koch) существует проблема. Вследствие двукратного применения ДКП к изображению при внедрении и извлечении ЦВЗ, а также применения обратного ДКП для возврата к целочисленным матрицам пикселей после внедрения соотношение коэффициентов частотной матрицы может нарушиться, а это недопустимо, так как от этого напрямую зависит результат работы алгоритма. Во избежание возникновения данной проблемы во время встраивания бита ЦВЗ необходимо производить принудительную корректировку значений коэффициентов частотной матрицы. Следует заметить, что такая модификация, согласно проведенному исследованию, не влечет за собой визуальных изменений изображения. Модифицированный алгоритм метода Коча (Koch) может быть представлен следующим образом:

1) изображение разбивается на блоки 8×8 пикселей;

2) в каждом блоке значения пикселей раскладываются на составляющие R, G и B, результат разложения записывается в три матрицы;

3) создается матрица ДКП тоже размером 8×8, элементы которой получаются по формуле (1);

4) к матрицам интенсивностей каждого из цветов R, G и B применяется прямое ДКП посредством их умножения справа на транспонированную матрицу ДКП, а затем умножения полученных матриц слева на саму матрицу ДКП. На выходе получается по три матрицы частотных коэффициентов для каждого блока 8×8 пикселей исходного изображения. В каждую из них можно встроить по биту ЦВЗ;

5) начинается проход по матрицам частотных коэффициентов в области средних частот в поисках позиций коэффициентов $K1$ и $K2$ по горизонтали и вертикали и коэффициента силы встраивания ε, при которых внедренный и изъятый ЦВЗ совпадут. Значение коэффициента ε перебирается от 0 до 5 с шагом 0,1. Интервал значений от 0 до 5 был принят как пригодный для наименьшего искажения изображения вследствие встраивания. Алгоритм поиска прерывается, как только найдется первая такая пятерка, следовательно, внедрение будет произведено при минимальном возможном значении . Как только позиции коэффициентов $K1$ и $K2$ по горизонтали и вертикали и значение ε подобраны, производится внедрение ЦВЗ по формуле:

$$
\begin{aligned}
&if\ (s_i = 1)\\
&\quad if\ (|K1| - |K2| < \varepsilon)\\
&\qquad if\ (\mathrm{K1} >= 0)\\
&\qquad\quad K1' = |K2| + \varepsilon,\\
&\qquad else\\
&\qquad\quad K1' = -|K2| - \varepsilon;\\
&if\ (s_i = 0)\\
&\quad if\ (|K2| - |K1| < \varepsilon)\\
&\qquad if\ (\mathrm{K2} >= 0)\\
&\qquad\quad K2' = |K1| + \varepsilon,\\
&\qquad else\\
&\qquad\quad K2' = -|K1| - \varepsilon, \quad (3)
\end{aligned}
\tag{3}
$$

где s_i – встраиваемый бит ЦВЗ.

В данном случае формула, предложенная Кочем (Koch), видоизменена, и добавлена модификация значений коэффициентов частотной матрицы $K1$ и $K2$ посредством прибавления или вычитания значения коэффициента силы встраивания ε. При этом смысл, вложенный автором, остается прежним, а соотношение коэффициентов $K1$ и $K2$ остается верным, несмотря на возможность изменения их значений вследствие применения обратного ДКП, а затем повторного применения прямого ДКП для изъятия ЦВЗ. При этом визуально такое изменение заметно не будет. Найденные позиции коэффициентов $K1$ и $K2$ сохраняются для последующего извлечения ЦВЗ;

6) после внедрения ЦВЗ для возврата к целочисленным матрицам пикселей применяется обратное преобразование посредством умножения матриц частотных коэффициентов справа на матрицу ДКП, а затем умножения полученных матриц слева на транспонированную матрицу ДКП;

7) для изъятия ЦВЗ изображение повторно разбивается на блоки 8×8 пикселей, пиксели раскладываются на компоненты R, G и B, к матрицам R, G и B применяется прямое ДКП, после чего выявляемый бит равен единице, если $|K1'| > |K2'|$, и нулю в противном случае (позиции коэффициентов $K1$ и $K2$ известны).

Проведено исследование описанного метода на предмет зависимости значения коэффициента силы встраивания от яркости изображения-контейнера и размера встраиваемого ЦВЗ. Результаты этого исследования представлены в табл. 1 и 2.

Таблица 1. Исследование модифицированного алгоритма метода Коча (Koch) на предмет зависимости значения коэффициента силы встраивания от размера встраиваемого ЦВЗ
(Table 1. Research of the modified algorithm of a method of Koch about dependence of value of factor of force of embedding on the size of a built in digital watermark)

Длина ЦВЗ	Значение
1 – 12 символов	1.5
13 – 24 символов	1.7
25, 26 символов	2
27 – 29 символов	4

Результаты, представленные в табл. 1, можно изобразить в виде графика зависимости величины коэффициента силы встраивания от размера ЦВЗ, как показано на рис. 2.

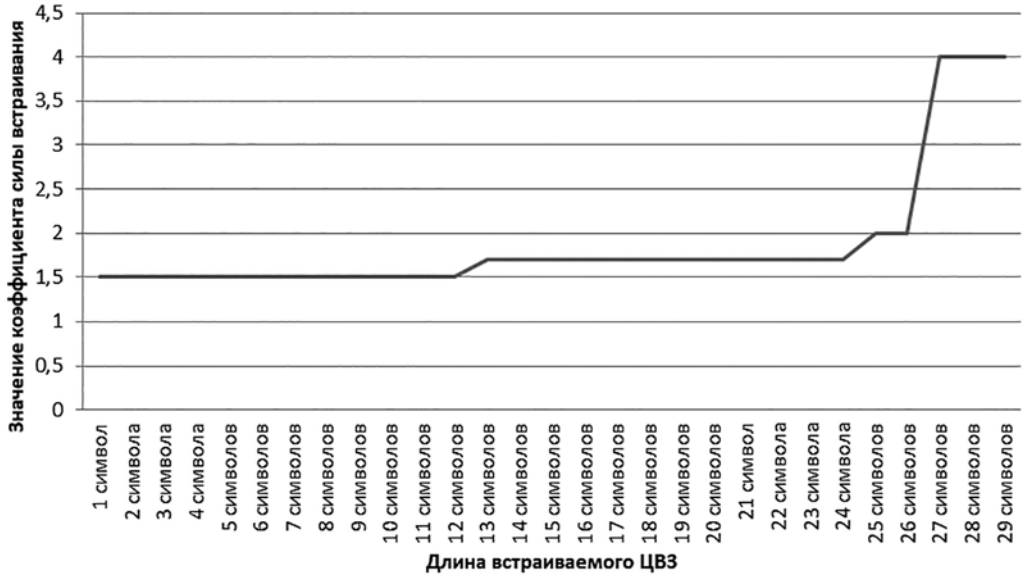


Рис. 2. График зависимости величины коэффициента силы встраивания от размера ЦВЗ
(Fig. 2. The schedule of dependence of size of factor of force of embedding from the size of a digital watermark)

Таблица 2. Исследование модифицированного алгоритма метода Кoча (Koch) на предмет зависимости значения коэффициента силы встраивания от яркости изображения-контейнера
Table 2. Research of the modified algorithm of a method of Koch about dependence of value of factor of force of embedding on brightness of the image-container

Длина ЦВЗ	Значение яркости изображения (из 255)	Значение
1 – 12 символов	40	2
1 – 12 символов	50	1.9
1 – 12 символов	60 – 70	1.9
1 – 12 символов	80 – 90	1.8
1 – 12 символов	100 – 120	2.1
1 – 12 символов	130	1.8
1 – 12 символов	140	1.4
1 – 12 символов	150	0.9
1 – 12 символов	160 – 210	0.5
1 – 12 символов	220	0.4
1 – 12 символов	230	0.1
1 – 12 символов	240	0

Результаты, представленные в табл. 2, можно изобразить в виде графика зависимости величины коэффициента силы встраивания ε от яркости изображения, как показано на рис. 3.

Рис. 3. График зависимости величины коэффициента силы встраивания от яркости изображения
(Fig. 3. The schedule of dependence of size of factor of force of embedding from brightness of the image)

Заключение

На основании вышеизложенного материала можно сделать вывод о том, что метод Кoча (Koch) является наиболее подходящим для встраивания ЦВЗ, в частности в изображения, так как он обладает рядом преимуществ по сравнению с другими методами. Единственной проблемой дан-

ного метода было то, что вследствие двукратного применения ДКП к изображению при внедрении и извлечении ЦВЗ, а также применения обратного ДКП для возврата к целочисленным матрицам пикселей после внедрения соотношение коэффициентов частотной матрицы может нарушиться, а это недопустимо, так как от этого напрямую зависит результат работы алгоритма. Во избежание возникновения данной проблемы алгоритм был модифицирован посредством принудительной корректировки значений коэффициентов частотной матрицы во время встраивания бита ЦВЗ. В ходе исследования был сделан вывод о том, что значение коэффициента силы встраивания прямо пропорционально длине встраиваемого текста и обратно пропорционально яркости изображения, в чем можно убедиться, ознакомившись с графиками на рис. 1 и 2. Причем, если в первом случае функция зависимости коэффициента силы встраивания от размера ЦВЗ явно возрастает, то в случае изменения яркости изображения могут происходить скачки значений коэффициента силы встраивания вверх, после чего снова наблюдается тенденция к снижению. Наряду с этим удалось установить, что при изображение размером 120 бит на 120 бит максимальная длина текста, который представляется возможным встроить, соответствует 29 символам. Параллельно был сделан вывод о том, что границы значения яркости изображения, пригодного для встраивания, соответствуют отрезку [40; 240]. Для изображений, яркость которых более 240 или менее 40, подбор коэффициента силы встраивания является сложной задачей.

СПИСОК ЛИТЕРАТУРЫ:

1. Сагайдак Д.А., Файзуллин Р.Т. Способ формирования цифрового водяного знака для физических и электронных документов//Компьютерная оптика. 2014. Т. 38. № 1. С. 94 – 104.
2. Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding. Proc. SPIE. – 1995. – Vol. 2420. – P. 40.
3. Moller, S. Computer Based Steganography: How It Works And Why Therefore Any Restriction On Cryptography Are Nonsense, At Best / S. Moller, A. Pfitzmann, I. Stirand // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science. – 1996. – Vol.1174. – P.7 - 21.
4. Aura, T. Practical Invisibility In Digital Communication / T. Aura // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Sciencею – 1996. – Vol.1174. – P. 265 - 278.
5. Хорошко, В.О. Основы компьютерной стеганографии: уч. пособие для студентов и аспирантов / В.О. Хорошко, О.Д. Азаров, М.Э. Шелест. – Винница: ВНТУ, 2003. – С. 143.
6. Белобокова, Ю. А. Модели и алгоритмы защитной маркировки для обеспечения аутентичности и целостности растровых изображений: диссертация на соискание ученой степени кандидата технических наук / Белобокова, Ю. А. URL: http://mgup.ru/public/files/4596.pdf (дата обращения: 29.05.2018). Загл. с экрана. Яз. рус.
7. Bloom J., Alonso R., Smart Search Steganalysisю. Proc. SPIE – 2003. Vol. – 5020. P. 167.
8. Fridrich J., Goljan. M. Practical Steganalysis of Digital Images State of the Art. Proc. SPIE – 2002. – Vol. 4675. – P.13.
9. Harmsena, J., Pearlmana W. Steganalysis of additive noise modelable information hiding. Proc. SPIE – 2003. – Vol. 5020. – P. 131 - 142.
10. Колобова, Алена К. Разработка алгоритмов внедрения и извлечения цифрового водяного знака, устойчивого к сжатию JPEG. Безопасность информационных технологий, [S.l.], v. 22, n. 1, mar. 2015. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/198>. Дата доступа: 10 oct. 2018.
11. Иваненко, Виталий Г.; Ушаков, Никита В. Защита изображений формата jpeg при помощи цифровых водяных знаков. Безопасность информационных технологий, [S.l.], v. 25, n. 2, p. 106 - 113, may 2018. ISSN 2074 - 7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Дата доступа: 10 oct. 2018. doi:http://dx.doi.org/10.26583/BIT.2018.2.09.
12. Pereira, S., Joseph, J., Deguillaume F. Template Based Recovery of FourierBased Watermarks Using Log-Polar and Log-Log Maps. IEEE Int. Conf. on Multimedia Computing and Systems, 1999, P. 5 – 15.
13. Koch, E., Zhao, J. Towards robust and hidden image copyright labeling, Proceedings of the IEEE International Workshop on Nonlinear Signal and Image Processing, P. 452-455, 1995.
14. Волосатова Т.М., Чичварин Н.В. Исследование и разработка алгоритма защиты проектной документации в CAD/CAM/CAE от несанкционированного доступа. Инженерный журнал: наука и инновации, 2014, вып. 2. URL: http://engjournal.ru/catalog/it/hidden/1201.html (дата обращения: 21.10.2018). Загл. с экрана. Яз. рус.

15. Земцов, А.Н. Робастный метод цифровой стеганографии на основе дискретного косинусного преобразования / Земцов, А.Н. Изд-во: ВолгГТУ, 2011. URL: https://vivliophica.com/articles/apsciences/441379 (дата обращения: 29.05.2018). Загл. с экрана. Яз. рус.

REFERENCES:

[1] Sagaidak D.A., Fayzullin R. T. Way of formation of a digital watermark for physical and electronic documents. Computer optics. 2014. Vol. 38. № 1. P. 94 - 104.
[2] Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding. Proc. SPIE. – 1995. – Vol. 2420. – P. 40.
[3] Moller, S. Computer Based Steganography: How It Works And Why Therefore Any Restriction On Cryptography Are Nonsense, At Best S. Moller, A. Pfitzmann, I. Stirand Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science. – 1996. – Vol. 1174. – P.7 - 21.
[4] Aura, T. Practical Invisibility In Digital Communication T. Aura. Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Sciencею – 1996. – Vol. 1174. – P. 265 - 278.
[5] Khoroshko, V.O. Basics of computer steganography: the manual for students and post-graduate students. V. O. Khoroshko, O.D. Azarov, M.E. Shelest. – Vinnitsa: VNTU, 2003. – P. 143.
[6] Belobokova, J. A. Models and algorithms of protective marks for maintenance of authenticity and integrity of raster images [the Electronic resource]: thesis for the degree of candidate of technical Sciences [the Electronic resource] Belobokova, J.A. URL: http://mgup.ru/public/files/4596.pdf (date of recourse: 29.05.2018). The title from the screen. (in Russian).
[7] Bloom J., Alonso R., Smart Search Steganalysisю. Proc. SPIE – 2003. Vol. – 5020. P. 167.
[8] Fridrich J., Goljan. M. Practical Steganalysis of Digital Images State of the Art. Proc. SPIE – 2002. – Vol. 4675. – P.13.
[9] Harmsena, J., Pearlmana W. Steganalysis of additive noise modeable information hiding. Proc. SPIE – 2003. – Vol. 5020. – P.131 - 142.
[10] Kolobova, Alena K. The Development of Algorithms of Embedding and Extraction of Resistant to JPEG Compression Digital Watermark. IT Security (Russia), [S.l.], v. 22, n. 1, mar. 2015. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/198>. Date accessed: 10 oct. 2018.
[11] Ivanenko, Vitaliy G.; Ushakov, Nikita V.. JPEG digital watermarking for copyright protection. IT Security (Russia), [S.l.], v. 25, n. 2, p. 106 - 113, may 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Date accessed: 10 oct. 2018. doi:http://dx.doi.org/10.26583/BIT.2018.2.09.
[12] Pereira, S., Joseph, J., Deguillaume F. Template Based Recovery of FourierBased Watermarks Using Log-Polar and Log-Log Maps. IEEE Int. Conf. on Multimedia Computing and Systems, 1999, P. 5 – 15.
[13] Koch, E., Zhao, J. Towards robust and hidden image copyright labeling, Proceedings of the IEEE International Workshop on Nonlinear Signal and Image Processing, P. 452 - 455, 1995.
[14] Volosatova T.M., Chichvarin N.V. Research and working out of algorithm of protection of the design documentation in CAD/CAM/CAE from unapproved access. Engineering magazine: a science and innovations, 2014, Release 2. URL: http://engjournal.ru/catalog/it/hidden/1201.html (date of recourse: 21.10.2018). The title from the screen. (in Russian).
[15] Zemtsov, A.N. The robust digital steganography method based on discrete cosine transformation Zemtsov, A.N. Publishing house: ВолгГТУ, 2011. URL: https://vivliophica.com/articles/apsciences/441379 (date of recourse: 29.05.2018). The title from the screen. (in Russian).

Поступила в редакцию - 16 октября 2018 г. Окончательный вариант – 07 ноября 2018 г.
Received – October 16, 2018. The final version – November 07, 2018.

Сергей И. Журин[1,2], Дмитрий Е. Комарков[3]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[2]АО «Федеральный центр науки и высоких технологий «Специальное научно-производственное объединение «Элерон»,
ул. Генерала Белова, 14, г. Москва, 115563, Россия
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА

DOI: http://dx.doi.org/10.26583/bit.2018.4.09

Аннотация. Целевой фишинг является одним из методов социальной инженерии. При целевом фишинге текст электронного письма составляется с учетом знаний о конкретном предприятии и сотруднике (часто) с использованием знаний социологии и психологии таким образом, чтобы вызвать желание открыть прикрепленный файл или нажать на ссылку. Основная трудность защиты от такого письма состоит в том, что методы автоматизированного анализа не дают гарантии его обнаружения, т.к. современные киберпреступники используют новые текстовые формулировки, уязвимости нулевого дня, а также средства автоматизации для инжектирования эксплойтов в файлы, что снижает эффективность сигнатурного анализа антивирусных программ. Каждая из существующих технологий обнаружения в отдельности не позволяет обеспечить защиту от целевого фишинга. Однако объединение технологий (фильтрация спама, межсетевые экраны, антивирусы) с обязательным включением организационных мер, в том числе обучения и тестирования персонала, позволяет в комплексе защитить внешний информационный периметр организации от целевого фишинга. В статье приведен детальный анализ технологии реализации целевого фишинга с анализом причин возможностей его реализации двумя типовыми методами: запуском эксплойта при переходе по ссылке и при запуске файла. Приведен обзор уязвимостей 2016 – 2017 года, использованных для целевых атак. Приведены современные технологии защиты и их сравнительный анализ. Отмечено, что каждая из технологий не позволяет в отдельности обеспечить защиту от целевого фишинга. Предложены наиболее эффективные современные методы защиты на основе их сравнительного анализа и анализа современных информационных угроз.

Ключевые слова: APT, фишинг, целевой фишинг, социальная инженерия, внедрение ПО.
Для цитирования: ЖУРИН, Сергей И.; КОМАРКОВ, Дмитрий Е. ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 95-107, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1164>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.09.

Sergey I. Zhurin[1,2], Dmitry E. Komarkov[3]
[1]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
[2]Joint Stock Company "Federal Center of Science and High Technologies "SNPO "Eleron",
14, Gen. Belova str., Moscow, 115563, Russia
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

Protection of external information perimeter of organization from spear phishing

DOI: http://dx.doi.org/10.26583/bit.2018.4.09

Abstract. Spear phishing is one of the social engineering techniques. In case of spear phishing the email text is compiled taking into account the knowledge about a particular company and rather often about the employee using sociology and psychology in such a way that cause the desire to open the attached file or to click on the link. The main difficulty of protection against such e-mails is that the methods of automated analysis do not guarantee its detection, as modern cyber criminals use new text formulations, zero-day vulnerabilities, as well as automation tools to inject exploits into files, which reduces the effectiveness of signature analysis of anti-virus programs. Each of the existing detection technologies alone does not provide protection against spear phishing. However, the combination of technologies (spam filtering, firewalls, anti-viruses), with the mandatory organizational measures, including training and testing of personnel, allows to protect the external information perimeter of the company from the spear phishing. The paper presents a detailed analysis of the technology of spear phishing implemented by two typical methods: the launch of the exploit when clicking on the link and when one runs an executable file. An overview of the vulnerability used in 2016 - 2017 for the attacks is presented. Modern technologies of protection and their comparative analysis are given. It is noted that each of the technologies used separately does not allow an effective protection against spear phishing. On the basis of comparative analysis and analysis of modern information threats the most effective modern methods of protection are proposed.

Keywords: APT, phishing, spearphishing, social engineering, software implementation.

For citation: ZHURIN, Sergey I.; KOMARKOV, Dmitry E. Protection of external information perimeter of organization from spear phishing. IT Security (Russia), [S.l.], v. 25, n. 4, p. 95-107, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1164>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.09.

Введение

В наши дни внешние кибератаки представляют серьезную угрозу для корпоративной среды. Их последствиями могут быть похищенные файлы (пример – Корейская АЭС в 2014 году), нарушение управления производственными процессами (пример, завод по обогащению урана в Натанзе (Иран), вирус Stuxnet в 2009 году).

Кибератаки могут начинаться с поиска оборудования, подключенного к Интернету, например, с использованием открытой платформы SHODAN с последующим подбором пароля или с прослушивания каналов связи, но эти атаки эффективно защищаются простыми мерами, такими как установка сложных паролей и исключение паролей по умолчанию, или шифрацией трафика соответственно. *Наиболее простым способом начала атаки, от которого защититься сложнее, является целевой фишинг.*

По данным компании Group-IB, ежедневно жертвами финансового фишинга в России становятся более 900 клиентов различных банков, что в три раза превышает ежедневное количество жертв от вредоносных программ, а около 10 – 15 % посетителей финансовых фишинговых сайтов вводят на них свои данные [1]. В России, по оценкам Group-IB, действует 15 преступных групп, занимающихся фишингом, направленным на финансовые учреждения [1].

По данным Positive Technologies [2], в 2017 году наиболее популярными являлись кибератаки с использованием вредоносного ПО (39 %), а ущерб от них составил более 1,5 млрд. долл. США. Также в годовом отчете компании отмечается, что одним из главных способов распространения ПО в данном случае являлось фишинговое письмо, использующее методы социальной инженерии.

На данный момент не существует средств защиты информации, которые были бы способны гарантированно детектировать и предотвращать атаки, начинающиеся с целевого фишинга, в котором ставка киберпреступников делается на человеческий фактор, и только технических (программных) средств защиты в этом случае недостаточно. Данная статья направлена на анализ методов целевого фишинга и существующих мер защиты от внедрения вредоносного ПО в корпоративную среду данным путем. Также приводятся рекомендации по комплексности защиты от целевого фишинга.

1. Целевая атака

Целевые или таргетированные атаки используются для нападения на информационную инфраструктуру компаний [3, 4]. Перед атакой киберпреступники тщательно изучают средства защиты атакуемой организации.

При целевых атаках, как правило, преследуются следующие цели:

• похищение средств с банковских счетов и электронных кошельков [5], а также конфиденциальной, коммерческой информации;

• нечестная конкуренция: манипулирование процессами, подделка документов, ослабление конкурентов, вымогательство и шантаж;

• нарушение нормальной деятельности объектов [3].

Рассмотрим модель жизненного цикла целевой атаки, представленной на рис. 1, которая предложена Лабораторией Касперского.

Основной задачей *подготовки* является поиск цели, сбор о ней достаточно детальной приватной информации, опираясь на которую можно выявить слабые места в инфраструктуре. При этом выстраивается стратегия атаки, подбираются доступные инструменты, либо происходит их самостоятельная разработка.

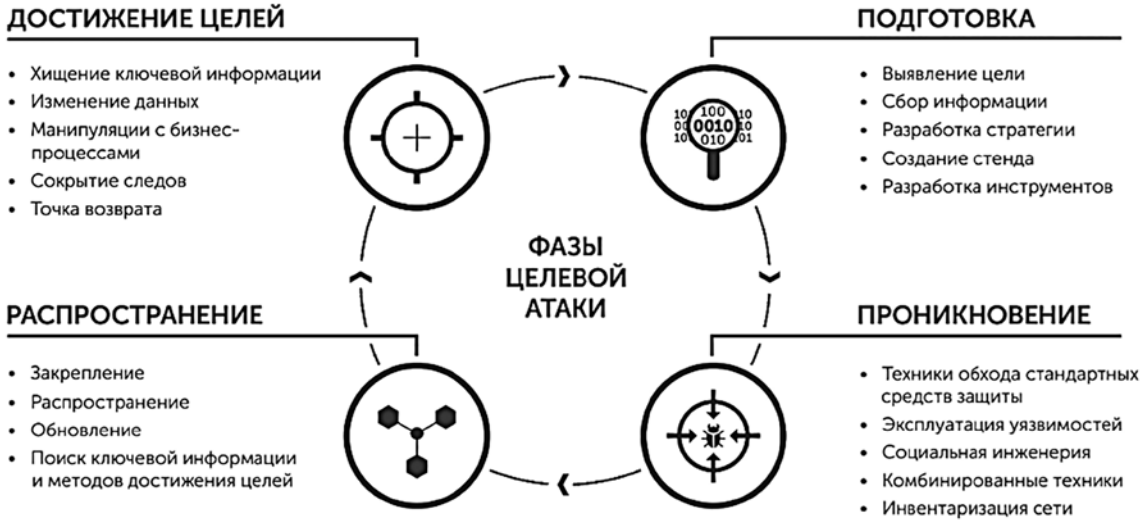


Рис. 1: Фазы целевой атаки

Рис. 1. Жизненный цикл целевой атаки
(Fig. 1. Life-cycle of target attack)

Проникновение – активная фаза целевой атаки, проводимая для первичного инфицирования цели и внутренней разведки. *Здесь широко используется целевой фишинг.* По окончании разведки и после определения принадлежности инфицированной рабочей станции по команде злоумышленника через центр управления загружается дополнительный вредоносный код.

Распространение – фаза закрепления внутри инфраструктуры. Максимально распространяя свой контроль, при необходимости корректируя версии вредоносного кода через центры управления.

Достижение цели – ключевая фаза целевой атаки, в зависимости от выбранной стратегии в ней может применяться хищение или изменение информации, манипуляции с бизнес-процессами компании.

2. Целевой фишинг – элемент целевой атаки

Целью фишинга [6] является получение доступа к конфиденциальным данным пользователей или установка вредоносного ПО с использованием методов социальной инженерии.

Главный инструмент фишинга – электронная почта. На почтовый ящик жертвы злоумышленник отправляет письмо, которое должно побудить его ввести необходимую информацию. Также сообщение может содержать вредоносное вложение, которое при этом проникнет в систему и будет собирать и отправлять информацию злоумышленнику. Особенность классического фишинга – массовая рассылка писем с идентичным содержанием.

Целевой фишинг (англ. spear-phishing), в отличие от обычного [7], направлен на конкретную цель, а значит является намного опаснее, поскольку киберпреступники специально собирают информацию о жертве, чтобы сделать свое послание убедительнее. Качественно сделанное письмо для целевого фишинга иногда очень трудно отличить от вполне легитимного письма, не преследующего зловредных целей. Данные особенности сделали метод одним из наиболее эффективных для проведения целевых атак.

Структура целевой фишинговой атаки показана на рис. 2.

Использование целевого фишинга как способа для проведения целевых атак является одним из самых эффективных. Это связано с тем, что метод использует уязвимости персонала, т.е. человеческий фактор [8]. Человек, как известно, является слабым звеном любой системы, т.к. способен принимать необдуманные и спонтанные решения.

Эксперты Positive Technologies провели исследование [2, 8], в котором рассмотрели влияние методов социальной инженерии на персонал нескольких крупных компаний путем рассылки тестовых писем, имитирующих атаку. В отчете были названы наиболее эффективные фишинговые сценарии (тема письма), статистика которых представлена на рис. 3.

Рис. 2. Структура целевой фишинговой атаки
(Fig. 2. Structure of spear-phishing attack)

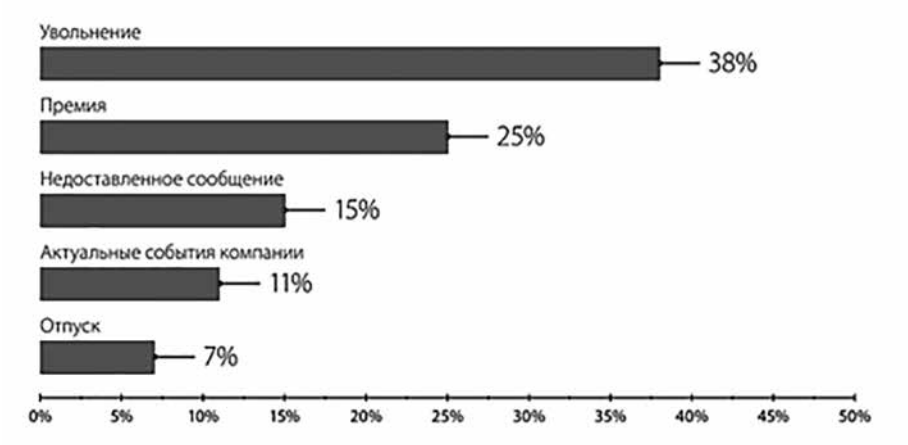


Рис. 3. Темы тестовых писем (доля успешных сценариев)
(Fig. 3. Themes of test letters (the proportion of successful scenarios))

3. Методы внедрения вредоносного кода с использованием целевого фишинга

Существует два типовых метода: вложение и ссылка, которые эксплуатируют уязвимости ПО. **Уязвимостью** программы является ошибка, допущенная программистами на этапе ее разработки. Это и позволяет злоумышленникам получить незаконный доступ к функциям программы или хранящимся в ней данным.

Ошибки могут появиться на любом этапе написания программы, от проектирования до выпуска готового продукта. Причины можно выделить следующие:

- ошибки на этапе проектирования и реализации ПО;
- оставление BackDoor для удаленной отладки;
- применение средств разработки различного происхождения;
- использование в составе ПО сторонних компонентов или свободно распространяемого кода;
- наличие в команде программистов-инсайдеров, которые преднамеренно вносят в написанный код дополнительные функции или элементы.

Любая программа, которая поступает на рынок, имеет уязвимости. И пока они не будут выявлены, разработчик не сможет их устранить. Здесь ключевым моментом является то, кто раньше сможет обнаружить ошибку *(уязвимость нулевого дня)* – сам разработчик или же злоумышленники.

Именно уязвимости нулевого дня используются при проведении целевых атак. Но найти ранее неизвестную уязвимость очень непросто. Поэтому атаки могут проводиться с использованием известных уязвимостей, которые еще совсем недавно стали таковыми. Это осуществимо только тогда, когда потенциальная жертва не установила необходимые обновления, в которых разработчик исправил данную ошибку, и злоумышленнику известна эта информация.

Найденным уязвимостям присваивают код с индексом CVE (Common Vulnerabili-ties and Exposures) с описанием в национальных базах данных, например на сайте ФСТЭК России. Примеры «популярных» уязвимостей [9], [10], [11], [12]:

- CVE-2016-0189 в Windows 10 позволяет удаленным злоумышленникам выполнять произвольный код или вызывать отказ в обслуживании;
- CVE-2016-7200 JavaScript позволяет выполнять произвольный код или вызывать отказ в обслуживании;
- CVE-2015-8651, CVE-2016-4117 – Adobe Flash Player позволяют выполнять произвольный код;
- CVE-2017-0037 в Internet Explorer 11 позволяет выполнять произвольный код.

Эксплойты

Для того, чтобы воспользоваться уязвимостью программы, используют *эксплойты*. Эксплойтом необязательно может быть программа, это может быть небольшой фрагмент вредоносного кода или набор команд, выполняющихся в определенном порядке. Используя уязвимость в какой-либо системной или прикладной программе, эксплойт позволяет получить несанкционированный доступ к приложению или операционной системе и возможность их эксплуатации.

Эксплойты для разных уязвимостей часто упакованы вместе – так, чтобы проверить систему-мишень на широкий спектр уязвимостей. Как только выявляются одна или несколько, в дело вступают соответствующие эксплойты, которые подгружают программы сбора информации об учетных записях пользователей, установленном программном обеспечении, активных процессах и средствах защиты и далее загружают, например, систему удаленного мониторинга, инжектируя вредоносный код в запущенные программы.

В 2017 году злоумышленники использовали в основном недостатки браузеров, но самой популярной среди них оказалась уязвимость, связанная с Microsoft Office.

Средства доставки

Проникнув благодаря уязвимости на целевой корпоративный компьютер, эксплойт запускает средство доставки [2], тип которого зависит от дизайна атаки: это могут быть валидатор, загрузчик или дроппер.

Валидатор является сборщиком данных и выполняет фильтрацию информации об учетных записях пользователей, установленном программном обеспечении, активных процессах и средствах защиты, передает шифрованные данные в центр управления атакой, и, в зависимости от полученной информации, злоумышленником принимается решение о дальнейшем развитии нападения, т.е. выбирается одна из следующих команд:

- загрузка дроппера – приступить к выполнению целевой атаки;
- самоуничтожение – компьютер и данные на нем не представляют ценности для целевой атаки;
- ожидание – решение откладывается, режим «сна».

Обладая минимальным размером и функционалом, валидатор не несет в себе уникальной информации о целевой атаке и ее организаторах, и, если он перехватывается средствами защиты, это не создает для киберпреступников угрозы утечки методов и средств, планируемых к применению.

Дроппер (Dropper) загружает из сети либо выделяет из самого себя компоненты, необходимые для проведения атаки (Payload) с их последующим выполнением. Также его задачей является обход средств защиты и обеспечение скрытности установки.

Загрузчик (*Downloader)* используется в целях быстрого заражения и при запуске выкачивает основной модуль Payload либо дроппер в зависимости от целей и планов киберпреступников.

Основной модуль *Payload* содержит основные компоненты для проведения атаки и может содержать различные средства сбора информации. Его полная загрузка означает окончание фазы внедрения.

Письмо с вредоносным вложением

Вложением может являться имитация отчета коллеги за предыдущий месяц или сообщение от банка, приславшего пользователю иск за неуплату по кредиту в формате Microsoft Office или *.pdf.

Файлы формата *.pdf часто содержат объекты JavaScript. Поэтому для злоумышленника достаточно просто создать некоторый скрипт, который использовал бы одну из уязвимостей движка от Adobe [13].

В документах Microsoft Office вредоносное ПО может загружаться при помощи макросов, которые содержит файл. При открытии документа исполнение макроса позволяет установить соединение с сервером злоумышленника и начать загрузку. Данная проблема существует довольно давно, поэтому в организациях поддержка макросов отключена по умолчанию. Но если пользователь не

осведомлен, то грамотное использование социальной инженерии может заставить его отключить защиту от макросов [13], [14].

На данный момент большинство способов эксплуатации уязвимостей Microsoft Office не требуют использования макросов. Например, используя самую популярную уязвимость 2017 года CVE-2017-0199, при открытии вложенного *.rtf файла можно подгрузить HTA-приложение, поддерживающее исполнение сценариев, со стороннего сервиса и запустить его.

Помимо рассмотренных случаев существует множество других офисных продуктов и форматов, с которыми они работают. Но принцип атаки один и тот же – запустить скрытый сценарий, который позволит загрузить ПО злоумышленника на атакуемый компьютер.

Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и Offensive Ware Multi Exploit Builder (OMEB) [1].

Письмо со ссылкой

В качестве содержания письма также может отправляться ссылка. Целью злоумышленника в данном случае является переход жертвы на определенный веб-ресурс, где, используя уязвимости самого сайта или браузера переходящего, преступник также пытается внедрить зловредное ПО.

Для проведения подобных операций создаются фишинговые сайты, которые живут, как правило, недолго. Они, как правило, являются точными копиями известных сайтов, полностью повторяют их дизайн и структуру. Но они являются лишь копиями, поэтому будут иметь отличающееся от оригиналов доменное имя.

При переходе по ссылке пользователь становится жертвой различных видов XSS-атак. Суть данных атак заключается в выполнении скрипта в браузере и последующем его взаимодействии с сервером злоумышленника. Эти операции позволяют получить доступ к данным браузера и дают возможность применять к нему эксплойты, а также красть cookie, данные авторизации или, например, выполнять HTTP-запросы от имени пользователя.

Мошенники не просто копируют сайт компании или банка, их логотипы и фирменные цвета, контент, контактные данные, регистрируют похожее доменное имя, они еще активно рекламируют свои ресурсы в соцсетях и поисковых системах. Например, пытаются вывести в топы выдачи ссылки на свои фишинговые сайты по запросу [1].

Еще несколько лет назад одного взгляда на адрес было достаточно, чтобы понять, что сайт фишинговый. Однако хакеры научились манипулировать отображением ссылки в адресной строке. В результате пользователь видит адрес, на 100 % совпадающий с официальным. Эта технология называется «спуфинг» (англ. spoofing - обман, мистификация) [1].

Преступники подделывают даже SSL-сертификат – это цифровое удостоверение сайта, которое подтверждает, что обмен данными между сайтом и браузером идет по защищенному каналу. Хакеры используют готовые фишинг-наборы (Phishing kits) – это уже готовый фишинговый сайт с конфигурационным файлом, в котором определяется логика работы фишингового сайта и то, куда должны быть отправлены скомпрометированные данные [1].

4. Анализ существующих мер защиты

4.1 Организационные меры

Фишинг как способ атаки успешен по большей части из-за человеческого фактора [14]. Человек, как известно, является слабым звеном в любой системе. Концентрация лишь на техническом оснащении системы защиты информации является большой ошибкой.

Осведомленность пользователя [14], [15], [16] может существенно повысить уровень защищенности организации.

Во-первых, необходимо минимизировать размещение электронных адресов на открытых сайтах (сайте компании, открытых торговых площадках, личных страницах пользователей и т.п.) и

ограничить доступ сотрудников к общей базе данных корпоративных адресов (в качестве примера можно привести известный пример с Эксклектоном, который продал базу данных корпоративных Министерства энергетики для целевого фишинга).

Во-вторых, для снижения уровня влияния человеческого фактора необходимо предпринять следующие меры:

- регламентирование политики использования корпоративной почты;
- обучение персонала;
- проведение тестирования.

Политика использования email

Выделим основные принципы такой политики:

- электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей, а не для личных целей;
- все электронные письма являются собственностью организации и не считаются персональными;
- организация может получить доступ к электронной почте сотрудников;
- пользователи не должны позволять кому-либо посылать письма, используя их идентификаторы;
- запрещение использования сторонних почтовых клиентов;
- справочники электронных адресов сотрудников доступны только внутри компании.

Обучение и тестирование персонала

Под обучением понимается повышение осведомленности пользователей. Персонал должен понимать возможности злоумышленников и способы атак, а также постоянно сохранять бдительность. Поэтому необходимо проводить соответствующие семинары и тренинги по темам:

- основные принципы фишинга;
- методы социальной инженерии;
- важность использования последних версий ПО;
- анализ расширений файлов и текста ссылок.

Администратору необходимо постоянно следить за обновлением ПО.

Для оценки подготовленности персонала к целевой атаке, организация может проводить тестирование. Тестирование осуществляется с использованием стандартных имеющихся программ, или со специально созданных почтовых ящиков, с обязательным информированием пользователей о проводимых учениях, за несколько недель до этого.

4.2 Программно-технические меры защиты

Системы фильтрации спама

Фильтрация нежелательных писем является первой ступенью защиты в борьбе с фишингом.

Анализ IP-адреса сервера отправителя

Данный вид анализа направлен на установление репутации IP отправителя, которая осуществляется путем его поиска в «черных списках». Подобная защита эффективна против массового фишинга, но бесполезна при целенаправленной атаке.

Анализ тела письма

Спам-фильтр может проверять содержимое письма: заголовок, тему, текст, ссылки и вложения. В текстовом содержании проверяется наличие словосочетаний, которые наиболее часто применяются при фишинговых методиках. Указанные ссылки при помощи алгоритмов анализируются на предмет схожести с известными ресурсами, а также, как и в случае с IP-адресами, осуществляется поиск доменных имен в списках нежелательных или имеющих подозрительную активность. Соответственно, у вложений проверяются имена и расширения.

SPF/DKIM-анализ

SPF является расширением для протокола отправки электронной почты, который позволяет получателям проверять IP-адрес отправителя с помощью просмотра списка авторизованных шлюзов для определенного домена в DNS-записях. То есть благодаря SPF можно проверить, не подделано ли доменное имя отправителя и является ли легитимным. Агенты передачи почты, получающие почтовые сообщения, могут запрашивать SPF-информацию с помощью DNS-запроса, верифицируя таким образом сервер отправителя.

DKIM является методом email аутентификации, дающим возможность получателю проверить, что письмо действительно было отправлено с заявленного домена. Вместо традиционного IP-адреса для определения отправителя сообщения DKIM добавляет в него цифровую подпись, связанную с именем домена организации. Подпись автоматически проверяется на стороне получателя, после чего, для определения репутации отправителя, применяются «белые списки» и «чёрные списки».

Использование данных технологий защищает от IP-спуфинга и подмены имен, что в значительной мере препятствуют массовому фишингу, но не защищает от целевого.

Межсетевые экраны

Межсетевой экран осуществляет контроль и фильтрацию проходящего через него сетевого трафика с использованием ряда правил. Работа экрана может осуществляться как на сетевом, так и на транспортном уровне и заключается в анализе заголовков пакетов.

При анализе заголовка сетевого пакета могут использоваться следующие параметры:

- IP-адреса источника и получателя;
- тип транспортного протокола;
- поля служебных заголовков протоколов сетевого и транспортного уровней;
- порт источника и получателя.

Межсетевой экран обычно используется в совокупности с другими средствами защиты информации, где его практическая значимость возрастает. Но в отдельности он не способен противостоять сложным и заранее продуманным атакам.

Антивирусные решения

Современные антивирусные решения включают в себя: сетевые экраны и спам-фильтры, работающие по тем же принципам, которые были описаны ранее. А также проводят анализ загружаемого или работающего ПО с использованием следующих методов:

- сигнатурный анализ;
- эвристический анализ;
- песочница.

Сигнатурный анализ детектирует только ранее известное вредоносное ПО. При этом файлы даже со старой инжектированной системой, удаленной мониторинга, могут быть не идентифицированы, особенно при инжектировании в новый файл. Эвристический анализ может выявить новое вредоносное ПО, однако при этом высок процент ошибки, что может потребовать время на дополнительный анализ. Песочница позволяет более эффективно идентифицировать такое ПО, например, загрузчики вредоносного ПО, например, перемещая время вперед и имитируя загрузку разных систем, браузеров.

IDS/IPS

Система обнаружения вторжений (IDS), как и система предотвращения вторжений (IPS), является программным или программно-аппаратным средством защиты информации. Данные системы предназначены для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими, и одним из требований к данным системам является обнаружение активности вредоносного ПО.

IDS производит поиск злонамеренных файлов сигнатурным анализом, а значит эксплуатация уязвимостей нулевого дня скорее всего останется незамеченной. Отличие IPS заключается в том, что данная система ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника, а значит более полезна в обеспечении безопасности.

Данные системы, в отличие от рассматриваемых ранее, имеют подсистему анализа данных, а значит обладают преимуществом, поскольку способны вести наблюдение за пользовательской активностью, а также выявлять аномальное поведение файлов, сообщая об этом администратору.

UTM-системы

Система UTM является комплексным решением и содержит:

- межсетевой экран;
- фильтр URL;
- антивирусное решение;
- спам-фильтры;
- IDS/IPS.

Все составляющие системы работают по ранее описанным принципам, но оптимизация их взаимодействия способна улучшить показатели по детектированию угроз.

Использование подобных решений для компании вытекает в ряд положительных моментов, таких как простота настройки и обеспечения системы безопасности, а также простота обучения персонала и уменьшение затрат на защиту.

Системы защиты конечных точек

EDR-системы разработаны для предотвращения атак со сложной структурой. Платформа EDR не просто защищает компьютерную систему от вредоносных тел, она умеет моментально замечать новейшие угрозы высокой сложности и одновременно проявлять реакцию на возникшую ситуацию. Под конечной точкой в данном случае подразумевается рабочая станция, сервер или любое другое компьютерное устройство.

С учетом того, что данные системы имеют достаточно сложное устройство, они, как правило, способны взаимодействовать с другими системами защиты, такими как SIEM.

Работа платформы EDR начинается с установки агента на компьютерное устройство пользователя (конечную точку). Затем осуществляется анализ действий приложений, запускаемого на компьютере, полученные данные отправляются в облако. Защитное решение способно классифицировать практически все приложения, по которым поступает информация, в том числе программы с вредоносным кодом и без него.

Основным компонентом подобных решений является система обнаружения таргетированной атаки, которая имеет:

- сетевые/почтовые сенсоры, позволяющие осуществлять сбор информации с различных контрольных точек;
- сенсоры рабочих станций, позволяющие увеличить охват и детализацию анализируемой информации;
- компонент динамического анализа объектов;
- центр по анализу аномалий – создание типовых шаблонов поведения и контроль отклонений от них;
- облачный репутационный сервис – обновляемая в реальном времени база знаний об угрозах, в том числе и по компонентам таргетированных атак.

Важным звеном EDR является анализатор аномалий, работа которого основывается на статистическом анализе информации, учитывающем частоту событий и их последовательность. Каналами сбора информации являются сетевые сенсоры и сенсоры рабочих станций. В процессе работы технологии формируется поведенческая модель, отклонение от которой может быть признаком вредоносной активности.

5. Оценка эффективности методов защиты

Как показал анализ, по отдельности средства защиты практически не способны противостоять внедрению вредоносного кода в корпоративную сеть. Следовательно, построение системы безопасности требует комплексного использования различных устройств и техник.

На основе проделанных исследований была проведена оценка эффективности средств защиты. Методы внедрения в данной схеме делятся по разным категориям, поэтому ее практическая ценность заключается в возможности оценки различных видов целевых атак путем усреднения значений. Например, UTM-система обладает средней эффективностью в борьбе с целевой атакой, которая использует фишинговое письмо со ссылкой, переход по которой позволит эксплойту для браузера использовать известную уязвимость и напрямую загрузить payload.

Организационные меры, по сути, не являются средством защиты информации, но их высокая эффективность против фишинга не позволяет не обратить на них внимание.

Экспертная оценка эффективности мер защиты представлена на рис. 4.

Эффективным решением для организации безопасности является внедрение системы защиты конечных точек как более эффективного средства защиты от внедрения ПО при целевых фишинговых атаках. Но данные системы имеют высокую стоимость и относительно сложную процедуру установки, а также требуют высококвалифицированного персонала, поэтому не все организации могут использовать их. Выходом из ситуации является выделение значительных усилий на введение организационных мер, а также использование средств защиты различного характера, т.к. только всесторонняя и комплексная защита способна оказывать противодействие данным атакам.

Если внедрение системы защиты конечных точек по ряду причин не может быть реализовано, то для построения системы защиты корпоративной сети вместе с внедрением организационных мер рекомендуется использовать UTM-системы ввиду простоты эксплуатации, а также потому, что совместно функционирующие спам-фильтры, межсетевой экран и антивирус хоть и не могут противостоять сложным фишинговым атакам, но способны защитить организацию от большинства менее качественно спланированных внедрений.

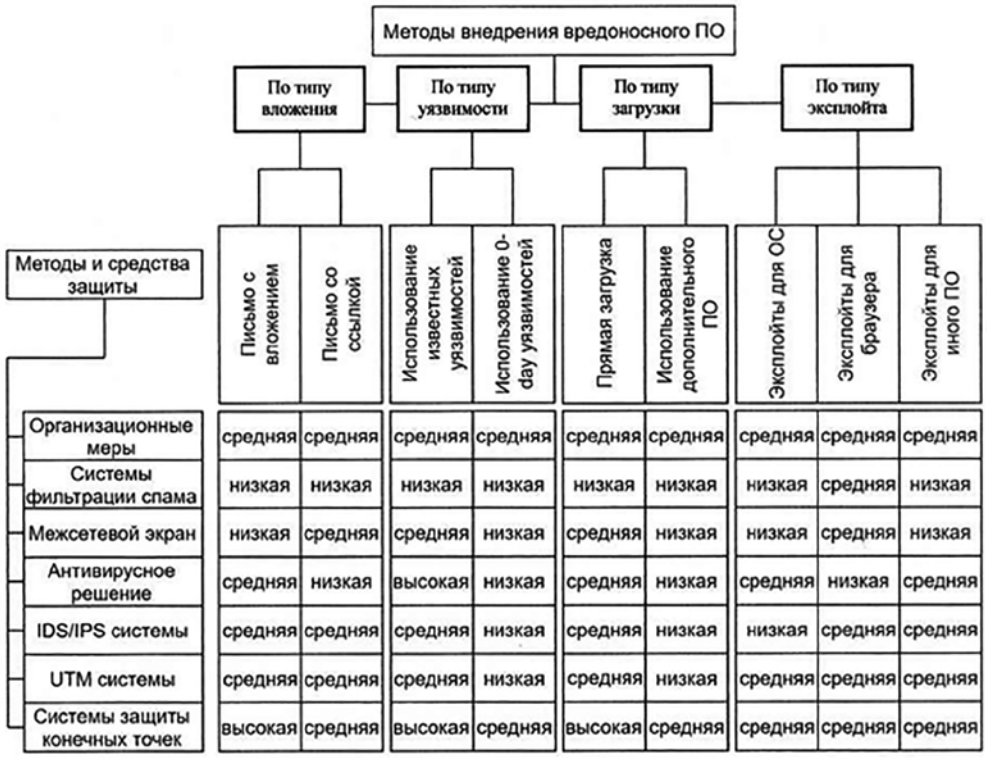


Рис. 4. Экспертная оценка эффективности мер защиты
(Fig. 4. Effectiveness of protection measures)

В табл. 1 представлена экспертная оценка эффективности и сложности внедрения мер защиты. Организационные меры, как видно, имеют наибольшую сложность внедрения.

Таблица 1. Экспертная оценка эффективности и сложности внедрения мер защиты

	Эффективность (в порядке убывания)	**Сложность внедрения (в порядке возрастания)**
1	Системы защиты конечных точек	Антивирусные решения
2	Организационные меры	Системы фильтрации спама
3	UTM системы	Межсетевые экраны
4	IPS/IDS системы	UTM системы
5	Антивирусные решения	IPS/IDS системы
6	Межсетевые экраны	Системы защиты конечных точек
7	Системы фильтрации спама	Организационные меры

Заключение

В целом был проведен анализ существующих методов и средств защиты, в результате которого произведена оценка их способности противостоять современным методам внедрения вредоносного ПО, после чего даны рекомендации по построению эффективной системы защиты. Приведенные рекомендации помогут выбрать меры защиты от целевого фишинга при проектировании защиты внешнего периметра организации.

В будущих исследованиях планируется исследование, сравнение и апробация программ для тестирования устойчивости к целевому фишингу (например, Gophish или SendPulse), а также более подробное исследование применяемых для фишинга уязвимостей.

СПИСОК ЛИТЕРАТУРЫ:

1. High-Tech Crime Trends 2017 [Электронный ресурс] // Отчет Group-IB. – Режим доступа к ресурсу URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
2. Актуальные киберугрозы 2017 года [Электронный ресурс] // Отчет Positive Technologies. – Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (дата обращения: 14.03.18).
3. Meicong Li, Wei Huang. The Study of APT Attack Stage Model [Электронный ресурс]. – Режим доступа к ресурсу URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (дата обращения: 18.03.18).
4. Анатомия таргетированной атаки [Электронный ресурс] // KasperskyLab. – Режим доступа к ресурсу URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 15.03.18).
5. B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges [Электронный ресурс]. //— Режим доступа к ресурсу URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (дата обращения: 25.03.18).
6. Spear-Phishing Attaks. Why they are successful and how to stop them. [Электронный ресурс] // Отчет FireEye.– Режим доступа к ресурсу URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (дата обращения: 25.03.18).
7. Как социальная инженерия открывает хакеру двери в вашу организацию. [Электронный ресурс] // Отчет Positive Technologies. – Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (дата обращения: 16.04.2018).
8. Актуальные киберугрозы 2017 – Тренды и прогнозы [Электронный ресурс] // Отчет Positive Technologies.– Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (дата обращения: 15.03.18).
9. Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks [Электронный ресурс]. — Режим доступа к ресурсу URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (дата обращения: 16.04.2018).
10. Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. [Электронный ресурс] // Отчет Recorded Future. — Режим доступа к ресурсу URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (дата обращения: 16.04.2018).

11. Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. [Электронный ресурс] // Отчет Recorded Future.– Режим доступа к ресурсу URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (дата обращения: 16.04.2018).
12. New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016. [Электронный ресурс] // Отчет Recorded Future. – Режим доступа к ресурсу URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (дата обращения: 16.04.2018).
13. Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing [Электронный ресурс]. – Режим доступа к ресурсу URL: https://dl.acm.org/citation.cfm?id=3025831(дата обращения: 16.04.2018).
14. Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks [Электронный ресурс]. – Режим доступа к ресурсу URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (датаобращения: 16.04.2018).
15. Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., Vol. 8, No. 3, 2015, p. 230 – 248.
16. Журин С.И. Основы противодействия инсайдерским угрозам. Учебное пособие. МИФИ 2014. 262 стр.

REFERENCES:

[1] High-Tech Crime Trends 2017. Group-IB Report. – URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
[2] Topical Cyber-threats 2017. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (Accessed: 14.03.18).
[3] Meicong Li, Wei Huang. The Study of APT Attack Stage Model. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (Accessed: 18.03.18).
[4] Targeted Attack Anatomy. Kaspersky Lab. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (Accessed: 15.03.18). (in Russian).
[5] B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges. – URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (Accessed: 25.03.18).
[6] Spear-Phishing Attacks. Why they are successful and how to stop them. FireEye Report. – URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (Accessed: 25.03.18).
[7] How social engineering opens a door to your organization. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (Accessed: 16.04.2018). (in Russian).
[8] Topical Cyberthreats 2017— Trends and forecasts. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (Accessed: 15.03.18). (in Russian).
[9] Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (Accessed: 16.04.2018).
[10] Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. RecordedFuture Report. – URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (Accessed: 16.04.2018).
[11] Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. RecordedFuture Report. — URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (Accessed: 16.04.2018).
[12] New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.] Recorded Future Report. – URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (Accessed: 16.04.2018).
[13] Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. – URL: https://dl.acm.org/citation.cfm?id=3025831(Accessed: 16.04.2018).
[14] Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (Accessed: 16.04.2018).
[15] Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., Vol. 8, No. 3, 2015, p. 230 – 248.
[16] Zhurin S.I. Basics of countermesuares against insider threats. Tutorial for students. MEPhI, 2014. p. 262.

Поступила в редакцию –07 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received –August 07, 2018. The final version – November 01, 2018.

Олег В. Казарин[1,2]
[1]Институт проблем информационной безопасности МГУ имени М.В. Ломоносова,
Мичуринский просп., 1, г. Москва, 119192, Россия
[2]Институт информационных наук и технологий безопасности РГГУ,
ул. Кировоградская, 25, корп. 2, г. Москва, 117534, Россия
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

СОКРЫТИЕ КООРДИНАТ В ОБОБЩЕННОЙ ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.10

Аннотация. В связи со стремительным развитием систем автопилотируемого транспорта (беспилотных автомобилей, беспилотных летательных аппаратов – дронов) все более актуальной становится задача предотвращения столкновений (задача об опасной близости), тем более в условиях большого количества участников движения и его интенсивности. Если появляется злоумышленник, способный контролировать одного или нескольких участников движения, стратегией которого является создание аварийной ситуации на дороге в виде столкновений беспилотных автомобилей, например, то возникает и необходимость защищаться от такого злонамеренного поведения. Одним из вариантов такой защиты является использование для решения этой прикладной задачи концепции многосторонних конфиденциальных вычислений, в том числе и потому, что будущие системы автопилотирования предполагают в некоторой локальной зоне управления движением возможность взаимодействия участников по схеме «каждый – с – каждым», что является необходимым условием для систем многосторонних конфиденциальных вычислений в условиях разного рода несанкционированных действий.

В отличие от ранее опубликованных результатов с использованием указанной концепции в модели с так называемым получестным противником в настоящей статье впервые предлагаются некоторые решения по защите участников движения от злонамеренного противника, который, раскрыв координаты движущихся объектов, пытается осуществить их столкновение, а также рассматривается расширение этой задачи на трехмерное измерение. В то же время показывается, что при реализации указанных систем на практике, скорее всего, возникнут ситуации, которые не решаются только математическими методами. Существует большой пул проблем, которые должны решаться различными организационно-техническими и управленческими методами. Тем не менее перспективы использования методов доказуемо безопасного сокрытия координат подобного типа выглядят, на взгляд автора, вполне привлекательными для специалистов в области информационной безопасности, связи, транспорта, распределенных систем.

Ключевые слова: системы автопилотируемого транспорта, сокрытие географических координат, конфиденциальные вычисления, конфиденциальное вычисление функции, двусторонние и многосторонние протоколы конфиденциальных вычислений.

Для цитирования: КАЗАРИН, Олег В. СОКРЫТИЕ КООРДИНАТ В ОБОБЩЕННОЙ ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 108-117, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1165>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.10.

Oleg V. Kazarin[1,2]
[1]Institute of Information Security Issues, Lomonosov MSU,
Michurinsky Pr., 1, Moscow, 119192, Russia
[2]Institute for Information Sciences and Security Technologies, RSUH,
Kirovogradskaya St., 25, bidg 2, Moscow, 117534,
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

Coordinate hiding in solving the generalized dangerous proximity problem
DOI: http://dx.doi.org/10.26583/bit.2018.4.10

Abstract. In connection with the rapid development of autopilot transportation systems (driverless cars, unmanned aerial vehicles – drones) all the more urgent becomes the problem of collision avoidance (the problem of dangerous proximity), especially in conditions of a large number of members of the traffic and its high intensity. If there is an attacker who is able to control one or more participants in the traffic, which strategy is to create an emergency on the road or collisions of unmanned vehicles there is a need to protect against such malicious behavior. One of the options of such protection is the use of the concept of multilateral confidential calculations to solve this particular problem. The future autopilot systems assume in some local traffic control zone the possibility of interaction of participants according to the "everyone-with-everyone" scheme, which is a necessary condition for multilateral confidential computing systems in conditions of various unauthorized actions.

In contrast to the previously published results using this concept in the model with the so-called semi-honest enemy, this article for the first time proposes some solutions to protect the traffic participants from the malicious actor, who, having revealed the coordinates of moving objects, tries to drive them to collision. It is also considered the expansion of this problem to three dimensions. At the same time, it is shown that the implementation of these systems in practice, most likely, does not help to avoid the problematic situations that are not solved only by mathematical methods. There is a large set of problems that must be solved by various organizational, technical and managerial methods. Nevertheless, the prospects of using the methods of provably safe coordinate hiding look, in the author's opinion, quite attractive for experts in the field of information security, communications, transport, and distributed systems.

Keywords: autopilot transport systems, geographic coordinates hiding, secure computation, secure function evaluation, two-party and multi-party protocols of secure computation.

For citation: KAZARIN, Oleg V. Coordinate hiding in solving the generalized dangerous proximity problem. IT Security (Russia), [S.l.], v. 25, n. 4, p. 108-117, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1165>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.10.

1. Введение и неформальная постановка задачи исследования

Задача об опасной близости возникает сегодня в авиации, на автомобильном, водном и железнодорожном транспорте. Еще более актуальной она станет уже в недалеком будущем – при реализации систем управления беспилотными автомобилями, беспилотными летательными аппаратами, безэкипажными надводными и подводными судами. Предотвращение столкновений движущихся объектов – это сложный, распределенный организационно-технологический процесс между различными участниками движения. Особую управленческую проблематичность такому процессу придают непреднамеренные и тем более злонамеренные деструктивные информационно-технические воздействия на этот процесс. Решение таких задач ведется на разных направлениях, в том числе и на научном.

В этом случае может анализироваться следующая проблемная ситуация. Рассматриваются два типа движущихся точечных объектов: *объект-запрос* (или просто – *запрос*) движется снизу-вверх (с юга на север) в прямоугольнике и *объект-данные* (или просто – *объект*) движутся слева-направо (с запада на восток) в этом же прямоугольнике [1 – 3]. При этом предположим, что траектории объектов, движущихся в одном из этих направлений внутри прямоугольника, не пересекаются. *Задача об опасной близости* (или *задача о предотвращении столкновений*) заключается в перечислении для каждого запроса тех и только тех объектов, которые будут находиться в некоторый момент времени в процессе своего движения на расстоянии не более, чем заданное расстояние r, где r – радиус круга с центром, представляющим собой движущийся объект (см. рис. 1). На рис. 2 представлено расширение этой задачи на трехмерное пространство.

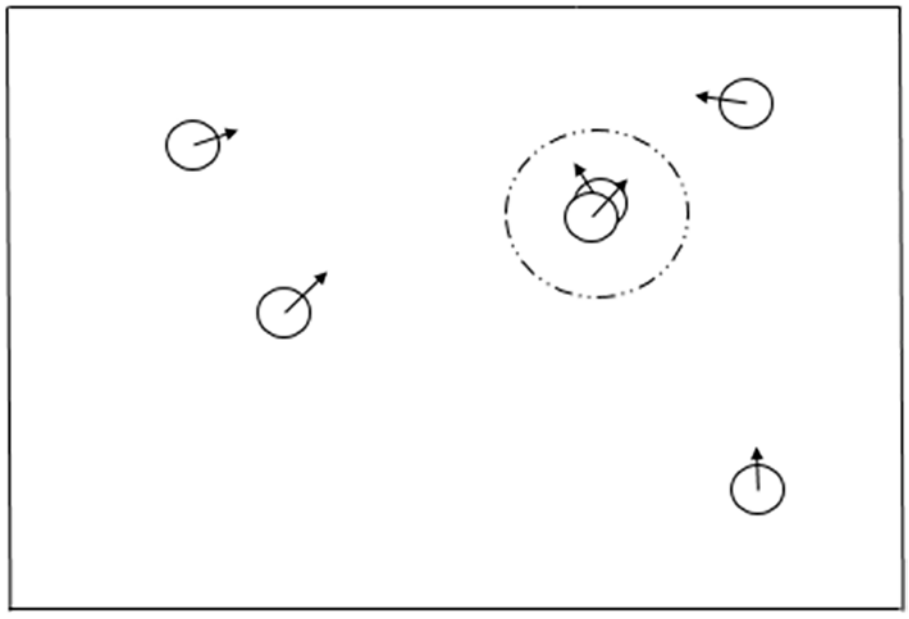


Рис. 1. Иллюстрация движения точечных объектов в двухмерной задаче об опасной близости
(Fig. 1. Illustration of a movement of point objects in a two-dimensional problem on dangerous closeness)

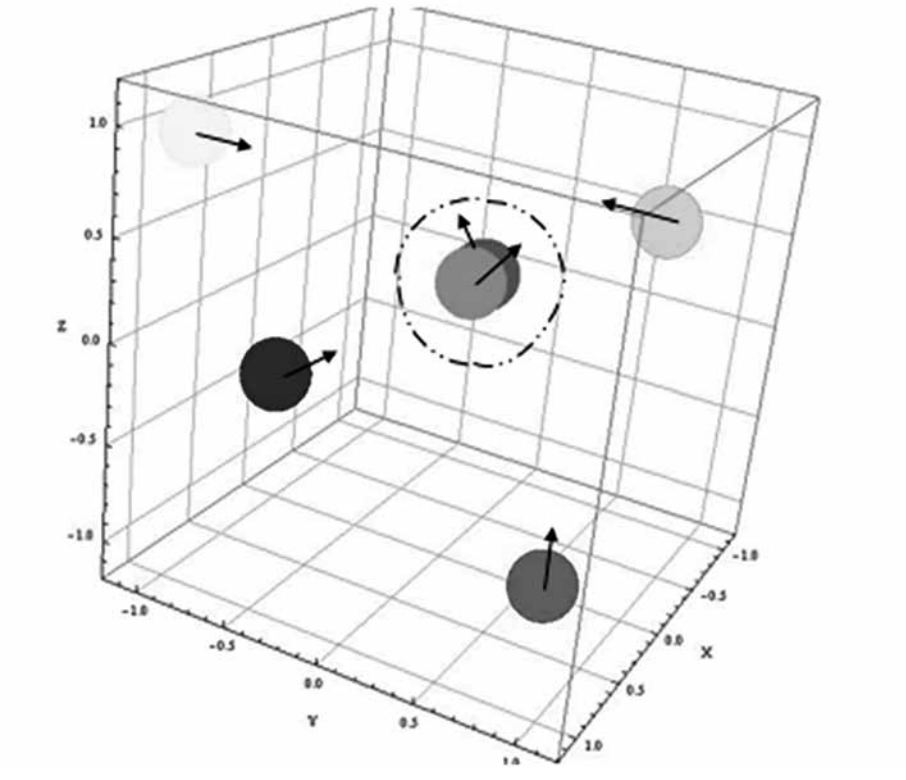


Рис. 2. Иллюстрация движения точечных объектов в трехмерной задаче об опасной близости
(Fig. 2. Illustration of a movement of point objects in a three-dimensional problem on dangerous closeness)

Предположим далее, что при движении объектов и запросов нам необходимо обеспечить не только невозможность их столкновения, но и *обеспечить конфиденциальность местоположения объектов и запросов* при этом. Для этого может использоваться концепция *многосторонних конфи-*

денциальных вычислений, суть которых может сводиться к *следующей постановке задачи*. Имеется процесс интерактивного взаимодействия (распределенный протокол взаимодействия) объектов и запросов между собой, для управления которым необходимо реализовать функциональность f,[1] с выполнением условий:

• *корректности*, когда f должна обеспечивать невозможность столкновения, даже если некоторая ограниченная часть объектов и запросов отклоняется от предписанных им действий;

• *конфиденциальности*, когда в результате взаимодействия ни один из объектов и запросов не получает никакой не предназначенной ему информации о других объектах и запросах.

Например, злоумышленник, контролирующий некоторую ограниченную часть объектов и запросов, получив такую информацию, предположим, координаты движения каких-либо объектов и запросов, может несанкционированно повлиять на процесс их взаимодействия с целью создания конфликтной ситуации (столкновения) с их участием.

2. Основные определения, модели, используемые протоколы

Основные определения, модели, используемые протоколы, формальная постановка задачи об опасной близости, в том числе и в конфиденциальном сценарии, а также основные подходы к доказательству безопасности протоколов (распределенных алгоритмов) ее решения приведены в работах [4 – 7]. Далее будут даны необходимые определения для решения задачи конфиденциального вычисления манхэттенского расстояния и конфиденциального вычисления пересечения двух окружностей. Будут также рассмотрены модели получестных и злонамеренных противников и сценарии их поведения при решении указанных задач.

Решение *задачи конфиденциального вычисления манхэттенского расстояния* можно описать в следующей постановке. Есть два участника, имеющие у себя конфиденциальные координаты (x_1,y_1) и (x_2,y_2). Обоим задано расстояние – ρ_m. Цель протокола, который далее будет обозначаться как протокол **ПВМР**, состоит в решении задачи, выполняется ли условие: $|\rho_m-|x_1-x_2||<|y_1-y_2|$, без раскрытия значений этих координат. Обозначается это следующим образом: b=**ПВМР**$((x_1,y_1),(x_2,y_2))$, где b=true, условие выполняется, b=false, в противном случае. В основе этого протокола лежит протокол Яо – протокол *конфиденциального вычисления функции сравнения двух чисел* [8].

Решение задачи конфиденциального вычисления пересечения двух окружностей, которая решается посредством двустороннего интерактивного протокола, было предложена в работе [9]. Протокол можно описать в следующей постановке. Есть два участника, имеющие у себя конфиденциальные координаты центров окружностей (x_1,y_1) и (x_2,y_2). Обоим задан радиус этих окружностей – ρ_o.[2] Цель протокола, который далее будет обозначаться как протокол **ПП2О**, состоит в решении задачи, имеют ли окружности с этими координатами их центров пересечение без раскрытия значений этих координат. Обозначается далее это следующим образом: b=**ПП2О**$((x_1,y_1),(x_2,y_2))$, где b=true, окружности с этими центрами пересекаются, b=false, в противном случае. В основе этого протокола лежит протокол Ду - Аталлаха – *протокол конфиденциального вычисления скалярного произведения 2-х векторов* [10].

В *модели получестного противника (Semi - Honest Adversary)* противник контролирует некоторых участников протокола и далее участники точно следуют транскрипции протокола, за некоторым исключением, – получестные участники протокола могут записывать и сохранять информацию на всех промежуточных этапах вычислений и попытаться что-либо узнать о конфиденциальном входе «контрагента» из нее (хотя в случае честного поведения они должны стирать такую информацию).

В модели *злонамеренного противника (Malicious Adversary)* противник контролирует некоторых участников протокола, которые независимым образом отклоняются от предписанных инструкций протокола.

---

[1] Функциональность, обеспечивающая невозможность столкновения.

[2] В оригинальной работе [9] – для каждой из окружностей задан свой радиус ρ_1 и ρ_2.

В случае успешной стратегии получестного противника, который получил контроль над одним или несколькими[3] из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) взаимодействия, нарушив таким образом правила обеспечения конфиденциальности местоположения объектов и запросов (если они установлены). В случае успешной стратегии злонамеренного противника, который получил контроль над одним или несколькими из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) и таким образом повлияет на скорость движения подконтрольного(-ых) ему объектов и запросов с тем, чтобы создать опасную близость (столкновение).

Протоколы конфиденциальных вычислений должны противостоять и первому, и второму типу противников, в том числе и при многостороннем взаимодействии с большим количеством участников движения и его интенсивностью и с установленным порогом на количество участников движения, находящихся под контролем противника.

3. Протоколы конфиденциального предотвращения столкновения КПС

3.1 Описание двустороннего протокола **КПС**

Протокол π далее именуется протоколом конфиденциального предотвращения столкновения и обозначается **КПС**, а по сложившейся в современной криптографии традиции участники протоколов в двухстороннем сценарии именуются **A** (Алисой) и **B** (Бобом).

В протоколе **КПС** необходимо определить, существует ли момент времени t, удовлетворяющий b=**ППО**$((x_1,y_1),(x_2,y_2))$ или b=**ПВМР**$((x_1,y_1),(x_2,y_2))$, где b=true, без раскрытия Бобу координаты $(x_{\mathbf{A}},y_{\mathrm{A}})$ и, соответственно, Алисе координаты $(x_{\mathrm{B}},y_{\mathrm{B}})$**.**

Протокол **КПС**

Конфиденциальный вход Алисы: $(x_{\mathbf{A}},y_{\mathrm{A}})$; конфиденциальный вход Боба: $(x_{\mathrm{B}},y_{\mathrm{B}})$.

Следующие шаги выполняются l раз, где шаг устанавливается каким-либо очевидным образом между моментом появления **A** на границе зоны (на границе прямоугольника) и моментом пересечения траектории движения **B** плюс один шаг.

1. Алиса и Боб выполняют протокол **ППО** (или протокол **ПВМР**) со своими входами $(x_{\mathbf{A}},y_{\mathrm{A}})$ и $(x_{\mathrm{B}},y_{\mathrm{B}})$ соответственно.[4]

2. Как только выходом протокола **ППО** (или протокол **ПВМР**) становится значение «true», то существует момент времени t, при котором возможно столкновение.

3. Если такой момент t существует, то присвоить b:=true, в противном случае b:=false.

Выход протокола. Если b=true, выдать «команду на понижение скорости» Алисе, если b=false, в противном случае.

3.2 Решение задачи об опасной близости для многих участников

Пусть множество J состоит из пронумерованных объектов, находящихся в опасной близости: $J(\rho,q,V)=\{o_i\in V|\exists t$: true=**ППО**$((x_i,y_i),(x_j,y_j))$, $i,j=1,2,...\}$.. *Библиотека* V является множеством объектов, находящихся в текущий момент времени t внутри рассматриваемого прямоугольника. Тройку (ρ,q,V) будем называть *задачей об опасной близости для многих участников*.

Алгоритмом A решения задачи об опасной близости будем называть совокупность процедур поиска, вставки и удаления в множестве *J. Вставка* объекта o в множество J является такое его преобразование, при котором библиотека V преобразуется в $V\cup\{o\}$ и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V). А *удаление* объекта o из множества J является такое его преобразование, при котором библиотека V преобразуется в $V\setminus\{o\}$ и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V).

[3] Числом не более заданного порога.

[4] Если x и y представлены географическими координатами, то $0<x<360$ и $0<y<180$ (с точностью до 1 градуса) или $0<x<3600000$ и $0<y<1800000$ (с точностью до 1 секунды).

Формулировку задачи об опасной близости в терминах информационных графов, можно найти в [1], где информационный граф рассматривается как модель данных с возможностью поиска, вставки и удаления в нем. В этой же работе предлагаются алгоритмы решения задачи об опасной близости путем ее сведения к задаче одномерного интервального поиска и доказываются утверждения о существовании таких алгоритмов *с логарифмической сложностью операций поиска, вставки и удаления.*

Таким образом, решение задачи об опасной близости для многих объектов сводится к реализации операций поиска, вставки и удаления над множеством J с библиотекой V (решению задачи одномерного интервального поиска в информационном графе), а конфиденциальность координат этих объектов по-прежнему можно обеспечить использованием протокола **КПС**.

3.3 Решение задачи об опасной близости для разных измерений

Цель протокола для решения задачи об опасной близости на прямой состоит в решении задачи, выполняется ли условие: $|x_1-x_2|<\rho_m$, не раскрывая значения координат. В этом случае такая задача может ставиться в двухмерном пространстве, если на плоскости объекты движутся строго вдоль одной из осей.

В случае трехмерного пространства ставится задача, выполняется ли условие: $|x_1-x_2|+|y_1-y_2|+|z_1-z_2|<\rho_m$, не раскрывая значения координат. Здесь также можно свести эту задачу к одномерному или двумерному случаю, если предположить, что объекты движутся строго в одной плоскости и вдоль двух или одной осей соответственно (для двумерного случая – см. рис. 3).

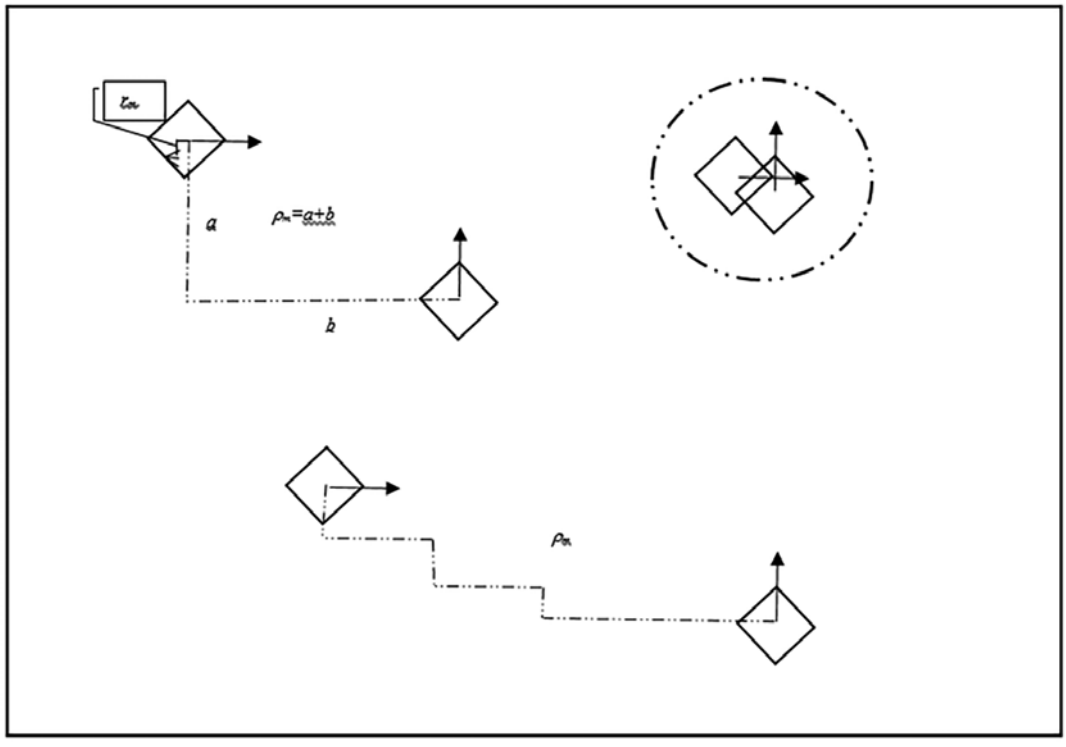


Рис. 3. Иллюстрация вычислений расстояний ρ_m для объектов с радиусом по Манхэттену r_m
(Fig. 3. Illustration of computation of distances ρ_m for objects with a Manhattan radius r_m)

Протокол **КПС** позволяет решать эти задачи, а протокол **ПП2О**, в случае существования его расширения на 3-мерный случай (на поверхность шара, на сферу), также позволит решать задачу об опасной близости «не через» вычисления манхэттенского расстояния для поверхности куба.

4. Варианты поведения злонамеренного противника в задаче об опасной близости

Обобщенное описание модели злонамеренного противника в конфиденциальных вычислениях может быть следующим [11, 12]. Рассматривается сеть взаимодействующих участников вычислений. Некоторые из них могут в некоторый момент времени приостановить отправку своих сообщений. В то же время предполагается, что они продолжают получать сообщения и могут выдавать «некую информацию» в свои выходные каналы. В другом варианте злонамеренного поведения нечестные участники могут произвольным образом сотрудничать друг с другом с целью получения необходимой для них информации или с целью нарушения процессов вычислений и взаимодействия. Они также могут «объединять» свои входы и изменять их.

Противники могут быть *статическими* и *динамическими*. *Статическим противником* является противник, который «сотрудничает» с фиксированным количеством нечестных участников («подкупленных» противником). При действиях *динамического противника* количество нечестных участников может меняться (в том числе непредсказуемым образом). Множество статических нечестных участников фиксировано в начале и процессе вычислений, множество динамических нечестных участников может меняться, как может меняться и характер их поведения.

Кроме того, противник может быть *пассивным* и *активным*, а также с *априорными* и *апостериорными* протокольными и раундовыми действиями. Пассивный противник не может изменять сообщения, циркулируемые в сети. Активный противник может знать все о внутренней конфигурации сети, может читать и изменять все сообщения нечестных участников и может выбирать сообщения, которые будут посылать нечестные участники при вычислениях. Активный динамический противник может в начале каждого раунда «подкупить» несколько новых участников. Таким образом, он может изучить информацию, получаемую ими в текущем раунде, и принять решение «подкупить» ли ему нового участника или нет. Такой противник может собирать и изменять все сообщения от нечестных участников к честным. Действия аналогичного характера активный противник может выполнить не только в течение раунда (в его начале и конце), но и до начала выполнения протокола и после его завершения. Противник называется *t-противником*, если он сотрудничает с t нечестными участниками.

В данной работе исследуются *следующие сценарии поведения злонамеренного противника* в задаче об опасной близости. Участники движения, контролируемые противником, могут:

- отказаться участвовать в протоколе, когда он инициируется, или преждевременно его прервать;
- отклоняться от инструкций протокола;
- изменять свои координаты или участвовать в протоколе с координатами других участников;
- пытаться раскрыть конфиденциальные координаты честных участников.

В конце концов, задача злонамеренного противника заключается в создании опасной ситуации посредством столкновения при движении участников взаимодействия.

Предположительно, используя представленные здесь протоколы для модели получестного противника, можно создавать протоколы, решающие задачи противодействия злонамеренному t-противнику и для случая с двумя участниками, и для случая со многими участниками. В случае обнаружения точечных объектов, подконтрольных последнему, они также заносятся в множество J для библиотеки V, даже, если не находятся в опасной близости.

В работах [13 – 15], например, приведены протоколы, – аналоги протокола Яо, в которых одна из сторон нарушает корректность протокола, отклоняясь некоторым образом от правильных его инструкций, а другая сторона обнаруживает это с высокой вероятностью. При этом доказательство безопасности таких вычислений может строиться через доказательство (вычислительной) неразличимости вычислений в идеальной модели (в модели с полностью доверенной дополнительной стороной) и реальной модели вычислений [11, 12].

5. Математический и физический миры

Рассматриваемые выше модели конфиденциальных вычислений описывают идеализированную («математическую») ситуацию в задаче об опасной близости. В физическом, реальном мире естественно все намного сложнее. Вот только несколько вопросов, на которые приходится отвечать в случае, если точечные объекты – это беспилотные автомобили в будущей системе автопилотирования:

- как обеспечить конфиденциальность координат беспилотного автомобиля, если сам автомобиль, скорее всего, будет иметь государственный номер, а следовательно, можно однозначно идентифицировать его владельца;
- как обеспечить эту конфиденциальность, если в локальной зоне управления большинства городов есть система видеонаблюдения[5] (даже цвет и марка автомобиля, могут также дать существенную информацию об автомобиле)[6];
- в случае использования в качестве основного криптографического примитива схем шифрования с открытым ключом [7], как реализовать оперативную «онлайн» инфраструктуру открытых ключей в локальной зоне управления движением;
- насколько значение предиката b=**ПВМР**$((x_1,y_1),(x_2,y_2))$ является существенным знанием для злоумышленников, говорящим о нахождении участников движения на расстоянии друг от друга, менее чем ρ_m, и позволяющим создать опасную ситуацию на дороге;
- существуют ли другие (некриптографические) методы решения исследуемой задачи, например, введение цифровых псевдонимов для участников или значительное намеренное огрубление результатов измерений координат местоположения или что-то подобное) и др.

Ответы на эти и другие подобного рода вопросы, на взгляд автора, являются безусловно интересными и заслуживающими пристального внимания специалистов в области информационной безопасности, связи, транспорта, распределенных систем.

Заключение

Представленные здесь соображения по решению задачи сокрытия координат участников взаимодействия позволяют «двигаться» в направлении создания практических протоколов для многосторонних конфиденциальных вычислений в модели со злонамеренным противником[7] для двух- и трехмерного пространства (то есть, с обеспечением конфиденциальности 2-х и 3-х географических координат точечных объектов.

При «перемещении» предлагаемых решений в реальный физический мир, скорее всего, появится множество проблем, связанных с практической реализацией протоколов конфиденциальных вычислений для (пока) гипотетических информационных систем подобного типа[8], которые наверняка возникнут вместе с конкретной моделью противника, конкретной технической реализацией протоколов в конкретной информационной системе и конкретной физической среде.

---

[5] Таким образом, противник, «подкупив», например, Боба и «взломав» систему видеонаблюдения, может получать конфиденциальные входы Алисы, а следовательно, может попытаться получить секретный ключ используемой схемы гомоморфного шифрования [7] и делать дальше «все, что ему вздумается». Или без «вскрытия» протокола **КПС** Боб может создать опасную ситуацию для Алисы, имея в своем распоряжении ее конфиденциальные входы, полученные от «взломанной» системы видеонаблюдения и т.д. и т.п.

[6] В этом смысле интересна система автопилотируемых летательных аппаратов (дронов), которые уже сейчас трудно поддаются визуальной идентификации.

[7] Тем более что теоретические результаты в области конфиденциальных вычислений предполагают (при некоторых условиях) возможность построения компиляторов, которые преобразуют любые протоколы для модели с получестным противником в эквивалентные протоколы для двух моделей со злонамеренным противником. См. аргументацию в [12, § 3.6].

[8] Подобные системы все чаще называются киберфизическими.

СПИСОК ЛИТЕРАТУРЫ:

1. Скиба Е. А. Логарифмическое решение задачи об опасной близости // Интеллектуальные системы. 2007. 11: 1 – 4. С. 693 – 719.
2. Снегова Е. А. Критерий сводимости задачи об опасной близости к одномерному интервальному поиску // Дискретная математика. 2011. Т. 23. Вып. 5. С. 138 – 159.
3. Снегова Е. А. Сложность задачи о предотвращении столкновении // Автореферат диссертации на соискание ученой степени кандидата физико-математических наук. МГУ имени М.В. Ломоносова, 2012. URL: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (дата обращения: 20.06.2018).
4. Казарин О. В. Практически реализуемые системы многосторонних конфиденциальных вычислений // Защита информации. INSIDE. 2016. № 3. С. 36 – 42.
5. Казарин О.В. О возможности сокрытия местоположения абонента сотовой связи с использованием методов конфиденциальных вычислений // Вопросы защиты информации. 2016. № 1. С. 39 – 47.
6. Казарин, Олег. Конфиденциальные вычисления в задаче об опасной близости. Безопасность информационных технологий, [S.l.], v. 24, n. 1, p. 39-48, apr. 2017. ISSN 2074-7136. Доступно на: . Дата доступа: 04 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.1.05.
7. Казарин О.В. Многосторонние конфиденциальные вычисления в задаче об предупреждении столкновений // Вестник компьютерных и информационных технологий. 2017. № 6. С. 50 – 56.
8. Yao A.C. Protocols for secure computations (extended abstract) // Proc. of 23-rd IEEE Symp. on Foundations of Computer Science. 1982. P. 160 – 164.
9. Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles // Journal of Information & Computational Science. 2011. № 8. P. 29 – 40.
10. Du W., Attalach M. J. Privacy-preserving cooperative scientific computations // Proceeding of the 2002 Workshop on New Security Paradigms – NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press. P. 127 – 135.
11. Казарин О.В. Теория и практика защиты программ. Доступно на: <http://ru.b-ok.org/book/629866/b75031>. Дата доступа: 19 october 2018.
12. Казарин О. В. Методология защиты программного обеспечения. – М.: МЦНМО, 2009. – 464 с.
13. Kreuter B., Shelat A., Shen C. Billion-gate secure computation with malicious adversaries// Proceedings of USENIX Security'12. 2012. P. 285 – 301.
14. Lindell Y., Pinkas B. An efficient protocol for secure two-party computation in the presence of malicious adversaries // Proceedings of the 26-th Annual International Conference on Advances in Cryptology –EUROCRYPT'07. 2007. P. 52 – 78.
15. Mohassel P., Franklin M. Efficiency tradeoffs for malicious two-party computation // Proceedings of Public Key Cryptography-PKC'06. 2006. P. 458 – 473.

REFERENCES:

[1] Skiba E.A. Logarithmic solution of the problem on dangerous closeness. Intellektual'nye sistemy, 2007, Vol. 11: 1–4. pp. 693–719. (in Russian).
[2] Snegova E.A. A criterion of reduction of the problem on dangerous closeness to the one-dimensional interval search. Diskretnaya matematika, 2011, Vol. 23, no. 5, pp. 138 – 159. (in Russian).
[3] Snegova E.A. Complexity of the problem on dangerous closeness. PhD thesis. Moscow: Izdatel'stvo MGU im. M. V. Lomonosova, 2012. Available at: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (accessed: 20.06.2018). (in Russian).
[4] Kazarin O.V. Real-life systems of multy-party secure computation. Zashhita informatsii. INSIDE, 2016, no 3, pp. 36 – 42. (in Russian).
[5] Kazarin O.V. On the possibility of hiding the geolocation of a subscriber of a cellular network using methods of secure computation. Voprosy zashhity informatsii, 2016, no 1, pp. 39 – 47. (in Russian).
[6] Kazarin, Oleg. Institute of Information Security Issues, Lomonosov MSU. IT Security (Russia), [S.l.], v. 24, n. 1, p. 39-48, apr. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/54>. Date accessed: 04 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.1.05.
[7] Kazarin O.V. Multi-party secure computation in the problem of collisions prevention. Vestnik komp'yuternyh i informacionnyh tekhnologij. 2017. no 6. pp. 50 – 56. (in Russian).

[8] Yao A.C. Protocols for secure computations (extended abstract). Proc. of 23-rd IEEE Symp. on Foundations of Computer Science. 1982. P. 160 – 164.
[9] Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles. Journal of Information & Computational Science. 2011. № 8. P. 29 – 40.
[10] Du W., Attalach M. J. Privacy-preserving cooperative scientific computations. Proceeding of the 2002 Workshop on New Security Paradigms – NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press. P. 127 – 135.
[11] Kazarin O.V. Theory and practice of software protection. Доступно на: <http://ru.b-ok.org/book/629866/b75031>. Дата доступа: 19 october 2018. (in Russian).
[12] Kazarin O.V. Methodology of software protection. – M.: MTSNMO, 2009. – 464 p. (in Russian).
[13] Kreuter B., Shelat A., Shen C. Billion-gate secure computation with malicious adversaries. Proceedings of USENIX Security'12. 2012. P. 285 – 301.
[14] Lindell Y., Pinkas B. An efficient protocol for secure two-party computation in the presence of malicious adversaries. Proceedings of the 26-th Annual International Conference on Advances in Cryptology –EUROCRYPT'07. 2007. P. 52 – 78.
[15] Mohassel P., Franklin M. Efficiency tradeoffs for malicious two-party computation. Proceedings of Public Key Cryptography-PKC'06. 2006. P. 458 – 473.

Поступила в редакцию - 04 июля 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – July 04, 2018. The final version – November 01, 2018.

АННОТАЦИИ

Евгений Б. Белов[1], Владимир П. Лось[2], Анатолий А. Малюк[3]
[1]ФУМО ВО ИБ,
Мичуринский просп., 70, г. Москва, Россия
e-mail: umoib@yandex.ru, https://orcid.org/0000-0003-4854-1220
[2]Центр исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА,
Вернадского просп., 78, г. Москва, Россия
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

ЦИФРОВАЯ ЭКОНОМИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Тенденции развития глобального информационного общества свидетельствуют о возрастании потребности в специалистах, обладающих высокой информационной культурой, в том числе обладающих знаниями и навыками обеспечения информационной безопасности. В Доктрине информационной безопасности Российской Федерации развитие и совершенствование системы соответствующей подготовки кадров заявлено в качестве одного из первоочередных мероприятий по реализации государственной политики в области формирования цифровой экономики. Подготовка кадров в данном случае должна предусматривать два направления – профессиональное и массовое обучение. В свою очередь, профессиональное обучение может быть основным и дополнительным. Основная цель массового обучения – формирование в обществе культуры информационной безопасности, недостаточный уровень которой отмечен в Доктрине информационной безопасности как одна из основных информационных угроз. Исходя из этого, в статье рассматриваются все актуальные сегодня проблемы как профессионального, так и массового обучения. При этом подчеркивается важность реализации парадигмы непрерывного образования (образования в течение всей жизни). Таким образом, основная цель данной статьи заключается в раскрытии важнейших проблем обеспечения непрерывного процесса формирования современной культуры информационной безопасности с использованием возможностей всех звеньев образовательной системы.
Ключевые слова: информационная безопасность, кадровое обеспечение отрасли информационной безопасности, осведомленность по вопросам информационной безопасности, профессиональное и массовое обучение в области информационной безопасности, культура информационной безопасности.

Владимир И. Будзко, Дмитрий А. Мельников
Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, г. Москва, 119333, Россия
e-mail: vbudzko@ipiran.ru, https://orcid.org/ 0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

ИСТОРИЧЕСКИЙ РАКУРС ТЕХНОЛОГИИ «BLOCKCHAIN». «ВСЁ НОВОЕ – ХОРОШО ЗАБЫТОЕ СТАРОЕ»

Аннотация. Блокчейн-технология (БЧ-технология) представляет неизменяемые распределённые системы цифровых реестров без центрального хранилища/репозитария, как правило, не имеющие единого центра управления. В настоящее время существует большой ажиотаж вокруг использова-

ния БЧ-технологии, хотя сама технология, с одной стороны, многим ещё не совсем понятна, а с другой (и это главное) – не нова. Поверхностное представление о БЧ-технологии как о феномене с «волшебными свойствами» приводит к многочисленным прогнозам о возможности революционных преобразований на основе её применения целых отраслей экономики и прежде всего, в кредитно-финансовой сфере (КФС). В связи с этим в настоящей статье представлены систематизированный анализ, история возникновения БЧ-технологии, ведущая своё начало с международных стандартов ISO 7498-2 от 1989 года и ITU-T X.800 от 1991 года. Дано краткое неформальное определение БЧ-технологии, рассмотрены ее основные принципы и компоненты, среди которых криптографические однонаправленные функции (ОНФ), транзакции, адреса и их извлечение, реестры, блоки, операции с последовательностями блоков. Представление БЧ-технологии как последовательности блоков, связанных на основе известных способов обеспечения целостности данных с использованием ассиметричной криптографии, позволяет сделать вывод о возможности только эволюционного развития ее применений, хотя и быстрыми темпами в масштабе реального времени, что является характерной особенностью современного этапа становления и всех остальных разновидностей IT-технологий. В заключение обращено внимание на необходимость проведения дополнительных исследований оценки защищённости и надёжности БЧ-технологии в аспекте оценки перспектив её применения в конкретных бизнес-приложениях и системах критической информационной инфраструктуры.

Ключевые слова: блокчейн, цифровой реестр, криптовалюта, электронный кошелёк, электронная подпись, транзакция, целостность виртуального соединения, открытый ключ, однонаправленная функция, компендиум, сертификат, аутентификация, неотказуемость.

Антон А. Конев[1], Татьяна Е. Минеева[1], Михаил Л. Соловьёв[2],
Александр А. Шелупанов[1], Мария П. Силич[1]

[1]Томский государственный университет систем управления и радиоэлектроники,
просп. Ленина, 40, г. Томск, 634050, Россия
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Сибирский государственный университет телекоммуникаций и информатики
ул. Кирова, 86, г. Новосибирск, 630102, Россия
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. При построении системы защиты информации одной из ключевых проблем становится создание комплекта нормативной документации. Регуляторы в сфере обеспечения информационной безопасности определяют перечень необходимой документации в основном применительно к механизмам защиты (аутентификация, антивирусная защита и т.п.) и практически не учитывают этапы жизненного цикла средств защиты информации и персонала организации. В статье предлагается подход к формализации составления перечня процессов управления информационной безопасностью, нуждающихся в регламентации. Данный подход позволяет при формировании политики информационной безопасности учитывать процессы управления персоналом и комплексом программно-аппаратных средств защиты информации, что необходимо для обеспечения высокого уровня защищенности объектов критической информационной инфраструктуры.

Ключевые слова: система защиты информации, жизненный цикл, процессы управления, объект критической информационной инфраструктуры.

Евгений А. Басыня[1, 2]
[1] Новосибирский государственный технический университет,
просп. К. Маркса, 20, г. Новосибирск, 630073, Россия
[2] Научно-исследовательский институт информационно-коммуникационных технологий,
ул. Депутатская, 48, г. Новосибирск, 630099, Россия
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

РАСПРЕДЕЛЕННАЯ СИСТЕМА СБОРА, ОБРАБОТКИ И АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Аннотация. Большинство сетевых инфраструктур государственных учреждений и частных предприятий функционируют на базе стека протоколов TCP/IP, обладающего существенными уязвимостями. В качестве примера стоит привести отсутствие проверки подлинности субъекта взаимодействия в базовых протоколах и технологиях данного стека. Часть уязвимостей можно устранить интеллектуальными функциями управляемого сетевого оборудования: от профилирования доступа до сегментации трафика. Немаловажным звеном защиты выступают комплексные межсетевые экраны, включающие системы обнаружения и предотвращения вторжений. Российскими и зарубежными учеными развиваются методы сигнатурного, эвристического, поведенческого, автомодельного, прогнозируемого и других способов анализа сетевого трафика и идентификации сетевых угроз. Однако предлагаемые решения не дают однозначного результата при использовании оверлейных технологий и криптографических протоколов. Также не уделяется надлежащее внимание обработке, анализу сетевого трафика и логов операционных систем Windows/Linux и приложений. Целью данной работы являлось исследование, разработка и программная реализация распределенной системы сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия. Ключевой задачей ставилось обеспечение объективного мониторинга сетевой информационной безопасности. Дополнительной задачей являлось обеспечение мониторинга работы пользователей персональных компьютеров под управлением операционных систем Windows и Linux. Для решения поставленной задачи была разработана концепция комплексной обработки трафика вычислительной сети и событий информационной безопасности как на стороне сервера, так и на стороне клиента. На обзор вынесен оригинальный сигнатурный и статистический метод составления базы знаний системы посредством тестирования и имитации известных сетевых и локальных атак с отслеживанием реакции операционных систем и приложений в среде виртуализации. Изложен подход к выполнению автоматизированного анализа коррелирующих событий с применением глубокого анализа содержимого пакетов и мониторинга локальной работы пользователей. Предложенное решение успешно апробировано и использовано в качестве одного из модулей обеспечения сетевой информационной безопасности системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, разрабатываемой автором.
Ключевые слова: IDS, IPS, SIEM, анализ событий информационной безопасности, мониторинг работы сети и пользователей.

Анатолий М. Тарасов
Академия управления МВД России,
ул. Зои и Александра Космодемьянских, 8, г. Москва, 125993, Россия
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

СТРУКТУРА И СОДЕРЖАНИЕ КОНВЕНЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

Аннотация. В статье актуализируется проблема противодействия киберпреступлениям на основе консолидации международных усилий в данном направлении наряду с противодействиями тер-

роризму, обороту наркотиков и другими правонарушениями, имеющими трансграничный характер. Приводятся результаты критического анализа структуры и содержания основных положений соответствующей Будапештской конвенции, принятой Советом Европы 23 ноября 2001 г. (ETS № 185). Анализ отражения в Конвенции вопросов организационно-правового регулирования борьбы с компьютерной преступностью проведен в сравнении с соответствующими нормами российского законодательства, в частности по терминологическим аспектам уголовного и уголовно-процессуального права в области компьютерной информации. Особое внимание обращается на критическое рассмотрение вопросов международного сотрудничества в свете новых вызовов и угроз в условиях все возрастающей конфронтации межгосударственных отношений. В заключение обосновывается необходимость принятия соответствующей конвенции Организацией Объединенных Наций с предложениями по содержанию ее основных направлений.
Ключевые слова: Конвенция Совета Европы, правоохранительные и судебные органы, правоохранительная деятельность, киберпреступность, международное сотрудничество, конфиденциальность, компьютерная техника, расследование, программное обеспечение, пароли и коды доступа, детская порнография, авторское право.

Александр Б. Саттаров, Наталья Г. Милославская
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ИЗУЧЕНИЮ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ» И СПОСОБОВ ЗАЩИТЫ ОТ НИХ

Аннотация. Для реализации образовательной программы подготовки магистров по направлению 10.04.01 «Информационная безопасность» под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в НИЯУ МИФИ разработана программная оболочка учебно-лабораторного комплекса (УЛК), предназначенная для изучения сетевых атак типа «Человек посередине». В УЛК смоделированы четыре основные атаки данного типа: UDP Hijacking, Session Hijacking, TCP Hijacking и Bucket brigade attack. В статье представлены два приложения УЛК: приложение преподавателя и приложение студента. Для оценки знаний студентов после выполнения лабораторной работы создан модуль оценки знаний «Тестирование», который включает в себя вопросы для проведения тестирования с помощью программной оболочки УЛК. Составлены методические указания по выполнению лабораторной работы. В рамках дисциплины «Защищенные информационные системы» кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ, реализующих выше указанную программу подготовки магистров, проведена успешная апробация разработанного УЛК. В заключении статьи указаны пути дальнейшего совершенствования УЛК.
Ключевые слова: учебно-лабораторный комплекс, атака типа «Человек посередине», UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.

Елена С. Басан, Александр С. Басан, Олег Б. Макаревич
Южный федеральный университет «ЮФУ»,
Институт компьютерных технологий и информационной безопасности,
ул. Чехова, 2, г. Таганрог, 347922, Россия
e-mail: ebasan@sfedu.ru, http://orcid.org/0000-0001-6127-4484
e-mail: asbasan@sfedu.ru, http://orcid.org/0000-0002-2973-2737
e-mail: obmakarevich@sfedu.ru, http://orcid.org/0000-0003-0066-8564

РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ УЗЛОВ В ГРУППЕ РОБОТОВ*

Аннотация. Данная статья посвящена вопросам обеспечения безопасности в группе мобильных роботов при реализации злоумышленником атак, направленных на свойство доступности информации. Проанализированы основные методы и подходы к обнаружению атак и аномалий для мобильных роботов, выделены основные достоинства и недостатки существующих подходов. Основной целью является разработка метода обнаружения аномального поведения, который позволил бы избежать создания эталонного распределения, либо базы сигнатур, либо правил для группы мобильных роботов. Метод должен в текущих условиях при динамически изменяющейся структуре сети выявлять аномалии. В статье представлен метод обнаружения аномального поведения узла сети на основе анализа параметров: остаточной энергии и сетевой загруженности узлов сети. Проводится анализ поведения отдельных роботов группы относительно отклонения от общего поведения с использованием вероятностных методов. Разрабатываемый метод обнаружения аномального поведения основан на использовании вероятностной оценки событий. Определяются три типа состояний узлов сети, построен граф переходов узла в каждое из состояний, а также определены параметры, влияющие на данные переходы. Разработанный метод демонстрирует высокий показатель обнаружения атаки «отказ в обслуживании» распределенной атаки «отказ в обслуживании» при количестве злоумышленных узлов, не превышающем или незначительно превышающем количество доверенных узлов. А также обеспечивает обнаружение атаки Сивиллы. Проведено экспериментальное исследование, включающее в себя разработку модели, имитирующей группу мобильных роботов, в частности сетевое взаимодействие между роботами. Разработаны, реализованы сценарии атак для группы мобильных роботов, позволяющие оценить эффективность разработанного метода обнаружения аномального поведения. Для определения эффективности разработанного метода использовались показатели: время обнаружения атакующих узлов; количество узлов злоумышленника, которое позволяет обнаружить разработанный метод.

Ключевые слова: мобильные роботы, аномальное поведение, вероятностные методы, групповое управление, атака, обнаружение.

Благодарности. Работа выполнена при финансовой поддержке Министерства образования и науки РФ (Инициативные научные проекты № 2.6244.2017/8.9).

Алексей С. Гераськин, София Ю. Стрельникова, Максим П. Завенягин
Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского
ул. Астраханская, 83, г. Саратов, 410012, Россия
e-mail: gerascinas@mail.ru, http://orcid.org/0000-0002-3118-1022
e-mail: sofia_strelnikova@mail.ru, http://orcid.org/0000-0001-7200-0577
e-mail: maximzombi@yandex.ru, http://orcid.org/0000-0002-8749-487X

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ УЛУЧШЕНИЯ РЕАЛИЗАЦИИ АЛГОРИТМА МЕТОДА КОЧА ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ИЗОБРАЖЕНИЯ

Аннотация. В современном информационном обществе проблема контроля использования прав собственности на цифровые информационные ресурсы становится все более актуальной. Одним из наиболее эффективных способов решения этой проблемы является использование цифровых водяных знаков – цифровых меток, не видимых без специального программного обеспечения и секретного ключа. Цифровой водяной знак – технология, созданная для защиты авторских прав

на мультимедийные файлы. Это может быть текст или логотип, однозначно идентифицирующий автора файла. Цифровые водяные знаки применяются в кодировании и декодировании акустической информации, в технологиях поиска и определения незаконных копий аудиоматериалов. В данной работе проводилось исследование алгоритмов встраивания цифровых водяных знаков именно в изображения. На практике чаще остальных для встраивания цифровых водяных знаков в изображения используют алгоритмы, основанные на дискретном косинусном преобразовании. В статье приводится исследование, которое позволяет заключить, что метод Коча (Koch) является наиболее эффективным для защиты авторских прав путем внедрения цифрового водяного знака в изображение. Проводится анализ недостатков метода. Вследствие двукратного применения дискретного косинусного преобразования к изображению при внедрении и извлечении цифрового водяного знака, а также применения обратного дискретного косинусного преобразования для возврата к целочисленным матрицам пикселей после внедрения соотношение коэффициентов частотной матрицы может нарушиться, а это недопустимо, так как от этого напрямую зависит результат работы алгоритма. Во избежание возникновения данной проблемы во время встраивания бита цифрового водяного знака предлагается проводить корректировку значений коэффициентов частотной матрицы. Приводится алгоритм реализации метода Коча и обосновывается его модернизация для встраивания цифровых водяных знаков. Описывается способ и алгоритм обратного преобразования. Приводятся результаты исследования на предмет зависимости значения коэффициента силы встраивания от яркости изображения-контейнера и размера встраиваемого цифрового водяного знака.
Ключевые слова: цифровой водяной знак, дискретное косинусное преобразование, метод Коча.

Сергей И. Журин[1,2], Дмитрий Е. Комарков[3]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[2]АО «Федеральный центр науки и высоких технологий «Специальное научно-производственное объединение «Элерон»,
ул. Генерала Белова, 14, г. Москва, 115563, Россия
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА

Аннотация. Целевой фишинг является одним из методов социальной инженерии. При целевом фишинге текст электронного письма составляется с учетом знаний о конкретном предприятии и сотруднике (часто) с использованием знаний социологии и психологии таким образом, чтобы вызвать желание открыть прикрепленный файл или нажать на ссылку. Основная трудность защиты от такого письма состоит в том, что методы автоматизированного анализа не дают гарантии его обнаружения, т.к. современные киберпреступники используют новые текстовые формулировки, уязвимости нулевого дня, а также средства автоматизации для инжектирования эксплойтов в файлы, что снижает эффективность сигнатурного анализа антивирусных программ. Каждая из существующих технологий обнаружения в отдельности не позволяет обеспечить защиту от целевого фишинга. Однако объединение технологий (фильтрация спама, межсетевые экраны, антивирусы) с обязательным включением организационных мер, в том числе обучения и тестирования персонала, позволяет в комплексе защитить внешний информационный периметр организации от целевого фишинга. В статье приведен детальный анализ технологии реализации целевого фишинга с ана-

лизом причин возможностей его реализации двумя типовыми методами: запуском эксплойта при переходе по ссылке и при запуске файла. Приведен обзор уязвимостей 2016 – 2017 года, использованных для целевых атак. Приведены современные технологии защиты и их сравнительный анализ. Отмечено, что каждая из технологий не позволяет в отдельности обеспечить защиту от целевого фишинга. Предложены наиболее эффективные современные методы защиты на основе их сравнительного анализа и анализа современных информационных угроз.
Ключевые слова: APT, фишинг, целевой фишинг, социальная инженерия, внедрение ПО.

Олег В. Казарин[1,2]
[1]Институт проблем информационной безопасности МГУ имени М.В. Ломоносова,
Мичуринский просп., 1, г. Москва, 119192, Россия
[2]Институт информационных наук и технологий безопасности РГГУ,
ул. Кировоградская, 25, корп. 2, г. Москва, 117534, Россия
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

СОКРЫТИЕ КООРДИНАТ В ОБОБЩЕННОЙ ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ

Аннотация. В связи со стремительным развитием систем автопилотируемого транспорта (беспилотных автомобилей, беспилотных летательных аппаратов – дронов) все более актуальной становится задача предотвращения столкновений (задача об опасной близости), тем более в условиях большого количества участников движения и его интенсивности. Если появляется злоумышленник, способный контролировать одного или нескольких участников движения, стратегией которого является создание аварийной ситуации на дороге в виде столкновений беспилотных автомобилей, например, то возникает и необходимость защищаться от такого злонамеренного поведения. Одним из вариантов такой защиты является использование для решения этой прикладной задачи концепции многосторонних конфиденциальных вычислений, в том числе и потому, что будущие системы автопилотирования предполагают в некоторой локальной зоне управления движением возможность взаимодействия участников по схеме «каждый – с – каждым», что является необходимым условием для систем многосторонних конфиденциальных вычислений в условиях разного рода несанкционированных действий.

В отличие от ранее опубликованных результатов с использованием указанной концепции в модели с так называемым получестным противником в настоящей статье впервые предлагаются некоторые решения по защите участников движения от злонамеренного противника, который, раскрыв координаты движущихся объектов, пытается осуществить их столкновение, а также рассматривается расширение этой задачи на трехмерное измерение. В то же время показывается, что при реализации указанных систем на практике, скорее всего, возникнут ситуации, которые не решаются только математическими методами. Существует большой пул проблем, которые должны решаться различными организационно-техническими и управленческими методами. Тем не менее перспективы использования методов доказуемо безопасного сокрытия координат подобного типа выглядят, на взгляд автора, вполне привлекательными для специалистов в области информационной безопасности, связи, транспорта, распределенных систем.
Ключевые слова: системы автопилотируемого транспорта, сокрытие географических координат, конфиденциальные вычисления, конфиденциальное вычисление функции, двусторонние и многосторонние протоколы конфиденциальных вычислений.

ABSTRACT

Evgeny B. Belov [1], Vladimir P. Los [2], Anatoly A. Malyuk [3]
[1]FUMO VO IB,
Michurinsky prosp., 70, Moscow, Russia
e-mail: umoib@yandex.ru, https://orcid.org/0000-0003-4854-1220
[2]Center for the Study of the Problems of Personnel Supply in the Information Security Industry RTU MIREA,
Vernadsky prosp., 78, Moscow, Russia
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048
[3]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute)
Kashirskoe sh., 31, Moscow, Russia
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

The digital economy and actual problems of the improvement of the training system in the field of information security

Abstract. Trends in the development of the global information society indicate an increasing need for professionals with well established information culture, including those with knowledge and skills to ensure information security. The development and improvement of the system of appropriate training is stated in the Doctrine of information security of the Russian Federation as one of the priority measures for the implementation of the state policy in the field of digital economy. Training in this case should include both professional and mass training. In turn, the professional training can be basic and additional. The main goal of mass education is to form a culture of information security in society, which insufficient level of was noted in the Doctrine of information security as one of the main information threats. Therefore, the paper deals with the whole spectrum of the current problems of both professional and mass training. The importance of implementing the paradigm of continuous education ("lifelong learning") is emphasized.
Thus, the main purpose of this paper is to reveal the most important problems of ensuring the continuous process of formation of modern culture of information security using the capabilities of all components of the educational system.
Keywords: information security, staffing of the information security industry, information security awareness, professional and mass training in the field of information security, information security culture.

Vladimir I. Budzko, Dmitry A. Melnikov
Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Vavilov str., 44/2, Moscow, 119333, Russia
e-mail: vbudzko@ipiran.ru, https://orcid.org/0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

The Historical View Of The Blockchain Technology. The More Things Change, the More They Stay the Same

Abstract. Blockchain technologies (BC) are immutable distributed systems of digital ledgers (i.e., without central repository) and, as rule, without central authority. Currently, there is a lot of excitement around the use of BC technology, although the technology itself, on the one hand, is still not quite clear to many ones, and on the other (and this is the main thing) is not new. Superficial understanding of the BC as a phenomenon with «magical properties» leads to numerous predictions about the possibility of revolutionary transformations based on its application to entire sectors of the economy and, above all, in the credit and financial sphere. In this regard, this article presents a systematized analysis, the history of the BC emergence, leading from the international standards ISO 7498-2 of 1989 and ITU-T X.800 of 1991, as well as a brief informal

definition of BC and considered are the basic principles and components of this technology, including cryptographic one-way functions (hashes), transactions, addresses and their retrieval, «digital wallets», ledgers, blocks, blockchain in operations. Representation of the BC as a sequence of blocks bounded base on known mechanisms of the data integrity with using asymmetric cryptography allows us to conclude that only its evolutionary development is possible, although at a rapid pace in real time. This is a characteristic feature of establishing modern stage of and all other IT types. In conclusion, attention is drawn to the need for additional research to assess the security and reliability of the BC in terms of assessing the prospects for its use in specific business applications and critical information infrastructure systems.
Keywords: blockchain; ledger; repository; cryptocurrency; digital wallet; digital signature; transaction; connection integrity; public key; one way function; compendium; certificate; authentication; non-repudiation.

Anton A. Konev[1], Tatiana E. Mineeva[1], Mikhail L. Soloviev[2],
Aleksander A. Shelupanov[1], Mariya P. Silich[1]
[1]Tomsk state university of control systems and radioelectronics,
Lenina Av., 40, Tomsk, 634050, Russia
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Siberian state university of telecommunications and information sciences
Kirova St, 86, Novosibirsk, 630102, Russia
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

Model of the life cycle of the information security system

Abstract. When building an information security system, one of the key problems is the creation of regulatory documents. Regulators in the field of information security determine the list of necessary documentation mainly in relation to protection mechanisms (authentication, anti-virus protection, etc.) and practically do not take into account the stages of the life cycle of information security tools and personnel of the organization. The article proposes an approach to formalization of the list of information security management processes that need regulation. This approach allows the formation of information security policy to take into account the processes of personnel management and the complex of software and hardware information security, which is necessary to ensure a high level of security of critical information infrastructure.
Keywords: information protection system, life cycle, management processes, classification.

Evgeny A. Basinya[1,2]
[1]Novosibirsk State Technical University
20 K. Marx Street, Novosibirsk, 630073, Russia
[2]Research Institute of Information and Communications Technologies
48 Deputatskaya Street, Novosibirsk, 630073, Russia
e-mail: director@nii-ikt.ru, https://orcid.org/0000-0003-3916-7783

Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure

Abstract. The majority of the network infrastructures of government agencies and private enterprises operate on the basis of a TCP/IP protocol stack, which has significant vulnerabilities. For illustrative purposes, it is worth mentioning the lack of verification of the interaction subject authenticity in the basic protocols and technologies of this stack. Some of the TCP/IP stack vulnerabilities can be eliminated by

the intelligent functions of managed network devices: from access profiling to traffic segmentation. Complex firewalls, which include intrusion detection and prevention systems, are also an important element of the network protection. Methods of signature, heuristic, behavioral, self-similar, predictable and other approaches for analyzing network traffic and identifying network threats are further being developed by Russian and foreign scientists. However, the proposed solutions do not give an unambiguous result when using overlay technologies and cryptographic protocols. Also, due attention is not being paid to the processing, analysis of network traffic and logs of Windows/Linux operating systems and applications. The aim of this work was the research, development and software implementation of a distributed system for collecting, processing and analyzing security information events of an enterprise network infrastructure. The key task was to ensure objective monitoring of network information security. An additional task was to ensure the monitoring of the activity of users of personal computers running Windows and Linux operating systems. In order to address this challenge, a concept for complex processing of computer network traffic and security information events both on the server and on the client sides was developed. An original signature and statistical method of compiling the knowledge base system by testing and simulating known network and local attacks with tracking the response of operating systems and applications in a virtualization environment is reviewed. The approach to performing the automated analysis of correlating events with the use of deep packets inspection (DPI) and monitoring of users' local activity is described. The reviewed solution was successfully tested and used as one of the modules for providing network information security of the system for intelligent adaptive enterprise network infrastructure management, designed by author.
Keywords: IDS, IPS, SIEM, security information events analysis, user and network activity monitoring.

Anatoly M. Tarasov
Management Academy of the Ministry of the Interior of Russia,
Zoi and Alexandra Kosmodemianskikh str., 8, Moscow, 125993, Russia
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

The structure and content of the convention on combating cybercrime

Abstract. Consolidation of international efforts plays a crucial role in combating cybercrime the same way as in counteracting to terrorism, drug trafficking and other offenses of cross-border nature. The results of a critical analysis of the structure and content of the major provisions of the Budapest European Convention of 23 November 2001 (ETS No. 185) are presented. The paper provides a comparative analysis of the Convention and the Russian legislation from the point of view of organizational and legal regulation of fight against computer crime. The accent is made on terminological aspects of criminal and criminal procedure law in the field of computer information. Particular attention is drawn to the critical consideration of issues of international cooperation in the light of new challenges and threats of an increasingly confrontational inter-state relations. The conclusion substantiates the need for the adoption of the relevant United Nations Convention with proposals on the content of its main statements.
Keywords: Council of Europe Convention, law enforcement and judicial authorities, law enforcement, cybercrime, international cooperation, privacy, computer technology, investigation, software, passwords and access codes, child pornography, copyright.

Alexander B. Sattarov, Natalia G. Miloslavskaya
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them

Abstract. For the implementation of the Master's program "Business Continuity and Information Security Maintenance" in the field of specialty 10.04.01 "Information Security", a software shell of the educational laboratory complex (ELC) designed to study the "Man in the middle" network attacks has been developed in the NRNU MEPhI. In the framework of the ELC four basic attacks of this type are modeled: UDP Hijacking, Session Hijacking, TCP Hijacking and Bucket brigade attack. The paper presents two ELC applications: the instructor's application and the student's application. To assess the students' knowledge after performing laboratory work, the "Testing" module for assessing progress testing has been created, which includes questions for testing using the ELC software shell. Methodical instructions on performance of laboratory work have been written. Within the framework of the "Protected Information Systems" discipline of the Information Security of Banking Systems Department of the NNIU MEPhI, implementing the above-mentioned Mastre's program, a successful approbation of the developed ELC has been carried out. In conclusion the ways to further improvement of the ELC are suggested.
Keywords: Educational and Laboratory System, Man-in-the-middle attack, MITM, UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.

Elena S. Basan, Alexander S. Basan, Oleg B. Makarevich
Southern Federal University "SFedU", Institute of Computer Technologies and Information Security, str. Chekhov, 2, Taganrog, 347922, Russia
e-mail: ebasan@sfedu.ru, http://orcid.org/0000-0001-6127-4484
e-mail: asbasan@sfedu.ru, http://orcid.org/0000-0002-2973-2737
e-mail: obmakarevich@sfedu.ru, http://orcid.org/0000-0003-0066-8564

Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots*

Abstract. The present paper examines the issues of security in a group of mobile robots in the implementation of malicious attacks aimed at the availability of information. The main methods and approaches for detecting attacks and mobile robots anomalies were analyzed. The major advantages and disadvantages of existing approaches were identified. The aim is to develop an attack detection method that allows avoiding a creation of either a reference distribution, or a signature database, or rules for a group of mobile robots. The method should detect anomalies within the current conditions with a dynamically changing network structure. The paper presents a method for detecting abnormal behavior of a network node based on analysis of parameters: the residual energy and network load. The behavior of individual robots of the group is analyzed with respect to the deviation from the general behavior using probabilistic methods, which avoids creating a reference distribution for describing the behavior of the node, as well as the creating of a signature database for detecting anomalies. The developed method of detecting abnormal behavior based on the probabilistic evaluation of events. Three types of a network node state were defined, a graph of node transitions to each state was constructed, and parameters that affect these transitions were determined. The developed method demonstrates a high detection rate of denial of service attacks and distributed denial of service attacks when the number of malicious nodes is not greater than or slightly greater than the amount trusted nodes. It also provides detection of the Sybil attack. An experimental study was carried out. It includes the development of a model to simulate a group of mobile robots, in particular a robot network. Scenarios of attacks were developed, implemented for a group of mobile robots. It allows evaluating the effectiveness of this method of anomalous behavior detection. To determine the effectiveness of the developed method, the following indicators were used: time of detection of attackers and the number of nodes of the attacker that can be detected.
Keywords: mobile robots, abnormal behavior, probabilistic methods, group control, attack, detection.

Acknowledgement. The work was supported by the Ministry of Education and Science of the Russian Federation (Initiative Science Projects No. 2.6244.2017 / 8.9).

Aleksey S. Geraskin, Sofiia Yu. Strelnikova, Maxim P. Zavenyagin
Saratov National Research State University named after N. G. Chernyshevsky
ul. Astrahanskaja, 83, g. Saratov, 410012, Russia
e-mail: gerascinas@mail.ru, http://orcid.org/0000-0002-3118-1022
e-mail: sofia_strelnikova@mail.ru, http://orcid.org/0000-0001-7200-0577
e-mail: maximzombi@yandex.ru, http://orcid.org/0000-0002-8749-487X

Research of possibility of improvement of realization of algorithm of method of koch for embedding of digital watermarks in images

Abstract. In a modern information society the problem of the control of use of the property rights to digital information resources becomes more and more actual. One of the most effective ways of the decision of this problem is use of digital watermarks - digital labels, not visible without the special software and a confidential key. A digital watermark - the technology created for protection of copyrights to multimedia files. It can be the text or a logo unequivocally identifying the author of a file. Digital watermarks are applied in coding and decoding of the acoustic information, in technologies of search and definition of illegal copies of audio materials. In the given work research of algorithms of embedding of digital watermarks in images was conducted. In practice more often the others for embedding of digital watermarks in images are used by the algorithms based on discrete cosine transformation. In article research which allows to conclude is resulted that the method of Koch is the most effective for protection of copyrights by introduction digital watermarks in the image. The analysis of lacks of a method is carried out. Owing to double application discrete cosine transformation to the image at introduction and extraction digital watermarks, and also applications of the return discrete cosine transformation for return to integer matrixes of pixels after introduction the parity of factors of a frequency matrix can be broken, and it is inadmissible, as the result of work of algorithm directly depends on it. Avoid occurrence of the given problem during embedding of bit digital watermarks it is offered to spend correction of values of factors of a frequency matrix. The algorithm of realization of a method of Koch is resulted and its modernization for embedding of digital watermarks is proved. The way and algorithm of return transformation is described. Results of research about dependence of value of factor of force of embedding ε from brightness of the image-container and built in digital watermark are resulted the size.
Keywords: digital watermark, discrete cosine transformation, a method of Koch.

Sergey I. Zhurin[1,2], Dmitry E. Komarkov[3]
[1]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
[2]Joint Stock Company "Federal Center of Science and High Technologies "SNPO "Eleron",
14, Gen. Belova str., Moscow, 115563, Russia
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

Protection of external information perimeter of organization from spear phishing

Abstract. Spear phishing is one of the social engineering techniques. In case of spear phishing the email text is compiled taking into account the knowledge about a particular company and rather often about the employee using sociology and psychology in such a way that cause the desire to open the attached file or to click on the link. The main difficulty of protection against such e-mails is that the methods of automated analysis do not guarantee its detection, as modern cyber criminals use new text formulations, zero-day vulnerabili-

ties, as well as automation tools to inject exploits into files, which reduces the effectiveness of signature analysis of anti-virus programs. Each of the existing detection technologies alone does not provide protection against spear phishing. However, the combination of technologies (spam filtering, firewalls, anti-viruses), with the mandatory organizational measures, including training and testing of personnel, allows to protect the external information perimeter of the company from the spear phishing. The paper presents a detailed analysis of the technology of spear phishing implemented by two typical methods: the launch of the exploit when clicking on the link and when one runs an executable file. An overview of the vulnerability used in 2016-2017 for the attacks is presented. Modern technologies of protection and their comparative analysis are given. It is noted that each of the technologies used separately does not allow an effective protection against spear phishing. On the basis of comparative analysis and analysis of modern information threats the most effective modern methods of protection are proposed.
Keywords: APT, phishing, spearphishing, social engineering, software implementation.

Oleg V. Kazarin[1,2]
[1]Institute of Information Security Issues, Lomonosov MSU,
Michurinsky Pr., 1, Moscow, 119192, Russia
[2]Institute for Information Sciences and Security Technologies, RSUH,
Kirovogradskaya St., 25, bidg 2, Moscow, 117534,
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

Coordinate hiding in solving the generalized dangerous proximity problem

Abstract. In connection with the rapid development of autopilot transportation systems (driverless cars, unmanned aerial vehicles – drones) all the more urgent becomes the problem of collision avoidance (the problem of dangerous proximity), especially in conditions of a large number of members of the traffic and its high intensity. If there is an attacker who is able to control one or more participants in the traffic, which strategy is to create an emergency on the road or collisions of unmanned vehicles there is a need to protect against such malicious behavior. One of the options of such protection is the use of the concept of multilateral confidential calculations to solve this particular problem. The future autopilot systems assume in some local traffic control zone the possibility of interaction of participants according to the "everyone-with-everyone" scheme, which is a necessary condition for multilateral confidential computing systems in conditions of various unauthorized actions.

In contrast to the previously published results using this concept in the model with the so-called semi-honest enemy, this article for the first time proposes some solutions to protect the traffic participants from the malicious actor, who, having revealed the coordinates of moving objects, tries to drive them to collision. It is also considered the expansion of this problem to three dimensions. At the same time, it is shown that the implementation of these systems in practice, most likely, does not help to avoid the problematic situations that are not solved only by mathematical methods. There is a large set of problems that must be solved by various organizational, technical and managerial methods. Nevertheless, the prospects of using the methods of provably safe coordinate hiding look, in the author's opinion, quite attractive for experts in the field of information security, communications, transport, and distributed systems.
Keywords: autopilot transport systems, geographic coordinates hiding, secure computation, secure function evaluation, two-party and multi-party protocols of secure computation.

ПРАВИЛА ДЛЯ АВТОРОВ

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;
– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;
– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы с почтовым адресом, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, ПРОПИСНЫМИ буквами), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив); аннотация (200 – 250 слов, по ширине, строчными буквами – см. **правила формления аннотации**);
– далее повторяются все сведения о статье **на английском языке.**
– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;
– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;
– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы, оформленный в соответствии с действующими стандартами (как правило, не менее 15 наименований в научной статье и 50 – в обзорной статье);
– после списка литературы идет REFERENCES, в котором указанные библиографические данные автора(авторов) и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации (т.е. латинскими буквами).

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).
Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи:

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).
Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.
В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.
В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.
Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.
Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. При этом

отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.
Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;
– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;
– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;
– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;
– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;
– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;
– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;
– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;
– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;
– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

Author Guidelines

The articles submitted to the editors must meet the following requirements:

– the topic of the article should be relevant, have scientific or practical significance and be published by the authors for the first time;
– the manuscript should be formatted only in * .doc or pdf format, A4 strip, size 12, TimesNewRoman font, one-and-a-half interval;
– in the beginning of the article there are information about the article in English: I.O. Name of authors (centered, lower case); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);
– further information on the article is in Russian: I.O. The authors' surname (for jubilus, lower case letters); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);
– then the text of the article is in Russian or English, size 12, interval one and a half, the recommended total volume of the article should not exceed 10 pages, including tables, illustrations;
– at the end of the article the LIST OF LITERATURE is given, in which the bibliographic list of sources of literature is indicated, drawn up in accordance with the current standards (as a rule, not less than 15 titles);
– after the list of literature is REFERENCES, in which these bibliographic sources should be written in Latin (ie Latin letters).

Rules to write a scientific abstract

Abstract is a source of information about the content of the paper and its research results. The structure of the abstract should correspond to the structure of the paper and should be not less than 100 words, but not more than 250 words.

The abstract includes the following aspects of the paper:

- subject and purpose of the paper;
- method or methodology described in the paper;
- results;
- discussion.

The abstract plays the following role:

- allows you to establish the main content of the paper, determine its relevance and decide whether to read the full text of the paper;
- provides information about the paper and eliminates the need to read the full text of the paper if the paper is of secondary interest to the reader;
- used in information systems, including automated ones, to search for documents and information (title, abstract and keywords are translated into English, and foreign readers judge the content of the paper by them).

The abstract should be informative (not contain general wordings) and original. The information contained in the title of the paper should not be repeated in the text of the abstract. The text of the abstract should not contain an interpretation of the content of the paper, criticisms and the author's point of view, as well as information that is not included in the paper. You should avoid unnecessary introductory phrases (for example, " the author is considering...").
Historical references, if they do not constitute the main content of the paper, the description of previously published works and well-known provisions are not given in the abstract.
The text of the abstract should use syntactic constructions peculiar to the language of scientific and technical documents, avoid complex grammatical structures.
The text of the abstract should use significant (key) words from the text of the paper.
The method or methodology of the work should be described if they are new or of interest from the point of view of this work. In the abstract of the paper describing the experimental work, indicate the data sources and the specific features of their processing.
The results are described very accurately and informative. The main theoretical and experimental results, actual data, discovered interrelations and regularities are presented. At the same time, preference is given to new results and data of long-term importance, important discoveries, conclusions that refute existing theories, as well as data that, in the author's opinion, have practical value.
Conclusions may be accompanied by recommendations, assessments, suggestions, hypotheses described in the paper.

Terms of publication of the article:
- the article should be sent by e-mail;
- the editorial board of the journal follows the ethical standards adopted in the international scientific community, relying on the recommendations of the Ethics Committee of scientific publications that do not contradict the norms of Russian legislation in the field of regulation of the activities of the media and copyright;
- articles that do not meet the requirements for presentation and processing are not considered or published;
- in one issue of the journal, as a rule, only one author's article is published, including co-authors;
- authors should provide only original works, if text or graphic information obtained from other persons is used, references to the relevant publications or the author's written permission are necessary;
- the decision to publish the manuscript is made by the editorial board on the basis of the result of peer review and expert evaluation by qualified specialists in the field of information security;
- in the case of receipt of the manuscript for publication, the author must promptly give answers to editorial questions related to comments on the article;
- in case of refusal to publish, the editorial board should provide the author with a copy of the review and justification for refusing the publication;
- submitting an article to more than one journal is simultaneously regarded as unethical behavior and is unacceptable;
- articles are published for free.

Rules for publication of texts

1. Articles must be submitted electronically (* .doc or * .rtf) with a printout (or a file in * .pdf format) - to avoid inaccuracies in reading the formulas.
2. Pictures, graphics, photographs and other types of illustrations should, if possible, not only be included in the text, but also separate files in the original format (not integrated into the Word document).
3. Abbreviations and abbreviations, which are not on the list of abbreviations, should be disclosed (in parentheses or in a footnote).
4. By providing links to formulas, expressions or restrictions in the text of the article, please make sure that the relevant objects in the article are numbered and numbered.
5. References to the literature should be given in the text in square brackets, in the case of citations, with pages.
6. When preparing a list of literature, it is desirable to pay attention to the availability of output data of works and to avoid repeated instructions of the same work under different numbers.
7. References to laws, regulations, confessions and so on should be indicated in the prescribed form: the Law of the Russian Federation "__" of x month xxxx, No. ___. Art. ___.
8. Foreign words, terms and surnames, the spelling of which allows variants, please write within the same article the same way.

Submission Preparation Checklist

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.
1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the "About the journal" page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Privacy Statement

The names and email addresses entered in this journal site page will be used exclusively for the purposes specified by this journal and will not be used for any other purposes or will not be given over to another individuals and organizations.

СПИСОК СОКРАЩЕНИЙ, ПРИНЯТЫХ В ЖУРНАЛЕ

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
БЧ – блокчейн
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КПО – комплекс программного обеспечения
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОКСО – Общероссийский классификатор специальностей по образованию
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СБЧ – система блокчейн
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись
ФГОС – федеральный государственный образовательный стандарт
ФУМО ИБ – федеральное учебно-методическое объединение по образованию в области информационной безопасности

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 9087.
Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 9087.
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода – 4 раза в год / Periodicity - 4 times a year

Подписка на журнал
производится в почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Технический редактор П.А. Золотухина
Корректор Авдюшкина М.Г.

Подписано в печать 20. 12. 2018 г. Формат 60 x 84 1/8.
Печ. л. 17,5. Уч. - изд. л. 17,5. Тираж 500 экз. Изд. № 002 - 3.

Национальный исследовательский ядерный университет «МИФИ».
Каширское ш., 31, Москва, 115409, Россия.
National Research Nuclear University MEPHI.
Kashirskoe shosse, 31, Moscow, 115409, Russia

Типография ООО «ТИПОГРАФИЯ»
115477, г. Москва, ул. Кантемировская, 60