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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(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.

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.

СОДЕРЖАНИЕ

CONTENT

Анатолий В. Марченко[1], Валерий Ю. Войналович[2], Сергей Н. Воронин[2]
[1]Федеральная служба по техническому и экспортному контролю,
105175, г. Москва, Старая Басманная, 17
e-mail: anatolijlev@yandex.ru, https://orcid.org/0000-0002-0207-6274
[2]Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю,
394020, г. Воронеж, ул. 9 Января, д. 280а
e-mail: niii1zi@yandex.ru, https://orcid.org/0000-0002-1848-1346
e-mail: snv-36@mail.ru, https://orcid.org/0000-0002-1002-0799

АНАЛИЗ СОСТОЯНИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.2.01

Аннотация. Актуальность проведения анализа нынешнего состояния системы подготовки специалистов в области информационной безопасности, обусловлена необходимостью совершенствования кадрового обеспечения в этой, безусловно, приоритетного направления деятельности Российской Федерации в условиях нарастания новых вызовов и угроз в информационной сфере. Материалы статьи представляют собой результаты анализа и обобщения данных о состоянии системы подготовки, профессиональной переподготовки и повышения квалификации специалистов, работающих в области информационной безопасности в интересах различных государственных структур от органов государственной власти до подведомственных им организаций. Исследование охватывает анализ таких основных компонент сферы оказания профессиональных образовательных услуг, как среднее профессиональное образование и высшую школу (бакалавриат, магистратуру и специалитет), исключая вопросы подготовки высококвалифицированных кадров через аспирантуру и системы переподготовки и повышения квалификации. Представленные аналитические материалы могут быть использованы, в частности, при разработке предложений по совершенствованию отечественной системы подготовки при формировании контрольных показателей приема граждан на обучение за счет бюджетных ассигнований федерального бюджета по направлениям подготовки и специальностям в области информационной безопасности.

Ключевые слова: информационная безопасность, подготовка кадров, контрольные цифры приема, обеспеченность кадрами.

Для цитирования. МАРЧЕНКО, Анатолий В.; ВОЙНАЛОВИЧ, Валерий Ю.; ВОРОНИН, Сергей Н.. АНАЛИЗ СОСТОЯНИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], n. 2, p. 6-22, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1106>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.01.

Anatoly V. Marchenko[1], Valery Yu. Voynalovich[2], Sergey N. Voronin[2]
[1]FSTEC of Russia,
105175, Staraya Basmannaya, 17, Moscow, Russia
e-mail: anatolijlev@yandex.ru, https://orcid.org/0000-0002-0207-6274
[2]State research and testing Institute of problems of technical protection of information of the FSTEC of Russia,
394020, Voronezh, street on January 9, 280a
e-mail: niii1zi@yandex.ru, https://orcid.org/0000-0002-1848-1346
e-mail: snv-36@mail.ru, https://orcid.org/0000-0002-1002-0799

The analysis of the training system for specialists working in the field of information security

DOI: http://dx.doi.org/10.26583/bit.2018.2.01

Abstract. The analysis of the training system for specialists working in the field of information security plays an important role to improve staffing in the field of information security in the Russian

Federation in the context of new challenges and threats in the information sphere. The article presents the results of analysis and summarizes the data on state of the system of training, retraining and advanced training provided for information security experts. The presented analytical materials are taking into account the results of the data analysis about the security specialists working in Federal Executive authorities (Federal authorities), regional executive authorities, local governmental bodies and their subordinate organizations, corporations, and organizations of licensees of the FSTEC of Russia. The presented analytical materials can be used for development of proposals in order to improve the national system of training, professional retraining and advanced training of information security specialists, as well as for development of control indicators for the admission of persons to the training in the field of information security at the expense of the Federal budget allocations.
Keywords: information security, training, admission control indicators, staffing.
For citation. MARCHENKO, Anatoly V.; VOYNALOVICH, Valery Yu.; VORONIN, Sergey N.. The analysis of the training system for specialists working in the field of information security. IT Security (Russia), [S.l.], n. 2, p. 6-22, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1106>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.01.

Введение

Актуальность проведения анализа нынешнего состояния системы подготовки специалистов в области информационной безопасности, обусловлена необходимостью совершенствования кадрового обеспечения этого, безусловно, приоритетного направления деятельности Российской Федерации в условиях нарастания новых вызовов и угроз в информационной сфере.

Материалы статьи представляют собой результаты анализа и обобщения данных о состоянии системы подготовки, профессиональной переподготовки и повышения квалификации специалистов, работающих в области информационной безопасности в интересах различных государственных структур от органов государственной власти до подведомственных им организаций.

Исследование охватывает анализ таких основных компонент сферы оказания профессиональных образовательных услуг, как среднее профессиональное образование и высшую школу (бакалавриат, магистратуру и специалитет), исключая вопросы подготовки высококвалифицированных кадров через аспирантуру и системы переподготовки и повышения квалификации.

Сбор статистических данных и формирование аналитических материалов проводился центром ответственности (ФСТЭК России) [1] в целях подготовки предложений по совершенствованию системы подготовки специалистов для государственной системы защиты информации. Практическим результатом исследования стало формирование предложений по контрольным цифрам приема (КЦП) для обучения по образовательным программам высшего образования за счет бюджетных ассигнований федерального бюджета по направлениям подготовки и специальностям в области информационной безопасности на 2018 год (далее – предложения по КЦП).

Состав сведений, необходимых (запрашиваемых) для формирования аналитических материалов, определялся исходя из их предназначения с учетом действующих документов, определяющих концептуальные основы развития кадрового обеспечения в различных отраслях [2, 3], а также исходя из порядка формирования КЦП для обучения по образовательным программам высшего образования за счет бюджетных ассигнований федерального бюджета [4].

В качестве опрашиваемых респондентов были определены 31 федеральный орган исполнительной власти и три госкорпорации, а также органы исполнительной власти субъектов Российской Федерации и организации-лицензиаты ФСТЭК России.

В результате проведенного анализа установлено, что в настоящее время в системе образования на федеральном и региональном уровнях созданы необходимые условия для эффективного решения задачи подготовки специалистов для государственной системы защиты

информации.

1 Организационная структура образования в области информационной безопасности

Организационно система образования в области информационной безопасности представляет собой совокупность взаимодействующих элементов, основными из которых являются:

- Минобрнауки России и другие заинтересованные федеральные органы исполнительной власти;
- Координационный совет в области образования «Инженерное дело, технологии и технические науки» Минобрнауки России;
- Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (УМО ИБ);
- образовательные организации высшего и среднего профессионального образования, осуществляющие образовательную деятельность по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность»;
- организации-работодатели.

2 Нормативно-методическое обеспечение образования в области информационной безопасности

Развитие и совершенствование организационно-методической основы рассматриваемой системы подготовки специалистов в области информационной безопасности координирует Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность».

Учебно-методическую основу системы составляют федеральные государственные образовательные стандарты (ФГОС) и разрабатываемые на их базе основные образовательные программ (ООП).

Приказами Минобрнауки России от 12 сентября 2013 г. № 1060 и № 1061 [6, 7], а также от 29 октября 2013 г. № 1199 утверждены перечни специальностей и направлений подготовки высшего и среднего профессионального образования укрупненной группы 10.00.00 «Информационная безопасность». Укрупненная группа специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (относящихся к области образования «Инженерное дело, технологии и технические науки») включает следующие уровни профессионального образования:

Среднее профессиональное образование

(Перечни профессий и специальностей среднего профессионального образования, утверждены приказом Минобрнауки России от 29 октября 2013 г. № 1199). [8]

Код специальности подготовки – 10.02.01, специальность подготовки – «Организация и технология защиты информации», квалификация – «Техник по защите информации», «Старший техник по защите информации».

Код специальности подготовки – 10.02.02, специальность подготовки – «Информационная безопасность телекоммуникационных систем», квалификация – «Техник по защите информации», «Старший техник по защите информации».

Код специальности подготовки – 10.02.03, специальность подготовки – «Информационная безопасность автоматизированных систем», квалификация – «Техник по защите информации», «Старший техник по защите информации».

Высшее образование – бакалавриат

(Перечни специальностей и направлений подготовки высшего образования, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1061).

Код направления подготовки – 10.03.01, наименование направления подготовки – «Информационная безопасность», квалификация – «Академический бакалавр».

Высшее образование – магистратура

(Перечни специальностей и направлений подготовки высшего образования, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1061).

Код направления подготовки – 10.04.01, наименование направления подготовки – «Информационная безопасность», квалификация – «Магистр».

Высшее образование – специалитет

(Перечни специальностей и направлений подготовки высшего образования, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1061).

Код специальности подготовки – 10.05.01, специальность подготовки – «Компьютерная безопасность», квалификация – «Специалист по защите информации». Включает в себя 8 специализаций, в т.ч.:

Специализация № 1 «Анализ безопасности компьютерных систем».

Специализация № 2 «Математические методы защиты информации».

Специализация № 3 «Безопасность распределенных компьютерных систем».

Специализация № 4 «Разработка защищенного программного обеспечения».

Специализация № 5 «Безопасность высокопроизводительных вычислительных систем».

Специализация № 6 «Безопасность программного обеспечения мобильных систем».

Специализация № 7 «Информационно-аналитическая и техническая экспертиза компьютерных систем».

Специализация № 8 «Информационная безопасность объектов информатизации на базе компьютерных систем».

Код специальности подготовки – 10.05.02, специальность подготовки – «Информационная безопасность телекоммуникационных систем», квалификация – «Специалист по защите информации». Включает в себя 12 специализаций, в т.ч.:

Специализация № 1 «Мониторинг в телекоммуникационных системах».

Специализация № 2 «Системы представительской связи».

Специализация № 3 «Сети специальной связи».

Специализация № 4 «Инструментальный контроль информационной безопасности телекоммуникационных систем».

Специализация № 5 «Системы специальной связи и информации для органов государственной власти».

Специализация № 6 «Информационная безопасность космических телекоммуникационных систем».

Специализация № 7 «Разработка защищенных телекоммуникационных систем».

Специализация № 8 «Системы подвижной цифровой защищенной связи».

Специализация № 9 «Защита информации в радиосвязи и телерадиовещании».

Специализация № 10 «Защита информации в системах связи и управления».

Специализация № 11 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте».

Специализация № 12 «Безопасность телекоммуникационных систем информационного взаимодействия».

Код специальности подготовки – 10.05.03, специальность подготовки – «Информационная безопасность автоматизированных систем», квалификация – «Специалист по защите информации». Включает в себя 10 специализаций, в т.ч.:

Специализация № 1 «Автоматизированные информационные системы специального назначения».

Специализация № 2 «Высокопроизводительные вычислительные системы специального назначения».

Специализация № 3 «Информационная безопасность автоматизированных систем критически важных объектов».

Специализация № 4 «Безопасность открытых информационных систем».

Специализация № 5 «Информационная безопасность автоматизированных банковских систем».

Специализация № 6 «Защищенные автоматизированные системы управления».

Специализация № 7 «Обеспечение информационной безопасности распределенных информационных систем».

Специализация № 8 «Анализ безопасности информационных систем».

Специализация № 9 «Создание автоматизированных систем в защищенном исполнении».

Специализация № 10 «Информационная безопасность автоматизированных систем на транспорте».

Код специальности подготовки – 10.05.04, специальность подготовки – «Информационно-аналитические системы безопасности», квалификация – «Специалист по защите информации». Включает в себя 3 специализации, в т.ч.:

Специализация № 1 «Автоматизация информационно-аналитической деятельности».

Специализация № 2 «Информационная безопасность финансовых и экономических структур».

Специализация № 3 «Технологии информационно-аналитического мониторинга».

Код специальности подготовки – 10.05.05, специальность подготовки – «Безопасность информационных технологий в правоохранительной сфере», квалификация – «Специалист по защите информации». Включает в себя 4 специализации, в т.ч.:

Специализация № 1 «Технологии защиты информации в правоохранительной сфере».

Специализация № 2 «Информационно-аналитическое обеспечение правоохранительной деятельности».

Специализация № 3 «Информационно-психологическое обеспечение правоохранительной деятельности».

Специализация № 4 «Компьютерная экспертиза при расследовании преступлений».

Код специальности подготовки – 10.05.06, специальность подготовки – «Криптография», квалификация – «Специалист по защите информации».

Код специальности подготовки – 10.05.07, специальность подготовки – «Противодействие техническим разведкам», квалификация – «Специалист по защите информации».

(Специальности 10.05.06 и 10.05.07 входят в перечни специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования, содержащих сведения, составляющие государственную тайну или служебную информацию ограниченного распространения, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1060.)

Высшее образование – подготовка кадров высшей квалификации

(Перечни специальностей и направлений подготовки высшего образования, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1061)

Код специальности подготовки – 10.06.01, специальность подготовки – «Информационная безопасность», квалификация – «Исследователь. Преподаватель-исследователь».

Укрупненная группа специальностей и направлений подготовки 10.00.00 Информационная безопасность и противодействие техническим разведкам

Код специальности подготовки – 10.07.01, специальность подготовки – «Информационная безопасность», квалификация – «Исследователь. Преподаватель-исследователь».

(Специальность 10.07.01 входит в перечень специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования, содержащих сведения, составляющие государственную тайну или служебную

информацию ограниченного распространения, утверждены приказом Минобрнауки России от 12 сентября 2013 г. № 1060.) [8]

3 Результаты анализа статистических данных

На основе анализа обобщенных сведений об образовательных организациях высшего и среднего профессионального образования в области информационной безопасности установлено следующее.

1) Подготовка специалистов в области информационной безопасности проводится:

- в системе высшего образования – 166 образовательными организациями,
- в системе среднего профессионального образования – 29 образовательными организациями.

Количество образовательных организаций, реализующих подготовку по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность», приведено в таблице 1.

2) Количество выпускников образовательных организаций, осуществляющих подготовку в области информационной безопасности, ежегодно возрастает. В 2015 году количество выпускников увеличилось на 48 % по сравнению с 2013 годом. Количество выпускников образовательных организаций по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах приведено на рисунке 1.

Таблица 1. Количество образовательных организаций, реализующих подготовку по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность»

Коды специальностей и направлений подготовки*	**Наименование специальностей и направлений подготовки**	**Квалификация**	**Количество образовательных организаций, реализующих подготовку**
Специальности подготовки среднего профессионального образования			
10.02.01	Организация и технология защиты информации	Техник по защите информации, старший техник по защите информации	8
10.02.02	Информационная безопасность телекоммуникационных систем	Техник по защите информации, старший техник по защите информации	7
10.02.03	Информационная безопасность автоматизированных систем	Техник по защите информации, старший техник по защите информации	14
090108.51	Информационная безопасность	Техник	1
Направления подготовки высшего образования			
10.03.01 (090900)	Информационная безопасность (ИБ)	Академический бакалавр	102
10.04.01 (090900)	Информационная безопасность	Магистр	32
10.06.01	Информационная безопасность	Исследователь, преподаватель-исследователь	6
Специальности подготовки высшего образования			
10.05.01 (090301)	Компьютерная безопасность (КБ)	Специалист по защите информации	25
10.05.02 (090302)	Информационная безопасность телекоммуникационных систем (ИБ ТКС)	Специалист по защите информации	25

Коды специальностей и направлений подготовки*	**Наименование специальностей и направлений подготовки**	**Квалификация**	**Количество образовательных организаций, реализующих подготовку**
10.05.03 (090303)	Информационная безопасность автоматизированных систем (ИБАС)	Специалист по защите информации	41
10.05.04 (090305)	Информационно-аналитические системы безопасности (ИАСБ)	Специалист по защите информации	5
10.05.05 (090915)	Безопасность информационных технологий в правоохранительной сфере	Специалист по защите информации	10
090103	Организация и технология защиты информации (ОиТЗИ)	Специалист по защите информации	22
090104	Комплексная защита объектов информатизации (КЗОИ)	Специалист по защите информации	14
090105	Комплексное обеспечение информационной безопасности автоматизированных систем (КОИБАС)	Специалист по защите информации	14

*Указаны коды специальностей и направлений подготовки высшего образования в соответствии с перечнями, утвержденными Минобрнауки России в 2013 году, а в скобках – в соответствии с перечнями, утвержденными Минобрнауки России до 2013 года

3) Наиболее интенсивно возрастает количество выпускников по направлению подготовки 10.03.01 «Информационная безопасность» (бакалавриат). Количество выпускников по указанному направлению подготовки увеличилось с 64 человек в 2014 году до 1747 человек в 2015 году. Распределение количества выпускников образовательных организаций высшего образования (в том числе обучавшихся за счет бюджетных ассигнований) по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах приведено на рисунках 2 и 3.

4) Характеристика (структура, общий состав) выпуска по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» в 2015 году приведена на рисунке 4. Распределение численности выпускников по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году с указанием вида финансового обеспечения получения образования приведено в таблице 2.

Общее количество выпускников образовательных организаций, ведущих подготовку по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность», составило в 2015 году 4827 человек, из них продолжили обучение в образовательных организациях по очной форме 598 человек. Общее количество выпускников, которые могли трудоустроиться в 2015 году, составило 3505 человек. Не трудоустраивались в 2015 году 724 выпускника по различным причинам: призыв на военную службу, по семейным обстоятельствам и т.п.

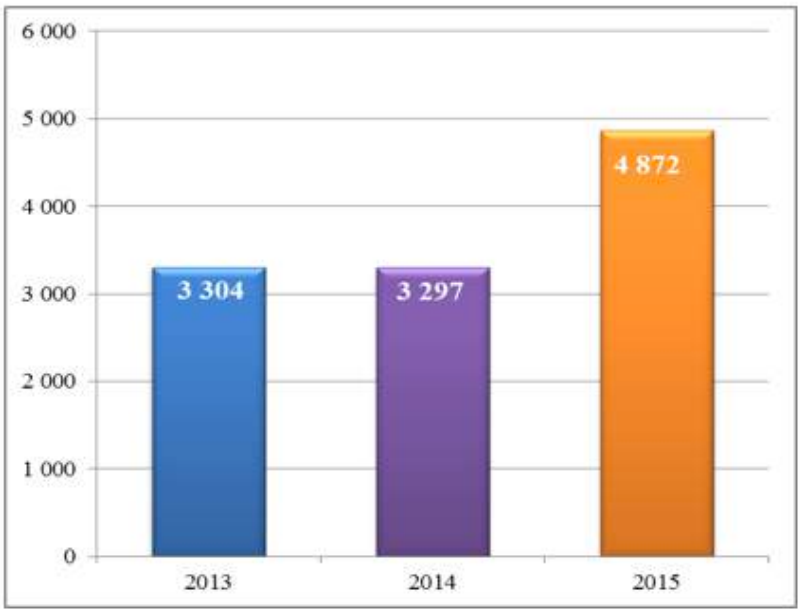


Рис. 1. Количество выпускников образовательных организаций по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах (Fig. 1. The number of graduates from educational institutions in the generalized field of 10.00 «Information security» in 2013-2015)

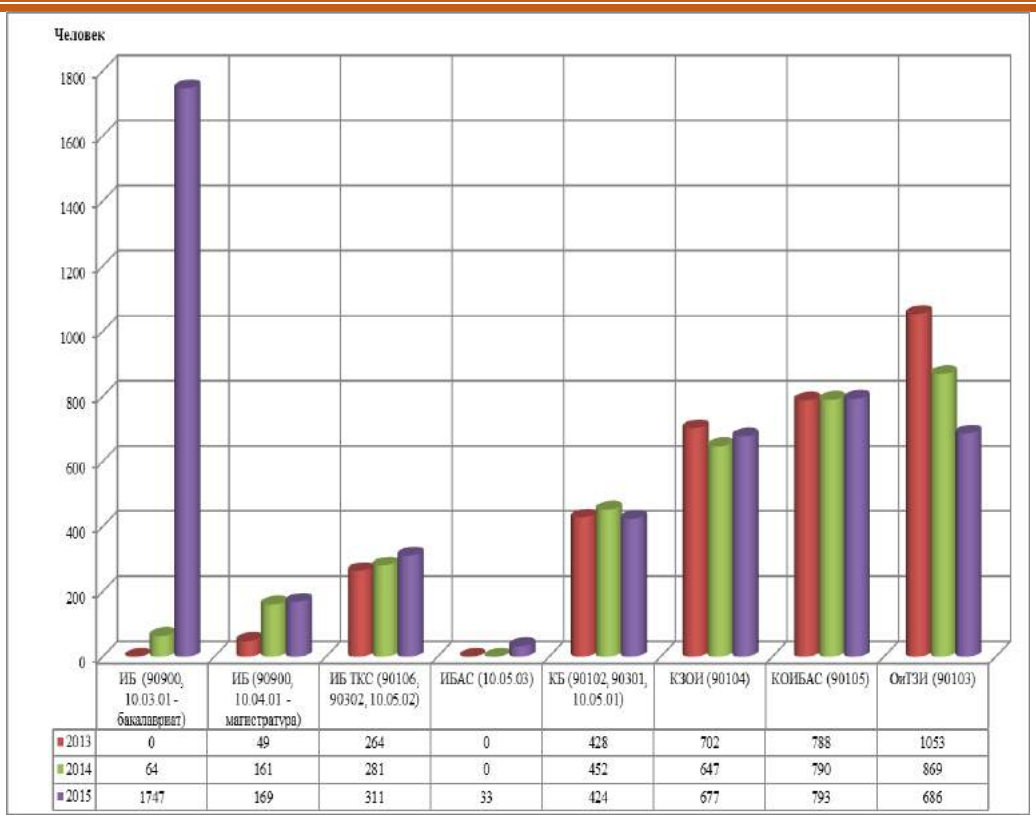
5) Направление на работу по специальностям в среднем получают около 50-55 % всех выпускников. Распределение количества выпускников образовательных организаций высшего образования 2013, 2014 и 2015 года, обучавшихся по очной форме обучения (за счет средств бюджетов всех уровней) по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» и получивших направление на работу, приведено на рисунках 5-7 соответственно.

В 2015 году из общего количества выпускников (3790 человек), обучающихся за счет бюджетных ассигнований, получили направление на работу 1517 выпускников, и 996 выпускников по разным причинам получили право свободного трудоустройства.

6) Наиболее популярной при приеме на обучение в 2015 году являлась специальность 10.05.01 «Компьютерная безопасность». Конкурс среди абитуриентов, подавших заявление на поступление на эту специальность, составил 10,3 человека на место. За последние три года отмечается рост популярности направления подготовки 10.04.01 «Информационная безопасность» (магистратура) и специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

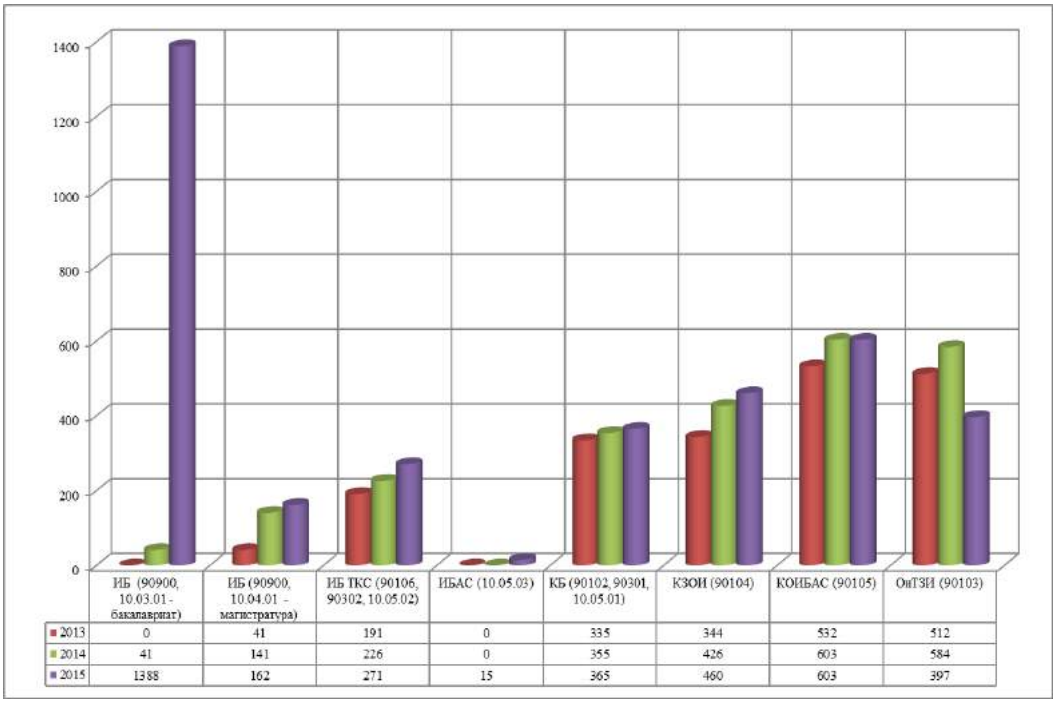
Распределение конкурса на обучение в образовательных организациях высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах приведено на рисунке 8.

7) Общее количество студентов, принятых на обучение по направлениям подготовки и специальностям в 2015 году, составляет 5901 человек. Наибольшее количество студентов принято на обучение в 2015 году по направлению подготовки 10.03.01 «Информационная безопасность» (бакалавриат), которое составило 2471 человек. Распределение численности принятых на обучение в образовательные организации высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году приведено на рисунке 9.



	ИБ (90900, 10.03.01 - бакалавриат)	ИБ (90900, 10.04.01 - магистратура)	ИБ ТКС (90106, 90302, 10.05.02)	ИБАС (10.05.03)	КБ (90102, 90301, 10.05.01)	КЗОИ (90104)	КОИБАС (90105)	ОиТЗИ (90103)
2013	0	49	264	0	428	702	788	1053
2014	64	161	281	0	452	647	790	869
2015	1747	169	311	33	424	677	793	686

Рис. 2. Распределение количества выпускников образовательных организаций высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах
(Fig. 2. Distribution of the number of graduates from higher education institutions in the field of 10.00.00 «Information security» in 2013-2015)



	ИБ (90900, 10.03.01 - бакалавриат)	ИБ (90900, 10.04.01 - магистратура)	ИБ ТКС (90106, 90302, 10.05.02)	ИБАС (10.05.03)	КБ (90102, 90301, 10.05.01)	КЗОИ (90104)	КОИБАС (90105)	ОиТЗИ (90103)
2013	0	41	191	0	335	344	532	512
2014	41	141	226	0	355	426	603	584
2015	1388	162	271	15	365	460	603	397

Рис. 3. Распределение выпускников образовательных организаций высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность», обучающихся за счет бюджетных ассигнований, в 2013-2015 годах
(Fig. 3. Distribution of the number of graduates from higher educational institutions in the field of 10.00.00 «Information security» trained at the expense of Federal budget allocations in 2013-2015)

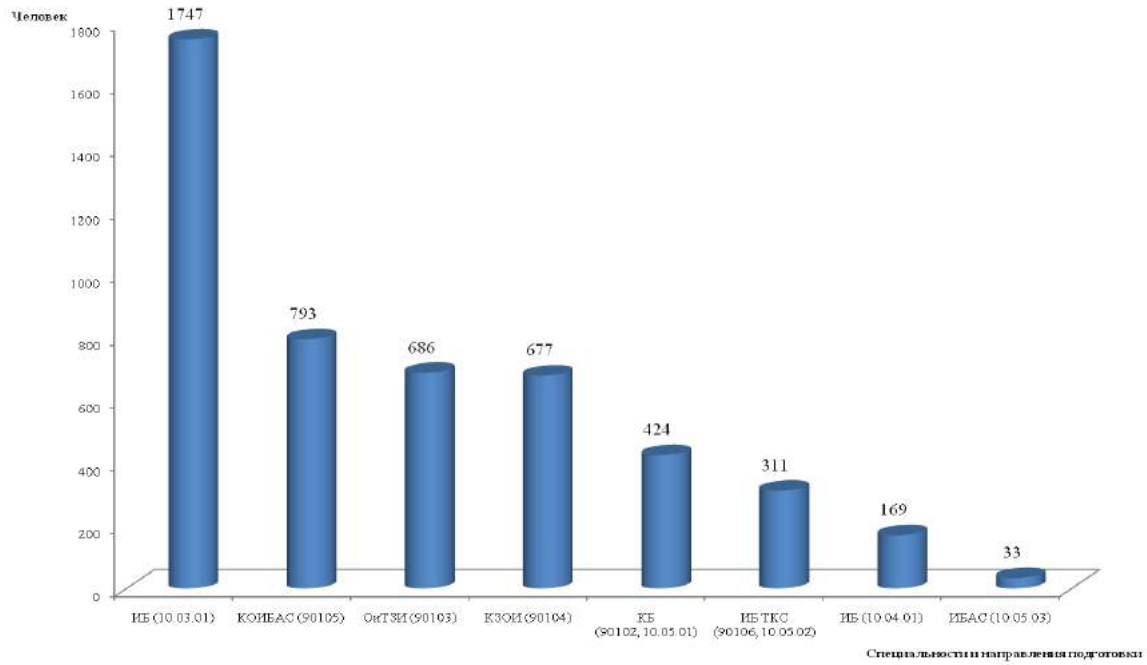


Рис. 4. Характеристика (структура, общий состав) выпуска по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» в 2015 году.
(Fig. 4. Figures (structure and general composition) for graduates in the generalized field of 10.00.00 «Information security» in 2015)

Таблица 2. Распределение количества выпускников по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году с указанием вида финансового обеспечения получения образования

Специальность, направление подготовки (код)	Завершили обучение в 2015 году, чел	Завершили обучение за счет бюджетных ассигнований федерального бюджета, чел	Завершили обучение с полным возмещением стоимости обучения, чел	Продолжили обучение в данной образовательной организации, чел	Итоговый (фактический) выпуск из образовательных организаций, чел
Информационная безопасность (10.03.01- бакалавриат)	1747	1388	323	452	1295
Комплексное обеспечение информационной безопасности автоматизированных систем (90105)	793	603	175	66	727
Организация и технология защиты информации (90103)	686	397	260	43	643
Комплексная защита объектов информатизации (90104)	677	460	217	24	653
Компьютерная безопасность (90102, 10.05.01)	424	365	59	9	415
Информационная безопасность телекоммуникационных систем (90106, 10.05.02)	311	271	40	3	308
Информационная безопасность (10.04.01- магистратура)	169	162	5	1	168
Информационная безопасность автоматизированных систем (10.05.03)	33	15	18	0	33
Всего:	4840	3661	1097	598	4242

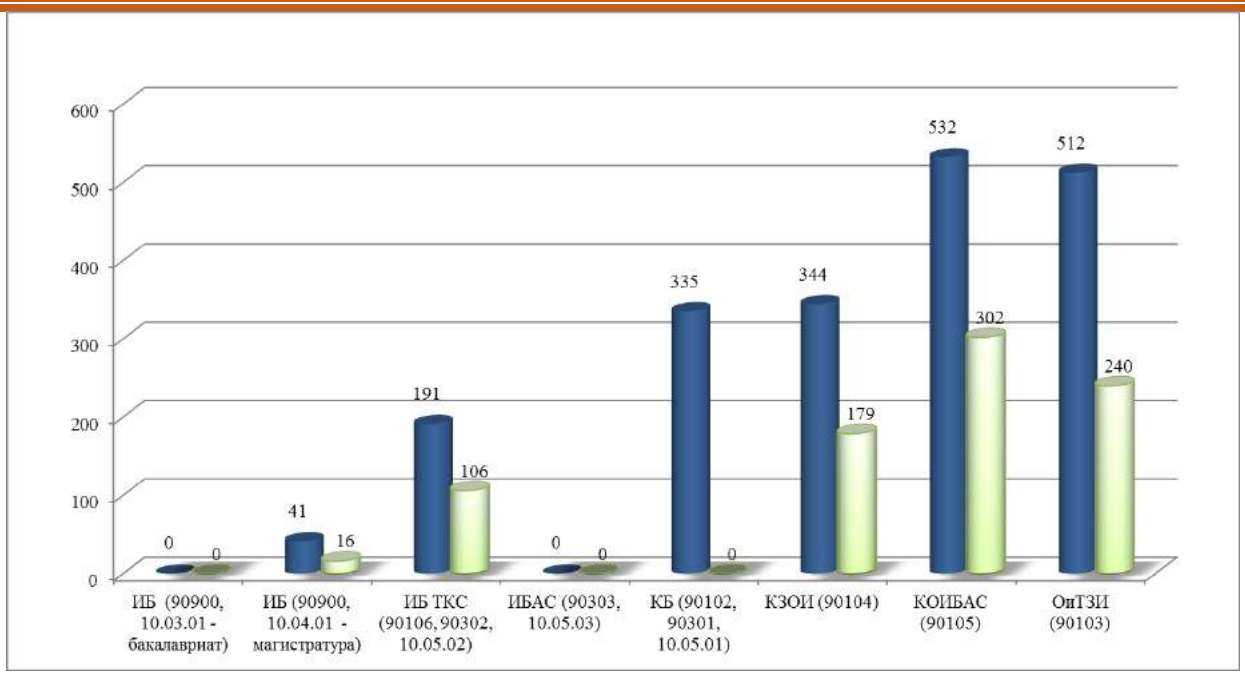


Рис. 5. Распределение количества выпускников образовательных организаций высшего образования 2013 года, обучавшихся по очной форме обучения (за счет средств бюджетов всех уровней) по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» и получивших направление на работу

(Fig. 5. Distribution of the number of graduates from higher educational institutions in 2013 who have been trained on full-time basis (at the expense of Federal budget allocations of any level) in the field of 10.00.00 «Information security» and received a position within this field)

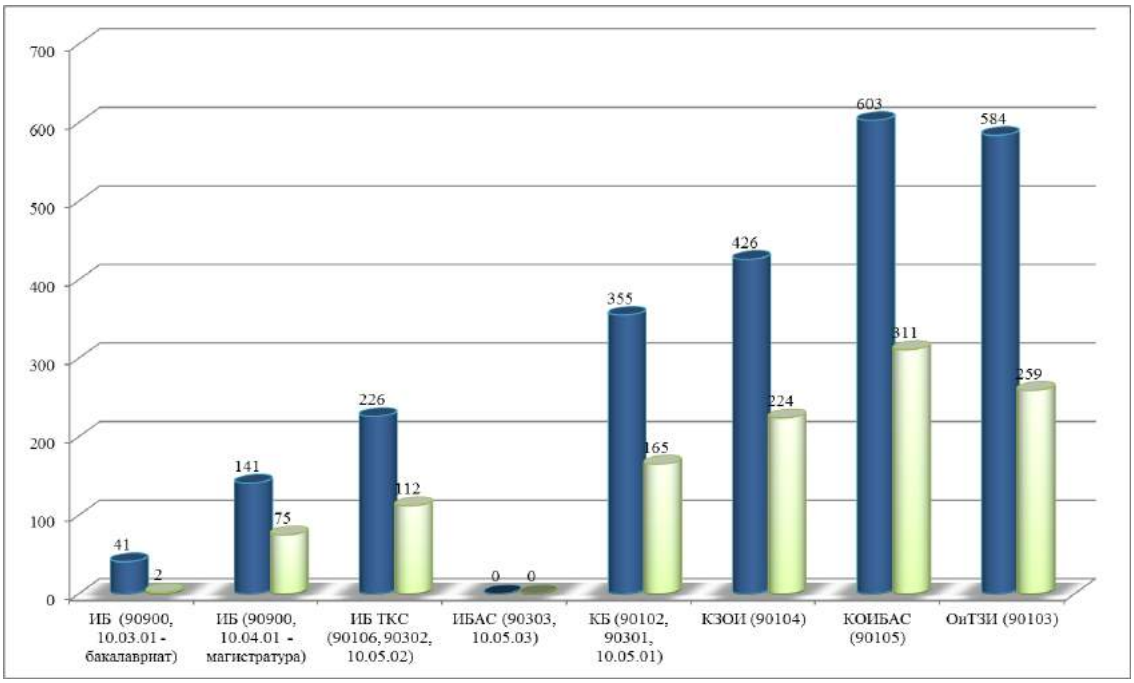


Рис. 6. Распределение численности выпускников образовательных организаций высшего образования 2014 года, обучавшихся по очной форме обучения (за счет средств бюджетов всех уровней) по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» и получивших направление на работу

(Fig. 6. Distribution of the number of graduates from higher educational institutions in 2014 who have been trained on full-time basis (at the expense of Federal budget allocations of any level) in the field of 10.00.00 «Information security» and received a position within this field)

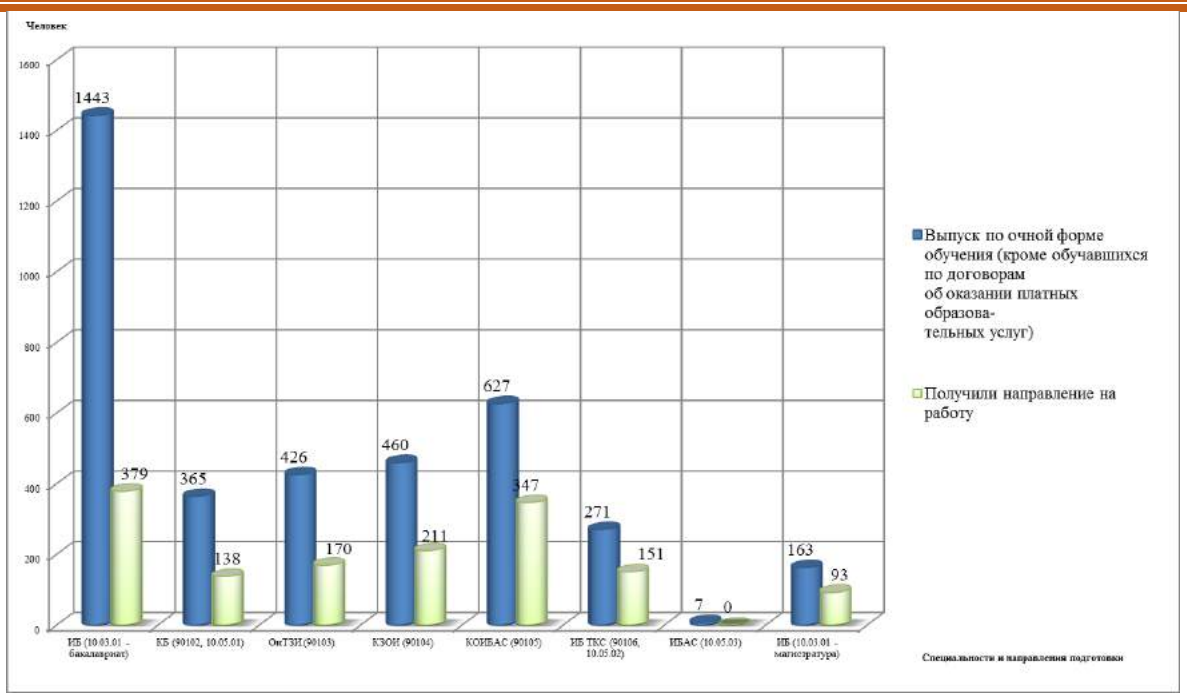
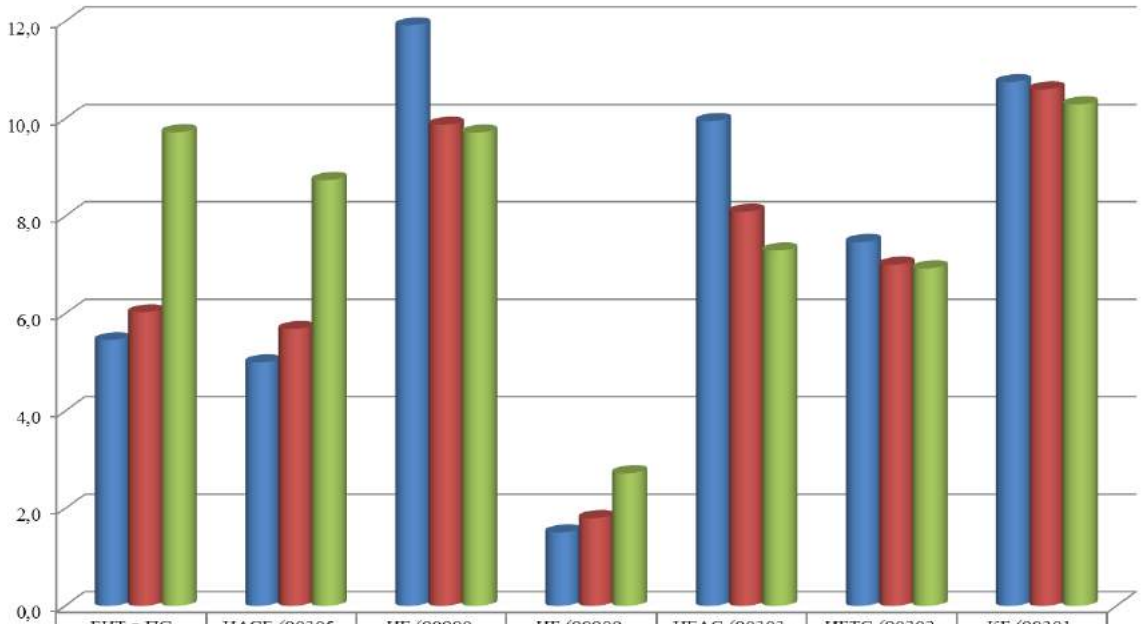


Рис. 7. Распределение количества выпускников образовательных организаций высшего образования 2015 года, обучавшихся по очной форме обучения (за счет средств бюджетов всех уровней) по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» и получивших направление на работу

(Fig. 7. Distribution of the number of graduates from higher educational institutions in 2015 who have been trained on full-time basis (at the expense of Federal budget allocations of any level) in the field of 10.00.00 «Information security» and received a position within this field)



	БИТ в ПС (10.05.05)	ИАСБ (90305, 10.05.04)	ИБ (90900, 10.03.01 - бакалавриат)	ИБ (90900, 10.04.01- магистратура)	ИБАС (90303, 10.05.03)	ИБТС (90302, 10.05.02)	КБ (90301, 10.05.01)
2013 год	5,5	5,0	11,9	1,5	10,0	7,5	10,8
2014 год	6,0	5,7	9,9	1,8	8,1	7,0	10,6
2015 год	9,7	8,7	9,7	2,7	7,3	6,9	10,3

Рис. 8. Распределение конкурса на обучение в образовательных организациях высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2013-2015 годах (человек на место)

(Fig. 8. Distribution of the average number of applicants competing for every place on training courses in higher educational institutions in the field of 10.00.00 «Information security» in 2013-2015)

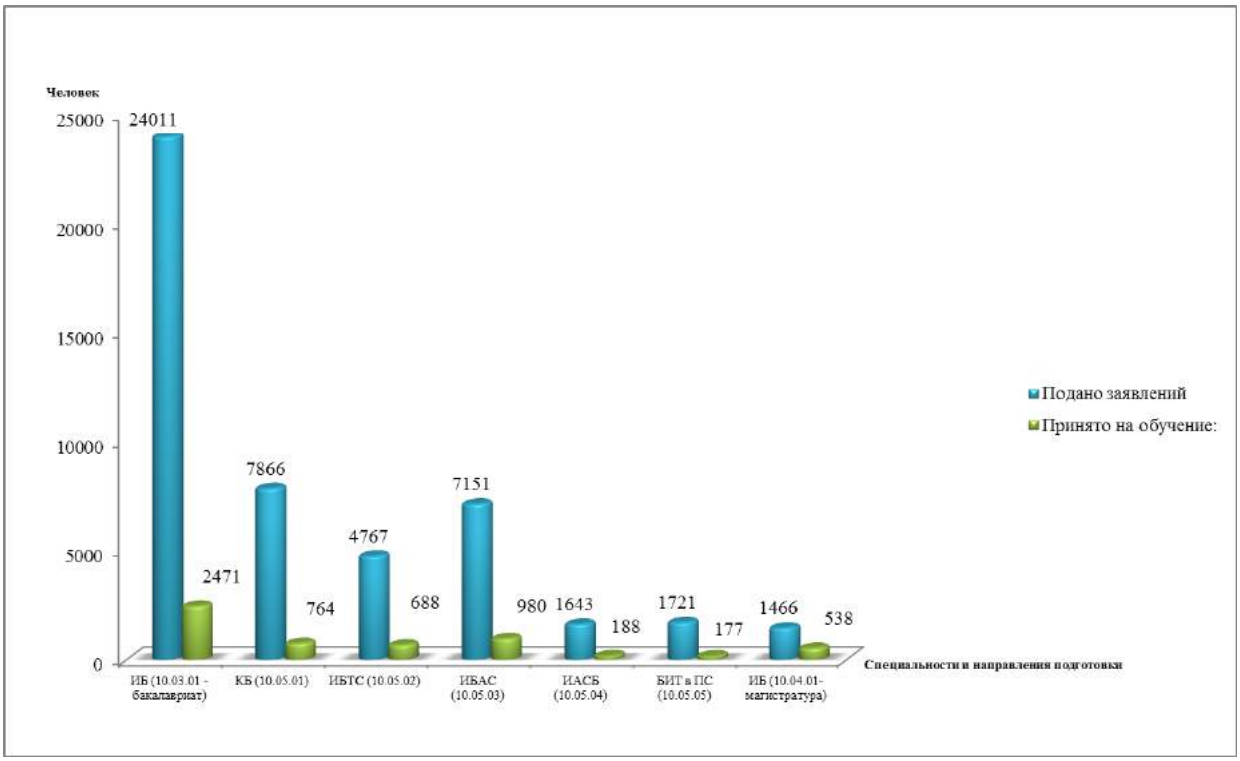


Рис. 9. Распределение численности принятых на обучение в образовательные организации высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году.

(Fig. 9. Distribution of the number of accepted for training courses in higher educational institutions in the field of 10.00.00 «Information security» in 2015)

8) Основным источником финансирования подготовки специалистов с высшим образованием по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» является федеральный бюджет. В 2015 году принято на обучение за счет средств федерального бюджета 4644 человек, что составляет 79 % от общего числа принятых на обучение. За счет бюджетных ассигнований субъектов Российской Федерации обучаются 1% (60 человек), и 20 % (1197 человек) обучаются на договорной основе с полным возмещением стоимости обучения. За счет бюджетных ассигнований местного бюджета по направлениям подготовки и специальностям 10.00.00 «Информационная безопасность» в 2015 году не принято ни одного человека.

Распределение количества, принятых на обучение по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году по источникам финансирования обучения приведено на рисунке 10.

9) Количество преподавателей дисциплин профессионального цикла в образовательных организациях по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» в системе высшего образования составляет – 2165 человек. Доля преподавателей, имеющих ученую степень, в общем числе преподавателей, обеспечивающих образовательный процесс по дисциплинам профессионального цикла, составляет – 742 человека (34 %), из них имеют ученую степень доктора наук – 113 человек. Характеристика квалификации преподавателей дисциплин профессионального цикла представлена на рисунке 11.

Базовое образование в области информационной безопасности имеют 19 % от общего числа преподавателей, прошли профессиональную переподготовку – 3 %, повышение квалификации в области информационной безопасности – 32 %.

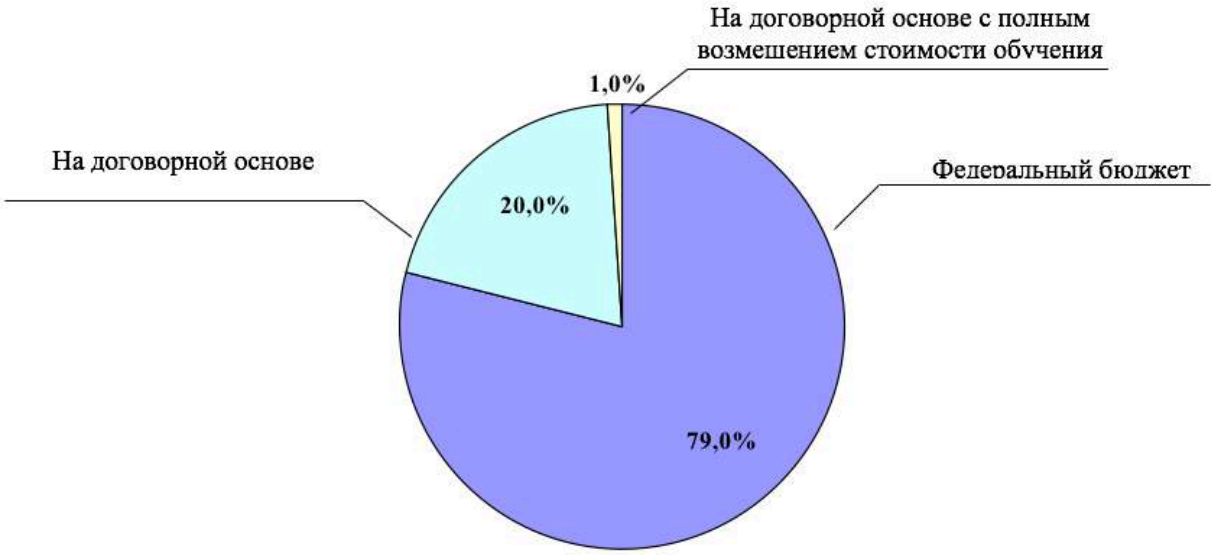


Рис. 10. Распределение количества принятых на обучение по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность» в 2015 году по источникам финансирования обучения
(Fig. 10. Distribution of the number accepted for training in the field 10.00.00 «Information security» in 2015 depending on the source of financing)

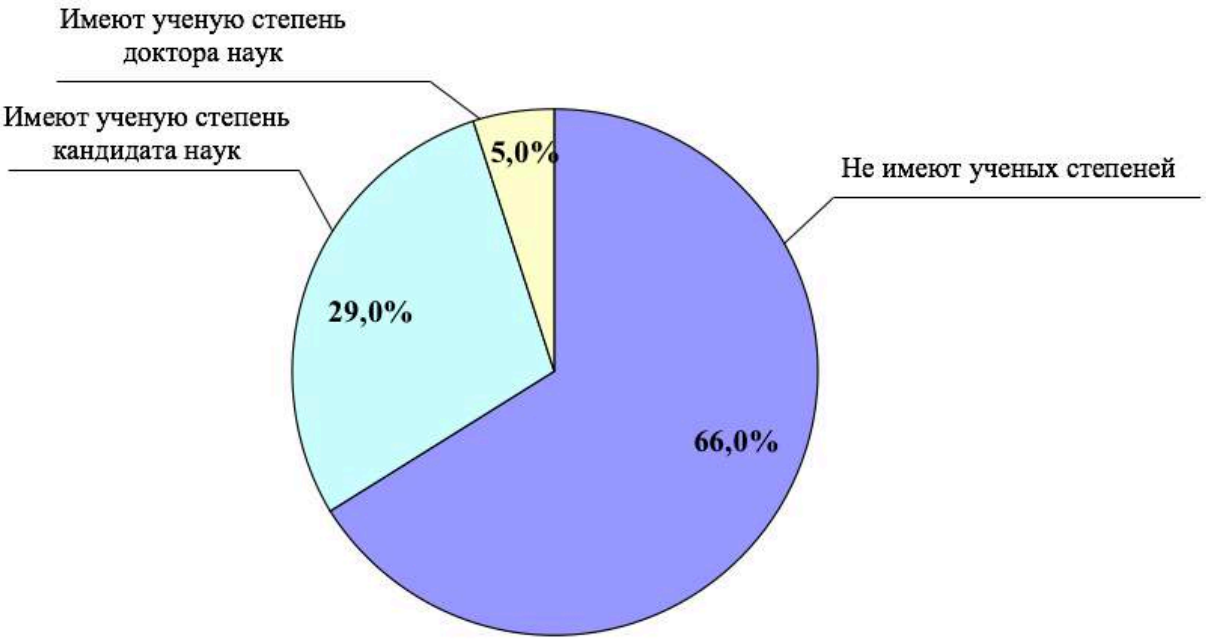


Рис. 11. Характеристика квалификации преподавателей дисциплин профессионального цикла (наличие ученых степеней)
(Fig. 11. The teacher's qualification for the professional cycle courses (academic degrees availability))

Доля преподавателей, имеющих образование в области информационной безопасности (базовое образование, профессиональная переподготовка или повышение квалификации в области информационной безопасности), представлена на рисунке 12.

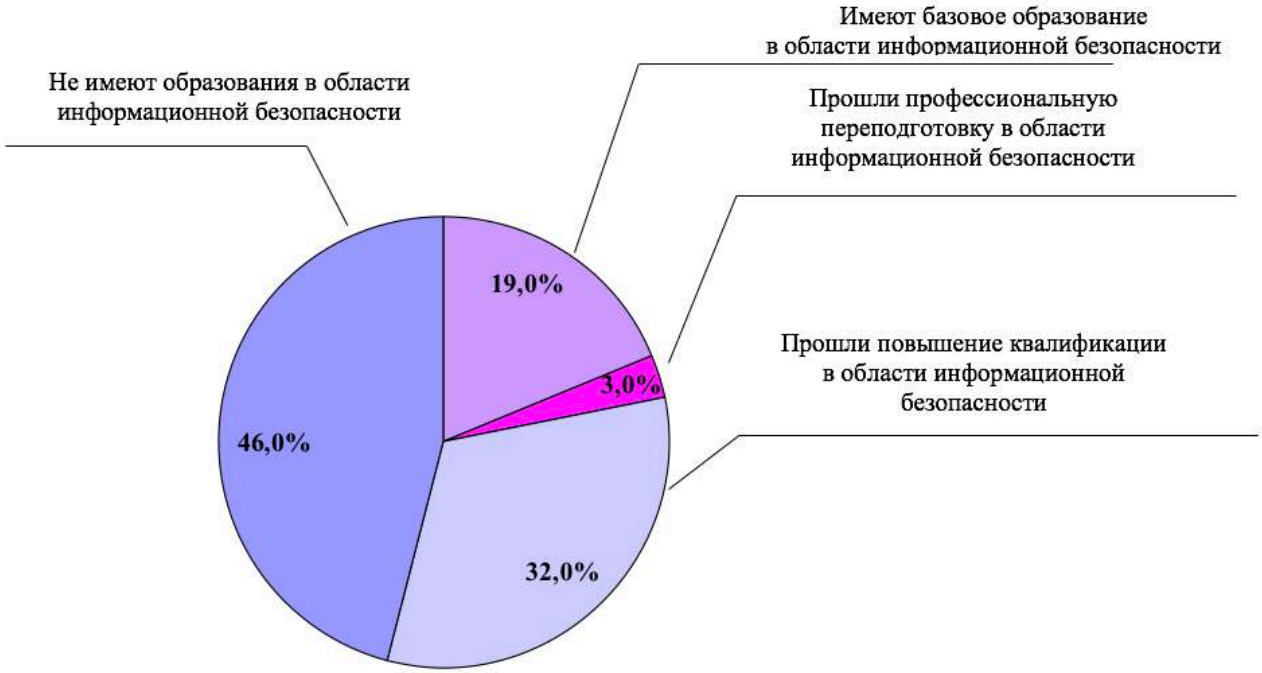


Рис. 12. Доля преподавателей, имеющих образование в области информационной безопасности (базовое образование, профессиональная переподготовка или повышение квалификации в области информационной безопасности)

(Fig. 12. Fraction of teachers having an education in the field of information security (basic education, retraining or advanced training in the field of information security))

Средний возраст преподавателей профессионального цикла и дисциплин специализации составляет 52 года, а их средний научно-педагогический стаж – 21 год. При этом средний стаж работы преподавателей в области информационной безопасности составляет – 9 лет, что обусловливается началом подготовки специалистов по защите информации по стандартам высшего профессионального образования второго поколения с 2000 года.

10) В целях определения состояния материально-технического обеспечения образовательного процесса, в т.ч. специализированным и лабораторным оборудованием, включая уникальные (экспериментальные) установки, стенды и другие технические средства или комплексы (полигоны) учебно-тренировочных средств, был проведен анализ около 100 отчетов образовательных организаций, реализующих программы в области обеспечения информационной безопасности по форме, разработанной УМО ИБ, а также обобщенных сведений об оснащенности образовательных организаций лабораториями и специализированным оборудованием для осуществления обучения по программам дисциплин профессионального цикла и дисциплин специализации 10.00.00 «Информационная безопасность» (по формам представления сведений).

Требования по материально-техническому обеспечению образовательных организаций, реализующих образовательные программы в области информационной безопасности, определяются условиями реализации ООП и устанавливаются Минобрнауки России во ФГОС.

Общее состояние материально-технического обеспечения образовательного процесса характеризуется следующим:

а) в полном объеме выполняют требования ФГОС ВО по наличию минимального перечня лабораторий только 56% образовательных организаций. В том числе имеют пять-шесть лабораторий – около 16% образовательных организаций, а семь и более лабораторий – около 40% образовательных организаций из числа образовательных организаций, выполняющих требования ФГОС.

При этом 20% образовательных организаций имеют уникальные (экспериментальные) постоянно совершенствующиеся установки, выпускающиеся в единичных экземплярах,

стенды или комплексы (полигоны) учебно-тренировочные средства в области обеспечения информационной безопасности;

б) около 10% от общего количества образовательных организаций имеют на своих площадях стендовое оборудование, размещенное предприятиями (организациями);

в) только в 15 образовательных организациях высшего образования в образовательный процесс внедрены типовые лабораторные практикумы, разработанные по заказу ФСТЭК России;

г) кроме того, отмечено, что не все образовательные организации имеют возможности в полной мере организовать учебную и производственную практики, которые требуют затрат на проживание и оплату суточных для обучающихся, проходящих практику, на приобретение транспортных услуг, в том числе расходы на проезд профессорско-преподавательского состава до места прохождения практики и обратно.

На основе статистической обработки ретроспективных данных [5] установлено, что доли бакалавров, специалистов и магистров в общем числе обучаемых составляют 37%, 48% и 15% соответственно.

На основе статистической обработки материалов, а также данных Минобрнауки России [5] определены доли выпускников, которые трудоустраиваются по специальности в области защиты информации, по отношению к общему количеству поступивших на обучение по соответствующему уровню высшего образования.

Доля выпускников бакалавриата, которые трудоустраиваются, составляет менее 60%.

Около 87% выпускников специалитета трудоустраиваются по специальности в области защите информации.

Выпускники магистратуры, которые трудоустраиваются, составляют около 90%.

Заключение

Представленные выше результаты анализа обобщенных данных охватывают основные, хотя и не все компоненты сферы образовательных услуг в области информационной безопасности, что обеспечивает необходимую репрезентативность выборки статистических результатов, позволяющих сделать вывод о том, что система подготовки кадров для государственной системы защиты информации находится на удовлетворительном уровне.

Значения приведенных выше характеристик использовались в качестве исходных данных при формирования предварительных предложений по контрольным цифрам приема по специальностям и направлениям подготовки укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» для обучения по образовательным программам высшего образования за счет бюджетных ассигнований федерального бюджета на 2018/2019 учебный год.

СПИСОК ЛИТЕРАТУРЫ:

1. Об утверждении перечня федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в установленных сферах деятельности, других главных распорядителей средств федерального бюджета, общероссийских объединений работодателей и иных организаций, осуществляющих деятельность в соответствующей сфере, представляющих предложения о контрольных цифрах приема по специальностям и направлениям подготовки для обучения по образовательным программам бакалавриата, программам специалитета, программам магистратуры и программам ординатуры за счет бюджетных ассигнований федерального бюджета [приказ Минобрнауки России 02.10.2015 № 1102 в редакции приказа Минобрнауки России 13.07.2016 № 860].
2. Об утверждении концепции кадрового потенциала молодежной политики в Российской Федерации [приказ Минспорттуризма России 23.12.2008 №72]. [Вестник Минспорттуризма Российской Федерации, №3, 2008].
3. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года [распоряжение Правительства Российской Федерации 01.11.2013 № 2036-р]. Собрание законодательства Российской Федерации. – М., 2013, №46, ст. 5954.
4. Об утверждении Правил установления организациям, осуществляющим образовательную деятельность, контрольных цифр приема по профессиям, специальностям и направлениям подготовки и (или) укрупненным

группам профессий, специальностей и направлений подготовки для обучения по образовательным программам среднего профессионального и высшего образования за счет бюджетных ассигнований федерального бюджета, а также о признании утратившими силу некоторых актов Правительства Российской Федерации [постановление Правительства Российской Федерации 27.03.2015 № 285]. Собрание законодательства Российской Федерации. – М., 2015, №14, ст.2128.

5. Министерство образования и науки Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.минобрнауки.рф. – Загл. с экрана. – Яз. рус.
6. Об утверждении перечней специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования, содержащих сведения, составляющие государственную тайну или служебную информацию ограниченного распространения [приказ Минобрнауки России 12.09.2013 №1060].
7. Об утверждении перечней специальностей и направлений подготовки высшего образования [приказ Минобрнауки России 12.09.2013 №1061].
8. Перечни профессий и специальностей среднего профессионального образования [приказ: утв. Минобрнауки России 29.10.2013 № 1199].

REFERENCES:

[1] On approval of the list of the Federal bodies of Executive power performing functions of elaborating state policy and normative legal regulation in the established areas, other main managers of means of the Federal budget of the all-Russian associations of employers and other organizations working in the relevant field, presenting proposals on the control figures of reception on specialities and directions of training for training on educational programs of a bachelor degree, programs specialist, programs of master's degree and residency programs at the expense of Federal budget allocations [order of the Ministry Of Education And Science of the Russian Federation 02.10.2015 № 1102 as amended by order of the Ministry Of Education And Science of the Russian Federation 13.07.2016 № 860]. (in Russian).

[2] About the approval of the concept of personnel potential of youth policy in the Russian Federation [the order of the Ministry of sports and tourism of Russia 23.12.2008 No. 72]. [the Bulletin of the Ministry of sports and tourism of the Russian Federation, No. 3, 2008]. (in Russian).

[3] About the approval of Strategy of development of branch of information technologies in the Russian Federation for 2014-2020 and for prospect till 2025 [the order of the Government of the Russian Federation No. 2036-p]. Collection of the legislation of the Russian Federation - M., 2013, № 46, Art. 5954. (in Russian).

[4] About the approval of Rules of establishment to the organizations performing educational activity, control figures of acceptance for professions, specialties and the directions of preparation and (or) enlarged groups of professions, specialties and the directions of preparation for training for educational programs of average professional and higher education at the expense of budgetary appropriations of the Federal budget, and also about recognition become invalid for some acts of the Government of the Russian Federation [resolution of the Government of the Russian Federation No. 285] 27.03.2015. Collection of the legislation of the Russian Federation. – M., 2015, no. 14, article 2128. (in Russian).

[5] Ministry Of Education And Science of the Russian Federation [Electronic resource]. – Mode of access: http://www.минобрнауки.рф. The title. from the screen. - Yaz. Ruskyi. (in Russian).

[6] About the approval of lists of the specialties and the directions of preparation of the higher education applied at implementation of the educational programs of the higher education containing the data which are the state secret or office information of limited distribution [the order of the Ministry Of Education And Science of Russian Federation 12.09.2013 No. 1060]. (in Russian).

[7] About the approval of lists of specialties and the directions of preparation of the higher education [order of the Ministry Of Education And Science of the Russian Federation 12.09.2013 No. 1061]. (in Russian).

[8] Lists of professions and specialties of secondary vocational education [order: utv. of the Ministry Of Education And Science of the Russian Federation 29.10.2013 № 1199]. (in Russian).

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.

Дмитрий А. Мельников[1], Григорий П. Гавдан[2], Иван А. Корсаков[3]
[1]Федеральный исследовательский центр «Информатика и управление» РАН,
Россия, 119333, Москва, Вавилова, д.44, кор.2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]Национальный исследовательский ядерный университет «МИФИ»,
115409, Москва, Каширское шоссе, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]ГлавНИВЦ Управления Делами Президента Российской Федерации,
125009, г. Москва, Славянская площадь, д. 4, стр. 1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

К ВОПРОСУ О ЦЕЛИ И ЗАДАЧАХ НАЦИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ИНИЦИАТИВЫ США В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.2.02

Аннотация. В текущем году Россия вступила в трехлетний переходный период ввода в действие профессиональных стандартов, призванных заменить традиционные нормативные указания Единого квалификационного справочника должностей руководителей, специалистов и служащих (ЕКС). Несколько профстандартов утверждены и для области кадрового обеспечения информационной безопасности.

Однако с позиций высшей школы существующий массив утвержденных профстандартов затруднительно использовать в качестве нормативной основы для совершенствования и развития существующей системы образовательных стандартов по направлению информационная безопасность, хотя такая очевидная концептуальная задача была поставлена в рамках перехода от ЕКС к профстандартам.

В настоящей работе проанализирован зарубежный опыт по решению указанной задачи на достаточно впечатляющем примере США. В рамках национальной образовательной инициативы в области кибербезопасности было проведено системное исследование структуры трудовых (кадровых) ресурсов в изучаемой области, предлагаемое в качестве фундаментального справочного ресурса. Он может быть использован для ориентации пользователей различных категорий, включая образовательные организации, для решения своих задач обеспечения трудовыми ресурсами в области кибербезопасности.

Компонентами системной кадровой структуры в области кибербезопасности выступают такие категории, как специализации/специальности, функциональные должности, компетенции (знания, умения, навыки) и функциональные обязанности (или задачи, решаемые при исполнении той или иной должности).

В работе проанализирована представленная структура трудовых ресурсов в области кибербезопасности, её содержание, а также рассмотрено её значение для гармонизации отечественных образовательных стандартов в сфере кибербезопасности.

Ключевые слова: кибербезопасность, образование, трудовые ресурсы, компетенции, знания, умения, навыки, специальности, функциональные обязанности, функциональные должности.

Для цитирования. МЕЛЬНИКОВ, Дмитрий А.; ГАВДАН, Григорий П.; КОРСАКОВ, Иван А.. К ВОПРОСУ О ЦЕЛИ И ЗАДАЧАХ НАЦИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ИНИЦИАТИВЫ США В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], n. 2, p. 23-37, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1107>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.02.

Dmitriy A. Melnikov[1], Grigory P. Gavdan[2], Ivan A. Korsakov[3]
[1]Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Russian Federation, 119333, Moscow, Vavilov str., 44/2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]National Research Nuclear University MEPhI,
Russian Federation, 115409, Moscow, Kashirskoe shosse, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]GRCC Presidential Property Managenet Department of the Russian Federation,
Russian Federation, 125009, Moscow, Slaviaskaia sq., 4/1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

To the issue about the purpose and objectives the USA National initiative for cybersecurity education

DOI: http://dx.doi.org/10.26583/bit.2018.2.02

Abstract. In the current year, Russia entered a three-year transitional period for the implementation of professional standards designed to replace the traditional regulations of the Unified Qualification Handbook (UQH) for the positions of executives, specialists and employees. Several professional standards have been approved for the field of staffing of information security.

However, from the higher school point of view, the existing variety of approved professional standards can hardly be used as a normative basis for the improvement and development of the existing system of educational standards in the information security area, although such an obvious conceptual task was set in the framework of the transition from UQH to professional standards.

This paper analyses foreign experience in solving this problem using rather impressive example of the United States. A systematic study of the labor (personnel) resources structure in the cybersecurity field was carried on within the framework of the national initiative for cybersecurity education, which is proposed as a fundamental reference resource. That resource can be used to guide the various category users, including educational organizations, to solve their tasks of providing labor resources in the field of cybersecurity.

The cybersecurity workforce framework (CWF) components include such categories as specialty areas, work roles, knowledge, skills, abilities and tasks (performed for any kind of work).

The paper analyzes the presented CWF, its content, as well as its important role in harmonizing the Russian educational standards in the field of cybersecurity.

Keywords: cybersecurity, education, workforces, competences, speciality areas, knowledges, skills, abilities, work roles, tacks.

For citation. MELNIKOV, Dmitriy A.; GAVDAN, Grigory P.; KORSAKOV, Ivan A.. To the issue about the purpose and objectives the USA National initiative for cybersecurity education. IT Security (Russia), [S.l.], n. 2, p. 23-37, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1107>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.02.

Введение

В текущем году Россия вступила в трехлетний переходный период изменения действующей системы квалификаций, в частности, перехода от ЕКС к системе профессиональных стандартов [1]. В соответствии с действующим трудовым законодательством в области кадрового обеспечения информационной безопасности также появилось несколько профессиональных стандартов [2,3]. Ряд проектов находится в стадии утверждения, например, [4]. Не будем вдаваться в подробный анализ имеющегося массива профстандартов в интересующей нас области, что является предметом отдельного исследования. В этой связи, с позиции представителей высшей школы отметим лишь, что в настоящий момент этот массив не может быть использован в качестве нормативной основы совершенствования и развития системы образовательных стандартов, что закладывалось как одна из концептуальных задач перехода к новой системе оценки квалификации [5], представляя профстандарты как отражение взглядов и потребностей работодателей.

Тем интереснее проанализировать соответствующий опыт зарубежных партнеров из развитых стран, например, США [6]. В соответствии с президентским указом [7] реализована национальная образовательная инициатива NICE (*The National Initiative for Cybersecurity Education* [8][1]), которая представляет собой партнёрское объединение представителей правительства, научных академий и частного сектора экономики, возглавляемое национальным институтом стандартов и технологий министерства торговли США (NIST[2]). Целью такого

[1] Оригинальный англоязычный текст соответствущего документа, его аутентичный перевод, включая вербальную модель кадрового обеспечения, имеется в распоряжении редакции журнала.

[2] Национальный институт стандартов и технологий (NIST) был основан в 1901 году и в настоящее время является частью Министерства торговли США. NIST – одна из старейших в мире физико-технических лабораторий. Сегодня NIST проводит исследования и разработку от самых мельчайших наноустройств до катастрофоустойчивых небоскрёбов и глобальных сетей связи.

объединения, перманентно осуществляющего свою деятельность уже более пяти лет, является методическая поддержка интересов правительственных и бизнес-структур по созданию и развитию широкой сети образовательных учреждений и всей системы образования, обучения и подготовки кадров в интересующей нас области знаний [9].

NICE обеспечивает достижение поставленной цели на основе:

- ✓ тесного взаимодействия с правительственными, академическими (научными) и отраслевыми партнерами;
- ✓ уже существующих успешных образовательных программ, способствуя их совершенствованию и обновлению;
- ✓ своего лидирующего положения и современных взглядов на проблемы увеличения числа высококвалифицированных специалистов в области кибербезопасности, что помогает обеспечить защиту национальных интересов страны и конкурентоспособность её экономики.

NICE ориентирована на рост общего числа работников, подготовленных для защиты национальных интересов от существующих и будущих угроз, и сохраняющих конкурентоспособность на всём протяжении своей профессиональной деятельности, начиная с момента приёма на работу и заканчивая выходом на пенсию.

Основной задачей, решаемой в рамках NICE, была разработка системной структуры трудовых ресурсов CWF (*Cybersecurity Workforce Framework*) [8]. Словосочетание «*трудовые ресурсы*» (*cybersecurity workforce*, буквально «рабочая сила») является обобщённым наименованием массива работников, занимающих определённые должности, непосредственно влияющие на способность организации (независимо от её формы собственности) по защите своей системы управления, включая информационные ресурсы и бизнес-процессы (основную деятельность). Указанный массив включает хорошо известные должности, например, связанные с обеспечением безопасности информационных технологий (ИТ), а относительно новые должности включают приставку «кибер» (*cyber*), указывающую на определённые направления деятельности, при описании которых она становится языковой (речевой) нормой.

Важным системным компонентом рассматриваемой структуры является включение должностей не только работников технического профиля, но и гуманитарного (юристов, экономистов и т. д.), то есть тех, кто применяет свои знания при обеспечении успешной и плодотворной работы по основным направлениям деятельности своей организации. В частности, структура включает должности высококвалифицированных работников, востребованных в процессах по нейтрализации рисков кибербезопасности в рамках общих планов мероприятий по анализу и снижению рисков основной деятельности, принятых в организациях.

1 Назначение национальной образовательной инициативы

1.1 Цели и сферы применения CWF

CWF была разработана в качестве фундаментального справочного ресурса, предназначенного для ориентации пользователей в интересах подготовки и обеспечения системы кибербезопасности потребности в квалифицированных кадрах. Основой этого ресурса является единый тематический словарь терминов (ETC), который позволяет системно классифицировать и описывать практически все виды деятельности в области кибербезопасности.

Такой фундаментальный справочный ресурс позволяет выявить и развить связи, необходимые для выявления, отбора и повышения квалификации работников соответствущей области применения, работодателям целенаправленно использовать единый язык в программах профессионального развития при выборе возможных направлений обучения своих сотрудников.

Очевидно, что также упрощаются процессы выбора и определения штатных должностей организации, а также подготовки соответствующих должностных инструкций (обязанностей). В этом смысле CWF может выступать в качестве фундаментальной справочной базы разработки системы профстандартов. Кроме этого, CWF задает ETC, который может быть

использован в сфере образовательных услуг при разработке учебных программ как в системах отраслевой аттестации и сертификации, так и программ университетского уровня.

С прикладной точки зрения, CWF даёт возможность описать практически все направления деятельности в области кибербезопасности, то есть любой вид деятельности или должность, связанная с обеспечением кибербезопасности, могут быть описаны путём использования соответствующих сведений из одной или нескольких частей структуры. Для каждого вида деятельности или должности, связанной с обеспечением кибербезопасности, смысл решаемых задач или бизнес-процессов, а также бизнес приоритетов, будет определять, какой информацией, содержащейся в CWF, следует воспользоваться.

Очевидна возможность использования CWF для разработки всего комплекса учебно-методического обеспечения [10], а также рекомендаций по различным аспектам формирования, планирования и профессионального обучения трудовых ресурсов рассматриваемой области.

1.2 Целевая аудитория

В отличие от отечественного, статус профессиональных стандартов анализируемой CWF рассматривается как рекомендуемый ETC. Пользователи, которые ссылаются на CWF, должны применять её только в интересах решения своих локальных задач, связанных с различными процессами формирования, образования и профессионального обучения кадров.

1.2.1 Работодатели

Использование ETC CWF позволяет работодателям на единой фундаментальной справочной базе проводить инвентаризацию и дальнейшее развитие своей кадровой системы для:

- проверки укомплектованности и поиска кадров с целью более глубокого анализа и выявления наиболее сильных сторон и пробелов в их компетенциях (знаниях (*knowledge*), умениях (*skills*) и навыках (способностях, *abilities*)), а также в должностных обязанностях (*tasks*);
- определения образовательных и квалификационных требований с целью формирования перечня наиболее значимых компетенций для описания должностных обязанностей;
- улучшения качества описания должностей и объявлений об имеющихся вакансиях, для которых установлены соответствующие компетенции, когда должности и должностные инструкции уже определены;
- определения ключевых должностей и формирования направлений карьерного роста с целью стимулирования сотрудников на получение навыков, требуемых для назначения на такие должности;
- формирования общей терминологии, используемой кадровиками при приёме на работу, сохранении и обучении высококвалифицированных сотрудников.

1.2.2 Работающие и будущие специалисты в области кибербезопасности

CWF будет востребована теми, кто уже входит в состав подразделений обеспечения кибербезопасности, и теми, кто в перспективе планирует стать таким специалистом. На ее основе можно проанализировать задачи, решаемые различными категориями специалистов в (*categories*), а также предусмотренные должностными инструкциями. Это может помочь соискателям вакансий, а также студентам для понимания какие должности среди самых популярных вакансий и соответствующие им компетенции, связанные с обеспечение кибербезопасности, наиболее востребованы работодателями. Кроме того, CWF может быть полезна вспомогательным работникам, например, специалистам по кадровому обеспечению и советникам руководителей. В частности, использование CWF специалистами кадровых служб поможет им корректно оформлять необходимую документацию, что обеспечит правильное понимание претендентами будущих должностных обязанностей и соответствующего уровня профессиональной подготовки, необходимого для замещения таких вакансий и определения векторов карьерного роста.

В свою очередь при использовании ETC CWF в сфере образовательных услуг облегчает будущим соискателям поиск нужного образовательного учреждения и/или отраслевого центра сертификации, реализующих образовательные программы с соответствующими итогами обучения и объёмами знаний, которые отображаются в компетенциях и должностных обязанностях, востребованных работодателями.

1.2.3 Преподавательский состав

CWF окажет неоспоримую помощь преподавателям (научно-педагогическим работникам) при разработке ими учебных программ, программ сертификации (повышения квалификации), тем выпускных квалификационных работ, а также программ лекционных курсов, семинаров, практических занятий и лабораторных работ, которые охватывают компетенции и должностные обязанности (задачи, решаемые при замещении определённых должностей), описанные в CWF.

1.2.4 Компании-разработчики средств защиты информации

CWF позволяет технологическим компаниям (разрабатывающим и внедряющим соответствующие технические средства обеспечения кибербезопасности) устанавливать должности и определяемые ими функциональные обязанности, относящиеся к области кибербезопасности, а также компетенции, связанные с разработкой и эксплуатацией программных и программно-аппаратных комплексов и услугами, которые они предоставляют. В дальнейшем технологическая компания может разработать дополнительные инструкции и руководства в качестве вспомогательных материалов для специалистов, обслуживающих (включая точную настройку и администрирование) такие комплексы.

2 Взаимосвязи компонентов CWF

2.1 Компоненты CWF

CWF позволяет организовать не только кадровое обеспечение кибербезопасности, но и связанные с ней вспомогательные работы. Далее представлены и описаны основные компоненты CWF.

2.1.1 Категории специалистов

Категории специалистов представляют собой верхний уровень иерархии в модели CWF, демонстрирующий ее организационный «фундамент» (см. *Таблицу 1*). Выделено семь категорий специалистов, каждая из которых включает специализации и функциональные должности. Такая организация CWF разработана на основе анализа трудовой деятельности в области кибербезопасности, она объединяет направления трудовой деятельности и самих работников, которые имеют общие функциональные обязанности, независимо от наименования занимаемой должности или других условий трудового договора.

Таблица 1. Категории специалистов в CWF
(Table 1. NICE Framework Workforce Categories)

Категория	Описание
Обеспечение защищённости (SP)	Разработка концепций, проектов, закупка и/или создание защищённых информационно-технологических систем (ИТС), включая ответственность за все аспекты развития и совершенствования систем и/или сетей.
Эксплуатация и обслуживание (OM)	Обеспечение технической поддержки, администрирования и обслуживания необходимого для гарантированного эффективного и высокопроизводительного функционирования ИТС и её подсистемы обеспечения безопасности.
Контроль и управление (OV)	Включает общее руководство, организацию материально-технического обеспечения, разработку директив и инструкций, системы совершенствования и развития, а также нормативного и правового обеспечения, дающих возможность осуществлять эффективную деятельность по обеспечению кибербезопасности

Категория	Описание
Защита и отражение/парирование (PR)	Определение, анализ и отражение/парирование кибератак/киберугроз, затрагивающих функционирование внутренних ИТС и/или сетей.
Анализ (AN)	Проведение узкоспециализированного анализа и оценки входящей информации, связанной с кибербезопасностью, с целью определения её значимости для проведения разведывательных мероприятий.
Добывание информации и проведение операций (CO)	Проведение специализированных операций по предотвращению попыток противоправных действий и введению в заблуждение, а также добывание информации, затрагивающей кибербезопасности, которая может быть использована для совершенствования разведывательных мероприятий.
Расследование (IN)	Расследование инцидентов или киберпреступлений, связанных с функционированием ИТС и сетей, а также применением цифровых доказательств (свидетельств).

2.1.2 Специальности/специализации

Категории специалистов (см. *Таблицу 2*) задают группы основных направлениий трудовой деятельности по обеспечению кибербезопасности, которые называются специализациями (*specialty areas*). Каждая специализация отражает сферу более конкретной трудовой деятельности или функциональных обязанностей в области обеспечения кибербезопасности, включая иную связанную вспомогательную деятельность.

Таблица 2. Специальности/специализации в CWF
(Table. NICE Framework Specialty Areas)

Категория	Специализация/ специальность	Описание
Обеспечение защищённости (SP)	Анализ и снижение рисков (RSK)	Контроль, анализ и сопровождение процессов документирования, утверждения, оценки и авторизации, необходимых для обеспечения гарантий того, что существующие и новые ИТС отвечают требованиям обеспечения безопасности и снижения рисков организации. Обеспечение гарантий приемлемой трактовки риска, его анализа и надёжной защиты с учётом всех внутренних и внешних факторов (условий).
	Разработка ПО (DEV)	Разработка и написание новых (или обновление существующих) программ для компьютерных прикладных систем, базового программного обеспечения (включая операционные системы) или специализированных вспомогательных программ, используя лучшие надёжные методики написания программ.
	Архитектура систем (ARC)	Разработка концепций систем и дальнейшая работа на всех возможных этапах жизненного цикла создания и развития систем, внедрение технологий в системные проекты и процессы, в том числе в систему обеспечения кибербезопасности с учётом внешних условий (например, законодательство и нормативные акты и стандарты).
	Исследование и разработка технологий (TRD)	Проведение процедур оценки и интеграции технологий, реализация и обеспечение функционирования прототипа и/или оценка его полезности.
	Проектирование системных требований (SRP)	Проведение консультаций с заказчиками с целью определения и оценки функциональных требований, а также реализация таких требований в технических решениях. Разработка методических инструкций для пользователей о порядке применения и использования информационных систем с целью удовлетворения бизнес-потребностей.
	Тестирование и оценивание (TST)	Разработка и испытание (тестирование) систем с целью оценки их соответствия техническим заданиям и требованиям на основе принципов и использования методов эффективного экономического планирования, оценивания, проверки и утверждения технических, функциональных и эксплуа-

Категория	Специализация/ специальность	Описание
		тационных характеристик (включая функциональную совместимость) ИТС или их компонентов.
	Развитие систем (SYS)	Деятельность по созданию, развитию и совершенствованию систем на всех этапах их жизненного цикла.
Эксплуатация и обслуживание (OM)	Администрирование данных (DTA)	Разработка и администрирование БД и/или СУБД, которые позволяют хранить, запрашивать, защищать и использовать данные.
	Информационное обеспечение (KMG)	Обеспечивает и сопровождает процедуры и средства, позволяющих идентифицировать, документировать и получать доступ к интеллектуальным данным и информационным материалам.
	Обслуживание и техническая поддержка клиентов (STS)	Устранение проблем; инсталляция, настройка, диагностика и проведение техобслуживания и обучения клиентов на основе их требований или запросов (например, многоуровневая поддержка клиентов). Как правило, предоставление исходных данных об инциденте специалисту по реагированию на инциденты (IR).
	Сетевые службы (NET)	Инсталляция, настройка, испытание (тестирование), эксплуатация, обслуживание и обеспечение сетей и их сетевых экранов, включая программно-аппаратные комплексы (например, концентраторы, мосты, коммутаторы, мультиплексоры, маршрутизаторы, кабели, уполномоченные серверы (УПС) и заградительные распределённые системы) и ПО, которые позволяют совместно использовать и передавать данные в интересах всех форм информационного обмена с целью обеспечения безопасности информации и информационных систем.
	Системное администрирование (ADM)	Инсталляция, настройка, диагностика и обслуживание системы настройки сервера (программно-аппаратного комплекса и ПО) с целью гарантированного обеспечения его конфиденциальности, целостности и доступности. Ведение учётных записей, обслуживание сетевых экранов и обновление их данных. Ответственность за систему управления доступом, включая подсистему формирования и администрирования паролей и учётных записей.
	Системный анализ (ANA)	Анализ используемых организацией вычислительных систем и процессов, а также разработка проектов ИТС с целью оказания помощи организации функционировать результативно, эффективно и в более защищённом режиме. Объединение бизнеса и информационных технологий на основе понимания необходимости такого объединения и последующих возможных ограничений.
Контроль и управление (OV)	Юридическое консультирование и правовая защита (LGA)	Правовое консультирование и разработка рекомендаций для руководства и персонала по целому ряду актуальных тем в соответствующей предметной области. Распространение изменений в законодательстве и политике, ведение дел по поручению клиентов, используя для этого всевозможные письменные документы и вступления в судебных инстанциях, включая нормативные правовые документы и судебные разбирательства.
	Обучение, образование и осведомлённость (TEA)	Организация и проведение обучения персонала в соответствующей предметной области. Разработка, планирование, согласование, представление и/или оценивание приемлемых учебных курсов, методов и методик преподавания.
	Обеспечение кибербезопасности (MGT)	Контроль реализации программы по обеспечению кибербезопасности, конкретной программы или иной зоны ответственности, с целью задействования стратегических, кадро-

Категория	Специализация/ специальность	Описание
		вых, инфраструктурных и иных востребованных ресурсов, а также системы принудительного исполнения политики, системы планирования в чрезвычайных ситуациях и системы оповещения о состоянии защищённости.
	Стратегическое планирование и политика (SPP)	Разработка стратегий и планов и/или структуры правового обеспечения в случаях изменения политики, которые обеспечивают реализацию инициатив организации в сфере киберпространства или осуществление необходимых изменений/усовершенствований.
	Исполнительное киберруководство (EXL)	Контролирует, обеспечивает и/или руководит деятельностью и специалистами, осуществляющими такую деятельность, которая предусматривает проведение кибероперации и/или иных связанных с ними мероприятий.
	Обеспечение и сопровождение программ/проектов (PMA), а также закупка и комплектование	Использование научных знаний о данных, информации, процессах, организационном взаимодействии, способностях и аналитической экспертизе, а также системах, сетях и особенностях информационного обмена с целью реализации программ закупок и комплектования. Исполнение обязанностей, связанных с выполнением программ приобретения программно-аппаратных комплексов, ПО и информационных систем, а также реализацией политик сопровождения других программ. Оказание непосредственной поддержки процессам закупки и приобретения изделий и услуг, которые используют информационные технологии (включая системы национальной безопасности), основываясь при этом на законах и нормативных правовых актах в сфере информационных технологий, а также разработка рекомендаций в сфере информационных технологий на протяжении всего жизненного цикла программы закупок и комплектования.
Защита и отражение/парирование (PR)	Анализ подсистемы отражения/парирования кибератак (CDA)	Использование защитных мер и данных, добытых из различных источников для идентификации, анализа и подготовки отчёта о событиях, которые произошли или могут произойти в рамках сети, с целью защиты информации, информационных систем и сетей от возможных угроз.
	Инфраструктурная поддержка отражения/парирования кибератак (INF)	Тестирование, внедрение, реализация, обслуживание и проверка программно-аппаратных комплексов и ПО инфраструктуры, которое необходимо для обеспечения сети провайдера, предоставляющего услуги по защите вычислительной сети, и для обеспечения ресурсами. Мониторинг сети с целью активного противодействия несанкционированным процессам.
	Реагирование на инциденты (CIR)	Реагирование на кризисные или экстренные ситуации в рамках соответствующего сетевого сегмента с целью уменьшения негативных последствий от реализации прямых или потенциальных угроз. Применение способов снижения негативных последствий от реализации угроз, обеспечения готовности к несанкционированным действиям и реагирования на них и восстановления требуемого уровня защищённости (при необходимости) с целью достижения максимального уровня «живучести», защиты имущества и информационной безопасности. Расследование и анализ всех соответствующих процессов, относящихся к реагированию на инциденты.
	Оценка и снижение числа уязвимостей (VAM)	Экспертная оценка угроз и уязвимостей; определение нарушений в допустимых настройках, политике организации или локальной политике; оценка уровня риска; разработка и/или подготовка рекомендаций по использованию контрмер по снижению негативных последствий в различных ситуациях, связанных с функционированием систем или их эксплуата-

Категория	Специализация/ специальность	Описание
		цией.
Анализ (AN)	Анализ угроз (TWA)	Определение и оценка возможностей и направлений противоправной деятельности киберпреступников или иностранных разведывательных служб; предоставление полученных данных для оказания помощи на начальном этапе расследования или для информационного обеспечения уже ведущегося расследования, а также с целью поддержки иных мероприятий, направленных на обеспечения законности и правопорядка, включая контрразведывательные мероприятия.
	Анализ использования уязвимостей (EXP)	Анализ добытой информации с целью выявления уязвимостей и потенциальных возможностей их использования.
	Всесторонний анализ (ASA)	Анализ информации об угрозах, полученной из различных источников, образовательных курсов и ведомств, входящих в разведывательное сообщество. Обобщение и логически связывание между собой имеющихся разведывательных материалов; формирование представления о возможных последствиях.
	Целевые объекты (TGT)	Применение современных знаний об одном или нескольких регионах, странах, негосударственных организациях и/или технологиях.
	Языковый анализ (LNG)	Проведение языковой, культурологической и технической экспертизы с целью обеспечения процессов добывания информации, анализа и других мероприятий, связанных с обеспечением кибербезопасности.
Добывание информации и проведение операций (CO)	Операции по добыванию данных/информации (CLO)	Добывание информации на основе использования соответствующих стратегий и с учётом приоритетов, установленных в процессе обеспечения операций по добыванию информации.
	Планирование кибероперациий (OPL)	Реализация процесса всеобъемлющего планирования совместных мероприятий целеполагания и обеспечения кибербезопасности. Накопление информации и определение требований, необходимых для разработки подробных оперативных планов и приказов. Осуществление стратегического и оперативного планирования для всего спектра операций при проведении совместных информационных и операций в киберпространстве.
	Проведение кибер-операций (OPS)	Осуществление мероприятий по сбору и накоплению свидетельств противоправной деятельности киберпреступников или зарубежных разведывательных служб с целью снижения негативных последствий от реализации возможных и реальных угроз, защиты от шпионажа или внутренних угроз, иностранного саботажа, деятельности международных террористических организаций, либо с целью обеспечения иных разведывательных мероприятий.
Расследование (IN)	Киберрасследование (INV)	Применение тактических приёмов, способов и процедур с использованием всего спектра средств и методов расследования, включая (но этим не ограничивается) методы собеседования и допроса, слежения, контрслежения и обнаружения слежки, а также соответствующее сравнение преимуществ ведения прокурорского расследования или проведения разведывательных мероприятий.
	Цифровая криминалистика (FOR)	Добывание, обработка, хранение, анализ и предъявление компьютерных доказательств при проведении контрразведывательных и мероприятий по снижению негативных последствий от использования уязвимостей, а также при расследовании криминальных и мошеннических преступлений, или при проведении расследований правоохранительными

Категория	Специализация/ специальность	Описание
		органами.

2.1.3 Функциональные должности

Функциональные должности представляют собой более детальные классы деятельности по обеспечению кибербезопасности, включая иную связанную с ее обеспечением деятельность. Функциональные должности включают перечни необходимых для исполнения этих должностей атрибутов в форме компетенций и функциональных обязанностей, предусмотренных этими должностями.

Трудовая деятельность, связанная с исполнением функциональных обязанностей или занимаемой штатной должности, описывается с помощью выбора одной или нескольких функциональных должностей из CWF, соответствующих данной функциональной деятельности или должности, направленной на реализацию основных направлений деятельности или бизнес программ.

2.1.4 Компетенции

Компетенции являются характерными свойствами, которые необходимы при исполнении функциональных должностей, и, как правило, демонстрируются посредством соответствующего опыта, образования и уровня подготовки.

Знание (*knowledge*) — это совокупность информации, используемой непосредственно при исполнении функциональных обязанностей. CWF включает описания примерно 600 групп знаний.

Умение (*skill*) — это, как правило, способность продемонстрировать выполнение выученного психомоторного действия. Умения, с точки зрения психомоторики, характеризуют способность физически управлять орудием труда или инструментом, подобно руке или молотку. Умения, необходимые для обеспечения кибербезопасности, меньше всего зависят от физического манипулирования орудиями труда и инструментами, но больше зависят от применения программного инструментария, различных платформ (операционных систем), процедур или средств управления, которые воздействуют на состояние кибербезопасности организации или физического лица. CWF включает описания примерно 370 умений.

Навык (*ability*) — это способность выполнить требуемое действие или действие, которое приведёт к требуемому результату. CWF включает описания примерно 170 навыков.

2.1.5 Функциональные (должностные) обязанности (решаемые задачи)

Решаемая задача (функциональная обязанность) – это конкретно определённая часть работы, которая в совокупности другими задачами, составляет деятельность, определяемую конкретной специальностью/специализацией или функциональной должностью. CWF включает описания примерно 1000 функциональных обязанностей.

2.2 Взаимосвязи компонентов CWF

Иерархическая модель взаимосвязей компонентов CWF, характеризующих кадровое обеспечение деятельности в области кибербезопасности, показана на рисунке 1, где представлена категория специальностей, включающая специальности/специализации, которые, в свою очередь, состоят из одной или нескольких функциональных должностей. Каждая функциональная должность включает соответствующие компетенции и решаемые задачи (функциональные обязанности).

Объединение компонентов представленным способом существенно упрощает связи между специализациями, а также помогает согласовывать их со специализациями в других сферах трудовой деятельности. NICE предлагает вербальную гипертекстовую модель CWF, описывающую конкретные связи между функциональными должностями с компетенциями и

решаемыми задачами (функциональными обязанностями), в соответствии с иерархией компонет на рисунке 1, которая представлена в [8].

3 Сферы применения CWF

Использование CWF с целью понимания потребностей организации и оценки степени удовлетворения этих потребностей может оказать большую помощь организации при планировании, реализации и контроле выполнения программы по надёжному обеспечению кибербезопасности.

3.1 Идентификация потребностей в трудовых ресурсах

Обеспечение кибербезопасности — это быстроизменяющееся и расширяющаяся область деятельности. Такое расширение требует наличие кадрового состава, включающего высококвалифицированных работников, которые смогут помочь организациям реализовать функции (решить задачи) в условиях перманентного изменения внешних угроз. Так как организации определяют, что необходимо для эффективного снижения текущих и последующих рисков, связанных с кибербезопасностью, руководителям необходимо оценить необходимый качественный и количественный состав своих работников.

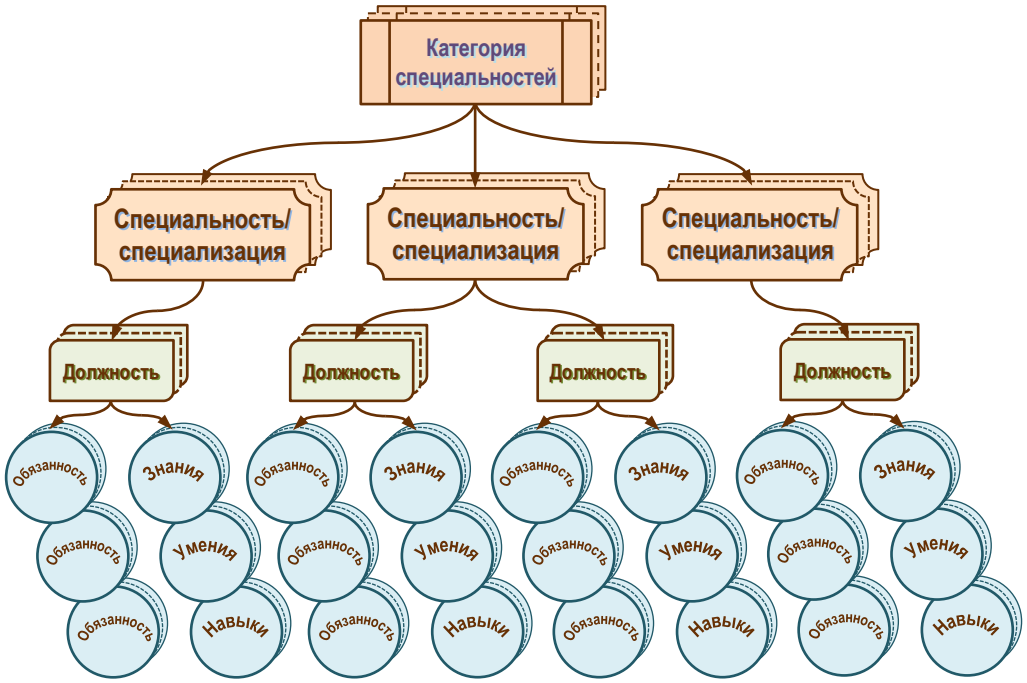


Рис. 1. Иерархическая модель взаимосвязей компонентов CWF
(Fig.1. Relationships among NICE Framework Components)

На рисунке 2 показано, что CWF является центральным ядром при оказании помощи работодателям, которые формируют работоспособный и профессионально пригодный кадровый состав [8].

Круговые стрелки в левой части рисунка 2 — это направления деятельности, которые могут повлиять на способность организации формировать и совершенствовать работоспособную и профессионально пригодную рабочую силу:

- использование ETC, предложенного CWF, способствует установлению прозрачных связей между научно-педагогическими работниками, специалистами органов аттестации/сертификации, работодателями и работниками;

▪ аналитическая работа по определению критичности бизнес-процессов позволит определить те компетенции и функциональные обязанности (решаемые задачи), которые имеют решающее значение для успешного исполнения функциональной должности, а также те, которые являются главными для нескольких функциональных должностей;

▪ проведение анализа профпригодности будет определять необходимый уровень подготовки (например, начальный уровень, эксперт) для тех штатных должностей (вакансий), которые объединяют в себе несколько функциональных должностей. Анализ профпригодности должен повысить качество выбора соответствующих необходимых функциональных обязанностей и компетенций, необходимых для описания функциональных должностей, которые составляют одну вакансию (штатную должность).

3.2 Подбор и наём высококвалифицированных кадров

Использование CWF в качестве направляющего документа окажет существенную помощь организациям при проведении стратегического планирования и найма кадрового состава.

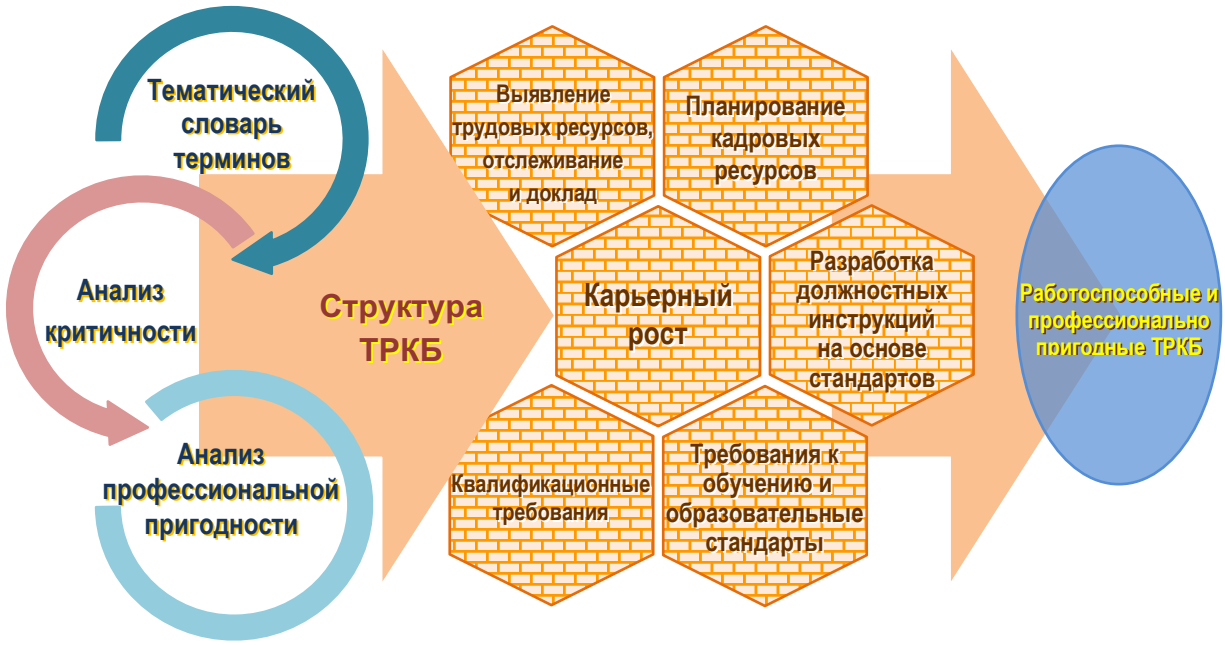


Рис. 2. «Строительные блоки» системы формирования профессионального кадрового состава (Fig. 2. Building Blocks for a Capable and Ready Cybersecurity Workforce)

Информация, представленная в CWF и используемая при создании штатного расписания, включения новых или при корректировке описаний штатных должностей, анонсируемых как вакансии и размещаемых в объявлениях, поможет претендентам, имеющим соответствующую квалификацию, найти конкретные интересующие их должности, которые они готовы исполнять. Решаемые функциональные задачи, используемые при описании должностных обязанностей и зон ответственности, а также компетенции, используемые для описания требуемых способностей и квалификации при исполнении должности, должны обеспечить претендентам на свободные вакансии и сотрудникам по кадровому обеспечению более эффективное взаимопонимание. Описание функциональных должностей и объявления о вакансиях с использованием терминологии, представленной в CWF, содержат критерии более качественной оценки, осуществляемой при проверке и принятии решения о приёме на работу претендентов.

Перечень решаемых задач, представленный в CWF, поможет организациям, в которых наблюдается недостаток кадров, точно определить конкретные задачи, не решаемые в таких организациях, и определить функциональные должности и специальности/специализации,

которые являются проблемными. Организациям следует взаимодействовать с научно-образовательными учреждениями, центрами сертификации и лицензирования, которые согласуют свои предложения с CWF. Организация может определить курсы переподготовки и повышения квалификации, которые необходимы для штатных специалистов с целью ликвидации недостатка квалифицированных кадров. Специалисты по каровому обеспечению, использующие информацию, представленную в CWF, способны на этой основе выявить претендентов на замещение имеющихся вакансий, обладающих необходимыми компетенциями.

3.3 Образование, переподготовка и повышение квалификации

Представленная в CWF идентификация функциональных обязанностей, в зависимости от функциональных должностей, помогает научно-педагогическим работникам дать обучаемым конкретные компетенции, которые могут продемонстрировать претенденты, как способность решать поставленные перед ними задачи по обеспечению кибербезопасности.

Научно-образовательные учреждения являются важной частью всеобщей сферы образовательных услуг. Сотрудничество государственных и частных организаций, например, на основе реализации научной программы, позволяет таким организациям обеспечить единство знаний и выделить наиболее востребованные способности. В свою очередь, разработка и реализация образовательных программ, которые гармонизированы с ETC, представленным в CWF, позволяет научно-образовательным учреждениям необходимую подготовку, востребованную работодателями. По мере увеличения числа студентов, осуществляющих поиск приемлемой работы, все больше студентов будет заинтересовано в выборе необходимых программ обучения для будущего карьерного роста.

3.4 Сохранение кадрового потенциала

Важной моментом совершенствования в деятельности любой организации является развитие и сохранение ее кадрового потенциала. Современный квалифицированный работник, как правило, обладает устоявшимися взаимоотношениями и связями, имеет опыт организационной работы и знания, вследствие чего его весьма трудно заменить другим сотрудником. Замещение вакансии после ухода работника повлечет за собой новые расходы, связанные с распространением рекламы и процедурой приёма на работу новых претендентов, затраты на обучение, снижение производительности и ухудшению морально-нравственной атмосферы в коллективе. Далее представлен перечень некоторых способов, обеспечивающих сохранение и развитие высококвалифицированных и талантливых кадров:

- для работников организации могут быть предложены пути карьерного роста, которые будут включать описание квалификационных требований, необходимых для будущего замещения перспективных и непрерывно совершенствующихся функциональных должностей, например, перечисленных в CWF;
- точное понимание штатными работниками компетенций и функциональных обязанностей поможет им определить дальнейшие шаги своего карьерного роста, которые потребуются для развития их профессионального потенциала, и которые помогут им стать профессионально пригодными для замещения желаемых вакансий;
- организация может предложить штатным сотрудникам должностную ротацию, которая даст им возможности для совершенствования и применения новых компетенций;
- организации могут определить, какие сотрудники проявляют усердие при совершенствовании своих компетенций, и выявить, таким образом, лидеров;
- организации могут разработать планы по развития и профессиональному совершенствованию штатных сотрудников, что, в свою очередь, поможет им понять, как они смогут приобрести компетенции, необходимые для замещения новых вакансий;
- с целью получения штатными сотрудниками организации новых единых компетенций могут быть определены возможности проведения занятий в составе групп;

- организации могут использовать обучение и контроль знаний, нацеленные на получение конкретных умений и навыков, с целью анализа профпригодности в реальных условиях;
- организации могут использовать штатный персонал для замещения важных и востребованных свободных или вновь введённых вакансий, связанных с обеспечением кибербезопасности, используя для этого повторный пересмотр резюме штатных сотрудников с целью выявления у них необходимых для этих вакансий компетенций;
- CWF полезна и для штатных сотрудников, которые желают перейти со своей занимаемой должности на другую, связанную с обеспечением кибербезопасности. Организация может охарактеризовать для благонадёжного сотрудника, не занимающегося вопросами обеспечения безопасности, необходимые компетентности, чтобы он вошёл в состав служб, берущих на себя решение всех задач обеспечения кибербезопасности.

4 Использование CWF в России

Безусловно, анализируемый стандарт может сыграть неоценимую роль в сфере совершенствования отечественной системы подготовки специалистов по кибербезопасности.

Во-первых, CWF как рекомендуемый единый справочник терминов и определений позволит уточнить, скорректировать и, возможно, дополнить основные направления подготовки специалистов по направлению «информационная безопасность».

Во-вторых, высшая школа и средне-профессиональные учебные заведения, участвующие в подготовке указанных специалистов, могут использовать CWF для корректировки существующих и разработки новых учебных планов и образовательных программ, что, несомненно, приведёт к повышению качества образовательного процесса и уровню профессиональной подготовки выпускников.

В-третьих, на основе CWF организации (независимо от формы собственности), производящие программные и программно-аппаратные средства и комплексы защиты информации, а также предоставляющие услуги по обеспечению информационной безопасности, смогут определить контингент выпускников, наиболее приемлемый для замещения вакантных должностей.

В-четвёртых, компании и организации, эксплуатирующие информационно-технологические системы (ИТС), составляющие часть (или основу) их бизнеса, смогут с помощью CWF определить свои потребности в создании собственных систем защиты, а также определить их кадровый состав в интересах снижения рисков, связанных с эксплуатацией самой ИТС, а также информационно-технологическим взаимодействием с партнёрами и предоставлением электронно-информационных услуг клиентам.

В-пятых, школьники и студенты на основе CWF смогут определить наиболее востребованные специальности/специализации в кибербезопасности, проанализировать образовательные программы ВУЗов и выбрать те, которые, по их мнению, обеспечат им (после их освоения) успешный карьерный и профессиональный рост. С другой стороны, повышение спроса на специальности в области кибербезопасности повысит конкуренцию среди образовательных учреждений, что, в свою очередь, повлечёт повышение качества образования.

Заключение

Представленный в статье анализ CWF, созданной в качестве фундаментального справочного ресурса, показывает наличие системного подхода к решению задачи обеспечения кадрами в области кибербезопасности. Наличие таких взаимосвязанных компонент CWF, как категории специальностей, специализации/специальности, функциональные должности, компетенции и функциональные обязанности (или задачи, решаемые при исполнении той или иной должности), позволяет объединить усилия работодателей и сферы образовательных услуг в области подготовки высококвалифицированных кадров.

Авторы приглашают научно-педагогических работников и представителей бизнес-партнеров к дальнейшему обсуждению рассмотренной проблемы для гармонизации с CWF существующих и новых образовательных стандартов, и программ по направлению «информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 3 декабря 2012 г. N 236-ФЗ. «О внесении изменений в Трудовой кодекс Российской Федерации и статью 1 Федерального закона «О техническом регулировании». http://ivo.garant.ru/#/document/70271730/paragraph/1.0. (дата обращения 27.03.2018).
2. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Приказ Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (дата обращения 27.03.2018).
3. Профессиональный стандарт «Специалист по технической защите информации». Приказ Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (дата обращения 27.03. 2018).
4. Профессиональный стандарт «Специалист по информационной безопасности ИКТ систем». Проект приказа Министерства труда и социальной защиты Российской Федерации. https://iecp.ru/docs/news/profstandart.pdf. (дата обращения 27.03.2018).
5. Михайлова Л.А. Профессиональные стандарты и их использование при проектировании образовательных программ. https://www.hse.ru/data/2014/09/18/1315026126. (дата обращения 27.03. 2018).
6. E. McDuffie, V. Piotrowski, «The Future of Cybersecurity Education». Computer, Vol. 47, Aug. 2014, p.p. 67 – 69. ISSN: 0018-9162. DOI: 10.1109/MC.2014.224.
7. Executive Order no. 13636, «Improving Critical Infrastructure Cybersecurity». DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. (дата обращения 27.03.2018).
8. NIST. «National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework». SP 800-181. August 2017. https://doi.org/10.6028/NIST.SP.800-181.
9. Электронный ресурс. https://www.nist.gov/itl/applied-cybersecurity/nice. (дата обращения 27.03.2018).
10. Лимаренко А.А. «Комплексное учебно-методическое обеспечение образовательного процесса». https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/03/05/kompleksnoe-uchebno-metodicheskoe-obespechenie. (дата обращения 28.03.2018).

REFERENCES:

[1] Federal Low of Russian Federation, December 3, 2012г. N 236-FZ. http://ivo.garant.ru/#/document/70271730/paragraph/1.0. (access date 27.03.2018). (in Russian).
[2] Proffesional Standart: «The Information Protection Specialist for the Automated Systems». Executive Order of Ministry of Labuor and Socisl Protection of Russian Federation, September 15, 2016. № 522n. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (access date 27.03.2018). (in Russian).
[3] Proffesional Standart: «The Specialist on Technical Protection of Information». Executive Order of Ministry of Labuor and Socisl Protection of Russian Federation, November 01, 2016. № 599n. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (access date 27.03. 2018). (in Russian).
[4] Proffesional Standart (draft): «The Specialist on Information Security of the Information Communication Technology Systems». Ministry of Labuor and Socisl Protection of Russian Federation. https://iecp.ru/docs/news/profstandart.pdf. (access date 27.03.2018). (in Russian).
[5] L.A. Mikhailova. «The Proffesional Standarts and Their Use for Educational Programms Developing». https://www.hse.ru/data/2014/09/18/1315026126. (access date 27.03. 2018). (in Russian).
[6] E. McDuffie, V. Piotrowski, «The Future of Cybersecurity Education». Computer, Vol. 47, Aug. 2014, p.p. 67–69. ISSN: 0018-9162. DOI: 10.1109/MC.2014.224.
[7] Executive Order no. 13636, «Improving Critical Infrastructure Cybersecurity». DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. (access date 27.03.2018).
[8] NIST. «National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework». SP 800-181. August 2017. https://doi.org/10.6028/NIST.SP.800-181.
[9] NICE. https://www.nist.gov/itl/applied-cybersecurity/nice. (access date 27.03.2018).
[10] A.A. Limarenko. «Complex Learning and Methodological Support of Educational Process». https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/03/05/kompleksnoe-uchebno-metodicheskoe-obespechenie. (access date 28.03.2018). (in Russian).

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.

Александр А. Голяков[1], Анатолий П. Дураковский[2], Егор А. Симахин[2]
[1]Учебный центр безопасности информации «МАСКОМ»,
119421, Москва, ул. Новаторов, д.40 корп.1
e-mail: gaa66@mail.ru, https://orcid.org/0000-0002-8715-3477
[2]Национальный исследовательский ядерный университет «МИФИ»,
115409, г. Москва, Каширское шоссе, 31
e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735
e-mail: dekryt@mail.ru, https://orcid.org/0000-0003-4019-9694

ПРИМЕНЕНИЕ ГЕНЕРАТОРА ЗАМЕЩЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ РЕАЛЬНОГО ЗАТУХАНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

DOI: http://dx.doi.org/10.26583/bit.2018.2.03

Аннотация. Наиболее трудоемкими операциями при оценке защищенности информации от ее утечки за счет побочных электромагнитных излучений (ПЭМИ) являются работы, связанные с определением реального затухания излученного информативного сигнала. Большой интерес представляет собой задача автоматизации данного вида измерений. На измерение затухания с помощью существующих автоматизированных комплексов требуется значительное время. Поэтому, как правило, измерения проводятся только на ограниченном количестве частот. Вместе с тем, спектр одиночного информативного импульса имеет лепестковую структуру и в каждом частотном лепестке является сплошным. Соответственно измерение значений затухания напряженности электромагнитного поля на отдельных частотах не отражает полноту характеристики затухания. Если же проводить измерения затухания по всему спектру информативного сигнала в заданном диапазоне частот, то необходимо провести несколько тысяч измерений, что делает такой подход не эффективным с точки зрения временных затрат. Современные специализированные автоматизированные измерительные системы (САИС) контроля защищенности по каналам ПЭМИ имеют режим измерения шума системы активной защиты, который можно использовать для измерения реального затухания. В данной работе описан и экспериментально подтвержден более точный и быстрый способ измерения реального затухания информативного сигнала на примере видеоподсистемы монитора с электронно-лучевой трубкой (ЭЛТ) с использованием САИС «Сигурд» и генератора замещения. Применение генератора замещения в автоматизированных измерениях позволяет существенно сократить временные затраты на проведение специальных исследований (СИ) по контролю защищенности информации от утечки за счет ПЭМИ.

Ключевые слова: генератор замещения, информационная безопасность, побочные электромагнитные излучения, реальное затухание.

Для цитирования. ГОЛЯКОВ, Александр А.; ДУРАКОВСКИЙ, Анатолий П.; СИМАХИН, Егор А.. ПРИМЕНЕНИЕ ГЕНЕРАТОРА ЗАМЕЩЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ РЕАЛЬНОГО ЗАТУХАНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ. Безопасность информационных технологий, [S.l.], n. 2, p. 38-53, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1108>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.03.

Alexander A. Golyakhov[1], Anatoly P. Durakovskiy[2], Egor A. Simakhin[2]
[1] Educational center of information security "MASKOM»,
119421, Moscow, ul. Novatorov, 40 korp.1
e-mail: gaa66@mail.ru, https://orcid.org/0000-0002-8715-3477
[2]National research nuclear university “MEPHI”,
115409, Moscow, Kashirskoye highway, 31
e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735
e-mail: dekryt@mail.ru, https://orcid.org/0000-0003-4019-9694

Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation

DOI: http://dx.doi.org/10.26583/bit.2018.1.03

Abstract. A determination of real attenuation of information signal's radiation on a way from the source to a possible location of intelligence devices is considered to be the most difficult operation while assessing information security against leakage of electromagnetic emanation. In this context the problem of automation of this kind of measurement is of great interest. It takes considerable effort and time to measure the attenuation by existing automated systems. That is why the measurements are generally taken within the limited range of frequencies only. Along with that, a spectre of a single information impulse has a leaf-structure and is solid on every frequency leaf. So electromagnetic field intensity attenuation measurement carried on the some preselected frequencies is not able to represent the complete attenuation characteristics. The measurements of attenuation in the whole informative signal spectre within the given frequency range requires a few thousand measurements, which makes the current method ineffective and time consuming. The relevant specialized automatized measurement systems of security verification has active protection system noise measurement mode, which can be used to measure the real attenuation. In this article a rather exact method of real attenuation of informative signal of video subsystem of electron-ray tube monitor measurement is described and confirmed in experiment. The measurements were made using specialized automatized system “Sigurd” and video subsystem informative signal noise generator. The described method allows a significant reduction of the time needed for specialized investigations of security verification on electromagnetic emanation.

Keywords: noise generator, information security, compromising emanation, attenuation of electromagnetic field, TEMPEST.

For citation. GOLYAKHOV, Alexander A.; DURAKOVSKIY, Anatoly P.; SIMAKHIN, Egor A.. Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation. IT Security (Russia), [S.l.], n. 2, p. 38-53, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1108>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.03.

Введение

В процессе обработки информации средства вычислительной техники излучают информативные электромагнитные волны. При перехвате данного излучения существует возможность восстановления конфиденциальной информации [1]. В связи с этим появляется потенциальная угроза информационной безопасности – утечка информации по каналу побочных электромагнитных излучений и наводок. Рассматриваемый канал работает фактически в реальном масштабе времени, является пассивным, что не дает возможности владельцу информации обнаружить нарушителя. Все это в совокупности говорит о высоком уровне опасности побочных излучений средств вычислительной техники. Поэтому в последние годы данному техническому каналу утечки информации уделяется пристальное внимание.

Впервые, с точки зрения защиты информации, опасность побочного электромагнитного излучения (или, как называют зарубежные исследователи, «компрометирующего электромагнитного излучения») была продемонстрирована в марте 1985 года на международном конгрессе по защите информации Securecom-85 в Каннах. Голландский инженер Вим ван Эйк, используя устройство в виде доработанного телевизионного приемника, продемонстрировал перехват информации с монитора компьютера, который находился рядом в здании [2]. В 2003 году были проведены эксперименты по исследованию характера и свойств компрометирующих излучений для мониторов с электронно-лучевой трубкой и жидкокристаллических мониторов [3]. В 2010

году группой французских исследователей была показана возможность снятия компрометирующего излучения работы компьютера с линий электропитания, расположенных в доме [4]. В 2011 году авторы [5] проанализировали и провели измерения ПЭМИ клавиатуры с интерфейсом PS/2. Эксперименты, проведенные исследователями, показали, что характеристика сигналов нажатия клавиш может быть восстановлена путем анализа полученных электромагнитных сигналов во временной области, что приводит к компрометации ввода информации с помощью клавиатуры. В 2012 году те же специалисты, проанализировав компрометирующие электромагнитные излучения цифровых сигналов, построили модель компрометирующего излучения [1]. В 2013, в журнале «IEEE Transaction on electromagnetic compatibility» была опубликована статья [6], в которой говорится о сложностях распознавания компрометирующих сигналов LVDS интерфейса мониторов. В 2014 году одной из тем 23-ей международной научно-технической конференции была работа [7], в которой исследуется опасность побочного излучения принтера. В том же году было проведено исследование ПЭМИ интерфейса USB 2.0 при передаче данных [8]. В 2016 году на симпозиуме PIERS, проходившем в Шанхае, была представлена работа польских исследователей [9], в которой описывается исследование компрометирующего излучения VGA и DVI интерфейсов. В том же году на 13-ой международной научно-технической конференции «Actual Problems of Electronics Instrument Engineering (APEIE)», обсуждалась работа отечественных исследователей на тему особенностей идентификации и анализа ПЭМИ от USB-флэш-накопителей [10]. Активно ведутся работы по исследованию компрометирующего излучения смартфонов и их интерфейсов [11-12]. Разрабатываются методы обнаружения и восстановления компрометирующего излучения USB клавиатуры [13-14]. Продолжается работа по разработке программно-аппаратных комплексов поиска компрометирующих излучений [15]. Обширные исследования в этой области показывают на актуальность защиты информации от ее утечки по данному техническому каналу. Особый интерес со стороны специалистов по технической защите информации представляют работы, связанные с определением реального затухания информативных сигналов, позволяющие оценить уязвимость объекта информатизации.

Описание метода определения реального затухания

Измерение реального затухания при проведении СИ по контролю защищенности осуществляют с помощью различных САИС, принцип работы которых основан на передаче по радиоканалу с управляющего компьютера значения частоты, на которой необходимо измерить затухание, на генератор синусоидальных сигналов с передающей антенной, и последующему измерению уровней сигналов, излученных генератором в первой (ближней) и во второй (дальней) точках, параллельно или последовательно в автоматическом или ручном режимах.

Данный подход имеет ряд достоинств и недостатков. К достоинствам можно отнести то, что с использованием генератора синусоидальных сигналов можно проводить измерение затухания на значительных расстояниях. К недостаткам – большие временные затраты на проведение измерений при определении затухания.

Имеющиеся недостатки возможно преодолеть, используя САИС «Сигурд» и мощный, стабильный по времени источник шумового сигнала в заданном диапазоне частот - генератор замещения. В этом случае отпадает необходимость в перестройке генератора синусоидальных сигналов по частоте, что, соответственно, исключает потери времени на установление связи и коммутацию. С учетом быстродействия современных анализаторов спектра последовательный анализ существующего диапазона измерений с учетом 20 накоплений можно провести примерно за 5-7 минут.

Для расчета коэффициента затухания информативного сигнала в каждом частотном лепестке целесообразно использовать формулу:

$$K_{OTCC(CA3)} = \frac{\sqrt{\sum_{j=1}^{k}(10^{\frac{E_{1_j}}{20}})^2}}{\sqrt{\sum_{j=1}^{k}(10^{\frac{E_{2_j}}{20}})^2}}, \quad (1)$$

где $E_{1(2)}$ – напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от исследуемого технического средства или средства активной защиты (САЗ), дБ(мкВ/м);

k – количество фильтров, укладывающихся в одном частотном лепестке.

Однако спектральная плотность информативного сигнала (идеального прямоугольного импульса) распределена по частотному лепестку не равномерно, а имеет форму огибающей $\sin(x)/x$. На рисунке 1 красным цветом представлен его спектр по модулю.

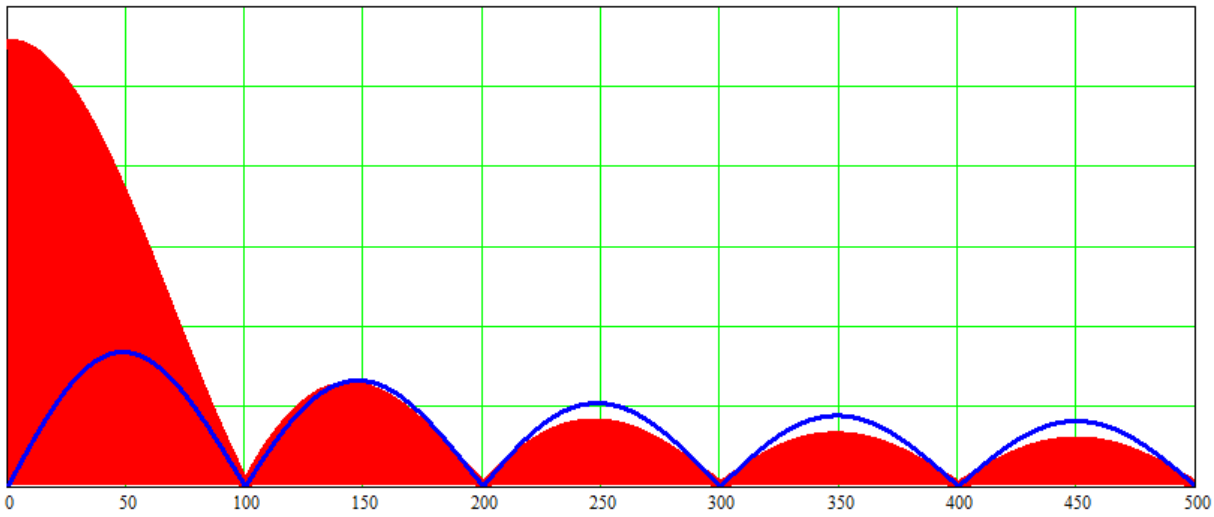


Рис. 1. Спектр информативного сигнала в токопроводящей цепи
(Fig. 1. Spectrum of informative signal)

В силу того, что электромагнитное поле возникает только при изменении напряжения или тока, случайная антенна будет излучать информативный импульс только на фронтах. Таким образом, форма информативного сигнала претерпевает определенные изменения, и спектр излученного сигнала, сохранив размер частотных лепестков, изменит форму. Модуль огибающей спектра сигнала, излученного случайной антенной, показан на рисунке 1 синей линией. Частотный лепесток становится симметричным, максимальная спектральная плотность находится в центре.

В общем случае форма огибающей спектра излученного сигнала зависит от многих факторов, и прежде всего, от формы информативного импульса, длительности фронта и спада, а также от излучательной способности случайной антенны.

Огибающую спектра излученного сигнала в первом приближении для инженерного расчета можно описать функцией:

$$q(f) = |\sin(\frac{\pi \cdot f}{\Delta F_л})|, \quad (2)$$

или

$$q(f) = |\sin(\pi \cdot f \cdot \tau_и)|, \quad (3)$$

где: f – частота, МГц;

$\Delta F_л$ – ширина частотного лепестка, МГц;

$\tau_и$ – длительность импульса, мкс.

Перейдем от огибающей спектра напряженности к огибающей энергетического спектра:

$$q_1(f) = 0,027 \cdot \left(|\sin(\frac{\pi \cdot f}{\Delta F_л})| \right)^2, \quad (4)$$

где 0,027 – нормировочный коэффициент, такой что:

$$\int_0^{\Delta F_л} q_1(f)df = 1. \quad (5)$$

Коэффициент приведен для ширины лепестка 75 МГц.

Для того, чтобы учесть распределение напряженности поля по частотному лепестку целесообразно использовать следующую формулу:

$$K_{ОТСС(САЗ)} = 20 \cdot \lg\left(\left(\sum_{j=1}^{k} \frac{(10^{E_{2_j}/20})^2 \cdot q_1(f_j) \cdot \Delta f_ф}{(10^{E_{1_j}/20})^2} \right)^{-1} \right), \quad (6)$$

где $E_{1(2)}$– напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

k – количество фильтров, укладывающихся в одном частотном лепестке;

$\Delta f_ф$– полоса фильтра, которым проводилось измерение, МГц,

Методику определения затухания с учетом формы, огибающей спектра информативного сигнала можно описать следующим образом:

1) Определить форму информативного сигнала с использование осциллографа или исходя из описания работы интерфейса, описать сигнал функцией от времени $y(t) = f(t)$;

2) Взять производную от функции времени $y_1(t) = \frac{dy(t)}{dt}$;

3) Выполнить преобразование Фурье от функции $y_1(t)$. При достаточно мощном излучении тестового сигнала, определится с формой, огибающей спектра можно задав тест пиксель через 10-20 пикселов, как показано на рисунке 2;

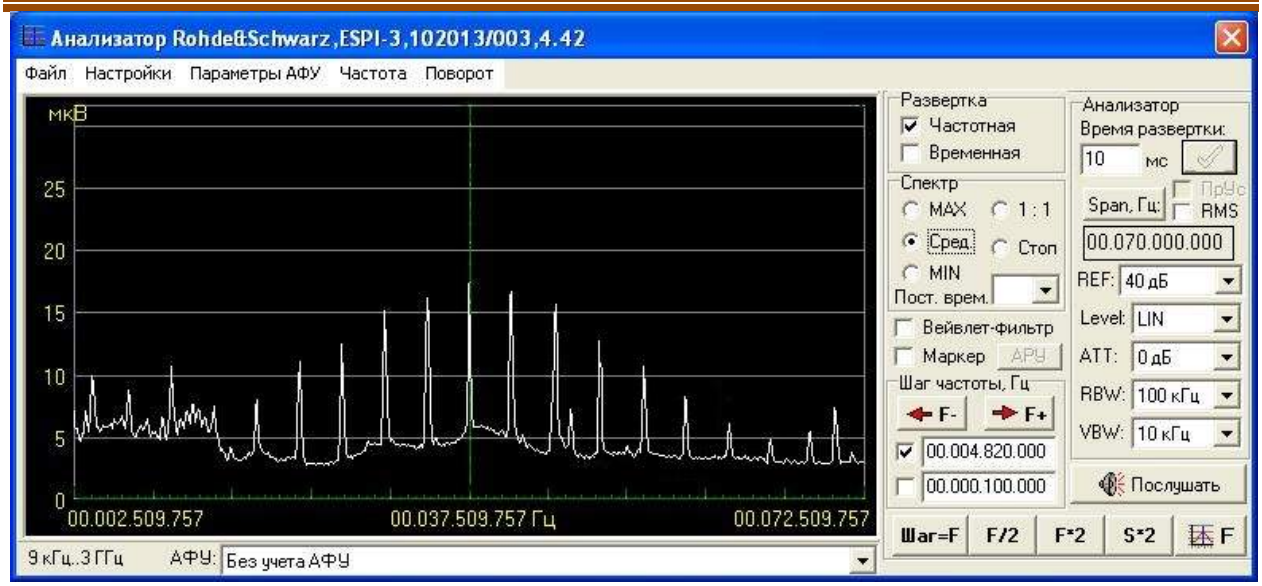


Рис. 2. Форма огибающей спектра частотного лепестка
(Fig. 2. The form of frequency lobe)

4) Аппроксимировать огибающую спектра любым известным способом и получить функцию $q(f)$;

5) Найти огибающую энергетического спектра $q_1(f)$, провести нормировку;

6) Измерить напряженность поля генератора замещения в первой и во второй точках фильтр к фильтру в частотном лепестке;

7) Произвести расчет затухания в частотном лепестке с учетом формы, огибающей спектра в соответствии с формулой (6).

Проведение измерений с использованием САИС «Сигурд»

В качестве исследуемого элемента средства вычислительной техники (СВТ) был выбран монитор с электронно-лучевой трубкой. В качестве генератора замещения использовалась совокупность генераторов шума (ГШ) – Соната Р2, ЛГШ-501 и SEL SP-21. Измерения затухания производились на расстоянии 10 м от ЭВМ. Исходными данными для проведения измерений являются значения сигналов и шумов, на найденных частотах гармоник тестового сигнала.

Методику проведения измерения затухания информативных сигналов с использованием САИС «Сигурд» и генератора замещения можно представить следующим образом:

1) Используя задание с результатами измерений сигналов и шумов на частотах гармоник тестового сигнала, или создав новое задание, перейти во вкладку «Верификация и измерение» для настройки параметров анализатора спектра при измерении САЗ. Для повышения точности измерений количество накоплений следует выбирать в диапазоне от 15 до 20. Для учета изменений настроек программой нажать кнопку «Сохранить задание», а затем для продолжения работы кнопку «Выбрать текущее задание», как показано на рисунке 3;

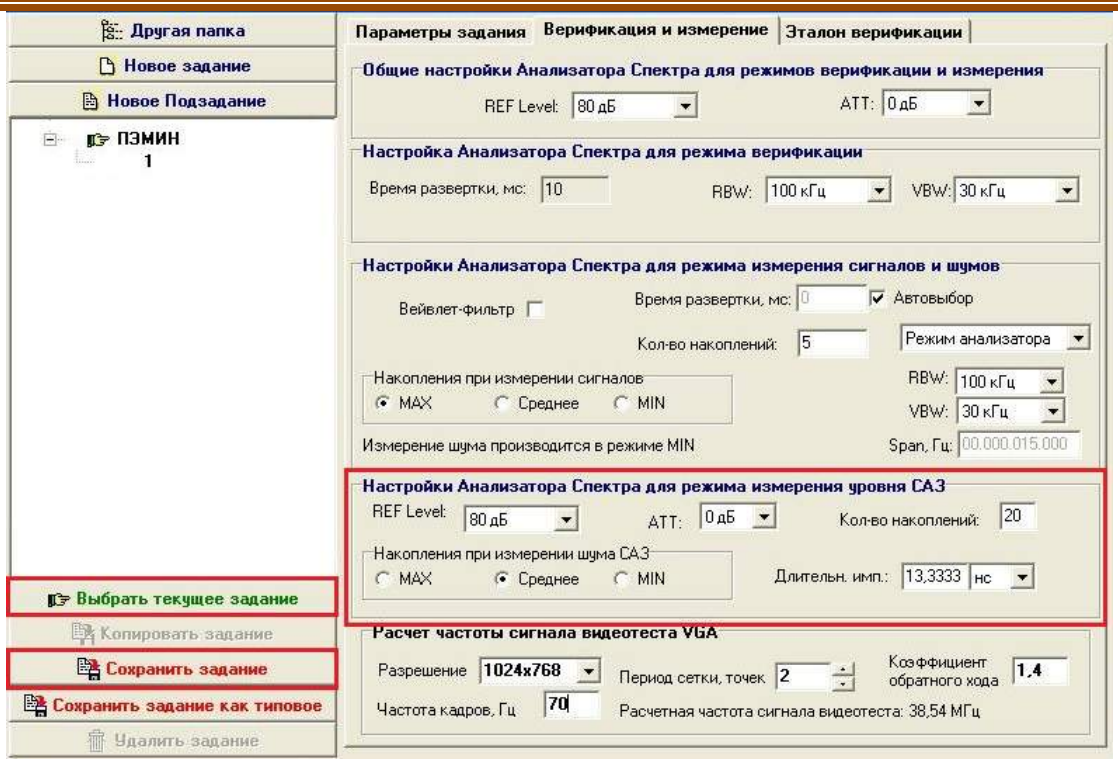


Рис. 3. «Параметры заданий» вкладка «Верификация и измерение»
(Fig. 3. "Job options" tab "Verification and measurement")

2) В поле «Выполняемые операции» окна «Задание» перейти во вкладку «САЗ». Заполнить поля «Длительность импульса» и «Порог отсеивания». Расчет длительности импульса может производиться автоматически исходя из значения частоты первой гармоники тестового сигнала, установленной во вкладке «Экспресс-поиск», при нажатии на кнопку «= полупериод Fтакт». Значение порога отсеивания показывает, насколько напряженность поля сосредоточенного источника должна превосходить средний уровень шума САЗ, чтобы не восприниматься за шум. Иллюстрация к данному пункту представлена на рисунке 4;

3) Выставить ГШ в месте размещения СВТ, включить их. Выставить приемную антенну на высоте 1 метр над уровнем поверхности в точке возможного размещения средства разведки в направлении ГШ. Выполнить измерения шума генераторов в дальней точке, нажав кнопку «Старт задания». Выключить ГШ. Поставить галочку в графе «Измерение САЗ в точке 2» и выполнить измерение объектового шума в дальней точке.

4) По окончанию работы программы, убедиться в том, что уровень шума от генератора не менее чем на 3 дБ превышает уровень объектового шума, просмотрев полученные измерения. Для этого в окне «Задание» нажать кнопку «Просмотр измерения САЗ». При отрицательном результате следует либо заменить используемые ГШ более мощными, либо произвести измерения на максимально возможном расстоянии, на котором выполняется вышеописанное условие. Для окончания просмотра снятых измерений нажать кнопку «Конец просмотра САЗ». Иллюстрации к данному пункту представлены на рисунках 5а и 5б;

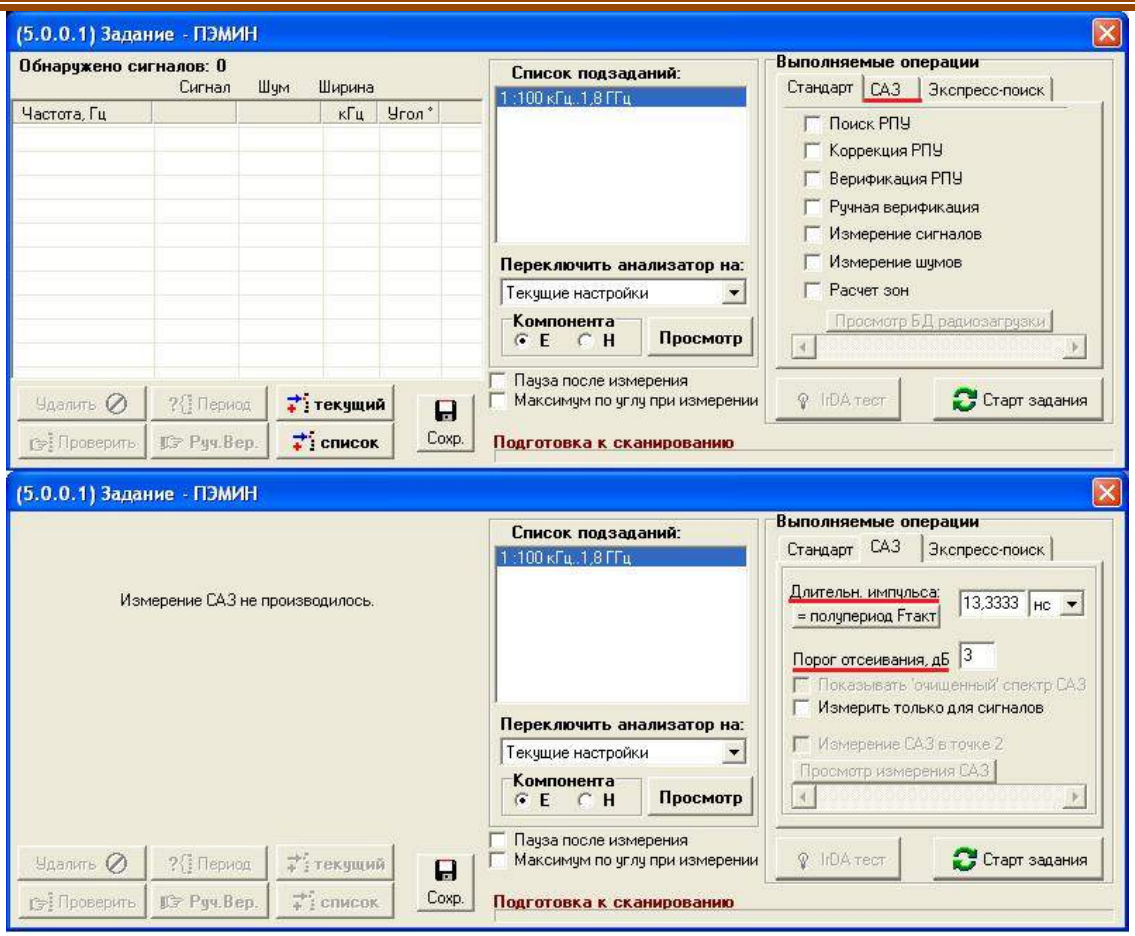


Рис. 4. Вкладка «САЗ»
(Fig. 4. Tab "APS")

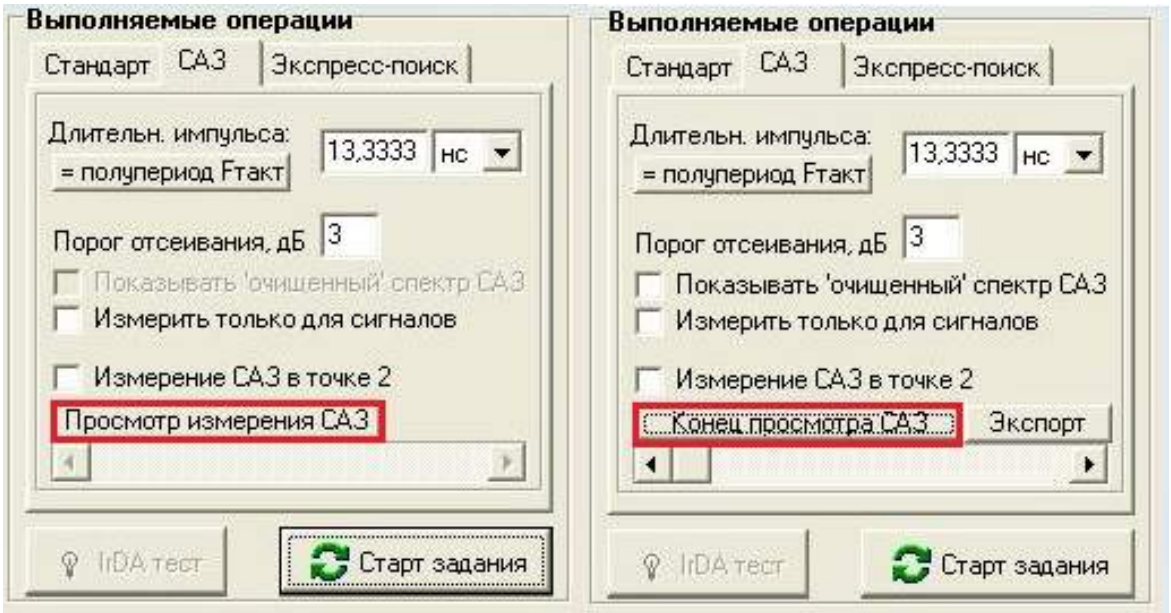


Рис. 5а. Подготовка к просмотру измерений шума
(Fig. 5a. Preparing to view noise measurements)

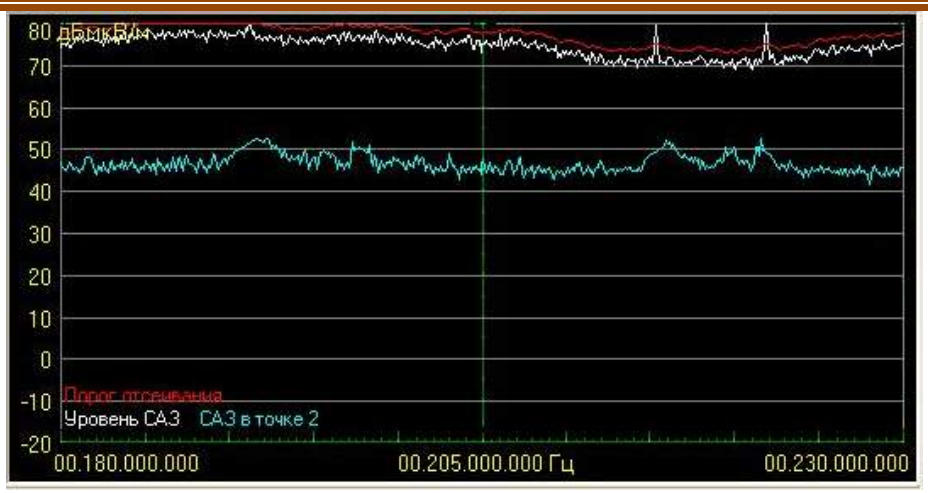


Рис. 5б. Просмотр измерений шума
(Fig. 5b. Viewing noise measurements)

5) При положительном результате для проверки расчета затухания, выполняемого системой «Сигурд» по формуле (1), нажать кнопку «Экспорт» для сохранения полученных данных в отдельный текстовый файл с помощью стандартных средств операционной системы управляющей ЭВМ;

6) Включить ГШ. Для корректного учета программой «Сигурд-Дельта» измерений необходимо повторно измерить уровень шума САЗ в дальней точке, нажав кнопку «Старт задания».

7) Выставить приемную антенну на высоте 1 метр над уровнем поверхности и на расстоянии 1 метра от антенны ГШ по оси, соединяющей текущее положение антенны и точку возможного размещения средства разведки. Снять галочку в графе «Измерение САЗ в точке 2» и нажать кнопку «Старт задания»;

8) Для проверки расчета затухания, выполняемого системой «Сигурд» по формуле (1), нажать кнопку «Экспорт» для сохранения полученных данных в отдельный текстовый файл;

9) Выключить ГШ;

10) Открыть расчетную программу «Сигурд-Дельта» нажав кнопку «Расчет» на панели управления программы «Сигурд – Интерфейс». Во вкладке «Атрибуты» программы «Сигурд–Дельта» необходимо выбрать вид исследования, в графе «Вид измерений» выбрать «в эфире», описать исследуемое техническое средство и выбрать средство измерения, с помощью которого проводились измерения. Иллюстрация к пункту 10 представлена на рисунке 6.

11) Для того чтобы программа «Сигурд-Дельта» учла снятый шум от генератора необходимо поставить галочку у поля «САЗ» в графе «’E’ – компонента». При этом появятся вкладки: «’E’ - сигналы», «САЗ для ’E’» и «Затухание ’E’»;

12) Перейти во вкладку «’E’ - сигналы». Если для измерения затухания использовалось новое задание, то используя кнопку загрузить сохраненные данные сигналов и шумов на частотах гармоник, либо вручную ввести значения сигналов и шумов из сохраненных результатов выполненного задания. Если для измерения затухания использовалось текущее задание, то значения сигналов и шумов отобразятся автоматически. Внести необходимые изменения в поля: «Предусилитель», «Антенна» и «Фидер».

13) Перейти во вкладку «САЗ для ’E’». Выставить необходимые настройки устройств в полях «Предусилитель», «Антенна» и «Фидер». Если при измерении шума САЗ антенно-фидерный тракт остался таким же, как при измерении сигналов, то поставить галочку в поле «Антенна, предусилитель и фидерный тракт такие же, как у сигналов».

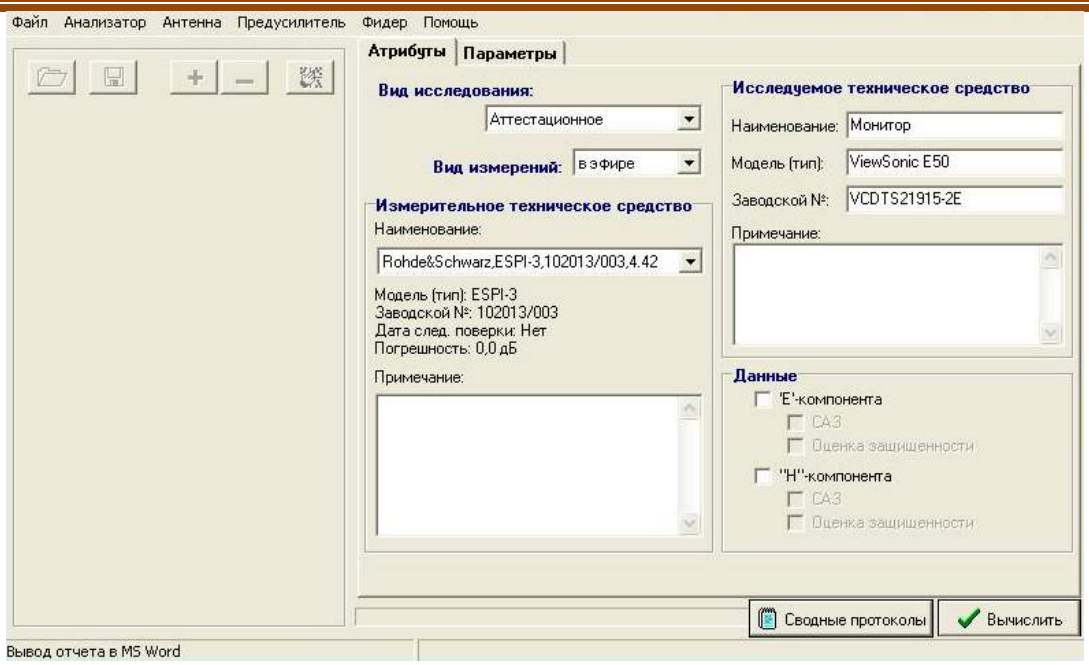


Рис. 6. Вкладка «Атрибуты»
(Fig. 6. Tab "Attribute")

Чтобы расчетная программа учла измеренный шум САЗ, необходимо в поле «АЧХ САЗ» выбрать графу «Измеренный спектр». В поле «Вариант измерения САЗ» необходимо выбрать графу «ГШ вблизи СВТ». При этом вместо вкладки «Затухание 'Е'» появится вкладка «Затухание ГШ — Е». Иллюстрация к пункту 13 представлена на рисунке 7;

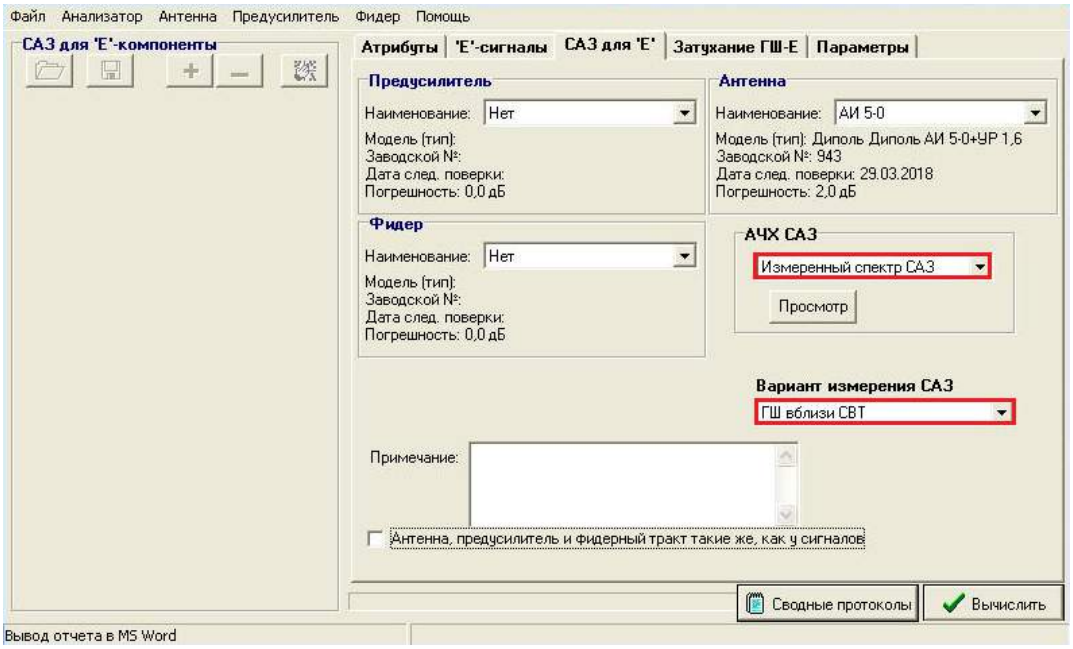


Рис. 7. Вкладка «САЗ для 'Е'»
(Fig. 7. Tab "APS for 'E'")

14) Перейти во вкладку «Затухание ГШ-Е». Выставить необходимые настройки устройств в полях «АФУ для т.1» и «АФУ для т.2». Если используемые устройства не изменились после измерения сигналов, то поставить галочку в полях «АФУ такие же, как у сигналов» и «АФУ как у сигналов». В раскрывающемся списке внизу вкладки выбрать графу «Измеренный спектр» для учета программой «Сигурд – Дельта» данных шума

генератора в первой и во второй точках. Иллюстрация к пункту 14 представлена на рисунке 8;

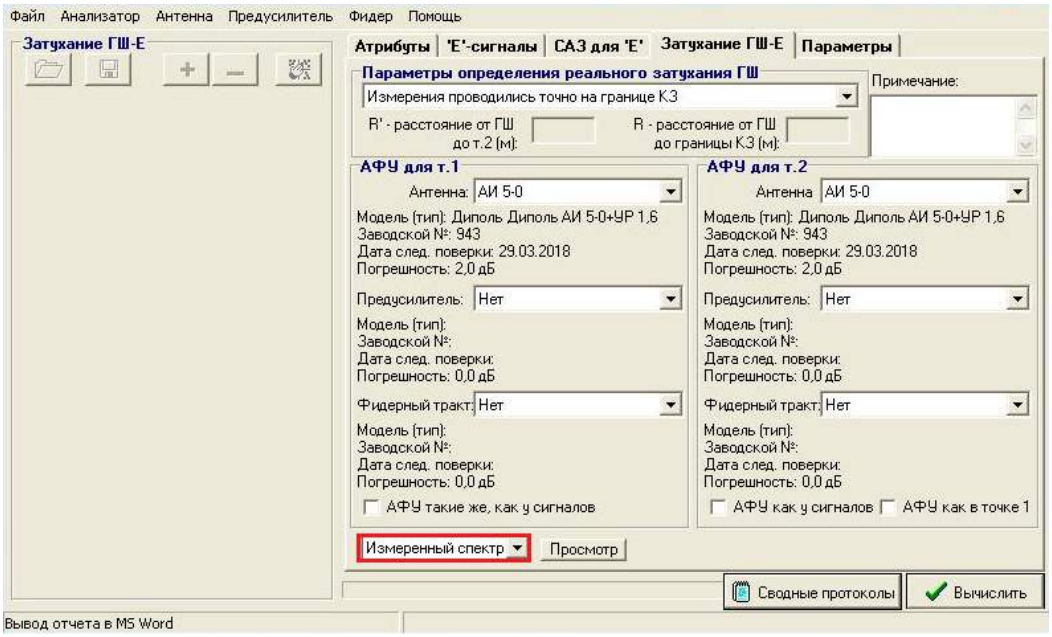


Рис. 8. Вкладка «Затухание ГШ-Е»
(Fig. 8. Tab "Attenuation NG-E")

15) Перейти во вкладку «Параметры» и выставить необходимые настройки, зависящие от тестового сигнала и ГШ, как представлено на рисунке 9;

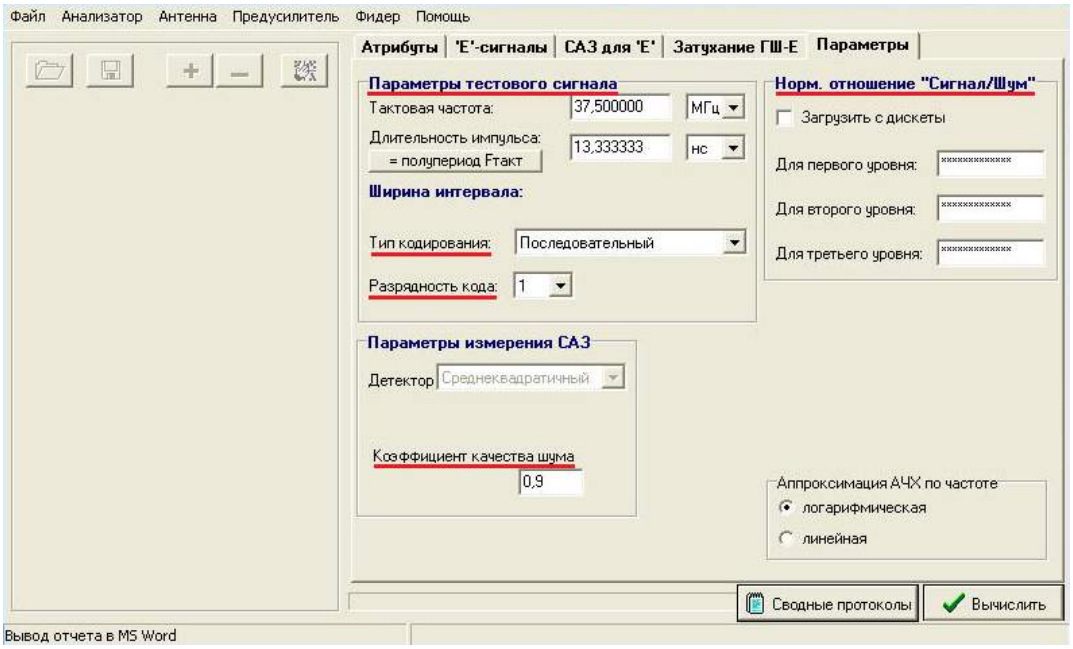


Рис. 9. Вкладка «Параметры»
(Fig. 9. Tab "Parameters")

16) Выбрать формат документа, в котором будет представлен расчет. Для этого необходимо в меню «Файл» выбрать пункт «Вывод отчета…». После выбора формата файла отчета нажать кнопку «Вычислить». На экране появится окно с полем «Вывод протоколов». Необходимо оставить галочку только в пункте «САЗ». И нажать кнопку «Да». Иллюстрация к пункту 16 представлена на рисунке 10.

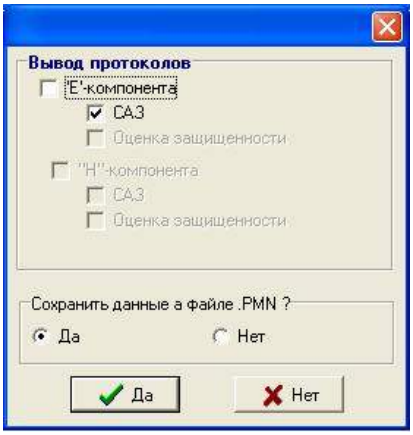


Рис. 10. Получение протокола
(Fig. 10. Reception of protocol)

Обработка измерений и результаты эксперимента

В «Протоколе инструментальной оценки эффективности САЗ» в таблице «Полный расчет», представлены полученные при измерении значения напряженности поля шума от генераторов шума «$E_{саз}$(B)» и «$E_{саз}$(L')» в каждом частотном лепестке в ближней и дальней точках соответственно.

Покажем, что САИС «Сигурд» может использоваться для измерения реального затухания сигналов ПЭМИ с генератором замещения. Для этого необходимо рассчитать коэффициенты затухания по формуле (1) и сравнить с отношением «Есаз(B)»/«Есаз(L')». Для учета формы спектра информативного сигнала при определении затухания произвести расчет по формуле (6). Получение исходных данных из текстовых файлов, нормировка функции огибающей энергетического спектра, а также расчеты по формуле (1) и формуле (6) в третьем частотном лепестке представлены на рисунке 11. Построение графиков шума ГШ в первой и во второй точке показано на рисунке 12.

Point1 =

	1	2	3
1	0.01	79.19	0.3
2	0.0103	78.91	0.3
3	0.0106	78.63	0.3
4	0.0109	78.34	0.3
5	0.0112	78.05	0.3
6	0.0115	77.75	0.3
7	0.0118	77.65	0.3
8	0.0121	77.39	0.3
9	0.0124	77.12	0.3
10	0.0127	76.85	0.3
11	0.013	76.57	0.3
12	0.0133	76.29	0.3
13	0.0136	76.01	0.3
14	0.0139	75.74	0.3
15	0.0142	75.47	0.3
16	0.0145	75.2	0.3

Point2 =

	1	2	3
1	0.01	79.36	0.3
2	0.0103	79.26	0.3
3	0.0106	78.98	0.3
4	0.0109	78.72	0.3
5	0.0112	78.48	0.3
6	0.0115	78.29	0.3
7	0.0118	78.03	0.3
8	0.0121	77.76	0.3
9	0.0124	77.48	0.3
10	0.0127	77.19	0.3
11	0.013	76.9	0.3
12	0.0133	76.61	0.3
13	0.0136	76.32	0.3
14	0.0139	76.03	0.3
15	0.0142	75.75	0.3
16	0.0145	75.48	0.3

$\Delta F_n := 75$

$$\frac{1}{\int_{\Delta F_n}^{2\cdot\Delta F_n} \left(\left|\sin\left(\frac{f\cdot\pi}{\Delta F_n}\right)\right|\right)^2 df} = 0.026666666666667$$

$$q1(f) := 0.026666666666667\cdot\left(\left|\sin\left(\frac{f\cdot\pi}{\Delta F_n}\right)\right|\right)^2$$

$$\int_{\Delta F_n}^{2\cdot\Delta F_n} q1(f)\, df = 1$$

$$K\_3 := 20\cdot\log\left[\frac{\sqrt{\sum_{j=4652}^{5401}\left[10^{\frac{(Point1^{(2)})_j}{20}}\right]^2}}{\sqrt{\sum_{j=4652}^{5401}\left[10^{\frac{(Point2^{(2)})_j}{20}}\right]^2}}\right]$$

$$K3 := 20\cdot\log\left[\frac{1}{\sqrt{\sum_{j=4652}^{5401}\left[10^{\frac{(Point2^{(2)})_j}{20}}\cdot 0.027\cdot\left[\left|\sin\left[\frac{(Point2^{(1)})_j\cdot\pi}{75}\right]\right|\right]^2\cdot 0.1\right]^2}}\right]$$

Рис. 11. Работа в Mathcad
(Fig. 11. Work in Mathcad)

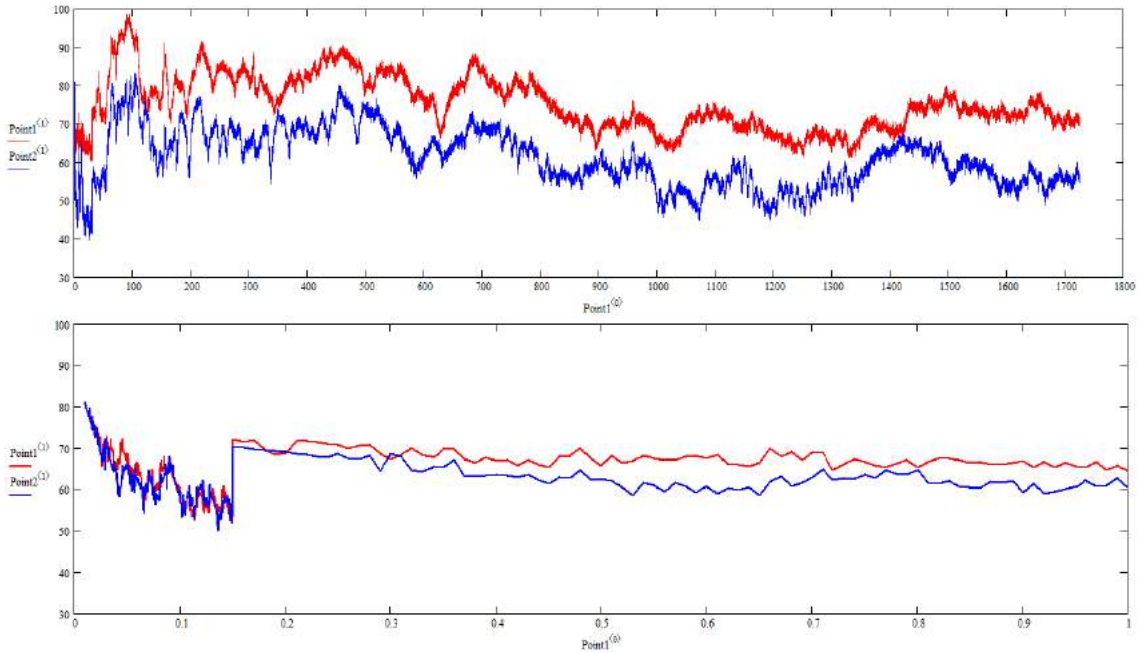


Рис. 12. График зависимости снятого шума от частоты
(Fig. 12. Graph of the frequency dependence of the noise)

Предварительно необходимо оценить эффективность работы генераторов шума, построив графики зависимости шума от частоты в первой и во второй точках. В текстовых файлах, полученных при измерениях САЗ в ближней и дальней точках необходимо заменить символ «,» на символ «.» для правильного учета данных инженерным математическим ПО Mathcad. На рисунке 12 показано, что шум от генераторов до частоты 1 МГц является неэффективным.

При ширине частотного лепестка в 75 МГц значениями затухания информативного сигнала до частоты 1 МГц можно пренебречь, либо оценить затухание на участке до 1 МГц по наименьшей частоте, на которой значение шума в первой точке в заданное количество раз превосходит значение во второй, при этом получится запас по защищенности.

Для более точного расчета затухания информативного сигнала в частотном лепестке можно получить «чистый» шум от генераторов шума. Для этого последовательно произвести измерения объектового шума в точке 1 и точке 2, сохранить результаты в текстовые файлы. В силу специфики программного обеспечения (ПО) САИС «Сигурд» измерение объектового шума в точке 2 необходимо проводить с настройками как в точке 1. Далее произвести расчет «чистого» шума по формуле:

$$E_{ш_j} = 20 \cdot \lg\left(\sqrt{\left(10^{\frac{E_{ГШ\,j}}{20}}\right)^2 - \left(10^{\frac{E_{ОШ\,j}}{20}}\right)^2}\right), \qquad (7)$$

где $E_{ш_j}$ – «чистый» шум на j-ой частоте, дБ(мкВ/м);

$E_{ГШ_j}$ – напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

$E_{ОШ_j}$ – напряженность электрической составляющей электромагнитного поля объектового шума при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты эксперимента

№ п/п	Fц инт. МГц	№№ сигн. интерв.	$К_С$	$К_{Ф1}$	$К'_{Ф1}$	$К_{Ф6}$	$К'_{Ф6}$	$К_{ГСС}$
1	37,5000	1, 2	13,34	14,18	13,26	15,90	18,84	19,442
2	112,5000	3, 4	16,71	15,87	15,87	7,65	7,70	19,831
3	187,5000	5, 6	14,10	13,88	13,88	10,03	10,08	9,913
4	262,5000	7, 8	16,36	16,60	16,60	14,85	14,90	17,553
5	337,5000	9, 10	12,65	12,04	12,04	8,31	8,36	6,746
6	412,5000	11, 12	15,24	15,52	15,05	14,99	15,05	19,389
7	487,5000	13	11,29	11,37	11,38	9,83	9,89	17,817
8	562,5000	14	16,07	16,08	16,09	16,71	16,80	18,495
9	712,5000	15	14,62	14,11	14,11	12,33	12,38	20,141
10	787,5000	16, 17	17,04	17,28	17,28	17,21	16,80	12,657
11	862,5000	18, 19	13,72	13,56	13,56	13,39	9,65	18,856

В таблице 1 приняты следующие обозначения:

1) $К_С$ - отношение «$E_{саз}$(В)»/«$E_{саз}$(L')» в каждом частотном лепестке, полученный из протокола специальных исследований (СИ) с САИС «Сигурд», дБ;

2) $К'_{Ф1}$ и $К_{Ф1}$ - коэффициенты затухания полученные по формуле (1) с выделением «чистого» шума и без, дБ;

3) $К'_{Ф6}$ и $К_{Ф6}$ - коэффициенты затухания полученные по формуле (6) с выделением «чистого» шума и без, дБ;

4) $К_{ГСС}$ - коэффициент затухания полученный при измерениях на частотах гармоник тестового сигнала с использованием генератора синусоидального сигнала, дБ(мкВ/м).

При вычислении значения $К_{ГСС}$ в частотном лепестке при наличии двух гармоник использовалась следующая формула:

$$K_{ГСС} = \frac{\sqrt{(E_1)^2 + (E_2)^2}}{\sqrt{\left(\frac{E_1}{K_1}\right)^2 + \left(\frac{E_2}{K_2}\right)^2}}, \quad (8)$$

где E_1 и E_2 – напряженности электромагнитного поля на частотах гармоник;

K_1 и K_2 – коэффициенты затухания электромагнитного поля на частотах гармоник.

Как видно из таблицы 1 коэффициент $К_С$ в сравнении с коэффициентами $К_{Ф1}$ имеет небольшой разброс значений не более 0,84 дБ. Он обусловлен тем, что в ПО «Сигурд» невозможно одновременно сохранить результаты измерений в точке 1 и точке 2, и поэтому значения в одной из точек в ПО «Сигурд» и файлах значений несколько отличаются. Соответственно можно сделать вывод, что с помощью ПО «Сигурд» можно осуществить расчет затухания в частотном лепестке по формуле (1). Разброс полученных значений не более 1 дБ между коэффициентами $К_{Ф1}$ и $К'_{Ф1}$ свидетельствует о том, что шум от генераторов в первой и во второй точках существенно превосходил объектовый шум.

Разница затухания в частотном лепестке между измерениями на частотах гармоник $К_{ГСС}$ и измерением фильтр к фильтру $К'_{Ф1}$ может составлять более 6 дБ, а при учете формы огибающей энергетического спектра информативного сигнала $К'_{Ф6}$ более 12

дБ, что свидетельствует о не оптимальности метода измерения затухания на частотах гармоник.

Заключение

В данной статье экспериментально подтверждена возможность использования генератора замещения и специализированной автоматизированной измерительной системы «Сигурд» для определения реального затухания сигналов на объекте информатизации.

Использование генератора замещения при проведении специальных исследований по контролю защищенности и оценке принятых мер защиты информации позволяет определить затухание электромагнитного поля во всем частотном лепестке, а не только на частотах гармоник. Такой подход позволяет более полно отразить характеристику затухания электромагнитного поля, при этом существенно увеличивается точность результатов измерений, и сокращается время проведения специальных исследований по контролю защищенности информации от утечки информации за счет побочных электромагнитных излучений.

СПИСОК ЛИТЕРАТУРЫ:

1. Litao Wang, Bin Yu. Research on the compromising electromagnetic emanation from digital signals, International Conference on Automatic Control and Artificial Intelligence(ACAI 2012), January 2012, Pages 1761-1764, DOI: 10.1049/cp.2012.1329.
2. Скрипник Д. Общие вопросы технической защиты информации. [Электронный ресурс] Режим доступа: https://www.intuit.ru/studies/courses/2291/591/lecture/12702 (дата обращения: 19.12.2017).
3. M. G. Kuhn, Compromising emanations: Eavesdropping risks of computer displays, Technical report UCAM-CL-TR-577 University of Cambridge, Computer Laboratory [Электронный ресурс], Режим доступа: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf (дата обращения 24.12.2017).
4. P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou Compromising Electromagnetic Field Radiated by In-House PLC Lines, IEEE Global Telecommunications Conference, December 2010, Pages 1-5, DOI:10.1109/GLOCOM.2010.5683144.
5. Litao Wang, Bin Yu. Analysis and measurement on the electromagnetic compromising emanations of computer keyboard, 17th International Conference on Computational Intelligence and Security, December 2011, Pages 640-643, DOI: 10.1109/CIS.2011.146.
6. M. G. Kuhn Compromising emanations of LCD TV sets, IEEE Transaction on electromagnetic compatibility, vol. 55, NO 3, June 2013, Pages. 564 – 570, DOI:10.1109/TEMC.2013.2252353.
7. И.Ф. Файсханов, А.С. Лучинин Исследование побочных электромагнитных излучений лазерного принтера, XXIII Международная научно-техническая конференция, Ноябрь 2014, Стр. 37-43, URI: http://elar.urfu.ru/bitstream/10995/46437/1/bip_2014_17.pdf
8. L. Nowosielski, M.Wnuk, Compromising emanations from USB 2 interface, Proceedings of PIERS 2014 in Guangzhou, August 2014, Pages 2666–2670.
9. Leszek Nowosielski, Rafal Przesmycki1, and Micha Nowosielski Compromising Emanations from VGA and DVI Interface, Progress In Electromagnetic Research Symposium (PIERS), August 2016, Pages 1024 – 1028, DOI:10.1109/PIERS.2016.7734570.
10. Andrey Ivanov, Ivan Reva, Andrey Ushakov Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), October 2016, Pages 156-158, DOI:10.1109/APEIE.2016.7806436
11. Degang Sun, Di Wei, Ning Zhang, Zhiqiang Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC), May 2016, Pages 190-193, DOI:10.1109/APEMC.2016.7523005
12. Jun Shi, Degang Sun, Abbas Yongacoglu, Meng Zhang, Dong Wei. Computer Recognition Based On the Compromising Emanations Fingerprint, Canadian Conference on Electrical and Computer Engineering (CCECE), May 2016, Pages 1-6, DOI: 10.1109/CCECE.2016.7726724.
13. Rostislav I. Sokolov, Renat R. Abdullin Determined Factor Parameter Analysis for System of Information Recovery from USB-Keyboard Compromising Emanations, International Applied Computational Electromagnetics Society Symposium - Italy (ACES), March 2017, Pages 1-2, DOI:10.23919/ROPACES.2017.7916332.

14. Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboard, 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), January 2016, Pages 1-4, DOI:10.1109/ICIEAM.2016.7911553.
15. Andrey Ivanov, Ivan Reva, Baryshnilov Yaroslav Development of Hardware-software Complex for Automatized Compromising Electromagnetic Emanation Search, 11th International Forum on Strategic Technology (IFOST), June 2016, Pages 1-3, DOI:10.1109/IFOST.2016.7884180.

REFERENCES:

[1] Litao Wang, Bin Yu. Research on the compromising electromagnetic emanation from digital signals, International Conference on Automatic Control and Artificial Intelligence(ACAI 2012), January 2012, Pages 1761-1764, DOI: 10.1049/cp.2012.1329.
[2] Skrypnyk D. General issues of technical protection of information. Mode of access: https://www.intuit.ru/studies/courses/2291/591/lecture/12702 (in Russian).
[3] M. G. Kuhn, Compromising emanations: Eavesdropping risks of computer displays, Technical report UCAM-CL-TR-577 University of Cambridge, Computer Laboratory Access mode: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf.
[4] P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou Compromising Electromagnetic Field Radiated by In-House PLC Lines, IEEE Global Telecommunications Conference, December 2010, Pages 1-5, DOI:10.1109/GLOCOM.2010.5683144.
[5] Litao Wang, Bin Yu. Analysis and measurement on the electromagnetic compromising emanations of computer keyboard, 17th International Conference on Computational Intelligence and Security, December 2011, Pages 640-643, DOI: 10.1109/CIS.2011.146.
[6] M. G. Kuhn Compromising emanations of LCD TV sets, IEEE Transaction on electromagnetic compatibility, vol. 55, NO 3, June 2013, Pages. 564 – 570, DOI:10.1109/TEMC.2013.2252353.
[7] I. F. Tashenov, A. S. Luchinin Study of side electromagnetic radiation of the laser printer, the XXIII international scientific-technical conference, November 2014, Pages 37-43, URI: http://hdl.handle.net/10995/46437 (in Russian).
[8] L. Nowosielski, M.Wnuk, Compromising emanations from USB 2 interface, Proceedings of PIERS 2014 in Guangzhou ISSN 1559-9450, August 2014, Pages 2666–2670.
[9] Leszek Nowosielski, Rafal Przesmycki1, and Micha Nowosielski Compromising Emanations from VGA and DVI Interface, Progress In Electromagnetic Research Symposium (PIERS), August 2016, Pages 1024 – 1028, DOI:10.1109/PIERS.2016.7734570.
[10] Andrey Ivanov, Ivan Reva, Andrey Ushakov Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), October 2016, Pages 156-158, DOI:10.1109/APEIE.2016.7806436
[11] Degang Sun, Di Wei, Ning Zhang, Zhiqiang Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC), May 2016, Pages 190-193, DOI:10.1109/APEMC.2016.7523005
[12] Jun Shi, Degang Sun, Abbas Yongacoglu, Meng Zhang, Dong Wei. Computer Recognition Based On the Compromising Emanations Fingerprint, Canadian Conference on Electrical and Computer Engineering (CCECE), May 2016, Pages 1-6, DOI: 10.1109/CCECE.2016.7726724.
[13] Rostislav I. Sokolov, Renat R. Abdullin Determined Factor Parameter Analysis for System of Information Recovery from USB-Keyboard Compromising Emanations, International Applied Computational Electromagnetics Society Symposium - Italy (ACES), March 2017, Pages 1-2, DOI:10.23919/ROPACES.2017.7916332.
[14] Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboard 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), January 2016, Pages 1-4, DOI:10.1109/ICIEAM.2016.7911553.
[15] Andrey Ivanov, Ivan Reva, Baryshnilov Yaroslav Development of Hardware-software Complex for Automatized Compromising Electromagnetic Emanation Search, 11th International Forum on Strategic Technology (IFOST), June 2016, Pages 1-3, DOI:10.1109/IFOST.2016.7884180.

Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант – 27 апреля 2018 г.
Received – December 18, 2017. The final version – April 27, 2018.

Сергей А. Климачев, Наталья А. Тишина
Оренбургский государственный университет,
пр-т Победы, 13, г. Оренбург, 460018, Россия
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru, https://orcid/0000-0002-7341-6985

МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ТОЧНОСТИ ОБНАРУЖЕНИЯ АТАК ОБЛАЧНОЙ СРЕДЫ

DOI: http://dx.doi.org/10.26583/bit.2018.2.04

Аннотация. Статья посвящена исследованию вопроса оценки эффективности систем обнаружения атак (СОА), применяемых для защиты вычислительных платформ, характеризующихся динамичностью, сложной организационно-технической структурой и наличием большого количества разнородных параметров ее компонент. Анализ существующих методик оценки СОА позволил выявить проблемы, в частности недостатки в обосновании количественных метрик, отражающих производительность, достоверность принимаемых решений СОА, что затрудняет доказуемость методики оценки СОА. Целью исследования является: повышение объективности оценки СОА, достичь которую можно с помощью разработки правильной методики и инструментов оценки, а также надежного экспериментального стенда. В статье предложены результаты разработки и апробации методики и программного обеспечения оценки эффективности СОА на основе построения оптимального множества количественных показателей точности обнаружения атак, позволяющие решать задачи сравнительного анализа СОА, обладающих схожими функциональными возможностями. В результате проведенных исследований решены следующие задачи: выбор универсальных количественных показателей для оценки точности обнаружения атак СОА; определение обобщенного показателя точности обнаружения атак на основе построения парето-оптимального множества наборов значений количественных показателей, отражающих обеспечение конфиденциальности, целостности и доступности информации и информационных ресурсов облачной среды; разработка функциональной модели, схемы и программного обеспечения экспериментального исследования СОА облачной среды.

Ключевые слова: оценка эффективности, количественные показатели эффективности, системы обнаружения атак, облачная среда.

Для цитирования. КЛИМАЧЕВ, Сергей А.; ТИШИНА, Наталья А.. МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ТОЧНОСТИ ОБНАРУЖЕНИЯ АТАК ОБЛАЧНОЙ СРЕДЫ. Безопасность информационных технологий, [S.l.], n. 2, p. 54-62, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1109>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.04.

Sergey A. Klimachev, Natalia A. Tishina
Orenburg State University,
Pobedy Av., 13 Orenburg, 460018, Russia,
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru https://orcid/0000-0002-7341-6985

Technique of experimental evaluation of cloud environment attacks detection accuracy

DOI: http://dx.doi.org/10.26583/bit.2018.2.04

Abstract. The article is devoted to research of efficiency evaluation of IDS used for dynamic and complex organizational and technical structure computing platform guard. The components of the platform have a set of heterogeneous parameters. Analysis of existing IDS evaluation technique revealed shortcomings in justification of quantitative metrics that describe the

efficiency and reliability IDS resolving. This makes if difficult to prove IDS evaluation technique. The purpose of the study is to increase IDS evaluation objectivity. To achive the purpose it is necessary to develop the correct technique, tools, experimental stand. The article proposes the results of development and approbation of the technique of IDS efficiency evaluation and software for it. The technique is based on defining of optimal set of attack detection accuracy scores. The technique and the software allow solving problems of comparative analysis of IDS that have similar functionality. As a result of the research, a number of task have been solved, including the selection of universal quantitative metrics for attack detection accuracy evaluation, the defining of summarised attack detection accuracy evaluation metric based on defining of pareto-optimal set of scores that ensure the confidentiality, integrity and accessibility of cloud environment information and information resources, the development of a functional model, a functional scheme and a software for cloud environment IDS research.
Keywords: efficiency evaluation, efficiency scores, IDS, cloud environment.
For citation. KLIMACHEV, Sergey A.; TISHINA, Natalia A.. Technique of experimental evaluation of cloud environment attacks detection accuracy. IT Security (Russia), [S.l.], n. 2, p. 54-62, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1109>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.04

Введение

Начало XXI века ознаменовалось бурным развитием облачных вычислений, повлекшим за собой рост популярности облачных сервисов и масштабный переход организаций на новую вычислительную платформу, в результате облачные вычисления стали рассматриваться в качестве альтернативы традиционным моделям обработки информации.

Однако передовой характер технологии и природа ее концепции определили не только преимущества облачных вычислений, но и проблемные стороны, центральное место в списке которых заняла безопасность. Статистика угроз и анализ рынка облачных вычислений показывают, что актуальность защиты облачной среды (ОС) (Cloud Environment) очень высока [1], [2]. Однако сложная организационно-техническая структура среды и наличие большого количества разнородных параметров ее компонент значительно усложняют задачу обеспечения безопасности. При этом использование программных систем защиты информации для поддержания безопасного состояния среды приводит к возникновению новых вопросов методологического и практического характера в области исследования средств защиты информации. Среди них выделяется вопрос оценки эффективности систем обнаружения компьютерных атак, называемых Федеральной службой безопасности (ФСБ России) системами обнаружения атак (СОА), а Федеральной службой по техническому и экспортному контролю (ФСТЭК России) – системами обнаружения вторжений (СОВ).

Существуют различные методики оценки эффективности СОА, отличающиеся множеством критериев и показателей, методами расчета показателей, множеством параметров системы.

Можно выделить такие проблемы существующих методик как:

– использование только качественных или нечетко определенных количественных показателей оценки (используются тривиальные или невыразительные показатели оценки);

– используемые классификации атак не помогают в достоверной и объективной оценке, так как не охватывают все аспекты атак, обеспечивающие полноту анализа при формировании подмножества атак;

– нет четко определенной методологии, организация и последовательность методики нарушают логический порядок;

– отсутствие репрезентативных тестовых наборов нападения, основанных на полной и правильной классификационной схеме атак.

В результате существенно затрудняется оценка функциональных возможностей СОА и обоснование выбора СОА для эксплуатации в конкретных условиях. Низкий уровень обоснования количественных показателей оценки эффективности, отражающих производительность, достоверность принимаемых решений СОА затрудняет доказуемость методики оценки СОА.

Методология количественного оценивания эффективности СОА предназначена для сравнения различных СОА и определения оптимальных параметров СОА, в ней выделяют критерий, показатель и метод:

– критерий – это область оценивания (обобщенный показатель), т.е. то, что необходимо оценить и правило выбора: например, максимальная точность обнаружения атак, максимальная скорость обнаружения атак и т.п.;

– показатель (мера или метрика) определяет конкретное свойство, которое оценивается для выбранного критерия: например, процент правильно распознанных атак, время обработки пакетов, уровень максимальной пропускной способности канала передачи данных и т.п.

– метод – это способ определения соответствующего значения для данного показателя: например, сравнение распознанных атак с последовательностью сгенерированных атак, оценка времени распознавания атак в секундах и т.п.

Среди количественных критериев, характеризующих эффективность СОА, таких как точность, полнота, производительность и оперативность обнаружения атак, недостаточно исследован важнейший критерий – точность обнаружения атак, характеризующий способность СОА правильно распознавать атакующие воздействия.

Таким образом, актуальной задачей становится разработка методики оценки точности обнаружения атак СОА, позволяющей осуществить выбор наилучшей СОА и определять оптимальные параметры СОА.

Для решения данной задачи необходимо выполнить:

- Выбор показателей оценки точности обнаружения атак.
- Выбор методов расчета показателей.
- Разработку экспериментального стенда.

Целью исследования является: повышение объективности оценки СОА путем разработки правильной методики и программного обеспечения оценки, а также экспериментального стенда.

Разработка методики оценки

Разрабатываемая методика должна учитывать существующие проблемы оценки, всеобъемлющие, универсальные количественные показатели точности СОА и условия её эксплуатации – характеристики ОС. Оценка может вестись в двух направлениях: определение точности обнаружения атак по параметрам СОА и определение наиболее эффективной по точности обнаружения атак одной из нескольких СОА.

Решение задачи выбора показателей оценки, которые отражают достоверность принимаемых решений СОА, является важным аспектом формирования методики оценки точности обнаружения атак. В ходе исследовательских разработок СОА было предложено множество различных количественных показателей. Наиболее часто применяются показатели, которые измеряют соотношение между входными и выходными событиями СОА, такие как [3]:

- TP (True positive): количество истинно-положительных распознаваний атак.
- TN (True negative): количество истинно-отрицательных распознаваний атак.
- FP (False positive): количество ложно-положительных распознаваний атак.
- FN (False negative): количество ложно-отрицательных распознаваний атак.

Используя эти простые показатели, получают оценку, размытую между ними,

поэтому целесообразнее получить математическое выражение для интегрального показателя или построить множество оптимальных наборов значений показателей.

Исследователями предлагались и более сложные соотношения для показателей, такие как кривая ROC (Receiver Operating Characteristic) – кривая эксплуатационной характеристики приемника [4, 5], P(I|A) – байесовский уровень обнаружения [6], совокупная стоимость [7], ожидаемая стоимость [8], CID (Intrusion Detection Capability) – способность обнаружения вторжений [9], E_{ID} (enhanced Bayesian detection rate) – расширенная байесовская оценка [10], R_R.(Attack Recognition Rate) – уровень распознавания атак [10].

Каждый из этих показателей был основан на различных теоретических подходах, таких как оптимизационный подход [11], байесовский и информационно-энтропийный подходы [12, 13], метод имитационного моделирования [10], оценка рисков информационной безопасности [14, 15]. Однако ни один из перечисленных подходов не лишен недостатков.

Одни методики позволяют выбрать лучшую СОА, сравнивая две или более системы, в то время как каждая сравниваемая система в отдельности не является эффективной. Другие методики учитывают соотношение только некоторых частных показателей и не учитывают, что эффективность СОА зависит от большого числа показателей, которые могут быть несравнимыми. Общий недостаток большинства существующих подходов: не учитывают классификацию атак, усредняя значение показателей по всем видам атак, в то время как некоторые СОА могут быть более точными по одному из видов атак, являющемуся более опасным для конкретной защищаемой среды.

В данной работе предлагается методика оценки СОА, основанная на построении множества оптимальных наборов значений количественных показателей точности обнаружения атак. Показатели характеризуют правильность распознавания атак категорий, соответствующих стандартной модели безопасности информации CIA (Confidentiality, Integrity, Availability):

1) k^C – уровень распознавания атак конфиденциальности,
2) k^I – уровень распознавания атак целостности,
3) k^A – уровень распознавания атак доступности,

такие, что

$$k^{\{C,I,A\}} = \frac{TP + TN}{TP + FP + TN + FN}, \quad (1)$$

где TP – количество верно распознанных атак соответствующей категории; TN – количество верно распознанных легитимных воздействий; FP – количество воздействий, неверно распознанных как атаки; FN – количество воздействий, неверно распознанных как легитимные.

Предполагается, что СОА $S*$ обеспечивает некоторую точность обнаружения атак и характеризуется некоторым множеством параметров P^S, а также существует множество векторов P, определяющее всевозможные значения этих параметров, причем каждому вектору $p_i \in P,\ i = \overline{1..n}$ ставится в соответствие некоторый вектор значений показателей точности обнаружения k_{p_i} множества векторов K. Тогда задача экспериментального исследования СОА будет заключаться в выделении оптимального вектора значений показателей точности обнаружения и соответствующего ему вектора значений параметров СОА:

$$\begin{cases} L(p_i, k_{p_i}) \to \max \\ p_i \in P : k_{p_i} = A(K,U), k_{p_i} \in K \end{cases}, \quad (2)$$

где $A(K,U)$ – алгоритм, определяющий оптимальный вектор значений показателей точности обнаружения из множества векторов K по заданным условиям U; $L(p_i,k_{p_i})$ – точность обнаружения атак, обеспечиваемая СОА.

Таким образом, задача определения наилучших значений параметров СОА сводится к задаче нахождения вектора оптимальных значений показателей точности, которая в свою очередь может быть решена на основе построения парето-оптимального множества.

Решение $k^* \in K$ называется оптимальным по Парето (парето-оптимальным), если не существует такого возможного решения $k \in K$, для которого имеет место неравенство $f(k) \geq f(k^*)$. Все парето-оптимальные решения образуют множество Парето ($P_f(K)$):

$$P_f(K) = \{k^* \in K \mid \nexists k \in K, f(k) \geq f(k^*)\}. \quad (3)$$

Для нахождения множества Парето будет использоваться алгоритм, приведенный в [16]. Выбор единственного вектора парето-оптимального множества будет осуществляться на основе обобщенного показателя (4):

$$k^{общ^*} = \sum_i w_i \cdot k_i,\ i \in \{C, I, A\}, \quad (4)$$

где w_i – весовой коэффициент значимости показателя точности обнаружения атак, определяемый экспертом (1).

Тогда наилучшим будет вектор, характеризующийся максимальным $k^{общ^*}$.

Таким образом, предложенный подход позволяет: осуществлять подбор параметров СОА, при которых обеспечивается конфиденциальность, целостность и доступность информации и информационных ресурсов ОС в наибольшей степени; проводить сравнительный анализ нескольких СОА на предмет выявления системы с наилучшими показателями точности обнаружения атак.

Программное обеспечение и схема эксперимента

Описанная методика была положена в основу аналитической компоненты программного средства оценки точности обнаружения атак СОА. Работоспособность программного средства подтверждена в результате эксперимента (рисунок 1), в котором в качестве анализируемой СОА выступила система Snort. Snort использует язык правил, комбинирующий возможности сигнатурного поиска, протокольного анализа и обнаружения аномалий. Схема экспериментального стенда облачной среды для испытаний СОА представлена на рисунке 2.

Основной отличительной особенностью экспериментального стенда для оценки СОА в условиях облачных вычислений является использование технологии виртуализации и балансировщика нагрузки. Обнаружение атак осуществляется либо путем маршрутизации всего трафика через СОА, установленную на выделенный сервер как на рисунке 2, либо же путем мониторинга трафика на каждом сервере в отдельности.

Для сравнительного анализа использовано 10 различных наборов правил. Выполнение атакующих воздействий осуществлялось в соответствии с планом (таблица 1), включающим три серии атак, направленных на нарушение конфиденциальности, целостности и доступности информации. Значение «1» плана определяет реализацию атаки, «0» - генерацию сетевой нагрузки. Каждая серия атак состоит из 10 позиций.

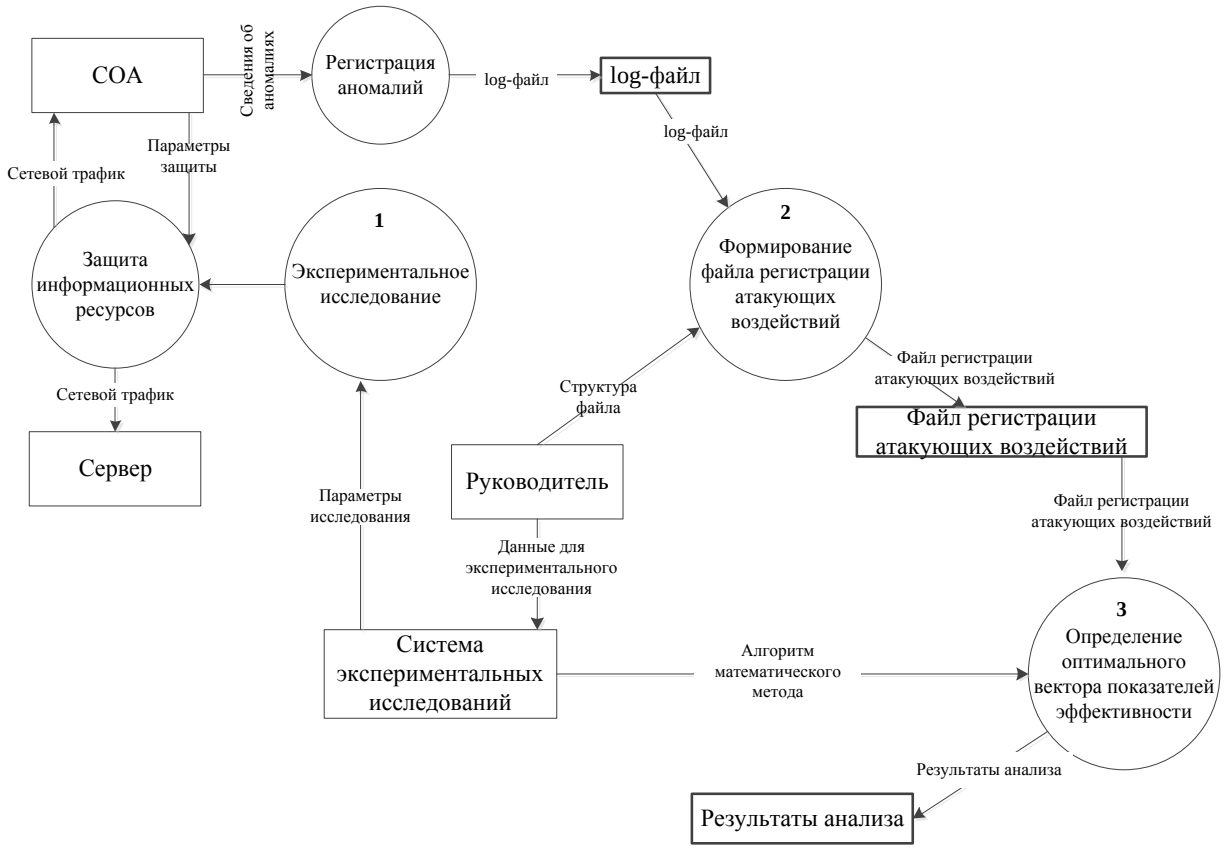


Рис. 1. Схема проведения эксперимента
(Fig. 1. Scheme of the experiment)

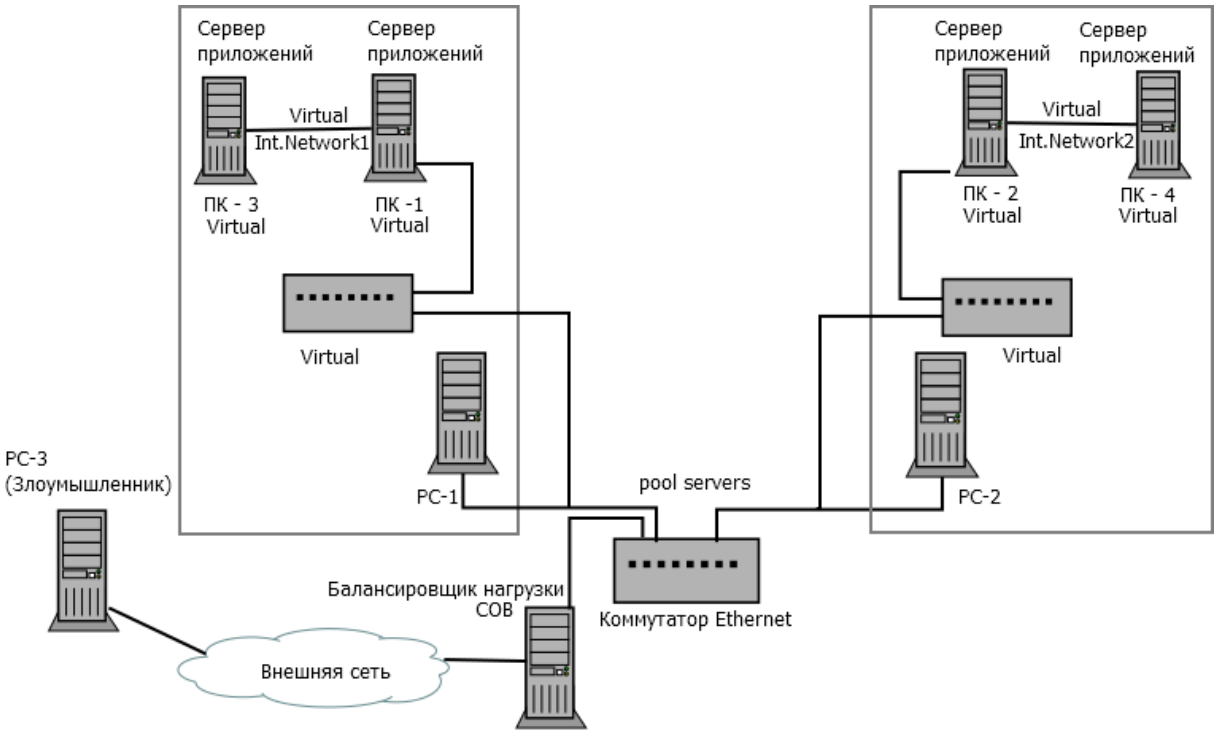


Рис. 2. Схема экспериментального стенда
(Fig. 2. The scheme of experimental stand)

Таблица 1. План выполнения атакующих воздействий

Серии атак	Атакующие воздействия									
Конфиденциальность	1	1	0	1	1	0	1	1	1	1
Целостность	1	0	1	1	1	0	1	0	1	1
Доступность	1	1	1	0	1	1	1	1	0	1

На основе результатов экспериментальных исследований в соответствии с вышеописанным планом и результатов анализа log-файлов СОА в соответствии с формулой (1) для каждого набора правил СОА Snort получены следующие показатели точности СОА (таблица 2).

Таблица 2. Показатели точности СОА

Показатель	Номер набора правил Snort									
	1	2	3	4	5	6	7	8	9	10
k_C	1	0,8	0,6	0,8	0,8	0,6	0,9	0,7	0,6	0,6
k_I	0,8	0,8	1	0,9	1	0,8	0,8	0,9	0,9	0,7
k_A	0,9	0,9	0,9	0,9	0,8	0,9	0,9	0,8	0,9	0,8

В результате нахождения парето-оптимального множества векторов показателей точности СОА наилучшим набором правил Snort определен набор №1 (рисунок 3).

Таким образом, предложенная методика на основе парето-оптимального множества позволила осуществить выбор наилучшего набора правил СОА, минимизируя участие эксперта в процессе оценивания.

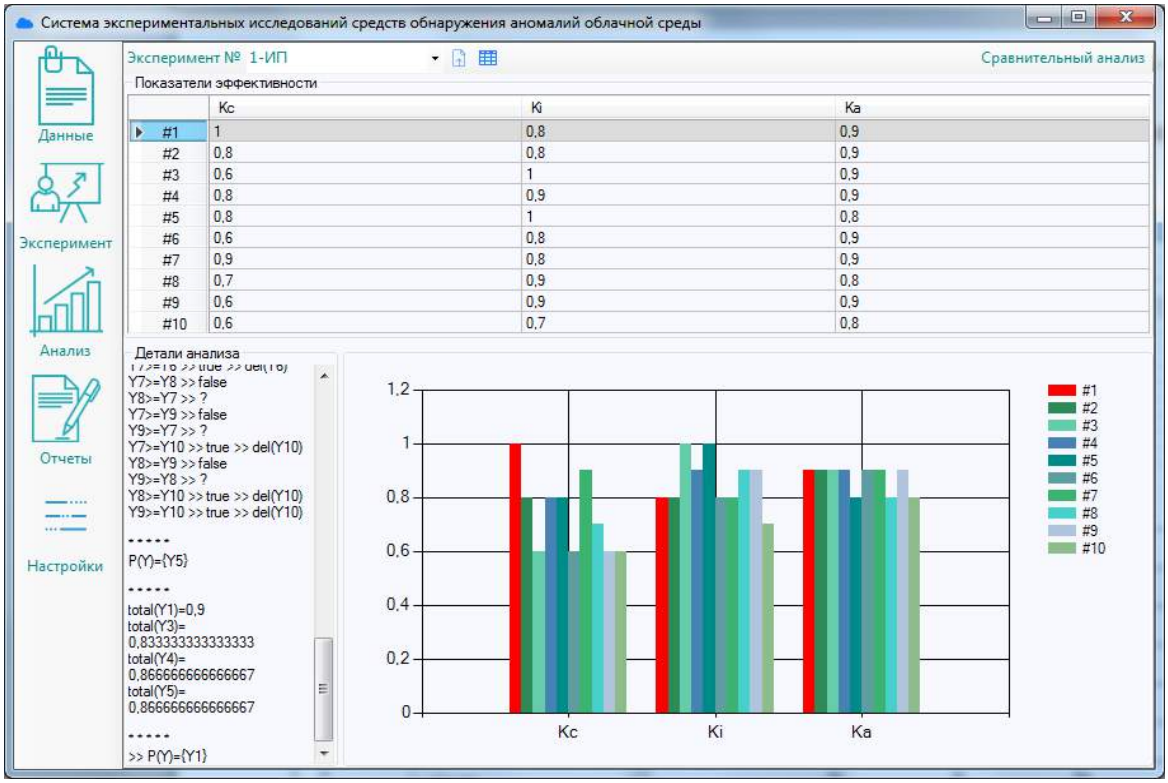


Рис. 3. Результаты экспериментальных исследований
(Fig. 3. The results of experimental studies)

Заключение

В результате проведенных исследований достигнуты следующие результаты:

– выбраны универсальные количественные показатели для оценки точности обнаружения атак СОА.

– определен обобщенный показатель точности обнаружения атак на основе построения парето-оптимального множества наборов значений количественных показателей, отражающих обеспечение конфиденциальности, целостности и доступности информации и информационных ресурсов ОС.

– разработаны схема проведения эксперимента, схема экспериментального стенда и программное обеспечение экспериментального исследования СОА облачной среды.

Таким образом, разработанная методика и программное обеспечение оценки позволяют вне зависимости от архитектуры СОА и реализованных в ней методов обнаружения атак осуществлять сравнительный анализ СОА, обладающих схожими функциональными возможностями на предмет выявления системы с наилучшими показателями точности обнаружения атак и определять наилучший набор значений параметров СОА.

СПИСОК ЛИТЕРАТУРЫ:

1. Architectures and Protocols for Secure Information Technology. Ruiz-Martinez, Pereniguez-Garcia, and Marin-Lopez (Eds.), IGI-Global, USA, 2013.
2. Security Issues in Cloud Environments – A Survey Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio. International Journal of Information Security, Volume 13 Issue 2, April 2014 pp. 113-170.
3. Vasim Iqbal Memon, Gajendra Singh Chandel A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency. Vasim Iqbal Memon, Gajendra Singh Chandel. Vasim Iqbal Memon et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 1), May 2014, pp.01-07.
4. Jacob W. Ulvila, John E. Gaffney, Jr Evaluation of Intrusion Detection Systems, Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003 [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844520.
5. Lippmann, R.; Fried, D.; Graf, I.; Haines, J.; Kendall, K.; Mcclung, D.; Weber, D.; Webster, S.; et al.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. Los Alamitos, CA, USA: IEEE, 2000, pp. 12–26.
6. Axelsson, S. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. In: Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99). Singapore: ACM Press, 1999, pp. 1–7.
7. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P.: Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. South Carolina, USA: IEEE, 2000, pp. 130–144.
8. Gaffney, J.E.; Ulvila, J.W. Evaluation of Intrusion Detectors: A Decision Theory Approach. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P'01). Oakland, CA, USA: IEEE, 2001, pp. 50–61.
9. Gu, G.; Fogla, P.; Dagon, D.; Lee, W.; Skoric, B.: Measuring Intrusion Detection Capability: An Information-Theoretic Approach. In: Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06). Taipei, Taiwan: ACM, 2006, pp. 90–101.
10. Nasr, Khalid. Performance analysis of wireless intrusion detection systems. PhD, Institut National Polytechnique de Toulouse, 2013 [Электронный ресурс]. – Режим доступа: http://oatao.univ-toulouse.fr/14136
11. Методы оценки эффективности систем защиты информационных систем. Н.А. Маслова Искусственный интеллект. — 2008. — № 4. — С. 253-264.
12. Зикратов Игорь Алексеевич, Одегов Степан Викторович Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода. Научно-технический вестник информационных технологий, механики и оптики. 2012. №4 (80) [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda
13. Анищенко В. В., Земцов Ю. В. Методика испытаний систем обнаружения атак. Известия ЮФУ. Технические науки. 2007. №1 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/metodika-ispytaniy-sistem-obnaruzhe-niya-atak.
14. Зикратов Игорь Алексеевич, Одегов Степан Викторович, Смирных Александр Валентинович Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования. Научно-технический вестник информационных технологий, механики и оптики. 2013. №1 (83) [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-v-oblachnyh-servisah-na-osnove-lineynogo-programmirovaniya.

15. Царегородцев А.В., Макаренко Е.В. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации. Национальные интересы: приоритеты и безопасность. 2014. №44 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1.
16. В.Д. Ногин. Принятие решений при многих критериях. Учебно-методическое пособие. – СПб. Издательство «ЮТАС», 2007. – 104 с.

REFERENCES:

[1] Architectures and Protocols for Secure Information Technology. Ruiz-Martinez, Pereniguez-Garcia, and Marin-Lopez (Eds.), IGI-Global, USA, 2013.
[2] Security Issues in Cloud Environments – A Survey Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio. International Journal of Information Security, Volume 13 Issue 2, April 2014 pp. 113-170.
[3] Vasim Iqbal Memon, Gajendra Singh Chandel A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency. Vasim Iqbal Memon, Gajendra Singh Chandel. Vasim Iqbal Memon et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 1), May 2014, pp.01-07.
[4] Jacob W. Ulvila, John E. Gaffney, Jr Evaluation of Intrusion Detection Systems, Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003 [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844520.
[5] Lippmann, R.; Fried, D.; Graf, I.; Haines, J.; Kendall, K.; Mcclung, D.; Weber, D.; Webster, S.; et al.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. Los Alamitos, CA, USA: IEEE, 2000, pp. 12–26.
[6] Axelsson, S. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. In: Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99). Singapore: ACM Press, 1999, pp. 1–7.
[7] Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P.: Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. South Carolina, USA: IEEE, 2000, pp. 130–144.
[8] Gaffney, J.E.; Ulvila, J.W. Evaluation of Intrusion Detectors: A Decision Theory Approach. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P'01). Oakland, CA, USA: IEEE, 2001, pp. 50–61.
[9] Gu, G.; Fogla, P.; Dagon, D.; Lee, W.; Skoric, B.: Measuring Intrusion Detection Capability: An Information-Theoretic Approach. In: Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06). Taipei, Taiwan: ACM, 2006, pp. 90–101.
[10] Nasr, Khalid. Performance analysis of wireless intrusion detection systems. PhD, Institut National Polytechnique de Toulouse, 2013 [Электронный ресурс]. – Режим доступа: http://oatao.univ-toulouse.fr/14136
[11] Methods for evaluating the effectiveness of information systems security. H. Ah. Maslov Artificial intelligence. - 2008. — No. 4. — P. 253-264. (in Russian).
[12] Zikratov Igor' Alekseyevich, Odegov Stepan Viktorovich Evaluation of information security in cloud computing based on Bayesian approach. Journal scientific and technical of information technologies, mechanics and optics. 2012. No. 4 (80) [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda. (in Russian).
[13] Anishchenko V. V., Zemtsov Y. V. Methods of testing systems to detect attacks. Izvestiya yufu. Technical science. 2007. No. 1 [Electronic resource]. - Access mode: http://cyberleninka.ru/article/n/metodika-ispytaniy-sistem-obnaruzhe-niya-atak. (in Russian).
[14] Zikratov Igor' Alekseyevich, Odegov Stepan Viktorovich, Smirnykh Aleksandr Valentinovich Assessment of information security risks in cloud services based on linear programming. Journal scientific and technical of information technologies, mechanics and optics. 2013. No. 1 (83) [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-v-oblachnyh-servisah-na-osnove-lineynogo-programmirovaniya. (in Russian).
[15] Tsaregorodtsev A.V., Makarenko Y.V. Methods of quantitative risk assessment in information security of cloud infrastructure of the organization. National interests: priorities and security. 2014. No. 44 [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1. (in Russian).
[16] Nogin V.D. Decision-making under many criteria. Educational and methodical manual. – SPb. Yutas publishing house, 2007. - 104 p. (in Russian).

Поступила в редакцию – 05 марта 2018 г. Окончательный вариант –27 апреля 2018 г.
Received – March 05, 2018. The final version – April 27, 2018.

Игорь Ю. Жуков, Олег Н. Мурашов
ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

ЗАЩИЩЕННЫЕ ПРОЦЕДУРЫ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ, ФОРМИРОВАНИЯ КЛЮЧА ФИСКАЛЬНОГО ПРИЗНАКА И ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2018.2.05

Аннотация. В статье дается описание криптографических механизмов взаимной аутентификации и формирования ключа фискального признака. Эти механизмы основаны на использовании блочного шифра «Кузнечик», определенного национальным стандартом Российской Федерации ГОСТ Р 34.12–2015 и реализованного в режиме гаммирования в соответствии ГОСТ Р 34.13–2015. Функции выработки имитовставки (кода аутентификации) заданы рекомендациями по стандартизации Р 50.1.113–2016.

Предлагаемое в данной работе решение направлено на обеспечение аутентификации и контроля целостности фискальных данных, передаваемых по каналам связи между фискальными накопителями и операторами фискальных данных, а также между операторами фискальных данных и уполномоченным органом. Форматы передаваемых фискальных данных, способы передачи фискальных данных и механизмы обеспечения конфиденциальности передаваемых фискальных данных определяются уполномоченным органом федеральной исполнительной власти.

В статье дано краткое описание модели протокола, проведен формальный анализ пассивных атак в предположении, что криптографическая стойкость исследуемого протокола зависит от стойкости используемых в нем криптографических преобразований, являющихся отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации. Так как указанные криптографические преобразования не могут быть скомпрометированы нарушителем, можно сделать вывод, что нарушителем также не может быть скомпрометирован и исследуемый протокол.

Ключевые слова: взаимная аутентификация, криптографические преобразования, мастер-ключ, фискальный признак, защита фискальных данных.

Для цитирования. ЖУКОВ, Игорь Ю.; МУРАШОВ, Олег Н.. ЗАЩИЩЕННЫЕ ПРОЦЕДУРЫ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ, ФОРМИРОВАНИЯ КЛЮЧА ФИСКАЛЬНОГО ПРИЗНАКА И ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], n. 2, p. 63-70, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1110>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.05.

Igor Y. Zhukov, Oleg N. Murashov
Ltd «The National Mobile Portal»,
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

A secure mutual authentication procedure, generate the key fiscal basis, and fiscal data protection

DOI: http://dx.doi.org/10.26583/bit.2018.2.05

Abstract. The paper describes cryptographic transformation for mutual authentication and creation of the fiscal sign key. This transformation based on using block encryption cipher named «Kuznetchik», described in the national standard of the Russian Federation GOST R 34.12-2015 and realized in gamma generation mode as it is described in the another national standard of the Russian Federation

GOST R 34.13-2015. The function of the integrity protection (authentication code) is defined by the recommendation for standardization R 50.1.113–2016.
The solution proposed in this paper is aimed for an authentication and integrity control of fiscal data transmitted through communication channels between fiscal storage devices and fiscal data operators, as well as between the fiscal data operators and the authorized agency. Formats of transmitted fiscal data, methods of transmission and mechanisms to ensure the confidentiality of transmitted fiscal data determined by the authorized agency of the Federal Executive power.
The article gives a short description of the protocol model, a formal analysis of passive attacks in the assumption that the cryptographic properties of the protocol depends on the feature of cryptographic transformations used, which are standardized solutions regulated by national standards, or national recommendations for standardization. Since the cryptographic transformations could not be compromised by the intruder we can conclude that the intruder also can not compromise the fiscal signs protection protocol.
Keywords: mutual authentication, cryptographic transformation, master key, fiscal sign, fiscal data protection.
For citation. ZHUKOV, Igor Y.; MURASHOV, Oleg N.. A secure mutual authentication procedure, generate the key fiscal basis, and fiscal data protection. IT Security (Russia), [S.l.], n. 2, p. 63-70, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1110>. Date accessed: 26 apr. 2018.
doi:http://dx.doi.org/10.26583/bit.2018.2.05.

Введение

Одним из важнейших направлений реализации программы «Цифровая экономика Российской Федерации» является развитие киберфизических систем, в частности, интернета вещей. При этом актуальной задачей становится обеспечение целостности и достоверности информационного обмена между элементами указанных систем. Решение этой задачи, как правило, достигается использованием защищенных процедур обмена информацией, основанных на применении симметричных криптографических преобразований и отечественных стандартов шифрования ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

Такая задача, в частности, возникает при реализации требований действующего законодательства по электронному обмену фискальной информацией между торговыми предприятиями и налоговыми органами [1-3]. Обязательное повсеместное использование таких процедур должно быть основано на применении стандартизованных криптографических механизмах, предложенных в [4, 7].

Настоящая работа содержит результаты исследований и обоснования криптографических качеств механизмов аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных в дополнение к исследованию безопасности ключевой системы фискального признака [5].

Под фискальным признаком [6] понимается достоверная информация, сформированная с использованием фискального накопителя и ключа фискального признака или с использованием средств формирования фискального признака и мастер-ключа. Последний предназначен для создания серии ключей фискального признака, а также проверки фискальных признаков, сформированных с использованием ключей фискального признака этой серии. Достоверность данных достигается в результате криптографического преобразования фискальных данных, наличие которого дает возможность выявления корректировки или фальсификации этих фискальных данных при их проверке с использованием фискального накопителя и (или) средства проверки фискального признака.

Предложенный в [4] протокол обмена представляет собой последовательность действий, в ходе которой:

- средством формирования фискальных признаков и средством проверки фискальных признаков вырабатывается разовый ключ K, однозначно зависящий от общего секретного ключа K_{FSC} и номера фискального документа *FDN*;
- выполняется аутентификация фискальных данных;
- выполняется аутентификация средства проверки фискального признака.

Следует отметить, что последовательность и размеры передаваемых сообщений жестко фиксированы соответствующими нормативными документами налоговой службы России [2, 3], что не позволяет модифицировать протокол и интегрировать в него дополнительные механизмы защиты, например, аутентификацию средства выработки фискального признака. Кроме того, следует учитывать [2, 3], что процедуры взаимной аутентификации могут выполняться в течение суток, то есть представлять собой последовательность обмена сообщениями, существенно разделенными между собой по времени.

1. Модель протокола

Для целей нашего исследования предлагаемого протокола требуется дать его схематичное описание (модель). Без ограничения общности будем считать, что общий ключ средства формирования и средства проверки фискального признака KFSC известен обоим участникам протокола заранее. Тогда, изложенный в [4] протокол может быть схематично описан следующим образом:

Средство формирования ФП		**Средство проверки ФП**
Дано: SN_{FSC}, *KFSC, FD; FDN*		Дано: K_{FSC}, SN_{FSV}
1. $K = KDF(K_{FSC}, FDN);$		
2. $FS = HMAC(K_{0...255}, FD);$		
3. $C = Enc(K_{256...511}, FS, FD);$		
	———SN_{FSC}, *FDN, FS, FD* или *C*———>	
		1. $K = KDF(K_{FSC}, FDN);$
		2. $FD = Dec(K_{256...511,} FS, C);$
		3. $FS` = Mac(K_{0...255}, FD);$
		4. *FS` != FS ——> выход с неудачей.*
		5. $M = SN_{FSV} \| SN_{FSC} \| FDN \| FS;$
		6. $FS_{FSV} = HMAC(K_{0...255}, M);$
	<——— *FDN,* $SN_{FSV,}$ FS_{FSV} ——	
4. $M = SN_{FSV} \| SN_{FSC} \| FDN \| FS;$		
5. $FS` = HMAC\ (K_{0...255}, M);$		
6. *FS` != FS ——> выход с неудачей.*		

2. Анализ пассивных атак

Учитывая, что все используемые криптографические преобразования являются отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации, мы проведем анализ пассивных атак достаточно формально, полагая, что все используемые преобразования являются стойкими относительно атак нарушителя (в естественных предположениях о его вычислительных, финансовых и временных ресурсах) [8].

2.1. Атака на ключ фискального признака

При перехвате нарушителем фискальных данных *FD* и соответствующего им фискального признака (часть значения ключевой функции хэширования $HMAC_{256}$) *FS* возникает задача определения секретного ключа K_1, используемого в преобразовании:

$$FS = HMAC\ (K_1, FD).$$

Учитывая, что данное преобразование регламентируется рекомендациями [7], мы считаем, что эта задача является трудноразрешимой для нарушителя [9].

Здесь стоит отметить, что в силу ограниченности множества возможных значений номера фискальных данных, ключи, используемые для шифрования, принадлежат небольшому множеству мощности 2^{32}. Однако дать такое описание этому множеству, что оно может быть эффективно выписано и, как следствие опробовано, в настоящее время не представляется возможным.

Аналогично, при перехвате нарушителем зашифрованного текста *C* возникает задача определения секретного ключа K_2, используемого в преобразовании:

$$C = Enc(K_2, FD),$$

где, *Enc* – алгоритм шифрования открытого текста *FD* с помощью блочного алгоритма «Кузнечик» в режиме гаммирования, согласно ГОСТ Р 34.13-2015. При этом, величина *FD* нарушителю неизвестна[1]. Данная задача является трудноразрешимой для нарушителя.

2.2. Подделка фискального признака

Подделка фискального признака FS_{FSV} заключается в вычислении значения *FS`*, удовлетворяющего равенству:

$$FS` = HMAC(K1, FD),$$

при известном значении *FD* и неизвестном значении ключа K_1. В силу выбора преобразования HMAC, данная задача является трудноразрешимой для нарушителя [9].

2.3. Аутентификация фискальных данных

Согласно изложенной схеме легко видеть, что средство проверки фискальных данных выполняет только аутентификацию данных. Детализируем данное высказывание и рассмотрим фрагмент изложенной выше последовательности действий:

Средство формирования ФП		**Средство проверки ФП**
2. $FS = Mac(K_{0...255}, FD);$		
3. $C = Enc(K_{256...511}, FS, FD);$		
	———SN_{FSC}; *FDN, FS, FD* или *C*———>	
		2. $FD = Dec(K_{256...511}, FS;C);$
		3. $FS` = HMAC(K_{0...255}, FD);$

В данном фрагменте протокола для фискальных данных FD средством выработки сначала вычисляется часть значения ключевой функции хэширования $HMAC_{256}$, то есть значение *FS*, а после данные *FD* передаются в открытом или зашифрованном виде.

Средство проверки получает сообщение, расшифровывает данные (в случае необходимости), а после вычисляет часть значения ключевой функции хэширования $HMAC_{256}$ на своей копии ключа *K*. В этом случае аутентификация данных выполняется, когда полученное *FS* и вычисленное средством проверки FS` значения совпадают (очевидно, что совпадение произойдет, когда ключи выработки значения ключевой функции хэширования совпадают, а переданные данные не были модифицированы при передаче) [10].

Тем не менее, данный фрагмент не позволяет аутентифицировать участника, отправившего сообщение. Действительно, предположим, что нарушитель сохранил переданные ранее данные и отправляет их повторно. В этой ситуации, с формальной точки зрения, именно нарушитель является инициатором протокола. Вместе с тем, средство проверки фискальных данных совершенно корректно обработает посланное сообщение, продолжит протокол и выдаст в ответ нарушителю корректное сообщение.

Отметим, что аутентификация данных, а не их источника (средства формирования фискальных данных), является достаточной для функционирования системы передачи

[1] В классической постановке задачи нарушителю известен открытый и зашифрованный тексты, которые используется для нахождения секретного ключа. Вместе с тем, в нашей ситуации один ключ используется для шифрования одного сообщения, следовательно, если нарушителю известен открытый текст *FD*, то определение секретного ключа на котором он зашифрован является бесполезной задачей.

фискальных данных, поскольку сами данные содержит в себе информацию о том, кто их выработал.

Вместе с тем, описанная нами ситуация должна рассматриваться как атака на средство проверки фискальных данных. Ситуация, в которой нарушитель может повторно послать данные, которые будут корректно обработаны средством проверки фискальных данных, должна рассматриваться как успешная атака на навязывание сообщений, приводящая к компрометации протокола.

Стоит отметить, что успех данной атаки связан с отсутствием каких-либо механизмов аутентификации серийного номера средства формирования фискальных данных. Кроме того, при аутентификации данных, выработанных средством формирования фискальных данных, не используется возможность учета реального время выработки значения фискального признака, а также возможность выработки ключа в момент выработки фискального признака (формально, все ключи средства формирования фискального признака могут быть выработаны заранее, для каждого из возможных значений номера фискального документа).

Учитывая жестко фиксированную в [8, 9] последовательность передачи сообщений, а также форматов передаваемых сообщений, криптографическими методами решить указанную проблему не представляется возможным. В связи с этим, в средстве проверки фискального признака должен быть реализован механизм контроля уникальности поступающих значений *FDN* – номеров фискальных документов, привязанный к конкретному серийному номеру средства формирования фискальных документов. Это может быть достигнуто, например, использованием в качестве последовательности *FDN* монотонно возрастающей последовательности целых чисел от 0 до $2^{32} - 1$.

2.4. Аутентификация средства проверки фискального признака

Рассматриваемый протокол осуществляет аутентификацию средства проверки фискального признака – средство формирования фискального признака доказуемо подтверждает, что оно отправило фискальный признак именно тому средству проверки фискальных признаков, которому оно предназначалось (то есть оно имеет такой же секретный ключ KFSC, что и средство формирования). Для иллюстрации этого рассмотрим фрагмент исследуемого протокола:

Средство формирования ФП		**Средство проверки ФП**
	———SN_{FSC}, *FDN, FS, FD* или *C*———>	
		5. $M = SN_{FSV} \mid\mid SN_{FSC} \mid\mid FDN \mid\mid FS;$
		6. $FS_{FSV} = HMAC(K_{0...255}, M);$
	<——— *FDN*, SN_{FSV}, FS_{FSV} ——	

Таким образом, для подтверждения факта владения ключом K_{FSC} средство формирования фискального признака направляет средству проверки фискального признака, характеризуемому заданным значением SN_{FSV} случайное значение (в качестве которого выступает значение ключевой функции хэширования *FS*). В ответ средство формирования получает значение ключевой функции хэширования FS_{FSV} под отправленным значением *FS*, вычисленное с использованием общего ключа K_{FSC}.

При этом, средство проверки фискального признака вычисляет свой ответ в процессе выполнения протокола, то есть аутентифицируется в реальном времени. Стоит также отметить, что данный протокол аутентификации является модификацией протокола аутентификации из ISO/IEC 9798-2, [10], с заменой функции шифрования на функцию вычисления ключевой функции хэширования.

Также как и в случае аутентификации фискальных данных, здесь есть некоторые особенности, влияющие на корректность работы протокола. Предположим, что программная или аппаратная реализация исследуемого протокола вычисляет ключ проверки части значения ключевой функции хэширования FS_{FSV} исходя из тех данных, что получены в ответном

сообщении от средства проверки фискальных данных. В этом случае, нарушитель может навязать ложное значение FS_{FSV} , перехваченное им ранее в другом сеансе передачи данных (с другим средством проверки фискальных данных и другим номером фискального документа). Из этого следует, что средство формирования фискального признака сначала должно проверять полученные значения SN_{FSC}, SN_{FSV} и FDN на совпадение с теми, что были использованы им при выработке фискального признака, и только потом переходить к проверке значения FS_{FSV}.

2.5. Об алгоритмах выработки фискального признака

Согласно [4] используется четыре типа фискального признака:

1) фискальный признак документа размером 48 бит;
2) фискальный признак архива размером 256 бит;
3) фискальный признак сообщения размером 64 бита;
4) фискальный признак оператора размером 128 бит.

Размеры фискальных признаков жестко фиксированы соответствующими нормативными документами ФНС России [2, 3].

В связи с вышесказанным, для вычисления фискальных признаков различных длин был выбран алгоритм $HMAC_{256}$, регламентируемый рекомендациями по стандартизации [7].

Данный алгоритм является криптографически обоснованным и позволяет выработать значение ключевой функции хэширования любой необходимой нем длины, методом взятия нужного значения значащих бит от начала вектора – результата преобразования.

При выработке фискальных признаков используются криптографические механизмы, регламентируемые национальными стандартами Российской Федерации или рекомендациями по стандартизации Технического комитета № 26 Росстандарта России «Криптографическая защита информации».

2.6. О сроке действия ключа фискального признака при работе в автономном режиме

Согласно нормативным требованиям налоговой службы срок действия ключа фискального признака при работе в автономном режиме должен составлять не менее 36 месяцев.

За время действия ключа средство выработки фискального признака может использовать данный ключ для выработки фискальных признаков, а также для обеспечения конфиденциальности данных, передаваемых совместно с фискальными признаками.

С точки зрения криптографической защиты информации накопление нарушителем передаваемой информации в течение столь длительного времени может привести к возможности определения секретного ключа и, как следствие, к нарушению конфиденциальности передаваемой информации.

Однако, исходя из условий эксплуатации средств выработки фискальных признаков работа контрольно-кассовой техники в автономном режиме, можно предположить либо отсутствие каналов связи, по которым может передаваться зашифрованная информация, либо отсутствие необходимости передачи зашифрованной информации. Тем самым не возникают предпосылок к накоплению нарушителем передаваемой информации и нарушению ее конфиденциальности.

Поскольку при проведении анализа нельзя в точности заявить, что в автономном режиме использования контрольно-кассовой техники зашифрованная информация не может передаваться вообще, было бы корректным определение границы максимально возможного объема передаваемой информации в автономном режиме, исходя из криптографических свойств алгоритма ключевой функции хэширования, а также модельных эксплуатационных характеристик работы контрольно-кассовой техники в автономном режиме. На наш взгляд, точное значение данной величины должно устанавливаться в ходе проведения тематических исследований конкретного типа аппаратуры, реализующей процедуры взаимной

аутентификации, формирования ключа фискального признака, а также защиты фискальных данных.

Заключение

Из приведенных выше результатов обоснования достаточности мер криптографической защиты, принятых в ходе выполнения криптографических механизмов протокола аутентификации и выработки ключа фискального признака [4], можно сделать следующие выводы.

- Исследуемый протокол допускает возможность повторного навязывания средству проверки фискального признака переданных ему ранее сообщений. Учитывая фиксированную в [2, 3] последовательность передачи сообщений, а также форматов передаваемых сообщений, защита от повторного навязывания должна быть реализована организационными методами, основанными на отслеживании уникальности обрабатываемых номеров фискальных документов.
- Криптографическая стойкость исследуемого протокола зависит от стойкости используемых в нем криптографических преобразований, являющихся отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации. В предположении, что указанные криптографические преобразования не могут быть скомпрометированы нарушителем, можно сделать вывод, что нарушителем также не может быть скомпрометирован и исследуемый протокол.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа» от 22.05.2003 N 54-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_42359. Дата обращения 28.02.2018.
2. Контрольно-кассовая техника. Описание интерфейса фискального накопителя. Версия 1.2 от 06.07.2016. Вводится в действие 01.07.2016. Отладочная версия ФН 1.32_1. https://pkfn.ru/files/opisanie.pdf. Дата обращения 28.02.2018.
3. Приказ ФНС России от 21 марта 2017 г., №ММВ-7-20/229. https://www.nalog.ru/rn77/about_fts/docs/6719054. Дата обращения 28.02.2018.
4. Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных (Проект). — 2018. — 28 стр. http://www.ramec.ru/services/soprovogdenie/standart/. Дата обращения 28.02.2018.
5. Горбатов, Виктор С; Жуков, Игорь Ю; Мурашов, Олег Н. Безопасность ключевой системы фискального признака. Проблемы информационной безопасности. Компьютерные системы. СПбПУ, № 1. 2018.
6. Словарь финансовых и юридических терминов. http://www.consultant.ru/law/ref/ju_dict/word/fiskalnyj_priznak_dokumenta/ Дата обращения 28.02.2018.
7. Р 50.1-113.2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. — Стандартинформ, Москва, 2016.
8. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. — М.: Академия. — 2009. — 272 с.
9. Preneel B. Analysis and Design of Cryptographic Hash Functions. — Doctoral dissertation. — Katholieke Universiteit Leuven. — January 1993. 321p.
10. Menezes A.V., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography.— CRC Press. — 1996. — 816p.

REFERENCES:

[1] Federal law «About application of cash registers with cash calculations and (or) calculations with use of electronic tools of payment» of 05/22/2003 N54-FZ (latest edition). http://www.consultant.ru/document/cons_doc_LAW_42359. Check date 02/28/2018. (in Russian).

[2] Cash register equipment. The Fiscal storage interface description. Version 1.2 of 07/06/2016. Enforced 07/01/2016. The debug version of FN 1.32_1. https://pkfn.ru/files/opisanie.pdf. Check date 02/28/2018. (in Russian).
[3] Order of the Federal tax service of 21 March 2017, №ММВ-7-20/229. https://www.nalog.ru/rn77/about_fts/docs/6719054 Check date 02/28/2018. (in Russian).
[4] Rosstandart. Information technology. Cryptographic protection of information. Recommendations for standardization. Cryptographic authentication mechanisms and development of key fiscal signs to use in means of generating and verifying fiscal characteristics, providing the operation with fiscal data of cash registers, operators and authorities (Draft).— 2018. — 28 p. (in Russian).
[5] Gorbatov, Victor S.; Zhukov, Igor Y.; Murashov, Oleg N. The security of the fiscal sign key system. The problems of the information security. Computer systems. SpbPU, № 1, 2018. (in Russian).
[6] Dictionary of financial and legal terms. http://www.consultant.ru/law/ref/ju_dict/word/fiskalnyj_priznak_dokumenta/. Check date 02/28/2018. (in Russian).
[7] R 50.1-113.2016. Information technology. Cryptographic protection of information. Cryptographic algorithms associated with the use of electronic digital signature algorithms and hashing functions. - Standartinform, Moscow, 2016. (in Russian).
[8] Cheremushkin A. V. Cryptographic protocol. The main characteristics and vulnerabilities. — Moscow.: Academia. — 2009. — 272 p. (in Russian).
[9] Preneel B. Analysis and Design of Cryptographic Hash Functions. — Doctoral dissertation. — Katholieke Universiteit Leuven. — January 1993. 321 p.
[10] Menezes A.V., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography.— CRC Press. — 1996. — 816 p.

Поступила в редакцию – 10 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 10, 2017. The final version – April 27, 2018.

Буян С. Донгак
Томский государственный университет систем управления и радиоэлектроники, ул. Ленина, д. 40, г. Томск, 634050, Россия
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ ОРГАНИЗАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.2.06

Аннотация. В статье рассмотрен вопрос мониторинга сетевой активности рабочих компьютеров сотрудников для обеспечения информационной безопасности организации от внешних угроз, связанных с использованием аппаратного и программного обеспечения иностранного производства, в том числе и информационными сервисами, которые собирают разного рода информацию о пользователях сети Интернет. Показаны основные проблемы, возникающие в процессе выполнения анализа защищенности организации в сфере информационной безопасности (далее – ИБ). Приведен краткий обзор существующих инструментальных решений мониторинга сетевого трафика. Проведен эксперимент в использовании аппаратных и программных средств иностранного производства в организации. Эксперимент направлен на выявление негативных факторов, влияющих на информационную безопасность. Представлены результаты эксперимента. Сделаны выводы о недостатках методов и средств информационной защиты, а также рассмотрен вопрос оптимального соотношения использования инструментария фильтрации сетевого трафика.

Ключевые слова: межсетевой экран, мониторинг трафика, сетевая активность, информационная безопасность.

Для цитирования. ДОНГАК, Буян С.. МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ ОРГАНИЗАЦИИ. Безопасность информационных технологий, [S.l.], n. 2, p. 71-79, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1111>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.06.

Buyan S. Dongak
Tomsk state University of control systems and Radioelectronics, Lenina str., 40, Tomsk, 634050, Russia
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

Monitoring of network activity of the employees automated workplaces

DOI: http://dx.doi.org/10.26583/bit.2018.2.06

Abstract. The article addresses the issue of monitoring of the network activity of employee's computers in order to ensure information security of the organization from external threats caused by the use of hardware and software of foreign origin, including services collecting all kinds of information about Internet users. The major problems arising in the process of analysis of the security of the organization in the field of information security are discussed. A brief overview of existing network traffic monitoring tool solutions is given. The experiment with the use of the foreign hardware and software in the organization was carried on. The experiment is aimed at identifying negative factors affecting the information security. The results of the experiment are presented. Finally the conclusions about the shortcomings of methods and means of information protection are made, as well as optimal ways to use the tools for the network traffic filtering are addressed.

Keywords: firewall, traffic monitoring, network activity, information security.

For citation. DONGAK, Buyan S.. Monitoring of network activity of the employees automated workplaces. IT Security (Russia), [S.l.], n. 2, p. 71-79, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1111>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.06.

Введение

Развитие информационных технологий в настоящее время обеспечивает повышение качества жизни людей. Сегодня невозможно представить мир без сотовых телефонов, Интернета, информационных систем, которые разработаны с основной целью – облегчить нашу жизнь, сделать ее комфортной и безопасной. Однако, существует и ряд вопросов, которые необходимо решить для их нормального функционирования. Основным и наиболее важным вопросом при создании и эксплуатации информационных систем является обеспечение информационной безопасности. Информационная безопасность достигается путем применения последовательных, взаимосвязанных действий, направленных на обеспечение конфиденциальности, целостности и доступности информации в информационных системах. В России данное направление с каждым годом усовершенствуется [1]: меняется законодательная база, нормотворческая и методическая база защиты информации, модернизируются системы и комплексы защиты информации, но несмотря на это, существует основная проблема, аппаратные и программные обеспечения иностранного производства, которые используются в нуждах, как в государственном, так и в частном секторе. К ней относится распространенность иностранного аппаратного и программного обеспечения [2]. Это и неудивительно — ведь российский рынок, в буквальном смысле, наводнен продукцией западных разработчиков. В условиях напряженной геополитической обстановки и открытой информационной войны, ряд российских экспертов в области информационной безопасности считают, что главной угрозой информационной безопасности является использование иностранного программного обеспечения с закрытым, либо сложным, либо постоянно обновляющимся программным кодом, отследить изменения которого невозможно в режиме реального времени [3].

В данной статье приведен эксперимент в использовании аппаратных и программных средств иностранного производства в нуждах организации, одной из целей которой является защита коммерческой тайны. Эксперимент направлен на выявление негативных факторов, влияющих на информационную безопасность.

Задача: Мониторинг сетевой активности автоматизированных рабочих мест сотрудников организации, находящихся внутри (NAT) защищаемой сети с использованием межсетевого экрана (МЭ) на внешней границе сети Интернет, а также оценка эффективности правил фильтрации сетевого трафика.

Объект исследования: Автоматизированные рабочие места сотрудников организации, на которых используются прикладные программные продукты, работающие с сетью Интернет.

Предмет исследования: Принцип работы фоновых прикладных программных продуктов, использующихся на автоматизированных рабочих местах сотрудников организации, в том числе и зарубежного производства, во время обновления самого себя (собственного кода) с использованием сети Интернет, а также сетевая активность интернет-браузера, использующего веб-ресурсы, предназначенные для сбора информации о пользователях сети Интернет.

Обзор методик и существующих инструментальных решений мониторинга сетевого трафика

На сегодняшний день наиболее актуальна проблема обеспечения информационной безопасности организации от внутренних угроз, связанных с

действиями собственных сотрудников, и от внешних угроз, в том числе при использовании аппаратных и программных средств иностранного производства. Данная проблематика изучается многими исследователями в области защиты информации. Так, например, исследователями рассматриваются различные варианты систем мониторинга действий персонала [4], в том числе предлагается методика мониторинга сетевой активности персонала на основе прокси-серверов и анализа URL-адресов запросов [5]. Иной подход предлагается в методике анализа существующих классификаций инсайдерских угроз [6] и злоумышленников [7] и [8].

Анализ различных методик выявления угроз позволяет сделать вывод об отсутствии в настоящее время всеобъемлющей и последовательной классификации информационных угроз, в виду отсутствия общего для исследователей терминологического поля. По этой причине в работе [9] предложен метод классификации угроз инсайдеров с использованием кластеризации инцидентов. Для определения критериев классификации и критериев оценки результатов был проведен анализ собранных статистических данных. На основе кластеризации инцидентов была разработана классификация угроз инсайдерской безопасности. В настоящее время инциденты ИБ стали не только более многочисленными и разнообразными, но и более разрушительными, так как превентивные средства управления и контроля на основе результатов оценки рисков ИБ снижают большинство, но не все инциденты ИБ [10]. Таким образом, для быстрого обнаружения инцидентов ИБ, необходима система управления инцидентами ИБ, сводящая к минимуму потери информации [11], смягчающая уязвимости, которые были использованы [12], и восстанавливающая ИТ-инфраструктуру организации и ее услуги. Такие системы могут быть реализованы на основе центра управления безопасностью (ЦУБ). На основе анализа проведенных исследований представлены миссия и основные функции ЦУБ. Автором [13] предложена классификация ЦУБ и основные показатели инцидентов ИБ. Определены серьезные ограничения первого поколения ЦУБ.

Для выявление негативных факторов, влияющих на информационную безопасность, по мнению ряда исследователей [14], необходимо точно определить возможности нарушителя, которые он может использовать для разработки и проведения атак. Модель нарушителя является важной частью информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывают различные методы классификации нарушителей, меж тем многие специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы [15], так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. Несмотря на то, что многие модели имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось.

Что касается инструментальных решений, то многими иностранными и отечественными компаниями, специализирующимися на мониторинге и анализе сетевого трафика, разработаны и предложены различные программные и программно-аппаратные инструменты [16]. Эти инструменты различаются, прежде всего, по уровню и совершенству используемых математических методов, положенных в основу процедур анализа трафика. В зависимости от этого, они обладают разными возможностями [17], например, анализаторы протоколов или сетевые сниферы, которые позволяют захватывать трафик локальных сетей, представлять его в удобном

для анализа виде, но, собственно, анализ данных оставляют администратору. Или, например, маршрутизаторы, поддерживающие протокол NetFlow [18], собирающие обобщенные данные о трафике глобальных сетей, передавая его для анализа программным системам, которые автоматизируют поиск атак и угроз. Системы обнаружения вторжений специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей [19].

Несмотря на имеющиеся инструментальные решения фильтрации сетевого трафика и мониторинга, любой новый тип атаки (особенно на 80 порт) имеет все шансы «просочиться» через межсетевые экраны и достичь внутренних серверов защищаемой сети. Обнаружить следы атак, которые смогли преодолеть барьер межсетевого экрана, можно путем мониторинга и аудита сетевого трафика.

Компании, специализирующие в области сетевой безопасности, предлагают комплексные инструментальные решения класса SIEM для управления событиями и информацией ИБ с целью выявления инцидентов в режиме реального времени и сетевых сканеров, работающих на эвристическом анализе сетевого трафика.

1. Экспериментальная часть

Вышеупомянутые работы авторов, без сомнения, минимизируют ущерб информационным системам. Остается еще одно направление, которое волнует многих специалистов в области информационной безопасности. Это использование иностранного программного обеспечения с закрытым, либо сложным, либо постоянно обновляющимся программным кодом, отследить изменения, которого невозможно в режиме реального времени [20]. Были проведены исследования, целью которых является изучение принципа функционирования фоновых прикладных программных продуктов на автоматизированных рабочих местах сотрудников организации, в том числе и зарубежного производства, во время обновления программного кода с использованием сети Интернет, а также сетевая активность интернет-браузера, использующего веб-ресурсы, предназначенные для сбора информации о пользователях сети Интернет.

Несмотря на то, что в данной организации выполняются все необходимые организационно-технические требования безопасности информации, и все информационные системы имеют аттестаты соответствия требованиям безопасности конфиденциальной информации, исследование показало ниже представленные результаты.

1.1. Ход эксперимента

В результате проведения ряда аудитов трафика на информационную безопасность выявлена особенность сетевой активности, связанная с работой иностранного программного обеспечениями. Так, современные процессоры Intel на АРМах пользователей позволяют использовать отладочный интерфейс через доступный на многих платформах порт USB 3.0 для получения полного контроля над системой, что дает возможность проводить атаки, которые не отслеживаются современными системами безопасности. Также, веб-ресурсы, использующие для работы программные продукты иностранного производства, являются самым популярным объектом для современных кибератак. Также, были зафиксированы скачковые увеличения исходящего интернет-трафика от пользовательских компьютеров. Такие скачки происходили во время политических мероприятий (например, в период выборов, общественно-значимых мероприятий). В результате исследования сетевого трафика, было выявлено, что ряд прикладных программных продуктов, в том числе и зарубежного производства (Adobe Reader, Cleaner), используя технические протоколы и порты (порты для обновлений, порт 80, 445), выгружают

внушительный объем преобразованной информации на различные зарубежные сайты и сервисы. Причем, выгрузка идет не с каждого компьютера одновременно, а используется некий последовательный алгоритм, который не вызывает подозрения у межсетевых экранов, администраторов сети и пользователей: например, в ночное время, когда пользователь находится не на рабочем месте или во время обеденного перерыва (см. рис. 1).

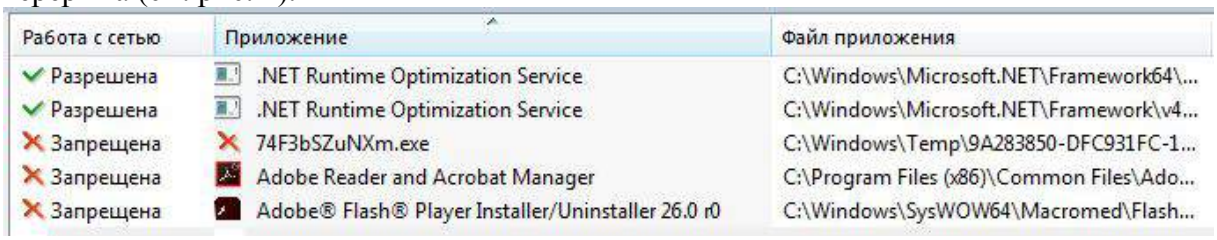


Рис. 1. Работа с сетью приложения была настроена на «запрещена» с помощью средства контроля активности приложений
(Fig. 1. Working with the application network was configured to "disabled" using the application activity monitoring tool)

Программное обеспечение предназначено для работы с офисными файлами, для чтения файлов в формате .pdf. Возникает вопрос, что может так долго и постоянно обновляться в программном продукте? (см. рис. 2).

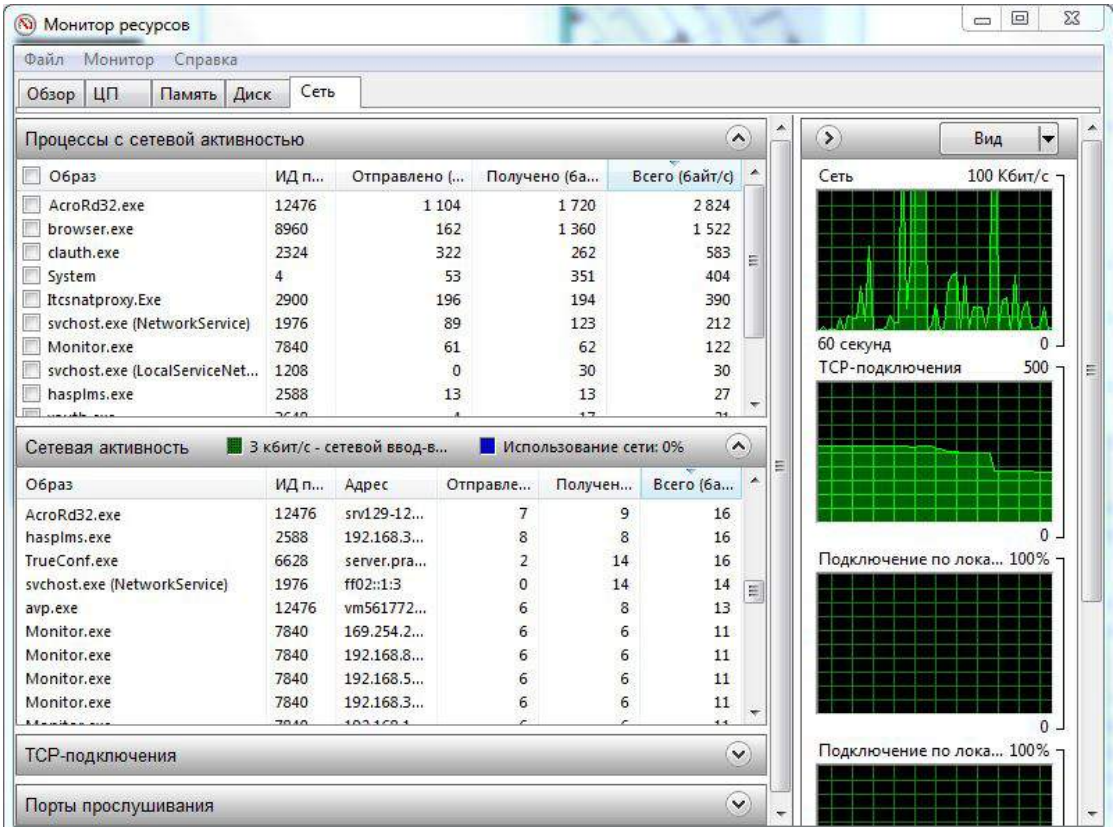


Рис. 2. Сетевая активность программного продукта AcroRd32.exe в режиме онлайн
(Fig. 2. Network activity software product AcroRd32.exe online)

Работающих в фоновом режиме программных продуктов очень много, только опытному пользователю видно, чем именно занимаются программные службы. Но не у всех пользователей данной организации наблюдаются аномалии сетевого трафика. В основном, жалобы на медленную работу компьютеров поступали от сотрудников, занимающих руководящие должности. Возникает дополнительный вопрос: каким

образом ПО распознает занимаемую должность пользователя? Ответ на этот вопрос будет подробно рассмотрен в дальнейших публикациях. На сегодняшний момент существует ряд гипотез, которые требуют экспериментальной проверки. Одной из самых вероятностных гипотез является способность распознавания должности пользователя по низкочастотным поисковым запросам в облачных поисковых системах, которые делают пользователи, занимающие руководящие посты в организации, в том числе специалисты в области информационной безопасности.

Также существует угроза того, что ПО «распознает» пользователя по анализу информации с контроллера домена сети организации, так как в доменной сети каждый сотрудник имеет свою учетную запись и определенное место (приоритет) в структуре сети. Системный администратор вносит данные сотрудника в контроллер домена, вплоть с указанием должностей и, таким образом, происходит учет и идентификация каждого пользователя, в том числе их сетевая активность в сети Интернет.

Для подтверждения гипотезы о возможности распознавания пользователя по учетной записи и временным отклонениям от нормы в работе проведен следующий эксперимент:

1) Зарегистрирован новый ПК в сети организации и создана локальная учетная запись – user-1;
2) Установлен весь необходимый офисный набор ПО для работы;
3) Результаты мониторинга сетевой активности «user-1» в течении первого месяца не показали каких-либо отклонений от нормы в дневное и ночное время работы. Сетевая активность была не выше средней активности каждого пользователя (см. рис. 3).

Рис. 3. Сетевая активность пользователя "user-1», в рабочее время
(Fig. 3. Network activity of user "user-1", during working hours)

4) Были внесены изменения в учетную запись «user-1» (была дописана высокая должность) в контроллере домена, работающего на базе Windows 2012 Server.

Результаты ночной сетевой активности данного пользователя значительно изменились (см. рис. 4).

Сетевой трафик в дневное (рабочее) время практически не меняется, но сильно меняются характеристики сетевого трафика в ночное время. Всего за одну ночь с 00:00 до 06:00 был зафиксирован 71 запрос на различные российские и зарубежные интернет-сервисы. При этом на компьютере были запущены: антивирусное программное обеспечение, офисные приложения и интернет-браузер Mozilla Firefox 12. На рисунке 4 показаны результаты запросов, которые исходят от зарубежных интернет-сервисов. Данные были получены из функционирующей в организации системы учета сетевого трафика сети Интернет на служебных автоматизированных рабочих местах. Выявление географии источников IP адресов осуществлялось в ручном режиме, с помощью интернет-сервиса http://2ip.ru/. В этом случае следует отметить, что разница входящего и исходящего трафика сильно отличается. Например, из рисунка 4 видно, что на первой

и второй строке находятся страны Европы (компания Akamai Technologies вх.-529 Мбит/с., исх.-538 Мбит/с и США вх.-1,79 Кбит/с и исх.-616 Мбит/с.).

Эта разница между входящим и исходящим трафиком ставит вопрос о том, какая именно информация (персональная, конфиденциальная, служебная) скачивается с ПК. И почему именно в ночное время.

При этом, несмотря на имеющиеся в организации многочисленные элементы систем защиты информации, не одна из них не подняла тревогу, т.к. это является открытым http трафиком, передающимся по 80-ту порту.

			Источник	Пользователь-1					
			Часы	00:00-06:00					
Страна	**Город**	**Компания**	**Ip-адрес или домен**	**Первое обращение**	**Количество соединений**	**% от макс. вх.**	**% от макс. исх.**	**Входящий трафик**	**Исходящий трафик**
	Европа	Akamai Technologies	2.20.255.64	25.08.2017 03:11	4			529	538
США	Маунтин-Вью	Google Inc. Ih-in-f139.1e100.r	64.233.161.139	25.08.2017 05:23	6			1.79 K	616
Норвегия	Осло	Opera Software AS	82.145.215.85	25.08.2017 00:38	8			7.24 K	3.47 K
США	Маунтин-Вью		173.194.32.134	25.08.2017 05:23	9			7.84 K	3.42 K
США	Маунтин-Вью		173.194.32.160	25.08.2017 00:23	3			6.68 K	3.11 K
Германия	okis.ru	Hetzner Online AG	188.40.66.5	25.08.2017 00:14	356	100%	3%	14.50 M	507.87 K
США	Маунтин-Вью		gvt1.com	25.08.2017 05:23	2			5.68 K	1.02 K
США	Маунтин-Вью		r6---sn-gvnuxaxjvh-v8cz.gvt1.cor	25.08.2017 05:23	1			4.14 K	685
США	Маунтин-Вью		redirector.gvt1.com	25.08.2017 05:23	1			1.54 K	364
Нидерланды		LeaseWeb Netherlands B.V	dnl-00.geo.kaspersky.com	25.08.2017 00:03	77	1%		190.33 K	17.18 K
Франция	Бонди	Customer LAN Network	dnl-01.geo.kaspersky.com	25.08.2017 02:05	17			20.59 K	3.67 K
Нидерланды		LeaseWeb Netherlands B.V	dnl-04.geo.kaspersky.com	25.08.2017 05:16	4			7.08 K	864
Нидерланды		LeaseWeb Netherlands B.V	dnl-05.geo.kaspersky.com	25.08.2017 04:56	2			3.54 K	432
Франция	Бонди	Customer LAN Network	dnl-06.geo.kaspersky.com	25.08.2017 03:36	8			12.39 K	1.67 K
Европа		Kaspersky Lab TLD	dnl-07.geo.kaspersky.com	25.08.2017 00:04	6			8.75 K	1.25 K
Британия		BBLZ9143	dnl-08.geo.kaspersky.com	25.08.2017 03:36	4			5.27 K	848
Британия		BBLZ9143	dnl-09.geo.kaspersky.com	25.08.2017 01:36	77			108.89 K	17.18 K
Европа		Kaspersky Lab TLD	dnl-10.geo.kaspersky.com	25.08.2017 01:36	14			21.15 K	2.92 K
Франция	Бонди	Customer LAN Network	dnl-14.geo.kaspersky.com	25.08.2017 04:06	4			6.18 K	856
Европа		Kaspersky Lab TLD	dnl-19.geo.kaspersky.com	25.08.2017 04:16	4			6.18 K	856
Германия	okis.ru	Hetzner Online AG	okis.ru	25.08.2017 00:14	557	93%	1%	13.58 M	238.71 K
Германия	okis.ru	Hetzner Online AG	surguul.okis.ru	25.08.2017 00:14	557	93%	1%	13.58 M	238.71 K
			windowsupdate.com	25.08.2017 03:11	1			317	286
			ctldl.windowsupdate.com	25.08.2017 03:11	1			317	286
Всего					**10569**			**43.11 M**	**5.92 M**

Рис. 4. Результаты ночной сетевой активности пользователя «user-1»
(Запросы отфильтрованы по иностранным сервисам)
(Fig. 4. Results of night network activity of the user-1
(Requests are filtered by foreign services))

Выводы

Проведенный эксперимент показал, что существует угроза утечки информации по техническим каналам. Утечка связана с распознаванием программными средствами общего назначения должностного положения пользователя на серверах под управлением Windows.

Таким образом, при использовании иностранного программного обеспечения со сложным, либо постоянно обновляющимся кодом существует вероятность полной информационной открытости рабочих мест сотрудников организации, в том числе угрозы массовой утечки служебной и конфиденциальной информации с ее первичной дифференциацией по должностному уровню пользователей ПК в организации.

Работа по выявлению негативных факторов информационной безопасности будет продолжена с акцентом на два направления:

1. Выявление факторов, провоцирующих ПО общего назначения на активное скачивание информации с ПК пользователя: изменения учетной записи, анализ отклонений от нормы во время работы ПК, действий пользователей с информацией на ПК, а также действий пользователей в облачных поисковых системах.
2. Расшифровка передаваемой с ПК исходящей информации.

В дальнейших исследованиях планируется постановка экспериментов и анализ полученной информации по указанным направлениям.

СПИСОК ЛИТЕРАТУРЫ:

1. Вестник Саратовской государственной юридической академии № 2 (115) – 2017 [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/v/setevye-informatsionnye-voyny-kak-faktor-ugrozy-globalnoy-bezopasnosti.
2. А.В. Царегородцев, М.М. Тараскин «Методы и средства защиты информации в государственном управлении. Учебное пособие. – Издательство «Проспект», 2017 – 193 с.
3. Шейн Харрис, «Кибервойна. Пятый театр военных действий» - Альпина нон-фикшн, 2015. – 392 с.
4. Лохин С.В., Семашко А.В., Егорова А.И. Система мониторинга сетевой активности персонала на основе прокси-сервера. Динамика сложных систем – XXI век. 2017. Том 11, №2. С. 25-29.
5. Лохин С.В., Семашко А.В. Мониторинг сетевой активности персонала в целях обеспечения информационной безопасности предприятия. Вопросы защиты информации. 2017., №2 (117). С. 53-57.
6. Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003.
7. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов. Доклады Томского государственного университета систем управления и радиоэлектроники. 2011 г., Т. 2. № 3. С. 236-248.
8. Garin E.V., Meshcheryakov R.V. METHOD FOR DETERMINATION OF THE SOCIAL GRAPH ORIENTATION BY THE ANALYSIS OF THE VERTICES VALENCE IN THE CONNECTIVITY COMPONENT. Вестник Южно-Уральского государственного университета. Серия: Математика. Механика. Физика. 2017. Т. 9. № 4. С. 5-12.
9. Зайцев А.С., Малюк А.А. Разработка классификации внутренних угроз информационной безопасности посредством кластеризации инцидентов. Безопасность информационных технологий. 2016., № 3. С. 20-33.
10. Cichonski P., Millar T., Grance T., Scarfone K. «NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide» August 2012.
11. Абросимов М.Б., Камил И.А., Разработка системы предотвращения вторжений с использованием параллельного программирования и системы отказоустойчивости. Безопасность информационных технологий. 2018., № 1 (25) С. 65-73.
12. Ходашинский И.А., Мещеряков Р.В., Горбунов И.В. Методы нечеткого извлечения знаний в задачах обнаружения вторжений. Вопросы защиты информации. 2012 г., № 1. С. 45-50.
13. Милославская Н.Г., Центры управления информационной безопасностью. Безопасность информационных технологий. 2016., № 4. С. 38-51.
14. Егошин Н.С., Конев А.А., Шелупанов А.А. Формирование модели нарушителя. Безопасность информационных технологий. 2017., № 4 (78) С. 19-26.
15. Мещеряков Р.В., Шелупанов А.А. Концептуальные вопросы информационной безопасности региона и подготовки кадров. Труды СПИИРАН. 2014. № 3 (34). С. 136-159.
16. Jean Y. Astier, Igor Y. Zhukov, Oleg N. Murashov, Alexey P. Bardin, A new OS architecture for IOT. Безопасность информационных технологий. 2018., № 1 (25) С. 19-33.
17. С.А. Бабин «Лаборатория хакера» - СПб.: БХВ-Петербург, 2016. – 240 с.: - ил. (Глазами хакера).
18. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – Спб.: Питер, 2016. – 992 с.: ил. – (Серия «Учебник для вузов).
19. Н. Скабцов «Аудит безопасности информационных систем» - СПб.: Питер, 2018. – 272 с.: ил. – (Серия «Библиотека программиста»).
20. Ерохин С.С., Мещеряков Р.В., Бондарчук С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта. Безопасность информационных технологий. 2007 г., № 4. С. 39-46.

REFERENCES:

[1] Bulletin of the Saratov state law Academy No. 2 (115) – 2017 [Electronic resource] access Mode: https://cyberleninka.ru/article/v/setevye-informatsionnye-voyny-kak-faktor-ugrozy-globalnoy-bezopasnosti. (in Russian).
[2] A. V. Tsaregorodtsev, M. M. Taraskin " Methods and means of information protection in public administration. Textbook. - Prospekt publishing house, 2017 - 193 p. (in Russian).
[3] Shane Harris, "The Cyberwar. The fifth theater of war " - Alpina non-fiction, 2015. - 392 sec. (in Russian).

[4] Lokhin, S. V., Semashko, A. V., Egorova A. I. System monitoring the network activity of the staff through a proxy server. Dynamics of complex systems – twenty-first century. 2017. Volume 11, No. 2. P. 25-29. (in Russian).
[5] Lokhin S. V., Semashko A.V. monitoring of network activity of the personnel for the purpose of ensuring information security of the enterprise. Information security issues. 2017., №2 (117). P. 53-57. (in Russian).
[6] Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003.
[7] Hodinski I. A., Savchuk M. V., Gorbunov I. V., Meshcheryakov R. V. Technology enhanced user authentication information processes. Reports of Tomsk state University of control systems and Radioelectronics. 2011, Vol.2. No. 3. P. 236-248. (in Russian).
[8] Garin E. V., Meshcheryakov R. V. METHOD FOR DETERMINATION OF THE SOCIAL GRAPH ORIENTATION BY THE ANALYSIS OF THE VALENCE VERTICES IN THE CONNECTIVITY COMPONENT. Bulletin of South Ural state University. Series: Mathematics. Mechanics. Physics. 2017. T. 9. No. 4. P. 5-12.
[9] Zaitsev, A. S.; Malyuk, A. A.. Development of information security insider threat classification using incident clustering. IT Security (Russia), [S.l.], v. 23, n. 3, p. 20-29, oct. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/14>. Date accessed: 30 may 2018. (in Russian).
[10] Cichonski, P., Millar, T., Grance, T., Scarfone K. "NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide," August 2012.
[11] Abrosimov, Mikhail B.; Kamil, Iehab A.. Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology. IT Security (Russia), [S.l.], v. 25, n. 1, p. 65-73, mar. 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06. (in Russian).
[12] Miloslavskaya, N. G. Information Security Operations Centers. IT Security (Russia), [S.l.], v. 23, n. 4, p. 38-51, dec. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/257>. Date accessed: 30 may 2018.(in Russian).
[13] Egoshin, Nikolay S; Konev, Anton A; Shelupanov, Aleksander A. Building a model of infringer. IT Security (Russia), [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/273>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2017.4.02.(in Russian).
[14] Mescheryakov R. V., Shelupanov A. A. Conceptual issues of information security in the region and training. Proceedings of SPIIRAS. 2014. No. 3 (34). P. 136-159.
[15] Astier, Jean Y. et al. A NEW OS ARCHITECTURE FOR IOT. IT Security (Russia), [S.l.], v. 25, n. 1, p. 19-33, mar. 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1090>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.02.
[16] S. A. Babin "hacker's Laboratory" - St. Petersburg.: BHV-Petersburg, 2016. - 240 p.: - ill. (Through the eyes of a hacker). (in Russian).
[17] Oliver W., Oliver N. Computer networks. Principles, technologies, protocols: Textbook for universities. 5th ed. – SPb.: Peter, 2016. - 992 p.: ill. (Series "Textbook for higher educational institutions). (in Russian).
[18] N. Skobtsov "Audit of information systems security" - SPb.: Peter, 2018. - 272 p.: ill. (Series "library of the programmer»). (in Russian).
[19] Erokhin S. S., Meshcheryakov R. V., Bondarchuk S. S. Models and methods for assessing information security and information security of the object. 2007, № 4. P. 39-46. (in Russian).

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.

Александр В. Мамаев[1], Кристина В. Мамаева[2]
[1]ООО «Лаборатория Цифровой Форензики»,
115191, Москва, Духовской переулок, дом 17, пом I ком 2а
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]Национальный Исследовательский Университет «Высшая Школа Экономики»,
101000, г. Москва, ул. Мясницкая, д. 20
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

КАК ЭКОСИСТЕМА ВИРТУАЛЬНЫХ АССИСТЕНТОВ МОЖЕТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2018.2.07

Аннотация. Количество преступлений, совершаемых в информационной сфере, постоянно возрастает. Одновременно возрастает совокупный ущерб, наносимый деятельностью киберпреступников: с 1,5 трлн долл. в 2015 году до 2 трлн. долл. к 2019 году. На этом фоне законодательство Европейского Сообщества в области защиты персональных данных, сформированное еще в 1990-е годы, ждут самые кардинальные изменения, что наверняка повлияет на позиции других стран. Персональные данные интернет-пользователей давно превратилось в объект купли-продажи на рынке электронной коммерции. Манипуляции с персональными данными вызывают серьезные возражения со стороны самих пользователей. Власти озабочены сохранностью и конфиденциальностью данных в соответствии с законодательством. Несмотря на это, количество инцидентов, связанных с утечкой или некорректным использованием персональных данных, возрастает по экспоненте: в декабре 2017 года юристы Hill Dickinson подали коллективный иск к Google, недовольные незаконным сбором персональных данных владельцев iPhone. Следом под удар попала компания Uber Technologies, несанкционированно рассылавшая SMS-оповещения клиентам. В марте 2018 года оправдываться за утечку данных 80 млн аккаунтов пришлось соцсети Facebook. Авторы статьи рассмотрели возможности внедрения экосистемы виртуальных ассистентов и технологии блокчейна для безопасной и деперсонализированной обработки персональных данных с последующим использованием, что открывает неожиданные перспективы перед machine-to-machine-marketing.

Ключевые слова: виртуальный ассистент, блокчейн, персональные данные, электронная коммерция.

Для цитирования. МАМАЕВ, Александр В.; МАМАЕВА, Кристина В.. КАК ЭКОСИСТЕМА ВИРТУАЛЬНЫХ АССИСТЕНТОВ МОЖЕТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], n. 2, p. 80-85, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1112>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.07.

Alexandr V. Mamaev[1], Kristina V. Mamaeva[2]
[1]CEO at 'Digital Forensics Laboratory LLC',
Dukhovskoy per., 17, bld. I, fl. 2A. 115191, Moscow,Russia
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]National Research University Higher School of Economics,
Myasnitskaya str., 20, 101000, Moscow, Russia
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

How the ecosystem of digital assistants can ensure the security of personal data

DOI: http://dx.doi.org/10.26583/bit.2018.2.07

Abstract. Number of cybercrimes is constantly rising both in Europe, and around the world. The costs incurred from such malicious activities are rising correspondingly. According to the data collected by Jupiter Research these costs increased from $1.5 trillion in 2015 to $2 trillion in 2019.

That is why European Union is expected to introduce major changes to the Personal Data Protection Acts which stayed mostly unchanged since the 1990s. The consequences of those changes will be felt in countries beyond the European Union. The personal data of internet users have long become a commodity on the e-commerce market. Yet the manipulations with the personal data cause concerns among both the users, who do not fully realize how and to what purposes their data are used, and governments, who try to protect the confidentiality remains by the law. Despite that the number of incidents with data leaks continues to rise exponentially. In December 2017 the lawyers from Hill Dickinson, a UK commercial law firm, filed a lawsuit against Google regarding unlawful collection of the iPhone users' data. Another company that is about to have problems with law is Uber Technologiesm, which sent SMS messages to its clients without obtaining formal permissions for that. Finally, in March 2018 it was Facebook which had to explain the way the personal data on more than 80 million users have leaked and ended up in the hands of a third party. The authors of this article assessed the possibilities for introducing the ecosystem of virtual assistants and blockchain technology for safe and depersonalized data processing as well as its further use. This system opens broad unexpected opportunities for the machine-to-machine-marketing.

Keywords: virtual assistants, blockchain, personal data, e-commerce.

For citation. MAMAEV, Alexandr V.; MAMAEVA, Kristina V.. How the ecosystem of digital assistants can ensure the security of personal data. IT Security (Russia), [S.l.], n. 2, p. 81-86, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1112>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.07.

На сегодняшний день одной из самых заметных и актуальных проблем является глобальный рост киберпреступности. Согласно данным Juniper Research, совокупный ущерб, наносимый деятельностью киберпреступников, вырастет с 1,5 трлн долл. в 2015 году до 2 триллиона долларов к 2019 году.

Малый и средний бизнес оказался более уязвим для киберпреступников в сравнении с крупными корпорациями. Более 50% предприятий с количеством сотрудников от 100 до 1 тыс. человек подвергались атакам киберпреступников, средний ущерб составил 879,582 долларов США [1].

Рядовые интернет-пользователи не уделяют должного внимания собственной информационной безопасности. Согласно исследованию Symantec, 87% пользователей интернета в США подключались к публичному Wi-Fi без применения дополнительных средств защиты. При этом более 60% респондентов полагали, что их данным ничего не угрожает [2].

Последние пять лет запомнились колоссальным количеством случаев утечек персональных данных, породив серьезные запросы на обеспечение информационной безопасности и вопросы – к руководству компаний, допустивших подобные инциденты. В частности, к самой популярной в мире социальной сети Facebook, которая столкнулась с обвинениями в утечке данных 80 млн пользователей, что серьезно ударило по капитализации компании и пошатнуло позиции топ-менеджмента [3].

Под влиянием общественности и американских властей, инициировавших проверку, корпорация приняла решение изменить систему управления персональных данных и ограничить объем сведений, предоставляемых компаниям сродни Cambridge Analytica, ставшей виновницей разразившегося скандала. Facebook также планирует запретить предоставлять сторонним поставщикам анонимизированные данные пользователей, которые позволяют оценить успешность проводимых рекламных кампаний [4]. Наконец, компания проверит все приложения «с подозрительной активностью» и запретит продолжать деятельность разработчикам, которые откажутся от проведения такой проверки. Все это приведет к тому, что сторонние компании потеряют возможность создавать таргетированную рекламу.

Однако есть куда более простое решение, позволяющее поставить точку в вопросе: устранить личный фактор, передав рекламные кампании в ведение виртуальных

помощников и персональных ассистентов, знающих потребности и запросы своих владельцев. В конечном счете, в основе бизнеса социальных сетей лежит задача электронной коммерции – маркетинг. В интернет-маркетинге ключевая ценность заключается в том, чтобы найти максимальное соответствие между потребностями потенциального покупателя и предлагаемым рекламным контентом. Именно это определяет успешность работы рекламы [5-6].

В настоящее время, маркетинг – это процесс многослойный: сначала специалист формирует требования к портрету покупателя, потом настраивает базовые параметры рекламных кампаний, после чего, в работу вступает информационно-аналитическая машина, которая к этому моменту уже обладает своей базой потенциальных покупателей или может обрабатывать данные из сторонних баз. Итак, такая информационная система будет работать по строгим критериям специалиста, заложенным в рекламной кампании. При этом процесс необходимо постоянно контролировать, вносить регулярные правки и уточнения. Если речь идет о необходимости привлечения большого объема трафика, то процесс будет усложняться, будут применяться дополнительные техники и подходы, например, programmatic.

Как видно, задача «достучаться» до своего покупателя уже сейчас является весьма сложно и трудоемкой. Развитие электронной коммерции, появление новых требований к инструментам, все это только усложнит работу маркетологов. Внедрение machine-to-machine-marketing позволяет выйти из этой ситуации, а также нивелировать угрозы личного фактора.

Данное направление – это результат естественного развития информационного общества и современных технологий. Развитие Интернета вещей приведет к тому, что вокруг человека почти все будет в виде «умного устройства», способного собирать поведенческую информацию о своем пользователе [7]. Другими словами, в скором времени, поведение человека, его привычки, потребности, особенности, ровным счетом абсолютно все будет подвергаться «протоколированию» «умными устройствами» и анализироваться специальными системами [8].

Таким образом, неминуемо пересечение взаимных возможностей интернет-маркетинга и интернета вещей, которое перерастет в новый вид M2M маркетинга, когда участие человека в процессе выбора будет минимально. Виртуальные частные ассистенты начнут самостоятельно принимать решения о выборе того или иного предложения на основании полного портрета своего владельца. Виртуальный ассистент (ВА) - это разговорный, генерируемый компьютером персонаж, который имитирует разговор для предоставления голосовой или текстовой информации пользователю через веб-сайт, киоск или мобильный интерфейс. Виртуальный ассистент может получать команды с помощью ввода текста, голоса или загрузки файла, например, изображения. ВА производят обработку естественного языка, чтобы исполнить команду и выдать ответ [9].

Для реализации в виртуальном ассистенте полноценной системы электронной коммерции необходимо выполнение нескольких условий. Во-первых, должно быть реализовано и поддерживаться сетевое взаимодействие, чтобы обеспечить режим двустороннего взаимодействия. Во-вторых, требуется поддержка технологии блокчейн для того, чтобы процесс взаимодействий был максимально прозрачным и надежным от попыток мошенничества. Рассмотрим по порядку данные требования.

Сетевое взаимодействие. Если не брать в расчет вопросы бизнеса, связанные с постепенным ростом аудитории активных пользователей, то в конечном счете получится новая экосистема виртуальных ассистентов. Это позволит избавить пользователей от большого числа мелких, незначительных действий во взаимодействии с другими людьми. M2M маркетинг - параллельный виртуальный мир, в котором ассистенты выполняют поручения своих владельцев: совершают покупки, обмениваются товарами, услугами, информацией, обеспечивают для своих владельцев непревзойденную доступность возможностей [10].

Система распределенного хранения данных – блокчейн. Одним из важнейших элементов во взаимодействии пользователей в виртуальном мире является вопрос доверия. Если на базе этого реализовывать еще и вопрос торгово-денежных отношений, то задача становится еще важнее. Для решения данной проблемы необходимо использовать такой инструмент, который позволит каждому участнику доверять друг другу при совершении операции [11]. На текущий момент предлагается использовать технологию блокчейна, особый вид хранения данных, при котором каждый новый блок криптографически связан с предыдущем. Для упрощения процессов взаиморасчета будет использована криптовалюта данного виртуального ассистента. Криптовалюта — разновидность цифровой валюты, в основе которой лежит технология блокчейн, а создание и контроль базируются на криптографических методах.

Таким образом, все операции будут реализованы через смарт-контракты, специальный алгоритм, позволяющий в автоматизированном режиме заключать и поддерживать выполнение коммерческих договоров в соответствии с заданными условиями. При этом, каждый участник может лично удостоверится в условиях, алгоритме каждого смарт-контракта и быть уверенным в неизменности и необратимости его действия. Именно это дает уверенность участникам процесса в то, что каждая сторона корректно исполнит свои обязательства.

Рассмотрим теперь, как будет применяться технология виртуального ассистента, изменяя привычную работу социальной сети. Сам механизм становится схожим с работой CPA-сетей, в которых рекламодатели ищут исполнителей в свои программы привлечения клиентского трафика. Однако, в предлагаемой схеме, будет только один вид программы – это продать товар или услугу. Исполнителем, в отличии от CPA-сетей, будет не произвольный «вебмастер», а сама сеть виртуальных ассистентов.

Пример работы ассистентов может выглядеть следующим образом: высокоперсонализированная сеть рекламодателя (например, производитель смартфонов) обращается к площадке (Facebook) с просьбой помочь в продаже 1 млн устройств по заданным параметрам (уровень дохода, предпочтения к марке, сроки оплаты, вплоть до любимого цвета). Соцсеть, не предоставляя заказчику доступа к базе данных, берется за заказ, отправляя таргетированные объявления персональным ассистентам интернет-пользователей.

Для гарантии безопасности и прозрачности всех операций процедура размещения товаров, как и оплата, проходит по технологии блокчейн, фиксирующей все шаги операции и верификации. Таким образом, продавец сможет контролировать путь товара и свою прибыль, посредник (Facebook) снимает с себя все риски перед рекламодателем, а пользователь, подписывая соглашение, дает разрешение на участие в этой схеме. Алгоритм работы предлагаемого механизма представлен на рисунке 1.

Как видно из алгоритма работы, персональные данные пользователей не покидают систему виртуального ассистента. Только в случае приобретения, пользователь сам укажет тот объем информации, минимально необходимый для получения купленного товара или услуги. Эта информация будет передана исполнителю.

Рассмотрим пример того, как виртуальный ассистент будет работать в интересах электронной коммерции, без ущерба для персональных данных пользователя. Описание: пользователь хочет купить обувь. Им уже был проведен предварительный поиск в интернете для определения желаемых параметров. Но покупка не совершена, так как хочется осуществить примерку. Задача: помочь совершить покупку.

На рисунке 2 представлена диаграмма последовательности действий, описывающая процесс решения возникшей задачи.

Как видно из алгоритма работы, персональные данные пользователей не покидают систему виртуального ассистента. Только в случае приобретения, пользователь сам укажет тот объем информации, минимально необходимый для получения купленного товара или услуги. Эта информация будет передана исполнителю.

Рассмотрим пример того, как виртуальный ассистент будет работать в интересах электронной коммерции, без ущерба для персональных данных пользователя. Описание: пользователь хочет купить обувь. Им уже был проведен предварительный поиск в интернете для определения желаемых параметров. Но покупка не совершена, так как хочется осуществить примерку. Задача: помочь совершить покупку.

На рисунке 2 представлена диаграмма последовательности действий, описывающая процесс решения возникшей задачи.

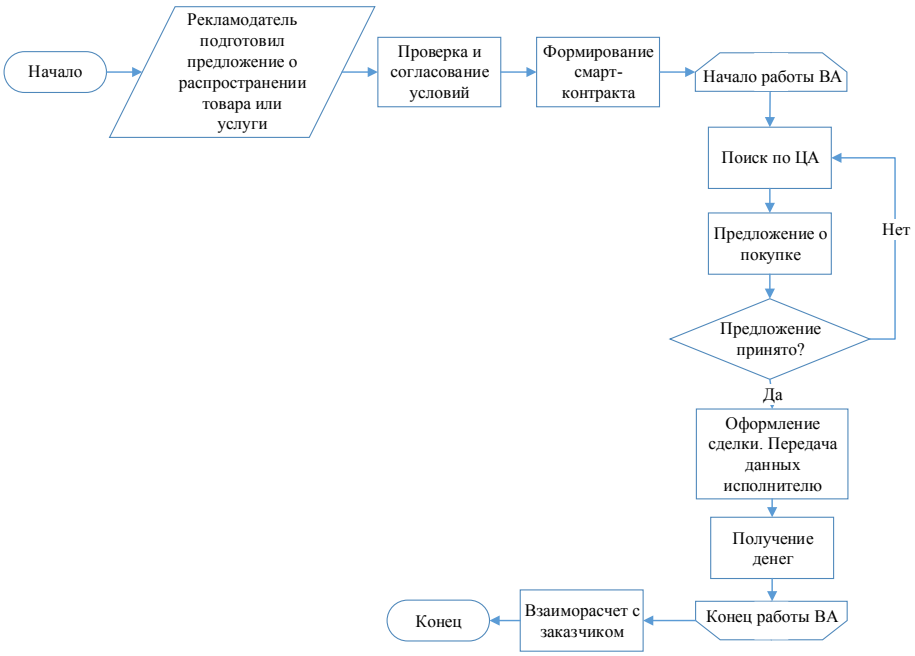


Рис. 1. Алгоритм продажи товаров и услуг через виртуальных ассистентов
(Fig.1. Algorithm for the sale of goods and services through virtual assistants)

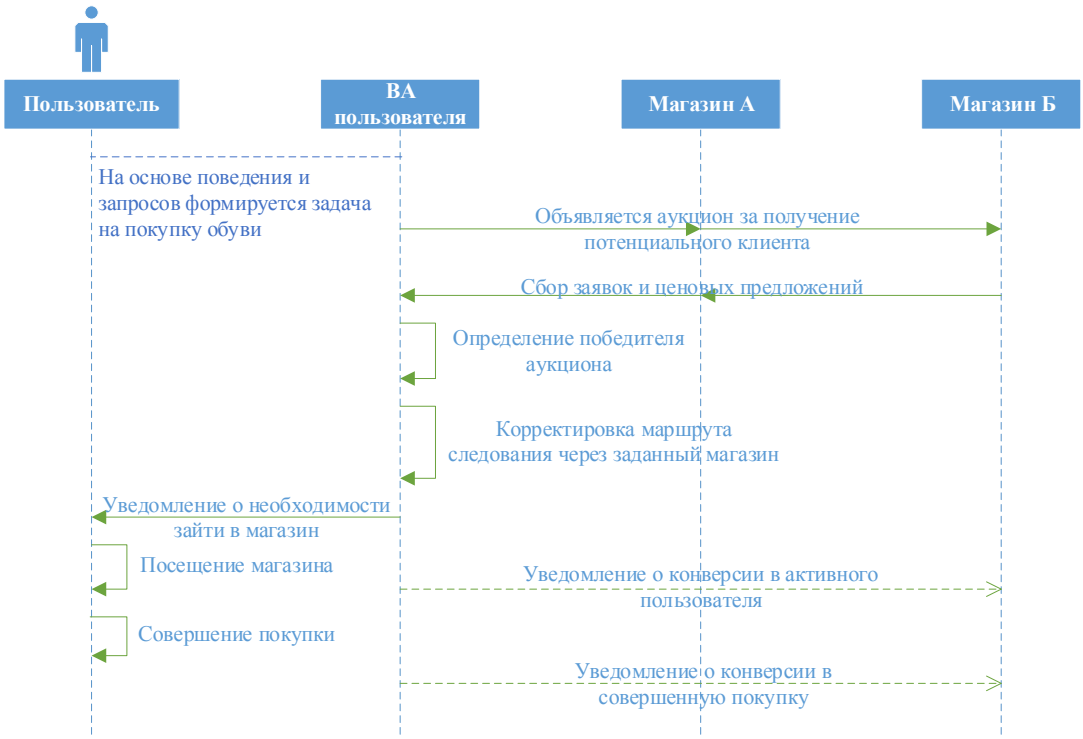


Рис. 2. Диаграмма последовательности действия для рассматриваемого примера
(Fig. 2. Sequence diagram for the example in question)

СПИСОК ЛИТЕРАТУРЫ:

1. The Global Risks Report 2016 [Электронный ресурс] – URL: https://www.weforum.org/reports/the-global-risks-report-2016/.
2. L. Ponemon 2016 Ponemon Institute Cost of a Data Breach Study [Электронный ресурс] – URL: https://securityintelligence.com/media/2016-cost-data-breach-study/.
3. Zuckerberg launches Facebook's Washington defense [Электронный ресурс] – URL: http://www.reuters.tv/v/jqB/2018/04/09/zuckerberg-to-meet-with-lawmakers-ahead- of-hearing.
4. K. Chaykowski Facebook Curbs Information Shared With Data Brokers, Launches New User Privacy Tools [Электронный ресурс] – URL: https://www.forbes.com/sites/kathleenchaykowski/2018/03/29/facebook-to-curb-information- shared-with-data-brokers/#6be4a62fac1a.
5. М.Ю. Наумов, А.С. Чистяков Применение систем искусственного интеллекта в различных сферах деятельности. Постулат. 2017 №5.
6. Glukhov, V.V. Improving the efficiency of architectural solutions based on cloud services integration. V.V. Glukhov, I.V. Ilin, O.J. Iliashenko. Lecture Notes in Computer Science. -2016. -T. 9870. -pp. 512-524.
7. Росляков, А.В. Интернет вещей: учебное пособие [текст]. А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.
8. McKinsey Global Institute, Digital Globalization: the new era of global flows. Executive Summary, March 2016 .
9. Rob High «Эпоха когнитивных систем: Принцип построения и работы IBM Watson» [Электронный ресурс] – URL: http://www.interface.ru/iarticle/files/36855_77829297.pdf.
10. Unraveling the Hype: AI Marketing Readiness in Retail & E-Commerce [Электронный ресурс] – URL: https://engage.emarsys.com/en/study/ai-readiness (Дата обращения: 15.03.2018).
11. Коршунов Антон Анализ социальных сетей: методы и приложения. Труды ИСП РАН. 2014. №1. [Электронный ресурс] – URL: http://cyberleninka.ru/article/n/analiz-sotsialnyh-setey-metody-i-prilozheniya.

REFERENCES:

[1] The Global Risks Report 2016 [Electronic resource] – URL: https://www.weforum.org/reports/the-global-risks-report-2016/.
[2] L. Ponemon 2016 Ponemon Institute Cost of a Data Breach Study [Electronic resource] – URL: https://securityintelligence.com/media/2016-cost-data-breach-study/.
[3] Zuckerberg launches Facebook's Washington defense [Electronic resource] – URL: http://www.reuters.tv/v/jqB/2018/04/09/zuckerberg-to-meet-with-lawmakers-ahead- of-hearing.
[4] K. Chaykowski Facebook Curbs Information Shared With Data Brokers, Launches New User Privacy Tools [Electronic resource] – URL: https://www.forbes.com/sites/kathleenchaykowski/2018/03/29/facebook-to- curb-information- shared-with-data-brokers/#6be4a62fac1a.
[5] M.Ju. Naumov, A.S. Chistjakov.The use of artificial intelligence systems in various fields. Postulate. 2017 No. 5. (in Russian).
[6] Glukhov, V.V. Improving the efficiency of architectural solutions based on cloud services integration. V.V. Glukhov, I.V. Ilin, O.J. Iliashenko. Lecture Notes in Computer Science. -2016. -T. 9870. -pp. 512-524.
[7] Rosljakov, A.V. The Internet of things: a training manual [text]. A.V. Rosljakov, S.V. Vanjashin, A.Ju. Grebeshkov. – Samara: PGUTI, 2015. – 200 p. (in Russian).
[8] McKinsey Global Institute, Digital Globalization: the new era of global flows. Executive Summary, March 2016.
[9] Rob High «"The era of cognitive systems: the principle of construction and operation of IBM Watson»» [Electronic resource] – URL: http://www.interface.ru/iarticle/files/36855_77829297.pdf . (in Russian).
[10] Unraveling the Hype: AI Marketing Readiness in Retail & E-Commerce [Electronic resource] – URL: https://engage.emarsys.com/en/study/ai-readiness (Date of access: 15.03.2018)
[11] Korshunov Anton. Social media analysis: methods and applications. The proceedings of ISP RAS. 2014. №1. [Electronic resource] – URL: http://cyberleninka.ru/article/n/analiz-sotsialnyh-setey-metody-i-prilozheniya. (in Russian).

Поступила в редакцию – 28 марта 2018 г. Окончательный вариант –23 апреля 2018 г.
Received – March 28, 2018. The final version – April 23, 2018.

Антон А. Абрамов[1], Виктор С. Горбатов[2], Марина Н. Гришина[3]
[1]ФГУП «Главный научно-исследовательский вычислительный центр» Управления делами Президента Российской Федерации,
г. Москва, 121471, ул. Рябиновая, д. 43, корп. 1
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]ФГБУ НМИЦ имени академика В.И. Кулакова Министерства здравоохранения Российской Федерации,
ул. Академика Опарина, 4, г. Москва, 117198, Россия
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ВЕБ-ПОРТАЛА НА ПЛАТФОРМЕ OPEN JOURNAL SYSTEMS

DOI: http://dx.doi.org/10.26583/bit.2018.2.08

Аннотация. В этой статье рассматриваются основные угрозы безопасности веб-порталам, построенным на платформе Open Journal Systems. Платформа Open Journal Systems (далее OJS), изначально разработанная в рамках проекта Public Knowledge Project, является одной из самых популярных открытых платформ для электронных журналов. На 2016 год исходя из данных, которыми располагает проект Public Knowledge Project, насчитывается более 10 тысяч активных журналов, использующих платформу OJS. Для журнала переход на такую продвинутую и сложную платформу, которая позволяет полностью перенести весь рабочий процесс на единый веб-портал, является серьезным шагом и на него идут рецензируемые журналы, входящий в российские и зарубежные системы цитирования, а потому вопрос сохранности содержимого статей до их публикации очень важен для самого журнала, так и для авторов, которые хотят в журнале публиковаться. В этой работе рассматриваются наиболее актуальные угрозы для веб-порталов на платформе OJS, описана частная модель угроз безопасности, а также предложены меры, которые позволяют нейтрализовать эти угрозы.

Ключевые слова: частная модель угроз, модель нарушителя, веб-портал, угрозы информационной безопасности, меры защиты, php, xss, open journal systems.
Для цитирования. АБРАМОВ, Антон А.; ГОРБАТОВ, Виктор С.; ГРИШИНА, Марина Н.. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ВЕБ-ПОРТАЛА НА ПЛАТФОРМЕ OPEN JOURNAL SYSTEMS. Безопасность информационных технологий, [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1113>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.08.

Anton A. Abramov[1], Victor S. Gorbatov[2], Marina N. Grishina[3]
[1]Federal State Unitary Enterprise "Main Research Computing Center" of the Administrative Department of the President of the Russian Federation,
Moscow, 121471, Rybinovaya 43
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]National Research Nuclear University MEPHI,
Kashirskoe shosse, 31,Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]Federal state budget institution national medical research center named after academician V.I. Kulakova, Ministry of Health of the Russian,
Moscow, 117198, Academica Oparina 4
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

Information security threats in web-portals on the open journal systems platform

DOI: http://dx.doi.org/10.26583/bit.2018.2.08

Abstract. This article addresses the problem of security threats while working with web portals built on the Open Journal Systems platform. The Open Journal Systems (OJS) platform was originally developed as part of the Public Knowledge Project and it is one of the most popular open-source platforms for web journals today. Based on the data available in the Public Knowledge Project, there were more than 10,000 active journals using the open journal systems platform by the end of 2016. A migration of a journal to such advanced and complex platform helps to handle the entire workflow over a single web portal. Therefore it is an important move and only peer-reviewed journals that are part of Russian and Worldwide citation systems go for it. At the same time the problem of keeping privacy for a manuscript before it is published is very important for these journals and for authors who submit it to the journal. The paper describes the most common threats for the web portals on the OJS platform as well as a particular model of the security threats, and suggests the measures that could help to neutralize these threats.

Keywords: particular threat model, intruder model, web portal, information security threats, protection measures, php, xss, open journal systems.

For citation. ABRAMOV, Anton A.; GORBATOV, Victor S.; GRISHINA, Marina N.. Information security threats in web-portals on the open journal systems platform. IT Security (Russia), [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1113>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.08.

Введение

Повышение качества существующих и создание современных методов сбора информации, её хранения, обработки и распространения является существенной составляющей процесса развития информационных систем и информационных технологий. Потребность такого совершенствования связана с непрерывным ростом количества электронных документов и их доступностью, что в свою очередь очень затрудняет управление информацией и саму работу пользователя с ней. Для решения этой проблемы специалистами данной области была предложена идея Веб -порталов. Веб -портал является программной средой, которая обеспечивает унифицированный доступ к контенту, расположенному в информационных источниках. Портал структурирует информацию и предоставляет пользователям средства для её поиска. Веб-порталы обрабатывают и хранят огромное количество информации, которая подвержена различным угрозам. Таким образом, появляется острая необходимость в анализе угроз безопасности информации разнообразных веб-ресурсов и веб-порталов, в частности.

Частным случаем использования веб-порталов являются электронные журналы, публикуемые в сети интернет. Одной из наиболее распространенных платформ является платформа Open Journal Systems (далее OJS), изначально разработанная в рамках проекта Public Knowledge Project [1]. На 2016 год, исходя из данных, которыми располагает проект Public Knowledge Project, насчитывается более 10 тысяч активных журналов, использующих платформу Open Journal Systems [2]. На самом деле есть основания полагать, что реальная цифра на порядок выше, т.к. только для России официально насчитывается около 170 журналов, хотя на одной только электронной платформе Elpub, которая базируется на OJS, насчитывается более 260 журналов. OJS разрабатывается как платформа с открытым исходным кодом и дорабатывается мировым сообществом, в том числе активно в этом процессе участвуют и российские разработчики. Для журнала переход на такую продвинутую и сложную платформу, которая позволяет полностью перенести весь рабочий процесс на единый веб-портал, является серьезным шагом и на него идут рецензируемые журналы, входящие в российские и зарубежные системы цитирования, а потому вопрос

сохранности содержимого статей до их публикации очень важен, как для самого журнала, так и для авторов, которые хотят в журнале публиковаться.

В этой работе рассматриваются наиболее актуальные угрозы для веб-порталов на платформе OJS, а также описаны меры, которые позволяют нейтрализовать эти угрозы. Актуальность угроз определялась исходя из специфики работы электронных изданий со своими авторами, рецензентами и редакционной коллегией.

Современные работы, связанные с исследуемой тематикой

Веб-порталы представляют собой достаточно сложную систему, состоящую из множества компонентов, каждый из которых может содержать в себе уязвимости, которые становятся источниками угроз, по средствам которых, злоумышленник может реализовать атаку на веб-портал и нарушить целостность, доступность и конфиденциальность хранимых и обрабатываемых веб-порталом данных. Веб-портал построенный с использованием платформы OJS не является исключением, поэтому разумно взглянуть на современную ситуацию в области безопасности технологий, лежащих в основе OJS. Это позволяет сформулировать определенные требования и рекомендации к используемым компонентам и их конфигурации.

Ключевыми проблемами для большинства порталов являются уязвимости связанные:

- перехватом и подменой трафика между пользователем и сервером;
- исполнением произвольного кода;
- XSS атаками, «межсайтовый скриптинг»;
- загрузкой произвольных файлов;
- открытым доступ к конфигурационным файлам;
- слабым алгоритмом выявления «ботов».

Классическим способом получения данных является перехват траффика в незашифрованном канале, этот способ наиболее актуален если веб-портал использует не защищённый http протокол. Подобные атаки «человек посередине» много раз освещались в литературе и имеют подробное описание, как например в статье А. Малински и др. [3]. В связи с тем, что платформа OJS реализована на языке программирования PHP, то для нее характерны определенные уязвимости, связанные с произвольным исполнением кода и XSS. Методы по выявлению подобных уязвимостей, связанных с особенностями языка PHP хорошо описаны в статье М. Бакерса и др. [4]. В своей статье они представили метод межпроцедурного анализа для приложений PHP, основанный на статистических свойствах кода, который хорошо масштабируется для объемного исходного кода, что актуально в случае с OJS. Похожая работа, но в ключе XSS атак, касающаяся языка PHP, проделана А. Маршадих и З. Зааба и описана в недавней статье [5]. Интересной особенностью этого исследования является то, что помимо простого обнаружения PHP XSS уязвимостей предлагаются и методы устранения найденных уязвимостей, что очень полезно, если учесть тот факт, что исходные коды OJS очень объемны. Вообще тестирование исходных кодов большого объема задача не тривиальная: существует множество подходов для ее решения, в основном работает правило, чем качественнее тестирование, тем большую подготовительную работу требуется сделать. Подготовительные работы могут быть связаны с разбиением исходной системы на отдельные логические блоки, которые выполняют ряд конечных функций, разработка среды для тестирования этих блоков, разработка самих тестов, выполнение тестовых сценариев с протоколированием результатом и, наконец, анализ полученных результатов. Чтобы упростить эту работу применительно к языку программирования PHP, был разработан метод полуавтоматической генерации тестовых примеров, который описан в статье Б. Стивалета и Е. Фонга [6]. Получение доступа к конфигурационным файлам злоумышленником и

возможность манипуляции такими файлами – это серьезная уязвимость для веб-порталов, используя ее возможно получить ключи для прямого подключения к базам данных, с которыми работает веб-портал. Исследования подобного рода для множества различных конфигураций рассматриваются в статье Н. Бен-Ашер и др. [7]. Основной упор в своей работе авторы сделали на построение системы, которая способна менять используемую платформу, т.е. полностью, либо частично заменять стек используемых технологий, в том числе в работе рассматриваются и базовые уязвимости основных платформ. Распространённым способом выявления «ботов» и предотвращения «спам-атак», является reCAPTCHA, однако OJS версии 2.x.x использует первую версию этого алгоритма, его надежность достаточно хорошо изучена и принимая во внимание современные успехи в области компьютерного зрения reCAPTCHA v1 не представляет собой серьезной преграды для современных «ботов». Подробно этот процесс описан в работе Ф. Старка и др. [8]. Помимо прочего авторы предоставляют открытую реализацию алгоритма распознавания символов в CAPTCHA. В области исследования защищенности веб-порталов ведутся серьезные работы с применением передовых наработок, доступных исследователям. Появляются новые, более эффективные методы поиска известных уязвимостей, что существенно облегчает работу для тестирования безопасности веб-порталов и позволяет сформулировать более качественные рекомендации по использованию и настройки составных частей для больших веб-порталов.

Веб-портал и его назначение

Прежде чем перейти непосредственно к исследованию платформы OJS, с точки зрения безопасности, рассмотрим, что из себя представляют веб-порталы и какое место в структуре веб-портала занимает OJS, какие ограничения это накладывает на выбор технологий и прочие особенности построения систем на базе OJS. Веб-портал, в рамках данной статьи, следует рассмотреть, как некую информационную систему, обеспечивающую пользователям единый авторизованный персонифицированный доступ, как к внутренним, так и внешним ресурсам, а также приложениям организации. Веб-порталы классифицируются по специализации информации, целевой аудитории, решаемым задачам и используемым технологиям. Классификация порталов включает следующие основные классы: мегапортал; информационный; корпоративный; коммерческий; горизонтальный; вертикальный; торговый; портал публикации информации; портал приложений; портал управления; портал для совместной работы; портал знаний, - подробная классификация порталов и описание каждого из классов приведено в [9]. Выделим наиболее распространённые виды порталов. Горизонтальные порталы – эти порталы, как правило, предназначены для самой большой аудитории, и включают в себя информацию и услуги, носящие общий характер. То есть они имеют задачу охватить и предоставить как можно больше информации пользователям в разных сферах. Направленность данных порталов тесно связана с деятельностью средств массовой информации. Самыми распространенными мегапорталами являются, например, всем известный Rambler, Yandex, Yahoo! и Mail.ru. Вертикальные порталы также называют нишевыми. Это обычно сайты узкой тематики, которые рассчитаны на определенную целевую категорию пользователей. Вертикальные порталы предоставляют средства, информацию, статьи, исследования, какую-либо статистику по конкретной отрасли. Примерами данного класса порталов являются развлекательные, корпоративные, финансовые, религиозные и образовательные веб-ресурсы. Веб-порталы базирующихся на платформе OJS – это вертикальные порталы знаний.

Можно однозначно сказать, что любой портал включает в себя как минимум три основных функциональных модуля:

- модуль интеграции данных;
- модуль интеграции приложений и сервисов;

- модуль индексирования и поиска.

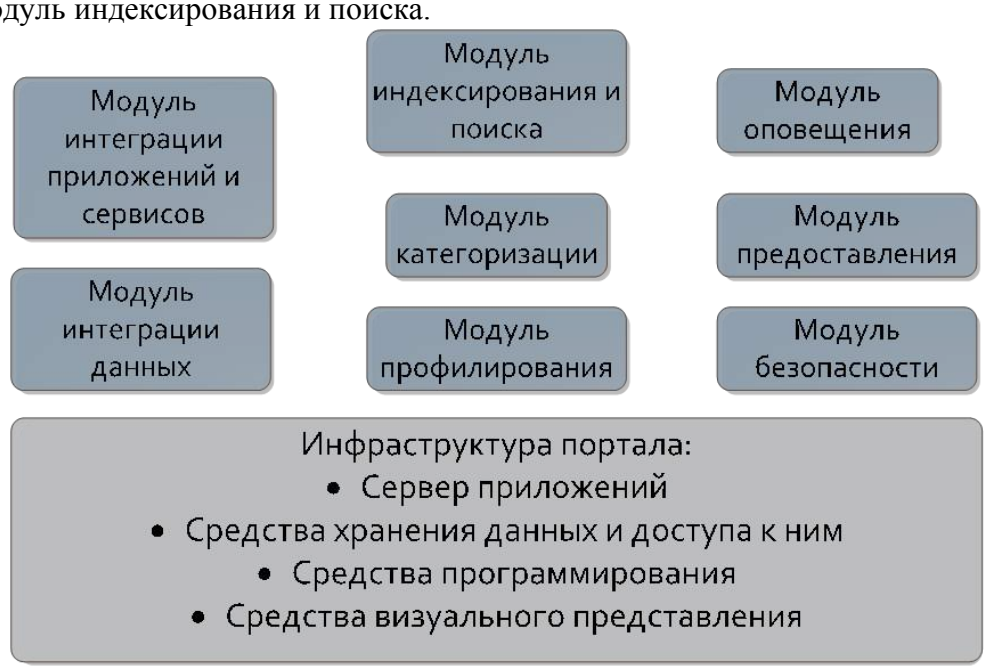


Рис.1. Функциональные модули веб-портала и его инфраструктура
(Fig.1. Functional modules of the web-portal and its infrastructure)

Модуль интеграции данных позволяет использовать средства организации целостного информационного пространства из большого количества различных источников информации. Основной направленностью данного модуля является организация унифицированного доступа к различным источникам информации, таким как: каталогом пользователей, реляционным базам данных, хранилищам документов и электронной почты.

Модуль интеграции приложений и сервисов предоставляет возможность интеграции в веб-портал программных приложений. Кроме того, благодаря данному модулю присутствует возможность расширения функциональности веб-портала за счёт использования сторонних сервисов. Однозначно различить программное приложение и сервис достаточно легко. Главное их отличие заключается в том, что программное приложение является самостоятельным программным продуктом и его использование возможно в рамках других веб-порталов, а сервисы являются частью портала и разрабатываются специально для каждого из них.

Модуль индексирования и поиска предназначен для ускорения поиска нужной информации для пользователя. При использовании этого модуля он сканирует все источники информации, находящиеся в распоряжении веб-портала, а затем индексирует каждый источник. При выполнении поиска после индексирования источников, скорость поиска значительно вырастает, за счёт предварительного отбрасывания большого количества источников, имеющих иной индекс. Это позволяет практически моментально получать релевантные ответы на поисковые запросы пользователей.

Модуль категоризации выполняют функции группировки и структуризации информационного пространства веб-портала. Происходит это путём разделения информационного пространства на информационные подмножества. В свою очередь, информационные пространства состоят из информационных единиц, которые связаны между собой по смыслу. Информационные единицы представляют собой различного рода документы, таблицы из базы данных, и так далее. Связь между информационными единицами обуславливается видом структуры, используемым в рамках веб-портала. Зачастую используются сетевая или иерархическая структура, либо их комбинация. Кроме

того, данный модуль предоставляет функциональность для формирования необходимой структуры.

Модуль профилирования позволяет осуществить явную или неявную персонификацию при использовании пользователем веб-портала. Для выполнения этого в соответствии каждому пользователю создаётся его профиль, который содержит в себе описание предпочтений и/или интересов, а также хранит историю его поисковых запросов. Рассмотрим отличия явной персонификации от неявной персонификации. При явной персонификации пользователю предлагается самостоятельно выбрать для себя способ отображения страниц портала и основную информации для отображения. При неявной персонификации происходит автоматический анализ всех действий пользователя с веб-порталом, на основе которых выделяются его предпочтения. После этого веб-портал, например, может предложить пользователю информацию, которую пользователь не искал, но которая соответствует его интересам.

Модуль оповещения используется для информирования пользователей о всевозможных новостях в портале. Это может быть, например, публикация свежей информации по конкретной, интересующей пользователя, тематике, регистрация новых пользователей, обновление уже прочитанных статей. В основе функционирования этого модуля лежит push-технология, которая для оповещения пользователей может использовать различные средства, например, через электронную почту.

Модуль представления позволяет формировать и изменять способ визуального отображения пользовательского интерфейса веб-портала. Как правило, в модуле используется подход, основанный на предоставления возможности сложения нескольких источников информации, путём комбинирования содержания, в целостное визуальное представление.

Модуль безопасности предназначен для идентификации пользователей при их авторизации на веб-портале, а также создания контекста безопасности при взаимодействии пользователя с функциональностью портала.

Реализация каждого функционального модуля зависит от используемой инфраструктуры веб-портала, к которой относятся: приложения; хранение данных и доступ к ним; средства программирования; средства визуального представления. Следует отметить, что именно от инфраструктуры во многом зависит управляемость, расширяемость и работоспособность веб-портала.

Выявление актуальных угроз на веб-порталы

Все рассмотренные угрозы безопасности веб-ресурсов можно условно разделить на группы.

Первая группа включает в себя недостаточную аутентификацию при доступе к ресурсам. В эту группу входят атаки на основе Подбора (Brute Force), Злоупотребление функционалом (Abuse of Functionality) и Предсказуемое расположение ресурсов (Predictable Resource Location). Основное отличие от недостаточной авторизации заключается в отсутствии проверки прав (или особенностей) уже авторизованного пользователя (например, обычный авторизованный пользователь может получить права администратора, просто зная адрес панели управления, если не производится проверка прав доступа). Эффективно противодействовать таким атакам можно только на уровне логики приложения. Часть атак, например, слишком частый перебор, могут быть заблокированы на уровне сетевой инфраструктуры.

Вторая группа – это недостаточная авторизация. Сюда можно отнести атаки, направленные на легкость перебора реквизитов доступа или использование каких-либо ошибок при проверке доступа к системе. Кроме техник «Подбора» (Brute Force) сюда входит «Угадывания доступа» (Credential and Session Prediction) и «Фиксация сессии»

(Session Fixation). Защита от атак этой группы предполагает комплекс требований к надежной системе авторизации пользователей.

Третья группа охватывает атаки на клиентов, это подмена содержания. Сюда входят все техники изменить содержимое веб-сайта без какого-либо взаимодействия с сервером, обслуживающим запросы — т.е. угроза реализуется за счет браузера пользователя (но при этом обычно сам браузер не является «слабым звеном»: проблемы заключаются в фильтрации контента на стороне сервера) или промежуточного кэш-сервера. Виды атак: «Подмена содержимого» (Content Spoofing), «Межсайтовые запросы» (XSS, Cross-Site Scripting), «Злоупотребление перенаправлениями» (URL Redirector Abuse), «Подделка межсайтовых запросов» (Cross-Site Request Forgery), «Расщепление HTTP-ответа» (HTTP Response Splitting, «Контрабанда HTTP-ответа» (HTTP Response Smuggling), а также «Обход маршрутизациии» (Routing Detour), «Расщепление HTTP-запроса» (HTTP Request Splitting) и «Контрабанда HTTP-запроса» (HTTP Request Smuggling). Значительная часть указанных угроз может быть блокирована еще на уровне настройки серверного окружения, но веб-приложения должны также тщательно фильтровать как поступающие данные, так и ответы пользователя.

Четвертая группа связана с выполнением произвольного кода. Атаки на выполнение произвольного кода являются классическими примерами взлома сайта через уязвимости. Злоумышленник может выполнить свой код и получить прямой доступ к серверу, на котором функционирует веб-портал, отправив определенным образом подготовленный запрос на сервер. Виды атаки, которые реализуют эту угрозу: Переполнение буфера (Buffer Overflow), Форматирование строки (Format String), Целочисленное переполнение (Integer Overflows), LDAP внедрение (LDAP Injection), Mail внедрение (Mail Command Injection), Нулевой байт (Null Byte Injection), Выполнение команд ОС (OS Commanding), Исполнение внешнего файла (RFI, Remote File Inclusion), Внедрение SSI (SSI Injection), Внедрение SQL (SQL Injection), Внедрение XPath (XPath Injection), Внедрение XML (XML Injection), Внедрение XQuery (XQuery Injection) и Внедрение XXE (XML ExternalEntities). Не все из указанных типов атак могут касаться определенного сайта, но корректно они блокируются только на уровне WAF (Web Application Firewall) или фильтрации данных в самом веб-приложении. Все оставшиеся атаки, связанные с ограниченностью серверных ресурсов, можно отнести также в отдельную группу. В частности, это Отказ в обслуживании (Denial of Service) и более точечные атаки — Злоупотребление SOAP (SOAP Array Abuse), Переполнение XML-атрибутов XML Attribute Blowup и Расширение XML-сущностей (XML Entity Expansion). Защита от них только на уровне веб-приложений, либо блокировки подозрительных запросов (сетевое оборудование или веб-прокси). Но при появление новых видов точечных атак необходиом проводить аудит веб-приложений на предмет уязвимости им.

Шестая группа – это угрозы, связанные с отказом веб-портала при достижении определенного количества запросов к его ресурсам в единицу времени, другими словами – это уязвимость к DDoS-атакам. Суть DoS-атаки заключается в том, что злоумышленник пытается сделать временно недоступным конкретный сервер, перегрузить сеть, процессор или переполнить диск. Цель атаки – просто вывести компьютер из строя, а не получить информацию, захватить все ресурсы компьютера-жертвы, чтобы другие пользователи не имели к ним доступа. К ресурсам относятся: память, процессорное время, дисковое пространство, сетевые ресурсы и т. д. Если подобная атака проводится одновременно сразу с большого числа компьютеров, то в этом случае говорят о DDoS-атаке.

Структура платформы OJS

Open Journal Systems (OJS) – это решение с открытым исходным кодом для управления и публикации научных журналов в Интернете. OJS является чрезвычайно

гибкой системой управления и издания журналов, которая может быть загружена бесплатно и установлена на локальный веб-сервер.

Она была разработана, чтобы сократить время и энергозатраты, связанные с канцелярскими и управленческими задачами редактирования журнала, одновременно улучшая учет и эффективность редакционных процессов. Она направлена на улучшение научного и открытого качества публикаций журналов посредством ряда нововведений, в том числе расширения опыта читателей, создания более прозрачных политик журнала и улучшения индексирования [10].

OJS – это система управления журналами / веб-сайтами / публикациями. OJS охватывает все аспекты публикаций онлайн – журналов, начиная с создания веб-сайта журнала, заканчивая задачами эксплуатации, такими, как процесс подачи публикации автором, экспертная оценка, редактирование, публикация, архивирования и индексирования журнала. OJS также помогает управлять аспектами организации журнала, в том числе отслеживанием работы редакторов, рецензентов и авторов, уведомлением читателей и оказанием помощи с корреспонденцией [10].

OJS является гибкой и масштабируемой. Одна установка OJS может поддерживать работу одного или нескольких журналов. Каждый журнал имеет свой собственный уникальный URL-адрес, а также свой собственный внешний вид. OJS может позволить одному редактору управлять всеми аспектами журнала и веб-сайта, или OJS будет поддерживать международную группу редакторов, несущих разную ответственность за несколько разделов журнала. OJS поддерживает принцип расширения доступа. Эта система предназначена не только для оказания помощи в публикации журналов, но и для демонстрирования, как затраты на публикацию журналов могут быть сокращены до уровня, при котором читатели получают «открытый доступ» к содержанию журнала.

Система OJS написана на PHP и может быть запущена на любом веб-сервере с поддержкой данного интерпретатора; в качестве базы данных используется MySQL или PostgreSQL. OJS поддерживает идентификаторы цифровых объектов, что позволяет регистрировать статьи в таких агентствах, как CrossRef, Multilingual European DOI Registration Agency и DataCite. Для вовлечения читателей в процесс создания журнала сообществом Public Knowledge Project был разработан набор инструментов Reading Tools, предоставляющий доступ к смежным исследованиям, тематическим новостям, законодательным актам и другим ресурсам в открытых базах данных. OJS многофункционален: имеется возможность провести информетрический анализ статей, поддерживается электронный кошелёк PayPal. Существует совместимость с системами научных конференций, таких как Easychair и Open Conference Systems. С помощью плагина LatexRender можно подключить возможность интерпретации Tex файлов и их рендеринга. OJS может рассматриваться как электронная библиотека, так как этот продукт обеспечивает доступ к контенту и расширенный поиск по нему (по автору, названию статьи, ключевым словам и др.). OJS позволяет проводить проверку загружаемого материала на плагиат с помощью встроенного модуля, путём поиска заимствований среди утверждений, не являющихся цитатами.

OJS состоит из 4 редакционных стадий: отправление материала, в котором рассматриваются новые заявки (отклоненные, закрепленные за разделом редакторы и т.д.); Рецензирование, в котором проводится экспертная оценка и авторские исправления; литературное редактирование, где прошедшие рецензию и исправления файлы отправляются для литературного редактирования; и публикация, где окончательная версия преобразуется в форматы для публикации (PDF, HTML и т.д.), скорректирована готова к публикации.

Подробная схема редакционного и издательского процессов OJS приведена на рисунке 2.

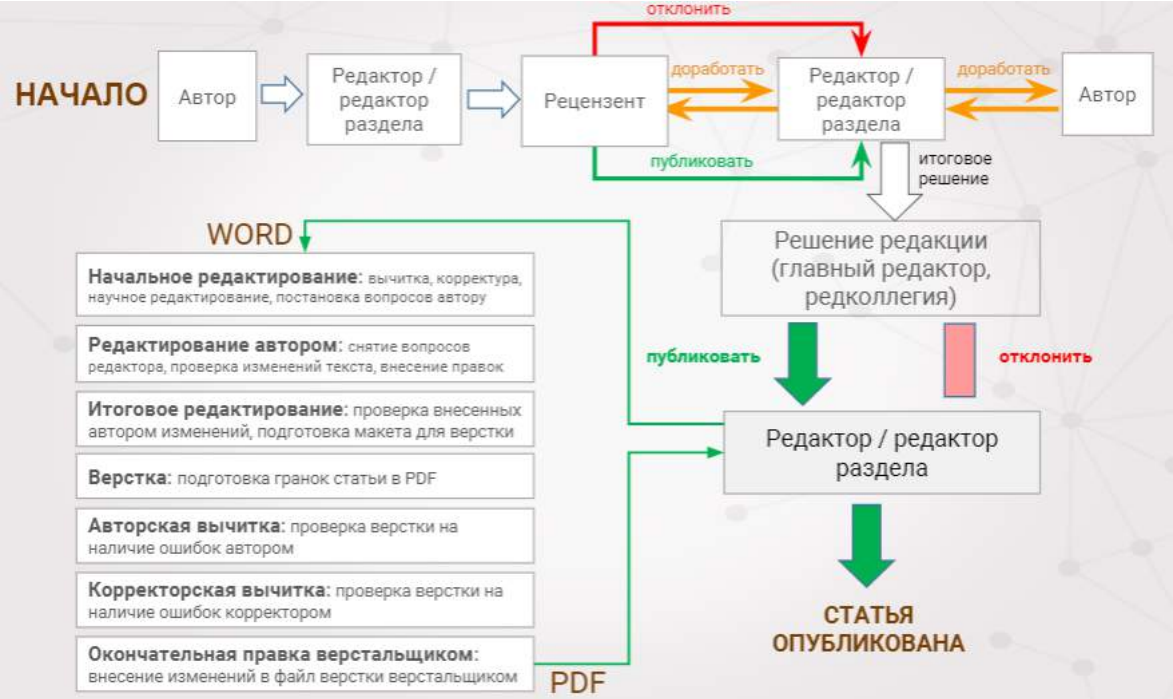


Рис. 2. Схема редакционно-издательского процесса OJS
(Fig. 2. Scheme of the OJS editorial and publishing process)

Структура управления OJS статьями в журнале происходит с помощью четырех редакционных этапов, которые могут выполняться одним или несколькими редакторами.

1. Очередь не назначенных статей: на этом этапе статья назначается одному или нескольким редакторам.

2. Рецензирование статьи: этап охватывает рецензирование и редакционное решение о публикации.

3. Редактирование статьи: этап включает литературное редактирование, верстку и корректуру. Статья закрепляется за определенным выпуском.

4. Содержание: статьи выстраиваются в необходимом порядке и публикуются.

Редакционные роли:

• Менеджер журнала: настраивает журнал и распределяет редакционные роли (может при этом выступать в нескольких ролях).

• Редактор: следит за редакционным процессом; может назначать статьи редакторам разделов, которые управляют рецензированием и редактированием статей; следит за графиком издания журнала.

• Редактор раздела: управляет рецензированием и редактированием принятых к публикации статей.

• Литературный редактор: работает со статьей с целью улучшить грамматику и ясность материала, отправляет автору запросы касательно возможных ошибок, обеспечивает высокое качество стиля статьи и библиографии.

• Верстальщик: преобразует отредактированные статьи в гранки форматов HTML, PDF, и/или PS для последующей публикации.

• Корректор: вычитывает гранки на предмет ошибок правописания и форматирования.

OJS обладает следующими особенностями: OJS может устанавливаться и управляться локально; редакторы настраивают требования, секции, процессы рецензирования, и т.д.; подача публикаций онлайн, двойная слепая рецензия и управление всем контентом; сложное индексирование контента; отзывчивый интерфейс читателя с

поддержкой различных тем; оповещение читателей посредством электронной почты; полная онлайн поддержка; многоязыковая поддержка; открытый код; отсутствие платной лицензии разработчиков

Дополнительные возможности: комментирование статей (анонимное или авторизованное) и администрирование комментариев; возможность проведения открытого рецензирования с публикацией рецензий; публикация тезисов научных работ, в том числе диссертаций, в виде отдельного потока на сайте (не в составе основного контента журнала. Как и любая другая система управления контентом, Open Journal Systems имеет ряд дополнительных модулей (плагинов), которые расширяют ее возможности (основной функционал). Например, существуют плагины, позволяющие индексировать содержимое журнала в Google Scholar и PubMed Central. Плагин подписки реализует поддержку стандартов RSS и Atom. Open Journal Systems соответствует стандартам проекта LOCKSS, что позволяет безопасно собирать, хранить и предоставлять доступ ко всем статьям журнала в долгосрочной перспективе. Часть этих плагинов загружается и устанавливается вместе с системой, т.е. входит в основной дистрибутив. Другая часть создается, дорабатывается и предлагается к использованию сообществом разработчиков.

Уязвимости OJS

Прежде всего, следует уточнить, что под уязвимостью информационной системы понимается любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы. Угрозой информационной системе называется потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы.

Рассмотрим уязвимости платформы Open Journal Systems. Для наглядности, динамика наличия уязвимостей у данной платформы отображена на рис. 3.

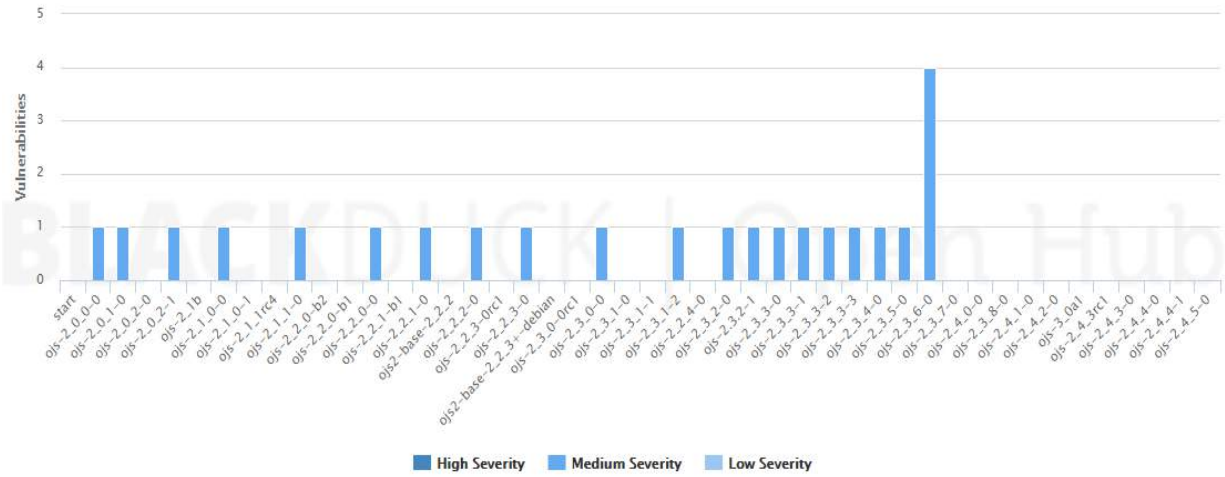


Рис. 3. Диаграмма наличия уязвимостей в зависимости от версии платформы
(Fig. 3. Diagram of vulnerabilities, depending on the version of the platform)

Как видно из диаграммы, наиболее уязвимой версией данной платформы является 2.3.6.0.

В список уязвимостей данной версии входят: произвольное манипулирование файлами в открытых журнальных системах: CVE-2012-1467 (В неё входит «Произвольное удаление файлов», «Переименование произвольного файла»); произвольная загрузка файлов в открытых журнальных системах: CVE-2012-1468; возможность XSS нападение в открытых журнальных системах: CVE-2012-1469. В более поздних версиях все уязвимости устранены. [11]

Частная модель угроз веб-портала на платформе OJS

Приведенная выше структурная модель веб-портала и платформы OJS, позволяет последовательно подойти к построению частной модели угроз безопасности исходя из назначения и внутреннего содержания отдельных модулей системы.

Возможные нарушители по признаку принадлежности к информационной системе делятся на две группы:

Внешние нарушители: клиенты, авторы статей и рецензенты; представители конкурирующих организаций, пользователи сети интернет, которые намеренно предпринимают действия по несанкционированному внедрению в процесс работы веб-портала.

Внутренние нарушители: пользователь системы (администратор, редактор, главный редактор, управляющий журнала); обслуживающий персонал; сотрудники отдела разработки и сопровождения веб-портала.

Исходя из особенностей функционирования портала, допущенные к нему физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам веб-портала в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- Администратор (категория I) отвечает за предварительное конфигурирование и создание журналов на сайте, имеют доступ к некоторым сервисным функциям платформы, таким как очистка кэша данных и шаблонов.
- Управляющий журнала (может быть несколько, если в рамках одного веб-портала функционирует несколько журналов) (категория II) отвечает за функционирование одного конкретного журнала, размещенного на веб-портале. Сюда входят задачи наполнения содержимого сайта информацией, конфигурирование сайта журнала, подключение/отключение/конфигурирование различных плагинов OJS в зависимости от нужд журнала.
- Редакторы и редакторы разделов журнала (категория III) отвечают за редакционный процесс в жизни журнала, они назначают рецензентов, принимают/отклоняют статьи исходя из издательских правил журнала, создают и удаляют выпуски, следят за корректностью ссылок и идентификаторов. Отличие между редактором и редактором раздела существует только внутри больших изданий, там редактор имеет права заниматься редакционным процессом в любом разделе журнала, а редактор раздела, только в строго заданных.
- Зарегистрированные авторы и читатели (категория IV) имеют возможность отправлять статьи в редакцию журнала, просматривать статьи, пользоваться инструментами читателя OJS, комментировать статьи, подписываться на рассылки.
- Рецензенты и верстальщики (категория V) имеют доступ к исходным файлам статей, для рецензентов в зависимости от политики рецензирования статьи могут предоставляться в обезличенном виде (за это отвечают редакторы), верстальщики размечают ссылки в статье и занимаются дополнительным оформлением работы.
- Не зарегистрированные пользователи (категория VI) в зависимости от конфигурации платформы администратором могут иметь доступ аналогичный читателям журнала, либо иметь доступ только к главной странице и новостям журнала.
- Сотрудники, обслуживающие серверы, на которых работают выделенные виртуальные машины и серверы mysql/postgresql, ftp (категория VII) занимаются поддержанием работы всех обслуживающих OJS систем, т.е. систем с использованием которых функционирует платформа. Имеют непосредственный доступ ко всей хранимой и обрабатываемой информации.

- Уполномоченный персонал разработчиков веб-портала, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов портала (категория VIII).

Далее рассмотрим угрозы безопасности, которые могут возникнуть в процессе функционирование веб-портала. При разработке угроз учитывались основные характеристики веб-портала, ресурсы, потенциально подверженные угрозам информационной безопасности, основные каналы реализации угроз безопасности, основные способы реализации угроз безопасности. Описание угроз в своей структуре содержит следующие наименования: название угрозы; возможные источники угрозы; способ реализации угрозы; используемые уязвимости; вид ресурсов, потенциально подверженных угрозе; нарушаемые характеристики безопасности ресурсов; возможные последствия реализации угрозы; рекомендации по нейтрализации угрозы, если имеются.

Основные угрозы безопасности информации веб-портала на платформе OJS

Название угрозы: Несанкционированный доступ к передаваемой информации с использованием программных или программно-аппаратных средств перехвата трафика.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: осуществление перехвата трафика путем использования специализированного ПО или комплекса.

Используемые уязвимости: Особенности протоколов сетей передачи данных и связанные с ними уязвимости.

Вид ресурсов, потенциально подверженных угрозе: Передаваемая и хранимая в системе информация.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная, либо полная потеря информации, хранимой в системе, искажение этой информации без возможности точного детектирования искаженных частей, частичная/полная дестабилизация работы веб-портала, утечка персональной и конфиденциальной информации.

Атаки, использующие угрозы такого типа могут иметь различные последствия для веб-портала, начиная с отсутствия какого-либо негативного влияния и заканчивая полным прекращением существования веб-портала как такового. Рассмотрим более подробно от чего эти последствия зависят. Наличие рассматриваемой угрозы следует из факта доступности передаваемого трафика третьим лицам, причем для перехвата данных пользователей локальных широковещательных сетей и беспроводных сетей не требуется дорогостоящего оборудования, а в большинстве случае достаточно обычного ПК с установленным специализированным программным обеспечением [3, 12]. Аналогичная ситуация возникает и в мобильных сетях передачи данных, однако с поправкой на необходимость наличия у злоумышленника аппаратной составляющей [13]. Подробно реализация атак описана в статьях [3, 12, 13]. Успех перехвата данных сомнений не вызывает и сам факт перехвата данных, в основном, не влияет на корректность процесса взаимодействия пользователя с веб-порталом. Масштаб последствий зависит от данных, которые сумел получить злоумышленник в ходе перехвата. В случае, когда данные передаются в открытом виде злоумышленник может восстановить перехваченный контекст соединения (так называемые «куки») и работать с веб-порталом от имени «жертвы», причем ему доступен весь функционал, который доступен «жертве» перехвата и не стоит пояснять, что если была перехвачена сессия администратора сайта, то удаление всех журналов с сайта занимает пару кликов. Стратегия с постоянным архивированием содержимого веб-портала в этом случае в полной мере не решает проблемы из-за которой возникает угроза и абсолютно не работает, когда злоумышленник производит точечные модификации данных, которые не влияют на корректность работы портала (например, подменяет рецензию на

статью). Поэтому главной и наиболее эффективной рекомендацией будет использование последних защищенных протоколов передачи данных, т.к. OJS функционирует с использованием протокола http, то логичным будет перейти на его защищенный аналог https с использованием TLS [14].

Название угрозы: Исполнение произвольного кода на стороне клиента или сервера.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: осуществление перехвата трафика путем использования специализированного ПО или комплекса.

Используемые уязвимости: Особенности конкретной реализации взаимодействия составных частей.

Вид ресурсов, потенциально подверженных угрозе: Хранимая и обрабатываемая в системе информация.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная, либо полная потеря информации, хранимой и обрабатываемой в системе, искажение этой информации без возможности точного детектирования искаженных частей, частичная/полная дестабилизация работы веб-портала, утечка персональной и конфиденциальной информации.

Существует несколько основных атак, которые базируются на возможности выполнения произвольного программного кода или запросов, которые не доступны пользователю. Целью атаки может быть, как другой пользователь системы, так и непосредственно сам веб-портал. Возможность выполнения произвольного кода на PHP для разных версий множество раз обсуждалась и описана во многих статьях, кроме того, существует ряд правил, которых нужно придерживаться разработчикам, чтобы избежать появления подобных уязвимостей. К таким правилам можно отнести использование экранирования спецсимволов в пользовательских запросах, использование различной кодировки для пользовательской части запроса и базовой часть, не использовать «опасные» функции языка PHP (например, eval (string $code), которая выполняет переданную в качестве параметра строку в интерпретаторе). Однако, когда речь идет о взаимодействие нескольких составных частей, то проблемы могут возникать на стыке их взаимодействия. В OJS используется «классический» набор для веб-сайтов PHP, MySQL, HTML. Такой набор хорошо изучен и с точки зрения атакующих и сточки зрения защиты информации [4,15]. Однако для OJS были обнаружены и описаны уязвимости связанные с возможностью выполнения произвольного PHP кода на стороне сервера и XSS атак, для версии 2.3.6 и ниже [16, 17, 18, 19]. Последствия подобных атак могут рознится в зависимости от дополнительных условий, таких как: уровень привилегий с которыми запускается произвольный код, область видимости для этого кода, на какой стороне будет работать код (на сервере веб-портала или на клиентской части «жертвы» атаки). В худшем случае, когда злоумышленник может выполнять свой код на стороне сервера с максимальными привилегиями, его возможности по манипуляциям над процессом работы веб-портала безграничны, однако, стоит сказать, что этот случай соответствует не рекомендованной конфигурации платформы. В случае корректной конфигурации злоумышленник может манипулировать только информацией доступной для записи, а это все загружаемые файлы статей, файлы шаблонов внешнего вида, временные файлы, различные изображения на сайте. При выполнения произвольного кода на стороне клиента злоумышленник по аналогии с предыдущей угрозой может получить доступ к идентификатору сессии пользователя и начать использование веб-портала от имени «жертвы» атаки, последствия в таком случае аналогичны угрозе, рассмотренной выше. В рамках данной работы было дополнительно проверено исправление уязвимостей версии 2.3.6 в последней из версии 2.x.x – это 2.4.8-1 и установлено, что уязвимости отсутствуют. Поэтому для веб-порталов

на платформе OJS рекомендуется использовать версию не ниже 2.4.8. Рекомендации по правам доступа на запись следующие права на запись должны быть только в папках папка public; cache; cache/t_cache; cache/t_compile; cache/_db. Конфигурационный файл рекомендуется настроить в текстовом редакторе и установить права только для чтения на стороне сервера, либо сначала установить права чтение/запись, а после установки и предварительной настройки платформы OJS изменить на «только для чтения».

Название угрозы: Загрузкой произвольных файлов на сервер веб-портала.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Загрузка данных на сервер веб-портала штатными средствами в том числе при их использовании не по назначению.

Используемые уязвимости: Отсутствие индикации загрузки больших файлов, либо большого количества файлов

Вид ресурсов, потенциально подверженных угрозе: Обрабатываемая на веб-портале информация.

Нарушаемые характеристики безопасности ресурсов: Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая требовала записи на диск/базу данных; недоступность веб-портала пока не будет произведена ручная очитка от лишних файлов.

Суть данной угрозы очень проста, т.к. веб-портал на платформе OJS позволяет загружать файлы статей и дополнительных материалов на сервер, то злоумышленник может попробовать загрузить очень большие файлы, либо быстро загружать очень маленькие с целью исчерпания свободного места на диске. Другой вариант – это загрузка больших объемов текста в служебные поля системы, которые сохраняются в базу данных, к таким полям относятся вся информация, связанная с пользователем, заполняемая в «личном кабинете», комментарии к статьям и объявлениям, служебные поля при заполнении формы подачи статьи в редакцию журнала. Атака достаточно тривиальна и не требует от атакующего наличия каких-либо специализированных средств. Хорошим способом защиты будет введение ограничения на максимальный объем загружаемых файлов, ограничение на частоту загрузки данных на сервер, ограничение максимальной длины полей, хранящихся в базе данных, хорошая защита от спама и «ботов».

Название угрозы: Раскрытие содержимого конфигурационных файлов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Получение доступа к файлу конфигурации OJS.

Используемые уязвимости: Ошибка в конфигурации сервера, на котором функционирует OJS.

Вид ресурсов, потенциально подверженных угрозе: База данных веб-портала

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая хранится в базе данных.

Подобная угроза появляется, когда сервер не достаточно хорошо настроен, по большей части это касается файла .htaccess, который позволяет ограничить доступ пользователей к определенным файлам и папкам сервера, при этом сама платформа OJS (ее исполняемый код) доступ к этим файлам имеет. Файл конфигурации OJS в таком случае можно получить, просматривая доступный файлы и папки через специальную функцию в любом веб браузере, либо попытаться запросить файл с сервера напрямую, зная его имя и местоположение. Получив доступ к содержимому файла злоумышленник получает доступ к информации для входа в базу данных системы и к другой ключевой конфигурационной информации, поэтому последним этапом на пути пользователя в базу данных будет служить межсетевой экран веб-портала, если он не сконфигурирован должным образом, либо отсутствует вообще, то злоумышленник получает полный доступ к информации,

хранящейся в базе данных веб-портала и может производить над ней любые манипуляции. В базе данных OJS хранит всю служебную текстовую информацию, кроме самих файлов статей и других загружаемых файлов. Для предотвращения подобной угрозы следует более тщательно подойти к вопросу конфигурирования OJS и инфраструктуры с которой он взаимодействует (например: с помощью служебного файла .htaccess ограничить пользователям доступ к файлу конфигурации OJS, настроить межсетевой экран между OJS и базой данных таким образом, чтобы он не позволял доступ туда извне.

Название угрозы: Раскрытие содержимого конфигурационных файлов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Получение доступа к файлу конфигурации OJS.

Используемые уязвимости: Ошибка в конфигурации сервера, на котором функционирует OJS.

Вид ресурсов, потенциально подверженных угрозе: База данных веб-портала

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая хранится в базе данных.

Подобная угроза появляется, когда сервер не достаточно хорошо настроен, по большей части это касается файла .htaccess, который позволяет ограничить доступ пользователей к определенным файлам и папкам сервера, при этом сама платформа OJS (ее исполняемый код) доступ к этим файлам имеет. Файл конфигурации OJS в таком случае можно получить, просматривая доступный файлы и папки через специальную функцию в любом веб браузере, либо попытаться запросить файл с сервера напрямую, зная его имя и местоположение. Получив доступ к содержимому файла, злоумышленник получает доступ к информации для входа в базу данных системы и к другой ключевой конфигурационной информации, поэтому последним этапом на пути пользователя в базу данных будет служить межсетевой экран веб-портала, если он не сконфигурирован должным образом, либо отсутствует вообще, то злоумышленник получает полный доступ к информации, хранящейся в базе данных веб-портала и может производить над ней любые манипуляции. В базе данных OJS хранит всю служебную текстовую информацию, кроме самих файлов статей и других загружаемых файлов. Для предотвращения подобной угрозы следует более тщательно подойти к вопросу конфигурирования OJS и инфраструктуры с которой он взаимодействует (например: с помощью служебного файла .htaccess ограничить пользователям доступ к файлу конфигурации OJS, настроить межсетевой экран между OJS и базой данных таким образом, чтобы он не позволял доступ туда извне [20].

Название угрозы: Исчерпание свободного дискового пространства и вычислительных ресурсов большим числом внешних запросов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Использование распределенных или централизованных систем для генерации большого числа реальных запросов к веб-порталу.

Используемые уязвимости: Слабый алгоритм выявления «ботов».

Вид ресурсов, потенциально подверженных угрозе: Данные, обрабатываемые веб-порталом.

Нарушаемые характеристики безопасности ресурсов: Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая требовала записи на диск/базу данных; недоступность веб-портала пока не будет произведена ручная очитка от лишних файлов на диске и записей в базе данных.

Ключом к появлению этой угрозы служит возможность в автоматическом режиме генерировать корректные с точки зрения взаимодействия пользователя с системой запросы, причем запросы должны быть максимально вычислительно затратные для веб-портала,

чтобы занять его ресурсы. К таким запросам может относиться: регистрация пользователя, написание комментария, отправка статьи на рассмотрение, загрузка файла, сложный запрос в базу данных и т.д. Как правило, человек на формирование такого запроса тратит много больше времени, чем веб-портал его обрабатывает, но когда такие запросы начинают приходить в автоматическом режиме, то система просто перестает справляться и в итоге исчерпывает все доступные ресурсы, что негативно сказывается на качестве работы веб-портала. Решением проблемы, помимо уже рассмотренного ранее ограничения на частоту загрузки данных на сервер, является использование полностью автоматизированного публичного теста Тьюринга для различения компьютеров и людей, известная как CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), это позволяет отбрасывать запросы, которые не могу пройти данный тест (на рисунке 3 представлен пример изображений из теста). Подразумевается, что для человека пройти подобный тест не составляет труда, а вот для компьютера тест – это непреодолимое препятствие. В OJS версии 2.x.x встроен модуль reCAPTCHA v1, который не плохо справлялся со своей задачей, но сейчас не представляет серьёзного препятствия для компьютера. В настоящее время существую системы, которые по разным оценкам достигают точности от 85% до 95% на задаче распознавания букв на генерируемой reCAPTCHA v1 картинке, что сопоставимо с точностью человека [8, 21].

Рис.3. Пример изображений reCAPTCHA v1
(Fig.3. example of reCAPTCHA v1 images)

Решением данной проблемы будет использование reCAPTCHA v2, которая на сегодняшний день широко используется в подавляющем большинстве веб-сайтов, как базовая защита от автоматически генерируемых запросов и достаточно хорошо зарекомендовала себя. Не смотря на значительно возросшую сложность задачи для компьютера, теперь вместо букв нужно определять факт наличия/отсутствия на изображениях или частях одного изображения определенных объектов (пример представлен на рисунке 4). Все же существуют методы, которые позволяют обойти и эту защиту, с меньшей вероятностью, порядка 50-70% и при определенных условиях, требуется достаточно производительная аппаратная платформа и даже при этом условии на обработку одного запроса потребуется прядка 20 секунд [22]. Не смотря на такие существенные успехи использование reCAPTCHA v2 остается оправданным и по сей день. В OJS версии 2.x.x официально отсутствует поддержка reCAPTCHA v2, поэтому в рамках работы по исследованию и доработке платформы была встроена поддержка reCAPTCHA v2 в OJS-2.4.8-1, что является одним из практических результатов проделанной работы.

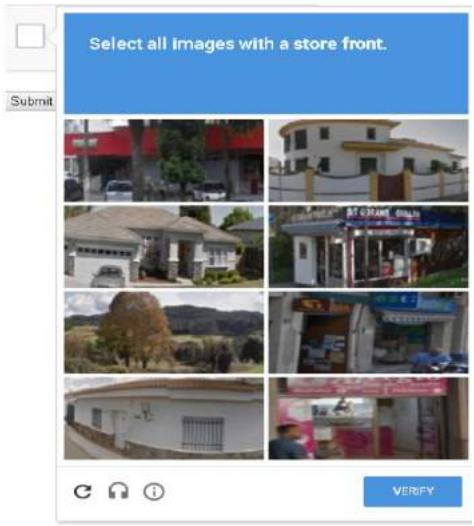


Рис. 4. Пример изображений reCAPTCHA v2
(Fig. 4. example of reCAPTCHA v2 images)

Название угрозы: Несанкционированный доступ к хранимой и обрабатываемой веб-порталом информации.

Источники угрозы: пользователи веб-портала категории VII и VIII.

Способ реализации угрозы: Непосредственное вмешательство в процесс функционирования веб-портала.

Используемые уязвимости: Наличие непосредственного доступа к оборудованию и исходным кодам веб-портала.

Вид ресурсов, потенциально подверженных угрозе: Данные обрабатываемые и харнимые веб-порталом.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Полная утрата конфиденциальности данных и самих данных, хранимых и обрабатываемых веб-порталом.

Подобного вида угроза возникает как факт того, что веб-порталу необходима аппаратная платформа, на которой он будет работать и если эта платформа находится в неподконтрольной зоне, а доступ к ней имеет неконтролируемый круг лиц, то утрата данных является делом времени. Лицам категории VII и VIII не составляет труда внедрится в процесс работы веб-портала и получить/изменить определенные данные. Поэтому рекомендацией будет размещать веб-порталы только на подконтрольных серверах и доступ, к которым имеет строго ограниченный круг лиц, а если это невозможно, то нужно иметь в виду, что такая угроза имеет место быть информировать об этом пользователей системы и не работать с данными, для которых крайне критична целостность, доступности и конфиденциальность.

Не трудно заметить, что источником для большинства рассмотренных выше угроз служат лица категории IV и VI, т.е. зарегистрированные авторы, читатели и незарегистрированные пользователи, эти две категории представляют наибольший интерес в частной модели угроз, т.к. создатели вертикального, информационного веб-портала знаний не могут контролировать и воздействовать на эти категории пользователей, соответственно появление злоумышленника в этих категориях наиболее вероятно. Кроме того, только для этой категории устранение базовых угроз, которые были перечислены выше не требует колоссальных человеческих и финансовых ресурсов. Лица всех оставшихся категорий должны относится к подконтрольному персоналу и появления там злоумышленника маловероятно. Однако, если это произойдет, то ущерб будет прямо завесить, от полномочий, которыми наделен сотрудник. В случае с I и II категориями

внутренний нарушитель может полностью прекратить существование журнала и веб-портала в целом, от такой угрозы может помочь только периодическое архивирование данных, это поможет восстановить работоспособность веб-портала, но не отменит факта нарушения конфиденциальности статей, находящихся в процессе рецензирования и личных данных пользователей. Лица категории III имеют доступ только к определенным разделам журнала, выпускам и статьям, от их преднамеренного деструктивного воздействия тоже спасает архивирование журнала, но аналогичным образом может быть нарушена целостность и конфиденциальность части данных, хранимых веб-порталом. Лица категории V имеют очень ограниченный функционал и могут только влиять на издательский процесс, но не на работу веб-портала.

Будущие работы

В рамках работ по исследованию и доработке платформы OJS 2.4.8-1 планируется провести дальнейшее тестирование и соответствующую доработку, для устранения обнаруженных недостатков как в обычном функционировании платформы, так и в функционировании систем безопасности. В настоящий момент уже был выявлен и устранен ряд проблем с корректностью работы частей системы, отвечающих за использование защищенного протокола https, платформа переведена под использование reCAPTCHA v2. В соответствии с описанной частной моделью угроз выбраны направления и сценарии для тестирования безопасности системы OJS, в том числе в условиях функционирования на различных программных платформах.

Заключение

В ходе работы были выявлены наиболее характерные угрозы безопасности для веб-порталов, функционирующих на платформе OJS и сформулированы рекомендации по нейтрализации этих угроз. Изучены уязвимости платформы Open Journal Systems, а также возможность типовых атак с их использованием. Приведена статистика уязвимостей всех версий данной платформы, в работе отражены наиболее опасные из них. Так же проведен поиск информации об атаках, совершённых на OJS. За последнее время был известен только один случай попытки злоумышленников провести акт мошенничества, однако компанией была оперативно выработана политика защиты.

С учетом вышесказанного представляется целесообразным использование автоматизированной электронной издательской системы Open Journal Systems в качестве системы управления научным журналом, т. к. она является наиболее динамично развивающейся и хорошо документированной в ней отсутствуют какие-либо непреодолимые проблемы с безопасностью хранимых и обрабатываемых данных. Кроме того, платформа хорошо поддается доработке, что служит существенным плюсом при обнаружении новых уязвимостей, однако требует от разработчика наличия определенных знаний и навыков.

СПИСОК ЛИТЕРАТУРЫ:

1. Public Knowledge Project. History. [Электронный ресурс] URL: https://pkp.sfu.ca/about/history/ (Дата обращения 26.03.2018 г.).
2. Juan Pablo Alperin. How Many Journals Use OJS? - 1 октября 2015 г. [Электронный ресурс] URL: https://pkp.sfu.ca/2015/10/01/how-many-journals-use-ojs/ (Дата обращения 26.03.2018 г.).
3. Maltinsky A., Giladi R., Shavitt Y. On network neutrality measurements (2017) ACM Transactions on Intelligent Systems and Technology, 8 (4), статья № 56 .
4. Backes M., Rieck K., Skoruppa M., Stock B., Yamaguchi F. Efficient and Flexible Discovery of PHP Application Vulnerabilities (2017) Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, статья № 7961989, pp. 334-349.

5. Marashdih A.W., Zaaba Z.F., Detection and removing cross site scripting vulnerability in PHP web application(2017) Proceedings - 2017 International Conference on Promising Electronic Technologies, ICPET 2017, статья № 8109033, pp. 26-31.
6. Stivalet B., Fong E. Large Scale Generation of Complex and Faulty PHP Test Cases (2016) Proceedings - 2016 IEEE International Conference on Software Testing, Verification and Validation, ICST 2016, статья № 7515499, pp. 409-415.
7. Ben-Asher N., Morris-King J., Thompson B., Glodek W.. Attacker skill, defender strategies and the effectiveness of migration-based moving target defense in cyber systems (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 21-30.
8. Stark F., Hazirbas C., Triebel R., Cremers D.. CAPTCHA Recognition with Active Deep Learning, In GCPR Workshop on New Challenges in Neural Computation, 2015.
9. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. «Информационная безопасность открытых систем: Учебник для вузов. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком. 2006. – 536 с.: ст. 117-118.
10. Спирин О.М., Лупаренко Л.А. «Опыт использования программной платформы Open Journal Systems для поддержки научно-образовательной деятельности» - 2017.Т.61 №5. С.196-218.
11. The Open Journal Systems Open Source Project on Open Hub: Security. [Электронный ресурс] URL: https://www.openhub.net/p/ojs2/security?filter%5Bmajor_version%5D=&filter%5Bperiod%5D=&filter%5Bversion%5D=69022&filter%5Bseverity%5D (Дата обращения 29.03.2018 г.).
12. Kavianpour A., Anderson M.C. An Overview of Wireless Network Security (2017) Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, статья № 7987214, pp. 306-309.
13. Khanpara P., Trivedi B. Security in mobile ad hoc networks (2017) Advances in Intelligent Systems and Computing, 508, pp. 501-511.
14. Guo Y., Cao Z., Yang W., Xiong G. A measurement and security analysis of SSL/TLS deployment in mobile applications (2018) Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 209, pp. 189-199.
15. Medeiros I., Beatriz M., Neves N., Correia M. Demonstrating a Tool for Injection Attack Prevention in MySQL (2017) Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, статья № 8023153, pp. 551-558.
16. CVE-2011-5195. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5195 (Дата обращения 01.04.2018 г.).
17. CVE-2011-5196. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5196 (Дата обращения 01.04.2018 г.).
18. CVE-2011-5197. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5197 (Дата обращения 01.04.2018 г.).
19. CVE-2012-1469. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1469 (Дата обращения 04.04.2018 г.).
20. Larsson E., Sigholm J. Papering over the cracks: The effects of introducing best practices on the web security ecosystem (2016) International Conference on Information Networking, 2016-March, статья № 7427064, pp. 1-6.
21. Starostenko O., Cruz-Perez C., Uceda-Ponga F., Alarcon-Aquino V. Breaking text-based CAPTCHAs with variable word and character orientation (2015) Pattern Recognition, 48 (4), pp. 1097-1108.
22. Sivakorn S., Polakis I. and Keromytis A. D., "I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 388-403. doi: 10.1109/EuroSP.2016.37.

REFERENCES:

[1] Public Knowledge Project. History. [Электронный ресурс] URL: https://pkp.sfu.ca/about/history/ (Дата обращения 26.03.2018 г.).
[2] Juan Pablo Alperin. How Many Journals Use OJS? - 1 октября 2015 г. [Электронный ресурс] URL: https://pkp.sfu.ca/2015/10/01/how-many-journals-use-ojs/ (Дата обращения 26.03.2018 г.).
[3] Maltinsky A., Giladi R., Shavitt Y. On network neutrality measurements (2017) ACM Transactions on Intelligent Systems and Technology, 8 (4), статья № 56 .
[4] Backes M., Rieck K., Skoruppa M., Stock B., Yamaguchi F. Efficient and Flexible Discovery of PHP Application Vulnerabilities (2017) Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, статья № 7961989, pp. 334-349.
[5] Marashdih A.W., Zaaba Z.F., Detection and removing cross site scripting vulnerability in PHP web application(2017) Proceedings - 2017 International Conference on Promising Electronic Technologies, ICPET 2017, статья № 8109033, pp. 26-31.

[6] Stivalet B., Fong E. Large Scale Generation of Complex and Faulty PHP Test Cases (2016) Proceedings - 2016 IEEE International Conference on Software Testing, Verification and Validation, ICST 2016, статья № 7515499, pp. 409-415.

[7] Ben-Asher N., Morris-King J., Thompson B., Glodek W.. Attacker skill, defender strategies and the effectiveness of migration-based moving target defense in cyber systems (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 21-30.

[8] Stark F., Hazirbas C., Triebel R., Cremers D.. CAPTCHA Recognition with Active Deep Learning, In GCPR Workshop on New Challenges in Neural Computation, 2015.

[9] Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. "Information security of open systems: A textbook for high schools. Volume 1 - Threats, vulnerabilities, attacks and approaches to protection. - M .: Hot line - Telecom. 2006. - 536 pp .: art. 117-118. (in Russian).

[10] Spirin O.M., Luparenko L.A. "Experience of using the Open Journal Systems software platform to support scientific and educational activities" - 2017.T.61 №5. P.196-218. (in Russian).

[11] The Open Journal Systems. Open Source Project on Open Hub: Security. [Web resource] URL: https://www.openhub.net/p/ojs2/security?filter%5Bmajor_version%5D=&filter%5Bperiod%5D=&filter%5Bversion%5D=69022&filter%5Bseverity%5D (Access date 29.03.2018)

[12] Kavianpour A., Anderson M.C. An Overview of Wireless Network Security (2017) Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, статья № 7987214, pp. 306-309.

[13] Khanpara P., Trivedi B. Security in mobile ad hoc networks (2017) Advances in Intelligent Systems and Computing, 508, pp. 501-511.

[14] Guo Y., Cao Z., Yang W., Xiong G. A measurement and security analysis of SSL/TLS deployment in mobile applications (2018) Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 209, pp. 189-199.

[15] Medeiros I., Beatriz M., Neves N., Correia M. Demonstrating a Tool for Injection Attack Prevention in MySQL (2017) Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, статья № 8023153, pp. 551-558.

[16] CVE-2011-5195. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5195 (Access date 01.04.2018)

[17] CVE-2011-5196. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5196 (Access date 01.04.2018)

[18] CVE-2011-5197. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5197 (Access date 01.04.2018)

[19] CVE-2012-1469. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1469 (Access date 04.04.2018)

[20] Larsson E., Sigholm J. Papering over the cracks: The effects of introducing best practices on the web security ecosystem (2016) International Conference on Information Networking, 2016-March, статья № 7427064, pp. 1-6.

[21] Starostenko O., Cruz-Perez C., Uceda-Ponga F., Alarcon-Aquino V. Breaking text-based CAPTCHAs with variable word and character orientation (2015) Pattern Recognition, 48 (4), pp. 1097-1108.

[22] Sivakorn S., Polakis I. and Keromytis A. D., "I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 388-403. doi: 10.1109/EuroSP.2016.37.

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.

Виталий Г. Иваненко, Никита В. Ушаков
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

ЗАЩИТА ИЗОБРАЖЕНИЙ ФОРМАТА JPEG ПРИ ПОМОЩИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

DOI: http://dx.doi.org/10.26583/bit.2018.2.09

Аннотация. В связи с бурным развитием мультимедийных технологий встает вопрос защиты авторского права произведений в цифровом виде, особенно изображений. Преимущества упрощенной передачи фотографий по сети перечеркиваются их возможным воровством или неправомерным размещением на других сайтах. Следовательно, необходимо защищать информацию различными техническими средствами, одним из таких средств и являются цифровые водяные знаки. Рассматриваются существующие методы защиты изображений при помощи цифровых водяных знаков, отмечается их главные преимущества и недостатки. Проводится сравнительный анализ данных методов встраивания цифровых водяных знаков в изображения. По итогам анализа выбран наиболее эффективный метод – метод дифференциального встраивания энергии. Отмечается, что данный метод лучше всего использовать для обеспечения целостности и ЦВЗ и контейнера. Система встраивания ЦВЗ должна предотвращать попытки злоумышленников изменять ЦВЗ и исходные данные в контейнере. Приводятся требования к ЦВЗ, встраиваемому для защиты изображений. Описываются основные атаки на изображение в формате JPEG. Изучаются модификации алгоритмов сокрытия данных в JPEG. Проводится исследование алгоритма ДЭВ на устойчивость. Под показателем устойчивости понимается специальное значение, расчет которого приводится в работе. Изучаются недостатки алгоритма ДЭВ, а также приводятся способы их устранения. При исследовании изображение со встроенным в него ЦВЗ подвергалось таким атакам, как сжатие, фильтрация, масштабирование. Делается вывод, что метод ДЭВ применим для защиты авторского права на изображения, при помощи данного метода возможно легко выявить каналы утечки информации при передаче изображений.

Ключевые слова: цифровые водяные знаки, дифференциальное встраивание энергии, изображения, встраивание информации, модификация алгоритма.

Для цитирования. ИВАНЕНКО, Виталий Г.; УШАКОВ, Никита В.. ЗАЩИТА ИЗОБРАЖЕНИЙ ФОРМАТА JPEG ПРИ ПОМОЩИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ. Безопасность информационных технологий, [S.l.], n. 2, p. 106-113, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Дата доступа: 06 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.09.

Vitaliy G. Ivanenko, Nikita V. Ushakov
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

JPEG digital watermarking for copyright protection

DOI: http://dx.doi.org/10.26583/bit.2018.2.09

Abstract. With the rapid growth of the multimedia technology, copyright protection has become a very important issue, especially for images. The advantages of easy photo distribution are discarded by their possible theft and unauthorized usage on different websites. Therefore, there is

a need in securing information with technical methods, for example digital watermarks. This paper reviews digital watermark embedding methods for image copyright protection, advantages and disadvantages of digital watermark usage are produced. Different watermarking algorithms are analyzed. Based on analysis results most effective algorithm is chosen – differential energy watermarking. It is noticed that the method excels at providing image integrity. Digital watermark embedding system should prevent illegal access to the digital watermark and its container. Requirements for digital watermark are produced. Possible image attacks are reviewed. Modern modifications of embedding algorithms are studied. Robustness of the differential energy watermark is investigated. Robustness is a special value, which formulae is given further in the article. DEW method modification is proposed, it's advantages over original algorithm are described. Digital watermark serves as an additional layer of defense which is in most cases unknown to the violator. Scope of studied image attacks includes compression, filtration, scaling. In conclusion, it's possible to use DEW watermarking in copyright protection, violator can easily be detected if images with embedded information are exchanged.

Keywords: digital watermarks, differential energy watermarking, images, embedding information, algorithm modification.

For citation. IVANENKO, Vitaliy G.; USHAKOV, Nikita V.. JPEG digital watermarking for copyright protection. IT Security (Russia), [S.l.], n. 2, p. 106-113, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Date accessed: 06 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.09.

Введение

На сегодняшний день широко распространена передача изображений через интернет. В связи с легкостью копирования изображений число нарушений авторских прав на такие работы неумолимо растет путем их размещения на торрентах и других пиратских сайтах. Таким образом, проблема защиты авторских прав на изображения является актуальной. Одним из основных технических средств защиты информации при её передаче в сети интернет является встраивание в защищаемый объект невидимых меток – цифровых водяных знаков (ЦВЗ) [1].

Одним из наиболее популярных форматов сжатия изображений является JPEG (Joint Photographic Experts Group). Данный алгоритм работает с областями 8x8 пикселей, на которых происходит плавное изменение яркости и цвета. Поэтому, если разложить матрицу данной области при помощи дискретного косинусного преобразования, то только первые коэффициенты будут значимыми. Это значит, по алгоритму JPEG изображение сжимается за счет плавности изменения цветов. В алгоритме используется дискретное косинусное преобразование(ДКП) для разложения, а также преобразования матриц коэффициентов 8x8 пикселей, в результате получается новая матрица коэффициентов. Также, применяется обратное преобразования для возвращения к исходному изображению. ДКП необходимо для разложения изображения по амплитудам частот, после дискретного косинусного преобразования получается матрица, большинство коэффициентов которой (кроме первых) близки к нулю. Следовательно, можно использовать квантование коэффициентов для их аппроксимации, при этом практически не теряя качество изображения [2].

В работе рассматриваются и анализируются наиболее распространённые алгоритмы внедрения ЦВЗ в формат изображений JPEG.

1 Алгоритм Куттера-Джордана-Боссена

Алгоритм Куттера-Джордана-Боссена (далее Kutter) является одним из наиболее эффективных методов встраивания информации в изображения [1].

Этот алгоритм впервые опубликован в 1998 году, однако и сейчас проводятся исследования данного алгоритма. Например, в исследованиях [2] предлагается

модифицировать алгоритм вводом дополнительных правил для устранения проблем извлечения данных. В работе [3] предлагается уменьшение изменения, которые ЦВЗ вносит в контейнер, что повышает надежность метода защиты. Также, предлагается модификация алгоритма на основе трёх составляющих цвета для повышения устойчивости алгоритма к различным видам атак, а также увеличения объема скрываемой информации в работе [4].

Суть алгоритма заключается в изменения яркости синей компоненты цветовой гаммы. Сокрытие информации основывается на наименьшей чувствительности человеческого зрения к синему цвету. Встраивание происходит по следующему принципу. Пусть z_i- — встраиваемый бит; *K — {R, G, B, P}* — контейнер; *p(x, y)* — текущая позиция (текущий пиксель) в координатной сетке контейнера.

В соответствии со спецификацией алгоритма JPEG яркость определяется следующей формулой:

$$l(p) = 0.299r(p) + 0.587g(p) + 0.114b(p). \quad (1)$$

Внедрение ЦВЗ осуществляется по формуле

$$\tilde{b}(p) = \begin{cases} b(p) - ql(p), \text{если } z_i = 0 \\ b(p) + ql(p), \text{если } z_i = 1 \end{cases}, \quad (2)$$

где q — параметр, определяющий энергию встраиваемого сигнала. Его величина прямо пропорциональна устойчивости и обратно пропорциональна скрытности вложения. Под устойчивостью понимается сохранение исходного ЦВЗ после различных воздействий на контейнер.

Обнаружение ЦВЗ выполняется на основании предсказания значения текущего пикселя на основании значений его соседей в пределах “пиксельного креста” размером 7x7 пикселей [2].

Оценка получается по следующей формуле:

$$\tilde{b}'(p) = \frac{1}{4c}\left(-2b'(p) + \sum_{i=-c}^{+c} b'(x+i, y) + \sum_{j=-c}^{+c} b'(x, y+j)\right), \quad (3)$$

где c - число пикселей сверху (снизу, слева и справа) от текущего пикселя. Если секретный бит встраивается r раз, то его значение находиться по формуле

$$\delta = -\frac{1}{r}\sum_{i=1}^{r} \tilde{b}_i{}'(p) - b_i(p). \quad (4)$$

При этом, нельзя гарантировать верное определение значения секретного бита, поскольку функция верификации не является обратной к функции внедрения.

Данный алгоритм может также использоваться для защиты видеозаписей при их распространении [5].

2 Метод замены наименее значащего бита(LSB)

Алгоритм встраивания LSB является самым популярным из-за его простоты.

Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ — это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения [6].

Популярность данного метода обусловлена его простотой и тем, что он позволяет

скрывать в относительно небольших файлах значительные объемы информации. Метод зачастую работает с растровыми изображениями, представленными в формате без компрессии, например, GIF и BMP. Метод НЗБ имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей [7].

Основной его недостаток — высокая чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто дополнительно применяют помехоустойчивое кодирование [8].

Для повышения устойчивости метода, а также более эффективного скрытия информации возможно использование данного метода совместно с криптографией [9].

3 Алгоритм ДЭВ

В основе рассматриваемого ниже метода лежит дифференциальное встраивание энергии (ДЭВ), под энергией при этом понимаются значение коэффициентов ДКП рассматриваемой области изображения, формула её расчета приводится чуть ниже.

Описанный в данной работе метод ДЭВ встраивает цифровой водяной знак, состоящий из l бит b_j $(j = 0, 1, 2, \ldots, l-1)$ в изображение. Каждый бит цифрового водяного знака внедряется в определенную область изображения, которая состоит из n блоков коэффициентов дискретного косинусного преобразования размера 8*8 [10].

В выбранную область изображения осуществляется встраивание бита ЦВЗ за счет модификации разности энергий D между высокочастотными (ВЧ) коэффициентами дискретного косинусного преобразования верхней и нижней части области. Подмножество ВЧ коэффициентов обозначается S(c). Если встраивается 0, то ВЧ коэффициенты нижней части области приравниваются к нулю, если 1, то верхней. ЦВЗ встраивается лишь за счет удаления определенных коэффициентов.

Для вычисления энергии субобласти A используется следующая формула:

$$E_{\mathrm{A}}(c, n, Q) = \sum_{d=0}^{n/2} \sum_{i \in S(c)} ([\theta_{i,d}]_{\mathrm{Q}})^2, \tag{5}$$

где $\theta_{i,d}$ - коэффициент ДКП с индексом i из d-го блока коэффициентов ДКП субобласти A; $[]_{\mathrm{Q}}$ — означает, что энергия вычисляется у квантованных коэффициентов. Вычислении энергии субобласти B осуществляется таким же образом.

Подмножество S(c) определяется на основе выбранного порога

$$\boldsymbol{S(c) = \{h \in 1, 63\} | (h \geq c)\}.}$$

Порог c показывает количество коэффициентов ДКП, которые не будут использоваться при встраивании, его необходимо выбрать при встраивании [11].

4 Сравнительные характеристики алгоритмов

В зависимости от решаемой задачи, используются различные алгоритмы. Если необходима проверка целостности файла-изображения, целесообразно использовать алгоритм, внедряющий хрупкий ЦВЗ, если необходимо передать секретное сообщение в файле-контейнере нужны уже другие характеристики для ЦВЗ, если необходимо подтверждение авторских прав на изображение, необходим выбор алгоритма, осуществляющий внедрение робастного ЦВЗ, устойчивого к атакам на контейнер и т д [12].

Для непосредственного выбора после описания характеристик, приведенных в таблице 1, даётся краткое заключение по каждому из алгоритмов.

Таблица 1. Алгоритмы сокрытия данных в JPEG

Название метода	Принцип работы	Преимущества	Недостатки
Kutter	Изменение яркости синей компоненты цветовой гаммы.	Устойчивость к сжатию, обрезке, изменения контрастности и фильтрации	Только для изображений с глубиной цвета 24 бита
LSB	Замена последнего бита	Невидимость ЦВЗ, высокая регулируемая пропускная способность	Уязвимость ко всем видам атак на контейнер[13]
ДЭВ	Модификация энергетической разности между коэффициентами блоков пикселей	Сложность удаления ЦВЗ, устойчивость к большинству виду атак	Низкая скорость встраивания ЦВЗ

Технология определения устойчивости того или иного алгоритма или стеганосистемы состоим из четырех шагов [14]:

1. Скрываемая информация внедряется в контейнер
2. Контейнер подвергается внешнему воздействию или атаке
3. Скрытая информация извлекается из контейнера
4. Извлеченная информация сравнивается с оригинальной и определяется степень их соответствия

Таблица 2. Устойчивость алгоритмов внедрения ЦВЗ в JPEG

Алгоритм	Сжатие	Масштабирование	Поворот	Обрезка
Kutter	+	–	–	+
LSB	–	–	–	–
ДЭВ	+	–	+	+

Наиболее перспективным для изображений формата JPEG является метод ДЭВ, так как он устойчив ко многим видам воздействий на контейнер. Кроме того, ЦВЗ, встроенный данным методом, невидим для человеческого глаза. Поэтому алгоритм ДЭВ был модифицирован и изучен более подробно.

5 Исследование алгоритма ДЭВ

Основные проблемы алгоритма ДЭВ:

– Высокочастотные коэффициенты ДКП легко отбрасываются фильтрами, в связи с чем алгоритм ДЭВ, использующий для внедрения ЦВЗ высокочастотные коэффициенты будет уязвим к этому воздействию на контейнер

– Алгоритм ДЭВ не учитывает, какое влияние на исходное изображение оказывает отбрасывание коэффициентов ДКП

Для решения этих проблемы предлагаются следующие модификации:

1. Алгоритм учитывает только низкочастотные АС коэффициенты ДКП и внедряет цифровой водяной знак в соответствии с предложенными масками яркости и контраста.

2. Алгоритм модифицирует коэффициенты ДКП только в соответствии с заранее рассчитываемом значении JND [15], что исключает вероятность искажения изображения из-за слишком высокой разности энергий D.

Также, было проведено исследование на устойчивость модифицированного алгоритма в соответствии с шагами, приведенными ранее. Оценку устойчивости проводилась при помощи коэффициента ошибочных бит BER (Bit Error Rate). Формула вычисления данного коэффициента имеет следующий вид:

$$\boldsymbol{BER}(\boldsymbol{S},\boldsymbol{S'}) = \frac{\sum \boldsymbol{p_i}}{\boldsymbol{N}}, \quad (6)$$

$$\text{где } p_i = \begin{cases} 1, & \text{если } s_j \neq s_j^m \\ 0, & \text{если } s_j = s_j^m. \end{cases}$$

s_j – j-й бит оригинала встраиваемой строки, S_j^m – бит извлеченной строки, N-общее количество бит цифрового водяного знака.

Если коэффициент BER=0, то внедряемая и извлеченная информация полностью идентичны. При BER=1 каждый бит извлеченного не соответствует оригинальному. Таким образом, при BER>0.5 ЦВЗ можно считать извлеченным полностью некорректно. Ошибки по большей части возникают на темных изображениях, где AC-коэффициентов (все коэффициенты, кроме первых, которые называются DC-коэффициентами) очень мало, или они вообще отсутствуют. Таким образом, на черном экране процент ошибок будет равен 50%, так как он высчитывается без исходной информации.

Таблица 3. Свойства изображений

	Разрешение (пиксели)
Изображение 1	1920*1200
Изображение 2	810*1080

Начнем с сжатия JPEG с потерями. Для проверки устойчивости к сжатию JPEG изображение-контейнер подвергалось сжатию JPEG во всем диапазоне значения коэффициента качества JPEG. Как можно увидеть из таблицы, оригинальный алгоритм не обладает достаточной устойчивостью к такого рода внешним воздействиям.

Таблица 4. Устойчивость к сжатию

Коэффициент качества JPEG(%)	100	90	80	70	60	50	40	30	20
Изображение 1(BER)	0.03	0.06	0.0.8	0.13	0.29	0.34	0.41	0.47	0.49
Изображение 2(BER)	0.04	0.07	0.0.7	0.15	0.31	0.37	0.39	0.40	0.47

Фильтрация является одним из наиболее вероятных внешних воздействий на контейнер с внедренным ЦВЗ, для исследования были выбраны 4 вида фильтров: низкочастотный фильтр, высокочастотный фильтр, усредняющий фильтр и контрастные фильтры, с размеров окна 3x3. Результаты приведены в таблице 4.

Таблица 5. Устойчивость к фильтрации

Фильтры	Низкочастотный	Высокочастотный	Усредняющий	Контрастный
Изображение 1(BER)	0.05	0.48	0.20	0
Изображение 2(BER)	0.04	0.46	0.22	0

В ходе эксперимента изображение восстанавливалось в оригинальный размер после масштабирования и потом производилось извлечение, результаты приведены в таблице 6.

Таблица 6. Устойчивость к масштабированию

Масштабирование(% от исходного изображения)	95	90	85	80
Изображение 1(BER)	0.34	0.41	0.47	0.49
Изображение 2(BER)	0.37	0.39	0.40	0.47

Из таблицы видно, что данный метод особенно уязвим к масштабированию даже после модификаций.

Заключение

На основании изложенного можно заключить, что метод ДЭВ применим для защиты авторского права на изображения, он обладает значительными преимуществами по сравнению с алгоритмами LSB и Куттера. Алгоритм LSB, не смотря на современные модификации обладает чрезвычайно низкой устойчивостью к атакам на контейнер, в связи с чем ЦВЗ, встроенный этим методом будет легко удален при передаче изображения по сети. при помощи данного метода возможно легко вычислить канал утечки информации. Проблемой же алгоритма Куттера является функция извлечения ЦВЗ – она не обратна функции встраивания, в связи с чем возникает проблема точного восстановления встроенного цифрового водяного знака. Алгоритм ДЭВ не обладает подобными недостатками, следовательно, он лучше обеспечивает защиту авторского права на изображения.

СПИСОК ЛИТЕРАТУРЫ:

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография: Стратегия развития информационного общества в РФ. М.: Солон-Пресс, 2009. - 265 с. - ISBN: 5-98003-011-5. С. 215–220.
2. А.Е. Дизер, Е.С. Дизер, Т.М. Опарина Модификация метода Куттера-Джордана-Боссена скрытого хранения информации в изображениях формата JPEG. Математические структуры и моделирование 2016. №3(39). С. 177-183.
3. Фомин Д.В. Модификация метода скрытия информации Куттера-Джордана-Боссена. Вестник Амурского государственного университета, 2014. Выпуск 65, Серия: естественные и экономические науки. С. 58-62.
4. Защелкин К.В. Усовершенствование метода скрытия данных Куттера-Джордана-Боссена. МНПК «Современные информационные и электронные технологи». 2013. с. 214-216.
5. Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganograhpic algorithm in video sequences. Young Researchers in Electrical and Electronic Engineering (ElConRus), 2017 IEEE Conference of Russian.
6. Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding. Proc. SPIE. — 1995. — Vol. 2420. — P.40.
7. Евсютин О.О. Модификация стеганографического метода LSB, основанная на использовании блочных клеточных автоматов. Информатика и системы управления, 2014, №1(39), с.15-22.
8. Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, №4, 2016, p.126-132.
9. Joshi K. Yadav R. A new LSB-S image steganography method blend with cryptography for secret communication. Third International Conference on Image Information Processing (ICIIP), 2015, p. 86-90.
10. Иваненко В.Г., Ушаков Н.В. Встраивание цифровых водяных знаков в видеозаписи. Безопасность информационных технологий — 2016. — №4. — с.21-24.
11. Ivanenko V. Ushakov N. Copyright protection for video content based on digital watermarking. BICA 2017: Biologically Inspired Cognitive Architectures (BICA) for Young Scientists p. 329-334.
12. Иваненко В.Г., Ушаков Н.В. Цифровые знаки в электронном документообороте. Безопасность информационных технологий — 2017. — №3. — с.37-42.
13. S.Tabasu Kannan, S.Azhagu Senthil A Frame work for various watermarking algorithms. Asian Journal of Computer Science and Technology ISSN 2249-0701 Vol.4, №1, 2015, p.21-28.

14. Abdullah Bamatraf, Rosziati Ibrahim, Mohd.Najib B. Mohd Salleh Digital watermaking algorithm using LSB. International Conference on Computer Application and Industrial Electronics (ICCAIE 2010), 2010, p.155-159.
15. Yaqing Niu, Matthew Kyan, Lin Ma, Azzedine Beghdadi, Sridhar Krishnan Visual salience's modulatory effect on just noticeable distortion profile and it's application in image watermarking. Signal Processing: Image Communication 28 (2013), p.917-928.

REFERENCES:

[1] Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography: Salon-Press Information society development strategy in Russia, 2009. (in Russian).
[2] A.E. Dizer, E.S. Dizer, T.M. Oparina Modification of The cutter-Jordan-Bossen method of hidden information storage in JPEG images. Mathematical structures and modeling 2016. №3(39). p. 177-183. (in Russian).
[3] Fomin D.V. Modification of method of concealment of information of Kutter-Jordan-Bossen. Bulletin of the Amur state University, 2014. Issue 65, Series: natural and economic Sciences. P. 58-62. (in Russian).
[4] Zashelkin K.V. Improved method of hiding data Cutter-Jordan-Bossen. International scientific-practical conference "Modern information and electronic technology». 2013. p. 214-216. (in Russian).
[5] Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganograhpic algorithm in video sequences. Young Researchers in Electrical and Electronic Engineering (ElConRus), 2017 IEEE Conference of Russian.
[6] Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding [Текст]. Proc. SPIE. — 1995. — Vol. 2420. — P.40.
[7] Evsyutin O.O. Modification of the steganographic method LSB, based on the use of block cellular automata. Informatics and control systems, 2014, №1(39), p.15-22 (in Russian).
[8] Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, №4, 2016, p.126-132.
[9] Joshi K. Yadav R. A new LSB-S image steganography method blend with cryptography for secret communication. Third International Conference on Image Information Processing (ICIIP), 2015, p. 86-90.
[10] Ivanenko V.G., Ushakov N.V. Embedding digital watermarks in video recording. Information technology security, 2016, №4, p. 21-24 (in Russian).
[11] Ivanenko V. Ushakov N. Copyright protection for video content based on digital watermarking. BICA 2017: Biologically Inspired Cognitive Architectures (BICA) for Young Scientists p. 329-334.
[12] Ivanenko V.G., Ushakov N.V. Digital watermarks in electronic document circulation. Bezopasnost' informacionnyh tekhnologij, 2017, №3, p. 37-42 (in Russian).
[13] S.Tabasu Kannan, S.Azhagu Senthil A Frame work for various watermarking algorithms. Asian Journal of Computer Science and Technology ISSN 2249-0701 Vol.4, №1, 2015, p.21-28.
[14] Abdullah Bamatraf, Rosziati Ibrahim, Mohd.Najib B. Mohd Salleh Digital watermaking algorithm using LSB. International Conference on Computer Application and Industrial Electronics (ICCAIE 2010), 2010, p.155-159.
[15] Yaqing Niu, Matthew Kyan, Lin Ma, Azzedine Beghdadi, Sridhar Krishnan Visual salience's modulatory effect on just noticeable distortion profile and it's application in image watermarking. Signal Processing: Image Communication 28 (2013), p.917-928.

Поступила в редакцию – 21 февраля 2018 г. Окончательный вариант –03 мая 2018 г.
Received – February 21, 2018. The final version – May 03, 2018.

Иван В. Нечта
Сибирский государственный университет телекоммуникаций и информатики,
ул. Кирова 86, Новосибирск, 630102, Россия
e-mail: ivannechta@gmail.com, http://orcid.org/0000-0003-0361-2742

НОВЫЙ МЕТОД СТЕГОАНАЛИЗА ТЕКСТОВЫХ ДАННЫХ, ПОЛУЧЕННЫХ КОДИРОВАНИЕМ ДЛИН СЕРИЙ СИНОНИМОВ

DOI: http://dx.doi.org/10.26583/bit.2018.2.10

Аннотация. В статье предложен новый метод стегоанализа, выявляющий текст, полученный методом кодирования длин серий синонимов. Анализируемый метод внедрения позволяет сохранять некоторые статистические свойства текста без изменений после внедрения скрытого сообщения. В частности, неизменными остаются: распределение вероятностей бит извлекаемого сообщения и распределение вероятностей использования синонимов текста, что обеспечивает высокую степень скрытности рассматриваемого метода внедрения. В ходе исследования было показано, что внедряемое сообщение изменяет статистическую структуру контейнера, и этот факт используется при стегоанализе. Разработанный стеготест сравнивает распределение вероятностей серий бит (с длиной не более 5 бит) в извлечённом из контейнера сообщении с эталонными распределениями, соответствующими пустому и заполненному контейнеру. Эталонные распределения были получены путём анализа 1000 контейнеров естественного текста, взятых из библиотеки Gutenberg Project. В работе рассматриваются два подхода к получению эталонных распределений. Первый подход предполагает анализ статистики сообщения, извлечённого из контейнера обычным способом (с помощью программы Tyrannosaurus Lex). Второй подход предполагает дополнительное преобразование сообщения в соответствии с анализируемым алгоритмом кодирования длин серий. Экспериментальные результаты позволяют утверждать о большей эффективности первого подхода. В качестве меры близости двух вероятностных распределений используется мера Кульбака-Лейблера. Показано, что реализованный метод позволяет обнаруживать наличие внедрения в контейнере с числом синонимов равным 500, при этом ошибка 1 рода равна 1.5%, ошибка 2 рода – 1.3%. По сравнению с известными аналогами предлагаемый метод имеет более высокую точность анализа при меньшем объёме входных данных.

Ключевые слова: стегоанализ, метод замены синонимов, tyrannosaurus lex.
Для цитирования. НЕЧТА, Иван В.. НОВЫЙ МЕТОД СТЕГОАНАЛИЗА ТЕКСТОВЫХ ДАННЫХ, ПОЛУЧЕННЫХ КОДИРОВАНИЕМ ДЛИН СЕРИЙ СИНОНИМОВ. Безопасность информационных технологий, [S.l.], n. 2, p. 114-120, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1118>. Дата доступа: 06 тау 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.10.

Ivan V. Nechta
Siberian state university of telecommunications and informatic sciences,
Kirova st., 86, Novosibirsk, 630102, Russia
e-mail: ivannechta@gmail.com,, http://orcid.org/0000-0003-0361-2742

New method of steganalysis for text data obtained by synonym run-length encoding

Abstract. In this article, we present a new stegoanalysis method for detecting a text obtained by the synonym Run-Length Encoding. The analyzed RLE-method allows us to keep some statistical properties of the text after a secret message embedding. In particular, the probabilities distribution of the bits in the extracted message and the probabilities distribution of using text synonyms keep unchanged, that ensures a high secrecy degree of the considered embedding method. In this paper we show that the embedded message changes the probabilities distribution

of bit-series lengths in the extracted message, and this fact is used for our stegoanalysis. It was shown that the embedded message breaks the statistical structure of the container, and this fact is used for the stegoanalysis. The constructed stegotest compares the probability distribution of runs (with length no more than 5 bits) in the message extracted from the container with reference distributions corresponding to an empty and embedded containers. Reference distributions were obtained by analysing of 1000 natural-text containers taken from the Gutenberg Project library. In this paper we consider two approaches for obtaining reference distributions. The first approach deals with analyzing the statistic of the message extracted from the container in the usual way (using the Tyrannosaurus Lex program). The second approach involves an additional decoding of the message in accordance with the analyzed run-length encoding algorithm. Experimental results allow us to assert that the first approach is more effective. The Kullback-Leibler measure is used as a divergence measure of two probability distributions. It was shown that the proposed method makes it possible to detect presence of the secret message in the container with a number of synonyms equal to 500, while false negative error is 1.5% and false positive error is 1.3%. In comparison with the known analogs, the proposed method demonstrates higher accuracy of analysis for a smaller size of input data.

Keywords: steganalysis, synonym substitution method, tyrannosaurus lex.

For citation. NECHTA, Ivan V.. New method of steganalysis for text data obtained by synonym run-length encoding. IT Security (Russia), [S.l.], n. 2, p. 114-120, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1118>. Date accessed: 06 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.10.

Введение

Классическая проблема стеганографии заключается в организации скрытого канала связи для обмена секретными сообщениями. Задача передачи скрытых данных впервые описана в работах Симмонса [1] и состоит в следующем. Пусть имеются два участника обмена сообщениями: Алиса и Боб. Их задача состоит в организации скрытой передачи данных под видом обычного обмена сообщениями. Постороннее лицо: Ева, анализирующая передаваемые сообщения, не должна заподозрить существование такого скрытого канала передачи данных. Алиса при помощи стеганографических алгоритмов встраивает секретное сообщение в безобидный на внешний вид объект данных, так называемый *контейнер*. Сам факт передачи контейнера по открытому каналу связи не является для Евы чем-то подозрительным. Боб, получив контейнер, сможет извлечь и прочитать секретное сообщение. Свойства стеганографических алгоритмов таковы, что Ева, подвергнув контейнер анализу, не сможет однозначно утверждать ни о наличии, ни об отсутствии факта внедрения скрытого сообщения.

На сегодняшний день известны различные методы стеганографии, использующие в качестве контейнера изображение, видео, аудио файлы и текст. Настоящее исследование посвящено методам текстовой стеганографии. Рассмотрим более подробно существующие методы внедрения скрытых данных в текстовые контейнеры, которые можно условно разделить на два класса.

Синтаксические методы. К данному классу принадлежат методы, например, описанные в работе [2], встраивающие в текст неотображаемые символы, дополнительные пробелы, которые в последствии не влияют на отображение текста. Существуют методы, например [3], использующие опечатки в определенных местах предложения. Данный класс методов является легко обнаружимым и в настоящее время активно не используются.

Семантические методы. В данный класс входят методы перефразирования предложений [4-5], в которых меняется форма их записи (активный, пассивный залог). Существуют методы, базирующиеся на переводе текста с одного языка на другой, например [6-7], в которых выбирается один из правильных вариантов перевода соответствующий скрываемому сообщению.

Известны методы генерации естественноподобных текстов по правилам контекстно-свободных грамматик языка, представленные в работе [8], такой текст является бессмысленным, но трудно обнаружимым (по сравнению с другими методами внедрения). Еще одним представителем данного класса является метод замены синонимов [9], в котором используется замена слов предложения на соответствующий скрываемому биту синоним. Смысл текста не меняется, но существует возможность нарушения устойчивых идиоматических выражений, что является недостатком метода.

Противоположной к задаче стеганографии является стегоанализ, заключающийся в выявлении факта передачи секретного сообщения. Считается, что синтаксические методы наиболее уязвимы к стегоанализу, так как легко обнаруживаются отклонения от грамматических правил языка в тексте. Семантические методы, напротив, являются более устойчивыми. Тем не менее, известно множество эффективных статистических методов анализа. Например, искусственно сгенерированный текст программой Texto [10] успешно обнаруживается в результате статистического анализа с помощью обычного архиватора, что описано в работе [11]. Известны методы, базирующиеся на статистических моделях n-грамматик (пар, троек словосочетаний), позволяющие проводить эффективный стегоанализ любых генерируемых текстов.

Метод замены синонимов успешно выявляется с помощью стегоанализа SVM-классификатором, представленного в работе [12]. Указанный метод базируется на анализе статистики встречаемости слов (синонимов) с определенным контекстом предложения. Для уменьшения статистических различий текста до и после внедрения, авторами статьи [13] была предложена модификация алгоритма замены синонимов. Во-первых, синоним выбирается с учётом вероятности его встречаемости в текстах английского языка. Во-вторых, встраивание бита скрытых данных осуществляется не в каждый синоним, а 0.3 бита на один синоним (в среднем), что понижает количество изменений исходного текста и, соответственно, нарушений его статистической структуры. В-третьих, известно, что распределение вероятностей бит сообщения, взятого из пустого и заполненного контейнера, при внедрении предыдущим методом [9] отличаются (что используется в стегоанализе [14]). Указанный алгоритм [13] позволяет сохранить соотношение изменённых нулевых и единичных бит. Согласно проведенным экспериментам стеготексты, полученные данным алгоритмом, практически не обнаруживаются при стегоанализе (ошибка при обнаружении стегоконтейнера достигает 90.27%).

В данном исследований предлагается метод стегоанализа текстов, полученных кодированием длин серий синонимов [13]. Анализируемый алгоритма внедрения использует длины серии бит (последовательность равных бит) для встраивания скрытых данных. Если серия имеет четную длину – внедрён ноль, нечетную – единица. Таким образом, меняя длину серий, встраивается секретное сообщение. Однако алгоритм имеет одну особенность, которая заключается в том, что при внедрении две стоящие подряд серии единичной длины удаляются (сливаясь в единую серию). Следовательно, стоит ожидать, что распределение вероятностей серий единичной длины у пустого и заполненного контейнера могут различаться. В настоящем исследовании реализуется данная идея для стегоанализа.

Описание предлагаемого метода. В рамках данного исследования рассматриваются два подхода к стеготесту. Оба варианта работают по одному и тому же алгоритму, представленному ниже, и отличаются только способом извлечения сообщения. Рассмотрим более подробно алгоритм стегоанализа.

Алгоритм 1. Алгоритм стегоанализа

Шаг 1. Извлечение сообщения из контейнера.

Шаг 2. Разбиение сообщения на элементы и расчет статистики.

Шаг 3. Классификация.

На первом шаге для извлечения сообщения из анализируемого контейнера мы используем исходную программу Tyrannosaurus Lex [9]. После извлечения сообщения получим *промежуточную* последовательность, состоящую из символов алфавита $A = \{0,1\}$. В первом подходе, мы используем для анализа *промежуточную* последовательность. Во втором подходе мы декодируем *промежуточную* последовательность в соответствии с алгоритмом кодирования длин серий [13] (назовем полученную последовательность *конечной*) и анализируем её.

Вторым шагом мы разбиваем извлечённое из контейнера сообщение на элементы. Предварительно введем следующее определение. *Серией* называется битовая последовательность $R = b_1, b_2, \dots, b_N : b_1 = b_2 = \dots = b_N;\ b \in \{0,1\}$. Здесь длина серии равна N.

В качестве элементов используются серии длины N, где $N \in [1; 5]$. После разбиения сообщения на элементы рассчитаем распределение их вероятностей. При обнаружении серии с длиной $N > 5$, она отбрасывалась и не учитывалась.

Для выполнения Шага 3 мы будем сравнивать полученное распределение со специальными эталонными распределениями, соответствующими пустому и заполненному контейнеру. Если полученное распределение «ближе» к эталонному распределению пустого контейнера, то анализируемый контейнер также признается пустым, в противном случае – признается заполненным. В качестве меры близости двух вероятностных распределений будем использовать меру Кульбака-Лейблера [15]. В ходе эксперимента использовались другие меры, но они оказались менее эффективны, чем упомянутая. Поэтому здесь будет рассмотрена только одна мера.

Далее рассмотрим процесс получения эталонных распределений. В качестве пустых контейнеров были подготовлены текстовые файлы, полученные из текстов архива Gutenberg Project [16], в количестве 1000 штук. Затем из контейнера извлекалась и анализировалась битовая последовательность в соответствии с Шагом 1 и 2 предлагаемого Алгоритма 1. Размер анализируемой последовательности составлял 1000 бит. Из полученных распределений вероятностей (обозначим их $Q_j = \{q_{j,1}, \dots, q_{j,N}\}$) вычислялось среднее арифметическое распределение (обозначим его $P = \{p_1, \dots, p_N\}$) согласно формуле 1, которое затем нормировалось. Нормировка необходима для выполнения требования о том, чтобы сумма вероятностей распределения равнялась единице. Таким образом, было получено эталонное распределение вероятностей, соответствующего пустому контейнеру. Здесь i - соответствует индексу вероятности элемента в распределении, j – соответствует номеру файла.

$$p_i = \frac{\sum_{j=1}^{1000} q_{j,i}}{1000} \quad (1)$$

Для получения эталонного распределения вероятностей, соответствующего заполненному контейнеру, производилось внедрение секретного сообщения в контейнер. Так как передаваемое сообщение предварительно шифруется и известно, что зашифрованное сообщение должно выглядеть неотличимым от истинно случайной последовательности (т.е. вероятности его бит равны 0.5 и между их появлением отсутствуют какие-либо закономерности), то мы имитировали секретное сообщение последовательностью, полученной из генератора псевдослучайных чисел.

Внедрение скрытого сообщения производилось по предложенному в работе [13] алгоритму. Далее сообщение обрабатывалось согласно Шагу 2 и 3 вышеописанного Алгоритма 1. В результате были получены следующие распределения вероятностей, представленные в таблице 1.

Таблица 1. Эталонные распределения вероятностей

Состояние	Анализируемая	Распределение вероятностей

контейнера	последовательность	
Пустой	промежуточная	{52.71, 24.39, 12.36, 6.77, 3.77}
Заполненный	промежуточная	{33.76, 35.58, 16.14, 9.63, 4.89}
Пустой	конечная	{55.16, 22.54, 12.05, 6.09, 4.16}
Заполненный	конечная	{51.62, 25.81, 12.90, 6.45, 3.22}

Из данных, представленных в таблице 1, видно, что количество серий в контейнере убывает с возрастанием её длины. Поэтому в тесте анализ проводится только по сериям с длиной не более 5 бит. Остальные серии при анализе не учитывались.

Анализ полученных результатов также позволяют утверждать, что стеготест на базе статистики промежуточной последовательности будет давать меньше ошибок, т.к. распределения вероятностей находятся «дальше» друг от друга. Для промежуточной последовательности (от пустого до заполненного) расстояние между распределениями вероятностей составляет 10.98, для конечной – 0.72. Далее мы будем рассматривать только один подход (на базе анализа промежуточной последовательности).

Экспериментальное исследование эффективности стегоанализа. Считается, что эффективность методов стегоанализа определяется его ошибками. Обычно используются следующие ошибки. Ошибка 1-го рода: случай, когда заполненный контейнер воспринимается как пустой. Ошибка 2-го рода: случай, когда пустой контейнер воспринимается как заполненный. Другой мерой ошибок, например, используемой в работе [13], является $Recall\ Rate\ (rr)$:

$$rr = \frac{tp}{tp+fn}, \tag{2}$$

где tp – количество правильно обнаруженных стегоконтейнеров, fn – количество стегоконтейнеров ошибочно распознанных как пустые контейнеры. Очевидно, что ошибка 1 рода (обозначим её как E_1) связана с $Recall\ Rate$ следующей зависимостью:

$$rr = 1 - E_1 \tag{3}$$

Для проведения экспериментальной оценки эффективности предложенного метода были отобраны тексты из архива Gutenberg Project [16], отличные от тех, которые использовались для получения эталонных распределений. Извлечение сообщения и заполнение контейнера проводилось с помощью программных средств, разработанных автором данной работы, по алгоритмам, описанным в предыдущей главе.

В результате были получены значения ошибок анализа 1000 контейнеров, представленные в таблице 2. В связи с тем, что объём внедрения в контейнеры одного размера может существенно отличаться (в зависимости от длины серий), то принято решение рассчитывать ошибку относительно длины *промежуточной* последовательности, что позволит осуществить объективную оценку результатов эксперимента.

Таблица 2. Результаты стегоанализа

Ошибки стегоанализа	Длина промежуточной последовательности, бит				
	100	200	300	400	500
Ошибка 1 рода	5.8%	3.9%	2.5%	1.4%	1.5%
Ошибка 2 рода	17.9%	6.1%	3.1%	1.6%	1.3%

Сравним полученные данные с результатами, представленными в работе [13]. Здесь используется SVM-классификатор, предложенный для стегоанализа текстовых данных в статье [12]. Согласно представленным авторами данным среднее количество синонимов в контейнере – 1738, что соответствует промежуточной последовательности размером в

1738 бит. Значение $Recall\ Rate$ на указанной длине составляет 9.73%, следовательно, ошибка 1 рода равна 90.27%.

Из анализа результатов, представленных в таблице 2 можно утверждать, что предлагаемый в данной работе стеготест существенно превосходит вышеупомянутый стегоанализ (SVM-классификатором) по эффективности, т.к. имеет меньше ошибок на более коротких анализируемых последовательностях.

Заключение.

В ходе работы был предложен метод стегоанализа текстовых данных, полученных кодированием длин серий синонимов [13]. Было установлено, что при внедрении указанным методом нарушается статистическая структура извлекаемого сообщения. В настоящей статье продемонстрировано, что для анализа статистических различий следует использовать промежуточную последовательность.

Полученные в результате эксперимента данные позволяют утверждать об эффективности предложенного метода стегоанализа. Реализованный алгоритм превосходит известные аналоги по точности обнаружения факта внедрения при меньших объёмах входных данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Simmons G.J. The prisoners problem and the subliminal channel. In Advances in Cryptology Proceedings of Crypto 83. Plenum Press: 1984. P. 51-67.
2. Koluguri A., Gouse S., Reddy P. B. Text steganography methods and its tools. Int. J. Adv. Sci. Tech. Res. 2014. V. 2. No. 4. P. 888-902.
3. Judge J. C. Steganography: past, present, future. Lawrence Livermore National Lab., CA (US), 2001. – №. UCRL-ID-151879.
4. Atallah M. et al. Natural language watermarking: Design, analysis, and a proof-of-concept implementation. Information Hiding. – Springer Berlin/Heidelberg, 2001. P. 185-200.
5. Meral H. M. et al. Natural language watermarking via morphosyntactic alterations. Computer Speech & Language. 2009. V. 23. No. 1. P. 107-125.
6. Grothoff C. et al. Translation-based steganography. International Workshop on Information Hiding. – Springer, Berlin, Heidelberg. 2005. P. 219-233.
7. Stutsman R. et al. Lost in just the translation. Proceedings of the 2006 ACM symposium on Applied computing. – ACM. 2006. P. 338-345.
8. Chapman M., Davida G. Hiding the hidden: A software system for concealing ciphertext as innocuous text. International Conference on Information and Communications Security. – Springer Berlin/Heidelberg, 1997. P. 335-345.
9. Winstein K. Lexical steganography through adaptive modulation of the word choice hash. URL: http://web.mit.edu/keithw/tlex/ (дата обращения: 20.01.2018).
10. Сайт программы «Texto». URL: http://www.nic.funet.fi/pub/crypt/steganography/texto.tar.gz (дата обращения: 20.01.2018).
11. Нечта И.В. Эффективный метод стегоанализа базирующийся на сжатии данных. Вестник СибГУТИ. 2010. №1. С. 50-55.
12. Xiang L. et al. Linguistic steganalysis using the features derived from synonym frequency. Multimedia tools and applications. 2014. V. 71. No. 3. P. 1893-1911.
13. Xiang L. et al. A novel linguistic steganography based on synonym run-length encoding. IEICE transactions on Information and Systems. 2017. V. 100. No. 2. P. 313-322.
14. Нечта И. В. Применение статистического анализа для обнаружения скрытых сообщений в текстовых данных. Вестник СибГУТИ. 2012. №. 1. С. 29-36.
15. Kullback S. Information Theory and statistics. — N. Y.: Dover Publications, 1997. — 399 p.
16. Сайт «Gutenberg Project». URL: http://www.gutenberg.org/wiki/Main_Page (дата обращения: 20.01.2018).

REFERENCES:

[1] Simmons G.J. The prisoners problem and the subliminal channel. In Advances in Cryptology Proceedings of Crypto 83. Plenum Press: 1984. P. 51-67.
[2] Koluguri A., Gouse S., Reddy P. B. Text steganography methods and its tools. Int. J. Adv. Sci. Tech. Res. 2014. V. 2. No. 4. P. 888-902.
[3] Judge J. C. Steganography: past, present, future. Lawrence Livermore National Lab., CA (US), 2001. – №. UCRL-ID-151879.
[4] Atallah M. et al. Natural language watermarking: Design, analysis, and a proof-of-concept implementation. Information Hiding. – Springer Berlin/Heidelberg, 2001. P. 185-200.
[5] Meral H. M. et al. Natural language watermarking via morphosyntactic alterations. Computer Speech & Language. 2009. V. 23. No. 1. P. 107-125.
[6] Grothoff C. et al. Translation-based steganography. International Workshop on Information Hiding. – Springer, Berlin, Heidelberg. 2005. P. 219-233.
[7] Stutsman R. et al. Lost in just the translation. Proceedings of the 2006 ACM symposium on Applied computing. – ACM. 2006. P. 338-345.
[8] Chapman M., Davida G. Hiding the hidden: A software system for concealing ciphertext as innocuous text. International Conference on Information and Communications Security. – Springer Berlin/Heidelberg, 1997. P. 335-345.
[9] Winstein K. Lexical steganography through adaptive modulation of the word choice hash. URL: http://web.mit.edu/keithw/tlex/ (дата обращения: 20.01.2018).
[10] Website «Texto». URL: http://www.nic.funet.fi/pub/crypt/steganography/texto.tar.gz (accessed 20.01.2018).
[11] Nechta I. V. Effective method of steganalysis based on the data compression. Vestnik SibSUTI. 2010. №1. P. 50-55. (in Russian).
[12] Xiang L. et al. Linguistic steganalysis using the features derived from synonym frequency. Multimedia tools and applications. 2014. V. 71. No. 3. P. 1893-1911.
[13] Xiang L. et al. A novel linguistic steganography based on synonym run-length encoding. IEICE transactions on Information and Systems. 2017. V. 100. No. 2. P. 313-322.
[14] Nechta I.V. Primenenie statisticheskogo analiza dlya obnaryjeniya skritih soobschenii v textovih dannih [Applying Statistical Methods for Secret Message Detection in Text Data]. Vestnik of SibSUTIS. 2012. №. 1. P. 29-36. (in Russian).
[15] Kullback S. Information Theory and statistics. — N. Y.: Dover Publications, 1997. — 399 p.
[16] Website «Gutenberg Project». URL: http://www.gutenberg.org/wiki/Main_Page (accessed 20.01.2018).

Поступила в редакцию – 23 марта 2018 г. Окончательный вариант – 04 мая 2018 г.
Received – March 23, 2018. The final version –May 04, 2018.

АННОТАЦИИ

Анатолий В. Марченко[1], Валерий Ю. Войналович[2], Сергей Н. Воронин[2]

[1]Федеральная служба по техническому и экспортному контролю,
105175, г. Москва, Старая Басманная, 17
e-mail: anatolijlev@yandex.ru, https://orcid.org/0000-0002-0207-6274
[2]Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю,
394020, г. Воронеж, ул. 9 Января, д. 280а
e-mail: niii1zi@yandex.ru, https://orcid.org/0000-0002-1848-1346
e-mail: snv-36@mail.ru, https://orcid.org/0000-0002-1002-0799

АНАЛИЗ СОСТОЯНИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Актуальность проведения анализа нынешнего состояния системы подготовки специалистов в области информационной безопасности, обусловлена необходимостью совершенствования кадрового обеспечения в этой, безусловно, приоритетного направления деятельности Российской Федерации в условиях нарастания новых вызовов и угроз в информационной сфере. Материалы статьи представляют собой результаты анализа и обобщения данных о состоянии системы подготовки, профессиональной переподготовки и повышения квалификации специалистов, работающих в области информационной безопасности в интересах различных государственных структур от органов государственной власти до подведомственных им организаций. Исследование охватывает анализ таких основных компонент сферы оказания профессиональных образовательных услуг, как среднее профессиональное образование и высшую школу (бакалавриат, магистратуру и специалитет), исключая вопросы подготовки высококвалифицированных кадров через аспирантуру и системы переподготовки и повышения квалификации. Представленные аналитические материалы могут быть использованы, в частности, при разработке предложений по совершенствованию отечественной системы подготовки при формировании контрольных показателей приема граждан на обучение за счет бюджетных ассигнований федерального бюджета по направлениям подготовки и специальностям в области информационной безопасности.
Ключевые слова: Информационная безопасность, подготовка кадров, контрольные цифры приема, обеспеченность кадрами.

Дмитрий А. Мельников[1], Григорий П. Гавдан[2], Иван А. Корсаков[3]

[1]Федеральный исследовательский центр «Информатика и управление» РАН,
Россия, 119333, Москва, Вавилова, д.44, кор.2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]Национальный исследовательский ядерный университет «МИФИ»,
115409, Москва, Каширское шоссе, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]ГлавНИВЦ Управления Делами Президента Российской Федерации,
125009, г. Москва, Славянская площадь, д. 4, стр. 1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

К ВОПРОСУ О ЦЕЛИ И ЗАДАЧАХ НАЦИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ИНИЦИАТИВЫ США В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Аннотация. В текущем году Россия вступила в трехлетний переходный период ввода в действие профессиональных стандартов, призванных заменить традиционные нормативные указания

Единого квалификационного справочника должностей руководителей, специалистов и служащих (ЕКС). Несколько профстандартов утверждены и для области кадрового обеспечения информационной безопасности.
Однако с позиций высшей школы существующий массив утвержденных профстандартов затруднительно использовать в качестве нормативной основы для совершенствования и развития существующей системы образовательных стандартов по направлению информационная безопасность, хотя такая очевидная концептуальная задача была поставлена в рамках перехода от ЕКС к профстандартам.
В настоящей работе проанализирован зарубежный опыт по решению указанной задачи на достаточно впечатляющем примере США. В рамках национальной образовательной инициативы в области кибербезопасности было проведено системное исследование структуры трудовых (кадровых) ресурсов в изучаемой области, предлагаемое в качестве фундаментального справочного ресурса. Он может быть использован для ориентации пользователей различных категорий, включая образовательные организации, для решения своих задач обеспечения трудовыми ресурсами в области кибербезопасности.
Компонентами системной кадровой структуры в области кибербезопасности выступают такие категории, как специализации/специальности, функциональные должности, компетенции (знания, умения, навыки) и функциональные обязанности (или задачи, решаемые при исполнении той или иной должности).
В работе проанализирована представленная структура трудовых ресурсов в области кибербезопасности, её содержание, а также рассмотрено её значение для гармонизации отечественных образовательных стандартов в сфере кибербезопасности.
Ключевые слова: кибербезопасность, образование, трудовые ресурсы, компетенции, знания, умения, навыки, специальности, функциональные обязанности, функциональные должности.

Александр А. Голяков[1], Анатолий П. Дураковский[2], Егор А. Симахин[2]

[1]Учебный центр безопасности информации «МАСКОМ»,
119421, Москва, ул. Новаторов, д.40 корп.1
e-mail: gaa66@mail.ru, https://orcid.org/0000-0002-8715-3477
[2]Национальный исследовательский ядерный университет «МИФИ»,
115409, г. Москва, Каширское шоссе, 31
e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735
e-mail: dekryt@mail.ru, https://orcid.org/0000-0003-4019-9694

ПРИМЕНЕНИЕ ГЕНЕРАТОРА ЗАМЕЩЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ РЕАЛЬНОГО ЗАТУХАНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Аннотация. Наиболее трудоемкими операциями при оценке защищенности информации от ее утечки за счет побочных электромагнитных излучений (ПЭМИ) являются работы, связанные с определением реального затухания излученного информативного сигнала. Большой интерес представляет собой задача автоматизации данного вида измерений. На измерение затухания с помощью существующих автоматизированных комплексов требуется значительное время. Поэтому, как правило, измерения проводятся только **на** ограниченном количестве частот. Вместе с тем, спектр одиночного информативного импульса имеет лепестковую структуру и в каждом частотном лепестке является сплошным. Соответственно измерение значений затухания напряженности электромагнитного поля на отдельных частотах не отражает полноту характеристики затухания. Если же проводить измерения затухания по всему спектру информативного сигнала в заданном диапазоне частот, то необходимо провести несколько тысяч измерений, что делает такой подход не эффективным с точки зрения временных затрат. Современные специализированные автоматизированные измерительные системы (САИС) контроля защищенности по каналам ПЭМИ имеют режим измерения шума системы активной защиты, который можно использовать для измерения реального затухания. В

данной работе описан и экспериментально подтвержден более точный и быстрый способ измерения реального затухания информативного сигнала на примере видеоподсистемы монитора с электронно-лучевой трубкой (ЭЛТ) с использованием САИС «Сигурд» и генератора замещения. Применение генератора замещения в автоматизированных измерениях позволяет существенно сократить временные затраты на проведение специальных исследований (СИ) по контролю защищенности информации от утечки за счет ПЭМИ.

Ключевые слова: генератор замещения, информационная безопасность, побочные электромагнитные излучения, реальное затухание.

Сергей А. Климачев, Наталья А. Тишина

Оренбургский государственный университет,
пр-т Победы, 13, г. Оренбург, 460018, Россия
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru https://orcid/0000-0002-7341-6985

МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ТОЧНОСТИ ОБНАРУЖЕНИЯ АТАК ОБЛАЧНОЙ СРЕДЫ

Аннотация. Статья посвящена исследованию вопроса оценки эффективности систем обнаружения атак (СОА), применяемых для защиты вычислительных платформ, характеризующихся динамичностью, сложной организационно-технической структурой и наличием большого количества разнородных параметров ее компонент. Анализ существующих методик оценки СОА позволил выявить проблемы, в частности недостатки в обосновании количественных метрик, отражающих производительность, достоверность принимаемых решений СОА, что затрудняет доказуемость методики оценки СОА. Целью исследования является: повышение объективности оценки СОА, достичь которую можно с помощью разработки правильной методики и инструментов оценки, а также надежного экспериментального стенда. В статье предложены результаты разработки и апробации методики и программного обеспечения оценки эффективности СОА на основе построения оптимального множества количественных показателей точности обнаружения атак, позволяющие решать задачи сравнительного анализа СОА, обладающих схожими функциональными возможностями. В результате проведенных исследований решены следующие задачи: выбор универсальных количественных показателей для оценки точности обнаружения атак СОА; определение обобщенного показателя точности обнаружения атак на основе построения парето-оптимального множества наборов значений количественных показателей, отражающих обеспечение конфиденциальности, целостности и доступности информации и информационных ресурсов облачной среды; разработка функциональной модели, схемы и программного обеспечения экспериментального исследования СОА облачной среды.

Ключевые слова: оценка эффективности, количественные показатели эффективности, системы обнаружения атак, облачная среда.

Игорь Ю. Жуков, Олег Н. Мурашов

ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

ЗАЩИЩЕННЫЕ ПРОЦЕДУРЫ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ, ФОРМИРОВАНИЯ КЛЮЧА ФИСКАЛЬНОГО ПРИЗНАКА И ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ

Аннотация. В статье дается описание криптографических механизмов взаимной аутентификации и формирования ключа фискального признака. Эти механизмы основаны на

использовании блочного шифра «Кузнечик», определенного национальным стандартом Российской Федерации ГОСТ Р 34.12–2015 и реализованного в режиме гаммирования в соответствии ГОСТ Р 34.13–2015. Функции выработки имитовставки (кода аутентификации) заданы рекомендациями по стандартизации Р 50.1.113–2016.

Предлагаемое в данной работе решение направлено на обеспечение аутентификации и контроля целостности фискальных данных, передаваемых по каналам связи между фискальными накопителями и операторами фискальных данных, а также между операторами фискальных данных и уполномоченным органом. Форматы передаваемых фискальных данных, способы передачи фискальных данных и механизмы обеспечения конфиденциальности передаваемых фискальных данных определяются уполномоченным органом федеральной исполнительной власти.

В статье дано краткое описание модели протокола, проведен формальный анализ пассивных атак в предположении, что криптографическая стойкость исследуемого протокола зависит от стойкости используемых в нем криптографических преобразований, являющихся отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации. Так как указанные криптографические преобразования не могут быть скомпрометированы нарушителем, можно сделать вывод, что нарушителем также не может быть скомпрометирован и исследуемый протокол.

Ключевые слова: взаимная аутентификация, криптографические преобразования, мастер-ключ, фискальный признак, защита фискальных данных.

Буян С. Донгак

Томский государственный университет систем управления и радиоэлектроники,
ул. Ленина, д. 40, г. Томск, 634050, Россия
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ ОРГАНИЗАЦИИ

Аннотация. В статье рассмотрен вопрос мониторинга сетевой активности рабочих компьютеров сотрудников для обеспечения информационной безопасности организации от внешних угроз, связанных с использованием аппаратного и программного обеспечения иностранного производства, в том числе и информационными сервисами, которые собирают разного рода информацию о пользователях сети Интернет. Показаны основные проблемы, возникающие в процессе выполнения анализа защищенности организации в сфере информационной безопасности (далее – ИБ). Приведен краткий обзор существующих инструментальных решений мониторинга сетевого трафика. Проведен эксперимент в использовании аппаратных и программных средств иностранного производства в организации. Эксперимент направлен на выявление негативных факторов, влияющих на информационную безопасность. Представлены результаты эксперимента. Сделаны выводы о недостатках методов и средств информационной защиты, а также рассмотрен вопрос оптимального соотношения использования инструментария фильтрации сетевого трафика.

Ключевые слова: межсетевой экран, мониторинг трафика, сетевая активность, информационная безопасность.

Александр В. Мамаев[1], Кристина В. Мамаева[2]

[1]ООО «Лаборатория Цифровой Форензики»,
115191, Москва, Духовской переулок, дом 17, пом I ком 2а
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]Национальный Исследовательский Университет «Высшая Школа Экономики»,
101000, г. Москва, ул. Мясницкая, д. 20
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

КАК ЭКОСИСТЕМА ВИРТУАЛЬНЫХ АССИСТЕНТОВ МОЖЕТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. Количество преступлений, совершаемых в информационной сфере, постоянно возрастает. Одновременно возрастает совокупный ущерб, наносимый деятельностью киберпреступников: с 1,5 трлн долл. в 2015 году до 2 трлн. долл. к 2019 году. На этом фоне законодательство Европейского Сообщества в области защиты персональных данных, сформированное еще в 1990-е годы, ждут самые кардинальные изменения, что наверняка повлияет на позиции других стран. Персональные данные интернет-пользователей давно превратилось в объект купли-продажи на рынке электронной коммерции. Манипуляции с персональными данными вызывают серьезные возражения со стороны самих пользователей. Власти озабочены сохранностью и конфиденциальностью данных в соответствии с законодательством. Несмотря на это, количество инцидентов, связанных с утечкой или некорректным использованием персональных данных, возрастает по экспоненте: в декабре 2017 года юристы Hill Dickinson подали коллективный иск к Google, недовольные незаконным сбором персональных данных владельцев iPhone. Следом под удар попала компания Uber Technologies, несанкционированно рассылавшая SMS-оповещения клиентам. В марте 2018 года оправдываться за утечку данных 80 млн аккаунтов пришлось соцсети Facebook. Авторы статьи рассмотрели возможности внедрения экосистемы виртуальных ассистентов и технологии блокчейна для безопасной и деперсонализированной обработки персональных данных с последующим использованием, что открывает неожиданные перспективы перед machine-to-machine-marketing.
Ключевые слова: виртуальный ассистент, блокчейн, персональные данные, электронная коммерция.

Антон А. Абрамов[1], Виктор С. Горбатов[2], Марина Н. Гришина[3]

[1]ФГУП «Главный научно-исследовательский вычислительный центр» Управления делами Президента Российской Федерации,
г. Москва, 121471, ул. Рябиновая, д. 43, корп. 1
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]ФГБУ НМИЦ имени академика В.И. Кулакова Министерства здравоохранения Российской Федерации,
ул. Академика Опарина, 4, г. Москва, 117198, Россия
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ВЕБ-ПОРТАЛА НА ПЛАТФОРМЕ OPEN JOURNAL SYSTEMS

Аннотация. В этой статье рассматриваются основные угрозы безопасности веб-порталам, построенным на платформе Open Journal Systems. Платформа Open Journal Systems (далее

OJS), изначально разработанная в рамках проекта Public Knowledge Project, является одной из самых популярных открытых платформ для электронных журналов. На 2016 год исходя из данных, которыми располагает проект Public Knowledge Project, насчитывается более 10 тысяч активных журналов, использующих платформу OJS. Для журнала переход на такую продвинутую и сложную платформу, которая позволяет полностью перенести весь рабочий процесс на единый веб-портал, является серьезным шагом и на него идут рецензируемые журналы, входящий в российские и зарубежные системы цитирования, а потому вопрос сохранности содержимого статей до их публикации очень важен для самого журнала, так и для авторов, которые хотят в журнале публиковаться. В этой работе рассматриваются наиболее актуальные угрозы для веб-порталов на платформе OJS, описана частная модель угроз безопасности, а также предложены меры, которые позволяют нейтрализовать эти угрозы.
Ключевые слова: частная модель угроз, модель нарушителя, веб-портал, угрозы информационной безопасности, меры защиты, php, xss, open journal systems.

Виталий Г. Иваненко, Никита В. Ушаков

Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409 , Россия
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

ЗАЩИТА ИЗОБРАЖЕНИЙ ФОРМАТА JPEG ПРИ ПОМОЩИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Аннотация. В связи с бурным развитием мультимедийных технологий встает вопрос защиты авторского права произведений в цифровом виде, особенно изображений. Преимущества упрощенной передачи фотографий по сети перечеркиваются их возможным воровством или неправомерным размещением на других сайтах. Следовательно, необходимо защищать информацию различными техническими средствами, одним из таких средств и являются цифровые водяные знаки. Рассматриваются существующие методы защиты изображений при помощи цифровых водяных знаков, отмечается их главные преимущества и недостатки. Проводится сравнительный анализ данных методов встраивания цифровых водяных знаков в изображения. По итогам анализа выбран наиболее эффективный метод – метод дифференциального встраивания энергии. Отмечается, что данный метод лучше всего использовать для обеспечения целостности и ЦВЗ и контейнера. Система встраивания ЦВЗ должна предотвращать попытки злоумышленников изменять ЦВЗ и исходные данные в контейнере. Приводятся требования к ЦВЗ, встраиваемому для защиты изображений. Описываются основные атаки на изображение в формате JPEG. Изучаются модификации алгоритмов сокрытия данных в JPEG. Проводится исследование алгоритма ДЭВ на устойчивость. Под показателем устойчивости понимается специальное значение, расчет которого приводится в работе. Изучаются недостатки алгоритма ДЭВ, а также приводятся способы их устранения. При исследовании изображение со встроенным в него ЦВЗ подвергалось таким атакам, как сжатие, фильтрация, масштабирование. Делается вывод, что метод ДЭВ применим для защиты авторского права на изображения, при помощи данного метода возможно легко выявить каналы утечки информации при передаче изображений.
Ключевые слова: цифровые водяные знаки, дифференциальное встраивание энергии, изображения, встраивание информации, модификация алгоритма.

Иван В. Нечта

Сибирский государственный университет телекоммуникаций и информатики,
ул. Кирова 86, Новосибирск, 630102, Россия
e-mail: ivannechta@gmail.com, http://orcid.org/0000-0003-0361-2742

НОВЫЙ МЕТОД СТЕГОАНАЛИЗА ТЕКСТОВЫХ ДАННЫХ, ПОЛУЧЕННЫХ КОДИРОВАНИЕМ ДЛИН СЕРИЙ СИНОНИМОВ

Аннотация. В статье предложен новый метод стегоанализа, выявляющий текст, полученный методом кодирования длин серий синонимов. Анализируемый метод внедрения позволяет сохранять некоторые статистические свойства текста без изменений после внедрения скрытого сообщения. В частности, неизменными остаются: распределение вероятностей бит извлекаемого сообщения и распределение вероятностей использования синонимов текста, что обеспечивает высокую степень скрытности рассматриваемого метода внедрения. В ходе исследования было показано, что внедряемое сообщение изменяет статистическую структуру контейнера, и этот факт используется при стегоанализе. Разработанный стеготест сравнивает распределение вероятностей серий бит (с длиной не более 5 бит) в извлечённом из контейнера сообщении с эталонными распределениями, соответствующими пустому и заполненному контейнеру. Эталонные распределения были получены путём анализа 1000 контейнеров естественного текста, взятых из библиотеки Gutenberg Project. В работе рассматриваются два подхода к получению эталонных распределений. Первый подход предполагает анализ статистики сообщения, извлечённого из контейнера обычным способом (с помощью программы Tyrannosaurus Lex). Второй подход предполагает дополнительное преобразование сообщения в соответствии с анализируемым алгоритмом кодирования длин серий. Экспериментальные результаты позволяют утверждать о большей эффективности первого подхода. В качестве меры близости двух вероятностных распределений используется мера Кульбака-Лейблера. Показано, что реализованный метод позволяет обнаруживать наличие внедрения в контейнере с числом синонимов равным 500, при этом ошибка 1 рода равна 1.5%, ошибка 2 рода – 1.3%. По сравнению с известными аналогами предлагаемый метод имеет более высокую точность анализа при меньшем объёме входных данных.
Ключевые слова: стегоанализ, метод замены синонимов, tyrannosaurus lex.

ABSTRACT

Anatoly V. Marchenko[1], Valery Yu. Voynalovich[2], Sergey N. Voronin[2]

[1]FSTEC of Russia,
105175, Staraya Basmannaya, 17, Moscow, Russia
e-mail: anatolijlev@yandex.ru, https://orcid.org/0000-0002-0207-6274
[2]State research and testing Institute of problems of technical protection of information of the FSTEC of Russia,
394020, Voronezh, street on January 9, 280a
e-mail: niii1zi@yandex.ru, https://orcid.org/0000-0002-1848-1346
e-mail: snv-36@mail.ru, https://orcid.org/0000-0002-1002-0799

The analysis of the training system for specialists working in the field of information security

Abstract. The analysis of the training system for specialists working in the field of information security plays an important role to improve staffing in the field of information security in the Russian Federation in the context of new challenges and threats in the information sphere. The article presents the results of analysis and summarizes the data on state of the system of training, retraining and advanced training provided for information security experts. The presented analytical materials are taking into account the results of the data analysis about the security specialists working in Federal Executive authorities (Federal authorities), regional executive authorities, local governmental bodies and their subordinate organizations, corporations, and organizations of licensees of the FSTEC of Russia. The presented analytical materials can be used for development of proposals in order to improve the national system of training, professional retraining and advanced training of information security specialists, as well as for development of control indicators for the admission of persons to the training in the field of information security at the expense of the Federal budget allocations.
Keywords: information security, training, admission control indicators, staffing.

Dmitriy A. Melnikov[1], Grigory P. Gavdan[2], Ivan A. Korsakov[3]

[1]Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Russian Federation, 119333, Moscow, Vavilov str., 44/2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]National Research Nuclear University MEPhI,
Russian Federation, 115409, Moscow, Kashirskoe shosse, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]GRCC Presidential Property Managenet Department of the Russian Federation,
Russian Federation, 125009, Moscow, Slaviaskaia sq., 4/1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

To the issue about the purpose and objectives the USA National initiative for cybersecurity education

Abstract. In the current year, Russia entered a three-year transitional period for the implementation of professional standards designed to replace the traditional regulations of the Unified Qualification Handbook (UQH) for the positions of executives, specialists and employees. Several professional standards have been approved for the field of staffing of information security.
However, from the higher school point of view, the existing variety of approved professional standards can hardly be used as a normative basis for the improvement and development of the existing system of

educational standards in the information security area, although such an obvious conceptual task was set in the framework of the transition from UQH to professional standards.
This paper analyses foreign experience in solving this problem using rather impressive example of the United States. A systematic study of the labor (personnel) resources structure in the cybersecurity field was carried on within the framework of the national initiative for cybersecurity education, which is proposed as a fundamental reference resource. That resource can be used to guide the various category users, including educational organizations, to solve their tasks of providing labor resources in the field of cybersecurity.
The cybersecurity workforce framework (CWF) components include such categories as specialty areas, work roles, knowledge, skills, abilities and tasks (performed for any kind of work).
The paper analyzes the presented CWF, its content, as well as its important role in harmonizing the Russian educational standards in the field of cybersecurity.
Keywords: cybersecurity, education, workforces, competences, speciality areas, knowledges, skills, abilities, work roles, tacks.

Alexander A. Golyakhov[1], Anatoly P. Durakovskiy[2], Egor A. Simakhin[2]

[1] Educational center of information security "MASKOM»,
119421, Moscow, ul. Novatorov, 40 korp.1
e-mail: gaa66@mail.ru, https://orcid.org/0000-0002-8715-3477
[2]National research nuclear university "MEPHI",
115409, Moscow, Kashirskoye highway, 31
e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735
e-mail: dekryt@mail.ru, https://orcid.org/0000-0003-4019-9694

Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation

Abstract. A determination of real attenuation of information signal's radiation on a way from the source to a possible location of intelligence devices is considered to be the most difficult operation while assessing information security against leakage of electromagnetic emanation. In this context the problem of automation of this kind of measurement is of great interest. It takes considerable effort and time to measure the attenuation by existing automated systems. That is why the measurements are generally taken within the limited range of frequencies only. Along with that, a spectre of a single information impulse has a leaf-structure and is solid on every frequency leaf. So electromagnetic field intensity attenuation measurement carried on the some preselected frequencies is not able to represent the complete attenuation characteristics. The measurements of attenuation in the whole informative signal spectre within the given frequency range requires a few thousand measurements, which makes the current method ineffective and time consuming. The relevant specialized automatized measurement systems of security verification has active protection system noise measurement mode, which can be used to measure the real attenuation. In this article a rather exact method of real attenuation of informative signal of video subsystem of electron-ray tube monitor measurement is described and confirmed in experiment. The measurements were made using specialized automatized system "Sigurd" and video subsystem informative signal noise generator. The described method allows a significant reduction of the time needed for specialized investigations of security verification on electromagnetic emanation.
Keywords: noise generator, information security, compromising emanation, attenuation of electromagnetic field, TEMPEST.

Sergey A. Klimachev, Natalia A. Tishina

Orenburg State University, Pobedy Av., 13 Orenburg, 460018, Russia,
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru https://orcid/0000-0002-7341-6985

Technique of experimental evaluation of cloud environment attacks detection accuracy

Abstract. The article is devoted to research of efficiency evaluation of IDS used for dynamic and complex organizational and technical structure computing platform guard. The components of the platform have a set of heterogeneous parameters. Analysis of existing IDS evaluation technique revealed shortcomings in justification of quantitative metrics that describe the efficiency and reliability IDS resolving. This makes if difficult to prove IDS evaluation technique. The purpose of the study is to increase IDS evaluation objectivity. To achive the purpose it is necessary to develop the correct technique, tools, experimental stand. The article proposes the results of development and approbation of the technique of IDS efficiency evaluation and software for it. The technique is based on defining of optimal set of attack detection accuracy scores. The technique and the software allow solving problems of comparative analysis of IDS that have similar functionality. As a result of the research, a number of task have been solved, including the selection of universal quantitative metrics for attack detection accuracy evaluation, the defining of summarised attack detection accuracy evaluation metric based on defining of pareto-optimal set of scores that ensure the confidentiality, integrity and accessibility of cloud environment information and information resources, the development of a functional model, a functional scheme and a software for cloud environment IDS research.
Keywords: efficiency evaluation, efficiency scores, IDS, cloud environment.

Igor Y. Zhukov, Oleg N. Murashov

Ltd «The National Mobile Portal»,
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

A secure mutual authentication procedure, generate the key fiscal basis, and fiscal data protection

Abstract. The paper describes cryptographic transformation for mutual authentication and creation of the fiscal sign key. This transformation based on using block encryption cipher named «Kuznetchik», described in the national standard of the Russian Federation GOST R 34.12-2015 and realized in gamma generation mode as it is described in the another national standard of the Russian Federation GOST R 34.13-2015. The function of the integrity protection (authentication code) is defined by the recommendation for standardization R 50.1.113–2016.
The solution proposed in this paper is aimed for an authentication and integrity control of fiscal data transmitted through communication channels between fiscal storage devices and fiscal data operators, as well as between the fiscal data operators and the authorized agency. Formats of transmitted fiscal data, methods of transmission and mechanisms to ensure the confidentiality of transmitted fiscal data determined by the authorized agency of the Federal Executive power.
The article gives a short description of the protocol model, a formal analysis of passive attacks in the assumption that the cryptographic properties of the protocol depends on the feature of cryptographic transformations used, which are standardized solutions regulated by national standards, or national recommendations for standardization. Since the cryptographic

transformations could not be compromised by the intruder we can conclude that the intruder also can not compromise the fiscal signs protection protocol.
Keywords: mutual authentication, cryptographic transformation, master key, fiscal sign, fiscal data protection.

Buyan S. Dongak

Tomsk state University of control systems and Radioelectronics,
Lenina str., 40, Tomsk, 634050, Russia
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

Monitoring of network activity of the employees automated workplaces

Abstract. The article addresses the issue of monitoring of the network activity of employee's computers in order to ensure information security of the organization from external threats caused by the use of hardware and software of foreign origin, including services collecting all kinds of information about Internet users. The major problems arising in the process of analysis of the security of the organization in the field of information security are discussed. A brief overview of existing network traffic monitoring tool solutions is given. The experiment with the use of the foreign hardware and software in the organization was carried on. The experiment is aimed at identifying negative factors affecting the information security. The results of the experiment are presented. Finally the conclusions about the shortcomings of methods and means of information protection are made, as well as optimal ways to use the tools for the network traffic filtering are addressed.
Keywords: firewall, traffic monitoring, network activity, information security.

Alexandr V. Mamaev[1], Kristina V. Mamaeva[2]

[1]CEO at 'Digital Forensics Laboratory LLC',
Dukhovskoy per., 17, bld. I, fl. 2A. 115191, Moscow,Russia
e-mail: a.mamaev@forensicservices.ru, http://orcid.org/0000-0002-1216-3486
[2]National Research University Higher School of Economics,
Myasnitskaya str., 20, 101000, Moscow, Russia
e-mail: solnce-tina18@mail.ru, http://orcid.org/0000-0003-0097-799X

How the ecosystem of digital assistants can ensure the security of personal data

Abstract. Number of cybercrimes is constantly rising both in Europe, and around the world. The costs incurred from such malicious activities are rising correspondingly. According to the data collected by Jupiter Research these costs increased from $1.5 trillion in 2015 to $2 trillion in 2019. That is why European Union is expected to introduce major changes to the Personal Data Protection Acts which stayed mostly unchanged since the 1990s. The consequences of those changes will be felt in countries beyond the European Union. The personal data of internet users have long become a commodity on the e-commerce market. Yet the manipulations with the personal data cause concerns among both the users, who do not fully realize how and to what purposes their data are used, and governments, who try to protect the confidentiality remains by the law. Despite that the number of incidents with data leaks continues to rise exponentially. In December 2017 the lawyers from Hill Dickinson, a UK commercial law firm, filed a lawsuit against Google regarding unlawful collection of the iPhone users' data. Another company that is about to have problems with law is Uber Technologiesm, which sent SMS messages to its clients without obtaining formal permissions for that. Finally, in March 2018 it was Facebook which had to explain the way the personal data on more than 80 million users have leaked and ended up in the hands of a third party. The authors of this article assessed the possibilities for introducing

the ecosystem of virtual assistants and blockchain technology for safe and depersonalized data processing as well as its further use. This system opens broad unexpected opportunities for the machine-to-machine-marketing.
Keywords: virtual assistants, blockchain, personal data, e-commerce.

Anton A. Abramov[1], Victor S. Gorbatov[2], Marina N. Grishina[3]

[1]Federal State Unitary Enterprise "Main Research Computing Center" of the Administrative Department of the President of the Russian Federation,
Moscow, 121471, Rybinovaya 43
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]National Research Nuclear University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]Federal state budget institution national medical research center named after academician V.I. Kulakova, Ministry of Health of the Russian,
Moscow, 117198, Academica Oparina 4
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

Information security threats in web-portals on the open journal systems platform

Abstract. This article addresses the problem of security threats while working with web portals built on the Open Journal Systems platform. The Open Journal Systems (OJS) platform was originally developed as part of the Public Knowledge Project and it is one of the most popular open-source platforms for web journals today. Based on the data available in the Public Knowledge Project, there were more than 10,000 active journals using the open journal systems platform by the end of 2016. A migration of a journal to such advanced and complex platform helps to handle the entire workflow over a single web portal. Therefore it is an important move and only peer-reviewed journals that are part of Russian and Worldwide citation systems go for it. At the same time the problem of keeping privacy for a manuscript before it is published is very important for these journals and for authors who submit it to the journal. The paper describes the most common threats for the web portals on the OJS platform as well as a particular model of the security threats, and suggests the measures that could help to neutralize these threats.
Keywords: particular threat model, intruder model, web portal, information security threats, protection measures, php, xss, open journal systems.

Vitaliy G. Ivanenko, Nikita V. Ushakov

National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

JPEG digital watermarking for copyright protection

Abstract. With the rapid growth of the multimedia technology, copyright protection has become a very important issue, especially for images. The advantages of easy photo distribution are discarded by their possible theft and unauthorized usage on different websites. Therefore, there is a need in securing information with technical methods, for example digital watermarks. This paper reviews digital watermark embedding methods for image copyright protection, advantages and disadvantages of digital watermark usage are produced. Different watermarking algorithms are analyzed. Based on analysis results most effective algorithm is chosen – differential energy

watermarking. It is noticed that the method excels at providing image integrity. Digital watermark embedding system should prevent illegal access to the digital watermark and its container. Requirements for digital watermark are produced. Possible image attacks are reviewed. Modern modifications of embedding algorithms are studied. Robustness of the differential energy watermark is investigated. Robustness is a special value, which formulae is given further in the article. DEW method modification is proposed, it's advantages over original algorithm are described. Digital watermark serves as an additional layer of defense which is in most cases unknown to the violator. Scope of studied image attacks includes compression, filtration, scaling. In conclusion, it's possible to use DEW watermarking in copyright protection, violator can easily be detected if images with embedded information are exchanged.
Keywords: digital watermarks, differential energy watermarking, images, embedding information, algorithm modification.

Ivan V. Nechta

Siberian state university of telecommunications and informatic sciences,
Kirova st., 86, Novosibirsk, 630102, Russia
e-mail: ivannechta@gmail.com, http://orcid.org/0000-0003-0361-2742

New method of steganalysis for text data obtained by synonym run-length encoding

Abstract. In this article, we present a new stegoanalysis method for detecting a text obtained by the synonym Run-Length Encoding. The analyzed RLE-method allows us to keep some statistical properties of the text after a secret message embedding. In particular, the probabilities distribution of the bits in the extracted message and the probabilities distribution of using text synonyms keep unchanged, that ensures a high secrecy degree of the considered embedding method. In this paper we show that the embedded message changes the probabilities distribution of bit-series lengths in the extracted message, and this fact is used for our stegoanalysis. It was shown that the embedded message breaks the statistical structure of the container, and this fact is used for the stegoanalysis. The constructed stegotest compares the probability distribution of runs (with length no more than 5 bits) in the message extracted from the container with reference distributions corresponding to an empty and embedded containers. Reference distributions were obtained by analysing of 1000 natural-text containers taken from the Gutenberg Project library. In this paper we consider two approaches for obtaining reference distributions. The first approach deals with analyzing the statistic of the message extracted from the container in the usual way (using the Tyrannosaurus Lex program). The second approach involves an additional decoding of the message in accordance with the analyzed run-length encoding algorithm. Experimental results allow us to assert that the first approach is more effective. The Kullback-Leibler measure is used as a divergence measure of two probability distributions. It was shown that the proposed method makes it possible to detect presence of the secret message in the container with a number of synonyms equal to 500, while false negative error is 1.5% and false positive error is 1.3%. In comparison with the known analogs, the proposed method demonstrates higher accuracy of analysis for a smaller size of input data.
Keywords: steganalysis, synonym substitution method, tyrannosaurus lex.

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, 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, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, ПРОПИСНЫМИ буквами); аннотация (200-250 слов, по ширине, строчными буквами); ключевые слова (не более шести, по ширине, курсив);
– далее идут сведения о статье **на английском языке**: Имя О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, строчными буквами, полужирно с подчеркиванием); аннотация (200–250 слов, по ширине, строчными буквами); ключевые слова (не более шести, по ширине, курсив);
– 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 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 эти библиографические источники должны быть написаны латиницей (т.е. латинскими буквами).

Условия опубликования статьи:

– статья может быть выслана по электронной почте или представлена в редакцию на бумажном (одном экземпляре) и электронном носителях (кроме дискет);
– 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 рецензирования и экспертной оценки квалифицированными специалистами в области ИБ;
– 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 публикации;
– подача статьи в более чем один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;
– статьи публикуются бесплатно.

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. Картинки, графики, фотографии и другие виды иллюстраций, по возможности, следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word).
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 желательно обращать внимание на наличие выходных данных работ и избегать повторных указаний одной и той же работы под разными номерами.
7. Ссылки на законы, нормативные акты, конференции и прочее желательно указывать по установленной форме: Закон РФ «__» от х месяца хххх г. № ___. Ст. ___.
8. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

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).

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.

Адрес редакции: Каширское шоссе, 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 9087.
Факс: +7 (499) 324-86-00.
Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 9087.
Fax: +7 (499) 324-86-00.
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода - 4раза в год / Periodicity - 4 times a year

Подписка на журнал
производится на почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Национальный исследовательский ядерный университет «МИФИ»
Каширское шоссе, 31, Москва, 115409, Россия

National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia