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, по которым журнал входит в этот перечень: 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки), 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические, физико-математические науки).

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

Ольга С. Макарова[1], Сергей В. Поршнев[1,2]
[1]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, ул. Мира, 19, Екатеринбург, 620002, Россия
[2]Институт математики и механики Уральского отделения Российской академии наук, ул. Софьи Ковалевской, 16, Екатеринбург, 620108, Россия
[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702
[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ, ВЛИЯЮЩИХ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ НАРУШИТЕЛЕМ

DOI: http://dx.doi.org/10.26583/bit.2021.2.01

Аннотация. Одной из актуальных задач информационной безопасности (ИБ) является прогнозирование вероятностей угроз ИБ для организации, реализуемых из-за компьютерной атаки (КА). Существующие методологии по оценке компьютерных атак (КА) Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), ФСТЭК России и ISO 27001 предлагают подходы к анализу КА с точки зрения организации. В статье предложен совершенно новый подход по прогнозированию КА с точки зрения нарушителя. Проведен анализ КА с точки зрения нарушителя. Выделены методов КА, обсуждаемых нарушителями в сети DarkNet, и их структуризация. Обоснованы этапы реализации КА с точки зрения нарушителя: теоретическая подготовка, практическая подготовка, достижение цели КА. Обоснован вывод о возможности использования математического аппарата клеточных автоматов при моделировании КА, так как динамика КА подобна динамике клеточного автомата. Определены параметры, влияющие на возможность реализации КА нарушителем, в частности, известность метода КА, наличие/достаточность средств защиты от данной КА и другие. Обоснованы количественные характеристики КА, определяющие весовым коэффициентом перехода (ВКП). Достаточность перечня выбранных количественных характеристик КА подтверждается результатами анализа КА, реализованной с помощью вредоносного программного обеспечения Petya, на узлы информационной инфраструктуры организаций, находящихся на территории Украины.
Ключевые слова: прогнозирование, компьютерные атаки, нарушитель, весовой коэффициент перехода, теория клеточный автомат.
Для цитирования: МАКАРОВА, Ольга С.; ПОРШНЕВ, Сергей В. ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ, ВЛИЯЮЩИХ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ НАРУШИТЕЛЕМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 06–20, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1336>. Дата доступа: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Благодарности. Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ).

Olga S. Makarova[1], Sergey V. Porshnev[1,2]
[1]Ural Federal University,
19 Mira str., Ekaterinburg, 620002, Russia
[2]Institute of mathematics and mechanics of the Ural branch of the Russian Academy of Sciences,
Sophia Kovalevskaya str., 16, Ekaterinburg, 620108, Russia
[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702
[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350

Determination of parameters affecting the possibility of computer attack implemented by an intruder

DOI: http://dx.doi.org/10.26583/bit.2021.2.01

Abstract. One of the urgent tasks of information security (IS) is to predict the probabilities of IS threats to an organization that are implemented due to a computer attack (CA). Existing methodologies for assessing CA are Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), FSTEC of Russia and ISO 27001/ They offer approaches to the analysis of CA from the organization point of view. The article offers a completely new approach to CA predicting from the intruder point of view. The analysis of the CA from the intruder point of view is carried out. The methods of CA discussed by intruder s in the DarkNet and their structuring are highlighted. The stages of the implementation of the SC from the intruder point of view are justified: theoretical training, practical training, achieving the goal of the CA. The conclusion about the possibility of using the mathematical apparatus of cellular automata in the simulation of the CA is justified, since the dynamics of the CA is similar to the dynamics of a cellular automaton. The parameters that affect the possibility of implementing the CA by the intruder are determined, in particular, the popularity of the CA method, the availability/sufficiency of means of protection against this CA, and others. The quantitative characteristics of the CA that determine the weighting factor of the transition (WCP) are justified. The sufficiency of the list of selected quantitative characteristics of the CA is confirmed by the results of the analysis of the CA, implemented with the help of the malicious software Petya, on the nodes of the information infrastructure of organizations located on the territory of Ukraine.

Keyword: prediction, computer attacks, intruder, weighting factor of the transition, theory of cellular automata.

For citation: MAKAROVA, Olga S.; PORSHNEV, Sergey V. Determination of parameters affecting the possibility of computer attack implemented by an intruder. IT Security (Russia), [S.l.], v. 28, n. 2, p. 06–20, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1336>. Date accessed: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Acknowledgement. The reported study was funded by Russian Ministry of Science (information security).

Введение

В [1–3] предложена научно обоснованная методика оценки вероятности компьютерной атаки (КА), в которой ключевые факторы КА выбираются на основе теории положений по криминологии, разработанной Ч. Беккариа и И. Бентамом [4–6], в соответствии с которой нарушитель реализует КА при условии достаточности ожидаемой выгоды от КА и наличия возможности ее реализации, поэтому вероятность реализации КА $p(EU)$ равняется отношению условной вероятности достаточности ожидаемой полезности от КА $p(EU/A)$ к вероятности наличия возможности реализации КА нарушителем $p(A)$:

$$p(EU) = \frac{p(EU/A)}{p(A)}. \quad (1)$$

При этом в (1) $p(EU/A)$ и $p(A)$ зависят от ключевых факторов КА.

Ключевые факторы КА определены и обоснованы в [1]:

1) выгода атакующего в случае успешной реализации атаки (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать те типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

2) защита от преследования (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать такие типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

3) длительность атаки (при оценке по данному показателю следует выбирать наиболее быструю атаку, напомним, что по данным Лаборатории Касперского средняя продолжительность целевой атаки составляет 100 дней [7]);

4) доступность методов для реализации атаки (при оценке по данному показателю будем оценивать доступность и известность технологии реализации атаки, наличие инструментов для реализации атаки в свободном доступе, а также активное обсуждение («объяснение») атаки на форумах DarkNet [8]).

Для удобства дальнейшего анализа и использования сгруппируем ключевые факторы в два укрупненных фактора КА:

– фактор «Возможность атаки» (критерии выбора объекта КА нарушителем, этапы и методы реализации КА, методы получения информации об объекте КА, критерии выбора объекта КА нарушителем, навыки нарушителя, длительность атаки);

– фактор «Ожидаемая полезность» (включает в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении КА нарушителем).

Анализ укрупненного фактора «Ожидаемая полезность» проведен в [3], где обосновано, что количество КА за определенный период времени зависит от вероятности того, что КА не будет своевременно обнаружена, тяжести наказания, наличия и величины альтернативных доходов (выгод) у нарушителя.

Отдельно отметим, что в [1] приведен анализ существующих подходов к анализу и прогнозированию компьютерных атак, в результате которого было выявлено, что классические подходы:

– рассматривают вероятность реализации КА с точки зрения тяжести последствий для организации;

– при оценке вероятности КА не учитывается динамика;

– определяют ограниченный набор вариантов возможных векторов КА при построении системы защиты информационной безопасности.

В данной статье приведено обоснование и анализ параметров, входящих в укрупненный фактор «Возможность атаки», для обоснования которой проводится анализ существующих моделей угроз ИБ и КА: Cyber Kill Chain [9, 10], Mitre Att&ck [11], NIST 800-115 [12], Certified Ethical Hacker (CEH) [13], методология ФСТЭК России [14, 15] и методологии ISO 27001 [16].

1. Анализ методов компьютерных атак

База Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge) была создана в 2013 г. для «составления структурированной матрицы используемых киберпреступниками приемов, чтобы упростить задачу реагирования на киберинциденты» [11]. Она содержит структурированный список тактик, техник и общеизвестных фактов о нарушителях, разделенный на группы в зависимости от этапа и цели использования, представленный в виде матрицы. Классификация методов, размещенных в базе Mitre Att&ck проведена на основе задачи, реализуемой нарушителем на объект КА, список которых содержит:

– получение первоначального доступа (Initial Access);
– выполнение (Execution);
– закрепление (Persistence);
– повышение привилегий (Privilege Escalation);
– обход защиты (Defense Evasion);
– получение учетных данных (Credential Access);

- обнаружение (Discovery);
- боковое перемещение (Lateral Movement);
- сбор данных (Collection);
- эксфильтрация или утечка данных (Exfiltration);
- командование и управление (Command and Control);
- влияние (Impact).

Напомним, что в методологии ФСТЭК России [14] под понятием «угроза безопасности информации (БИ)» подразумевается «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа» к информации. Результатом такого доступа могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке информации в информационной системе. При этом, априори, полагается, что каждая из угроз формируется взаимосвязью источников угроз, способов реализации угроз, уязвимостей и последствий [14, 15]. Структурная схема канала реализации угрозы БИ приведена на рис. 1.

Рис. 1. Структурная схема канала реализации угрозы
Fig. 1. Structural diagram of the threat implementation channel

При формировании перечня угроз БИ необходимо использовать банк данных угроз ФСТЭК России (более 200 угроз) [17], который в терминах Mitre Att&ck [9] представляет собой перечень возможных уязвимостей объектов КА (содержит информацию о более чем 27 тыс. уязвимостей) и методов реализации КА. Сама методология ФСТЭК России [14] позволяет сформировать полный перечень угроз (методов КА) и выполнить их классификацию по следующим признакам канала реализации угроз БИ:

- по виду защищаемой информации;
- по видам возможных источников;
- по способу реализации угрозы БИ;
- по виду нарушаемого свойства информации;
- по используемой уязвимости;
- по объекту воздействия.

Отметим, что помимо формирования перечня угроз БИ особое внимание необходимо также уделять оценке опасности реализации данной угрозы ИБ. Опасность реализации угрозы определяется, например, степенью негативных последствий для субъектов персональных данных (ПД). Действительно, любая система защиты информации, в том числе, предназначенная для обнаружения нарушителей, в первую очередь, нацелена на выявление действий, направленных против защищаемой информации, в частности, ПД. При этом в соответствие с методологией ISO 27001 [16] риски безопасности информации, меньшие некоторого приемлемого уровня, считаются приемлемыми. Такой уровень может быть у активов с низкой ценностью для организации. В результате КА на информационные ресурсы, не относящиеся к ценным активам для данной организации, может пройти незамеченной. Анализ фиксации обращений в правоохранительные органы по факту киберпреступлений показывает, что они происходят только в случае нарушения свойств критичной (защищаемой) организацией

информации. Краткий обзор тем активно обсуждаемых на форумах и чатах DarkNet [1–3, 18] можно поделить на следующие категории:

– продажа вредоносного программного обеспечения (ВПО);
– продажа эксплойтов;
– продажа данных;
– продажа доступов, т.е. сведений, с помощью которых можно осуществить несанкционированный доступ к сайту или серверу с последующей возможностью загрузки файлов или выполнения команд;
– продажа услуг.

Стоимость различного ПО и услуг в DarkNet варьируется от 1$ до 2540 $. На рис. 2 приведено процентное соотношение упоминаний о различных методах и инструментах реализации КА.

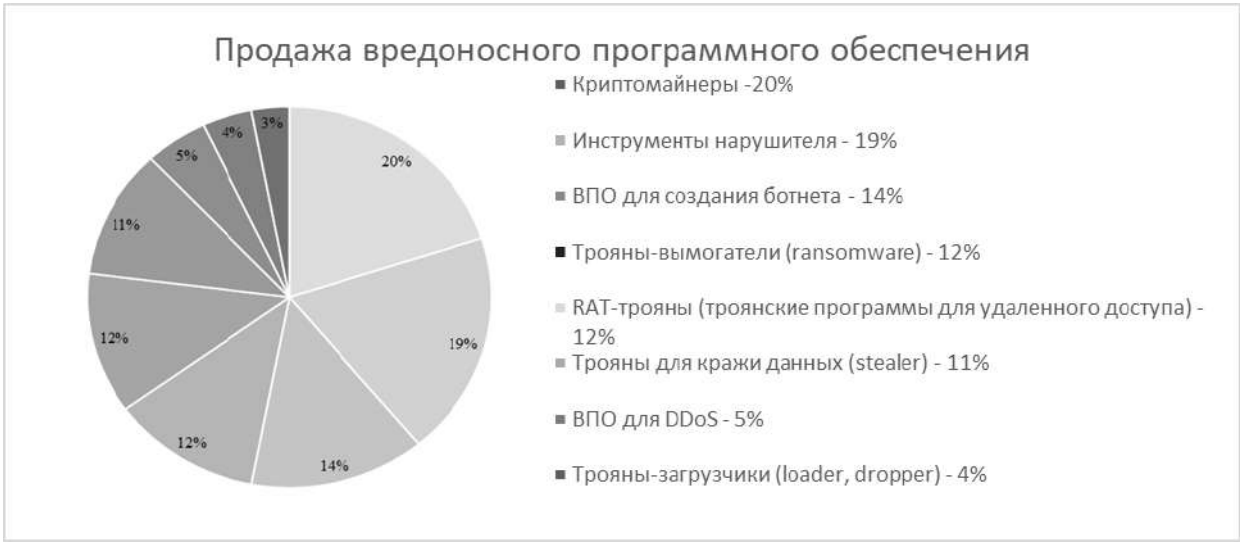

Рис. 2. Процентное соотношение продаваемых методов и инструментов для реализации КА в DarkNet
Fig. 2. Percentage of sold methods and tools for the implementation of CA in DarkNet

На рис. 3 приведено процентное соотношение данных о продаже различных услуг для реализации КА.

Анализ полученных данных позволяет сделать вывод, что выбор конкретного метода проведения КА определяется:

– наличием и известностью метода КА, в том числе в DarkNet;
– отсутствием мер защиты от КА;
– не реализуются мероприятия по мониторингу КА;
– отсутствием видимого вреда для объекта КА.

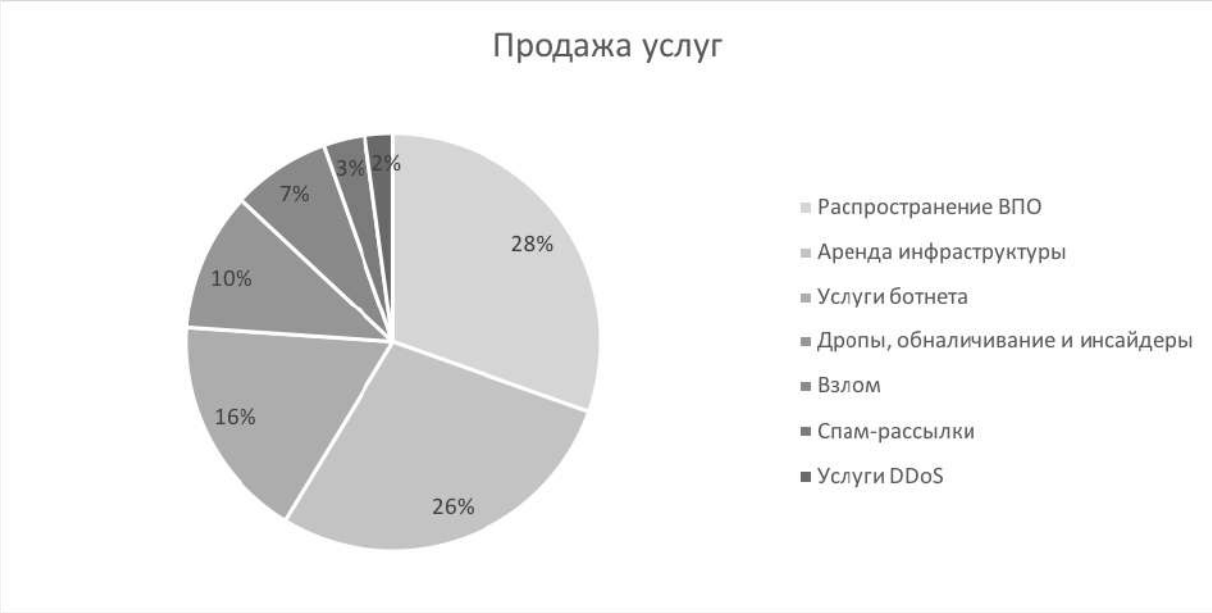

Рис. 3 Процентное соотношение данных о продаже различных услуг для реализации КА в DarkNet
Fig. 3. Percentage of data on the sale of various services for the implementation of CA in DarkNet

2. Этапы компьютерной атаки

В методологиях Cyber Kill Chain [9, 10], NIST 800-115 [12], Certified Ethical Hacker (CEH) [12] под угрозой понимается последовательность этапов действий, начиная с разведки и заканчивая действиями нарушителя по достижению поставленной им цели. Под целью нарушителя подразумевается нарушение конфиденциальности, целостности и/или доступности информации или компонентов информационной системы (ИС) организации. Для каждого этапа нарушитель использует различные методы. Отметим, что методологии NIST 800-115 и Certified Ethical Hacker (CEH) определяют этапы проведения тестирования на проникновение, т.е. эмулирование. Выделенные авторами этапы проведения КА в соответствии методологиями Cyber Kill Chain, NIST 800-115, Certified Ethical Hacker (CEH) приведены в табл. 1.

Из табл. 1 видно, что у обсуждаемых методологий имеется первый общий этап, не связанный с воздействием нарушителя на объект КА – этап теоретической подготовки. В рамках этого этапа нарушителем занимается сбором общедоступной информации, а также изучением инструментов и методов реализации атак. Данная работа схожа с работой исследователя, поэтому, даже, выявив подобную активность, достаточно трудно привлечь нарушителя к ответственности. Второй этап – практическая подготовка, который хоть и связан с активными действиями нарушителя, направленными на объект КА, однако, не приносит «видимого» вреда, а значит, не приводит к обнаружению – обращению в правоохранительные органы [8, 19]. Третий этап, связан с непосредственным нарушением свойств критической (защищаемой) информации. Особенность двух последних этапов заключается в том, что выявленная на первом этапе уязвимость и подготовленный эксплойт по ее эксплуатации на этапе практической реализации КА не гарантирует получение нарушителем запланированного результата. Соответственно, в ходе реализации КА присутствует «петля» или откат к предыдущему этапу для дополнительной подготовки.

Таблица 1. Этапы КА, выделенные в соответствие с методологиями Cyber Kill Chain NIST 800-115, Certified Ethical Hacker (CEH)

Обобщенные этапы КА	Cyber Kill Chain [9, 10]	NIST 800-115 [12]	Certified Ethical Hacker (CEH) [13]
Теоретическая подготовка – объединяет этапы, связанные с изучением объекта КА и подготовкой к КА	Этап «Reconnaissance» – Разведка. Включает исследование, идентификацию и выбор объекта КА. Этап «Weaponization» – Вооружение. Включает выбор и подготовку инструментов и ВПО для совершения КА.	Этап «Planning phase» – Планирования. Определяются правила, а также устанавливаются цели тестирования. Этап «Discovery phase» включает 2 части. Первая часть – это начало реального тестирования и охватывает сбор и сканирование информации. Вторая часть – это анализ уязвимостей, который включает сравнение служб, приложений и операционных систем просканированных узлов с базами данных уязвимостей	Этап «Reconnaissance» – Пассивная и активная разведка. Предполагает сбор информации о потенциальном объекте КА без обнаружения, включая сбор информации с общедоступных источников, отслеживание сетевого трафика и зонирование сети организации. Этап «Scanning» – Сканирование. Подтверждение информации, обнаруженной во время разведки, и ее использование для исследования сети
Практическая подготовка – объединяет этапы, связанные с практической реализации подготовитель-ной части КА	Этап «Delivery» – Доставка. Донесение вредоносного контента до целевой системы. Этап «Exploitation» – Эксплуатация уязвимости системы. Этап «Installation» – Инсталляция. Открытие удаленного доступа и другие действия с зараженной системой Этап «Command and Control (C&C)» – Получение управления. Управление зараженной системой.	Этап « Gaining access » – Получение доступа. Этап «Escalating Privileges» – Повышение полномочий доступа. Этап «System Browsing» – Получение доступа/управление целевой системой. Этап «Install Addition Tools» – Установка/запуск дополнительного ПО. На этих этапах проводится проверка идентифицированных на этапе «Discovery phase» уязвимостей путем их эксплуатации	Этап «Gaining access» – Получение доступа. Уязвимости, обнаруженные на этапе разведки и сканирования, используются для получения доступа к целевой системе
Достижение цели КА – связано с практической реализацией цели КА, в том числе, причинение вреда	Этап «Actions on Objective» – Выполнение действий. Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.	Этап «Reporting» – Подготовка отчета. Фиксация уязвимостей, эксплуатация которых может привести к успешной реализации реальной КА	Этап «Maintainig access» – реализация цели КА. Получение управления, сохранение доступа для будущих КА и реализация текущих целей КА.

Отметим, что методики КА, связанные с сокрытием следов присутствия нарушителя, мы не выделяем в отдельный этап КА, так как нарушитель стремится их использовать на каждом этапе проведения КА. Кроме того, нарушитель может защищать целевую систему от других нарушителей или специалистов по защите информации,

поддерживая свой эксклюзивный доступ с помощью специального ПО, например, с целью получения выкупа.

В соответствии с технологией Cyber Kill Chain [9, 10] известно, что прервать атаку можно на любом из этапов, тем самым разорвав цепочку действий нарушителя, ведущих его к цели КА. Данные методологии рассматривают КА, в первую очередь, с точки зрения подбора механизмов и средств защиты, но его можно рассмотреть и с точки зрения нарушителя. КА может быть технически прекращена нарушителем:

– если у него будет недостаточно навыков, методов и инструментов для КА, либо они не будут успешно реализовываться на любом из этапов КА.

– если КА будет обнаружена на этапе теоретической или практической подготовки.

3. Обоснование выбора математической модели, описывающей компьютерную атаку

Для моделирования КА обратимся к общей практике выявления и предупреждения правонарушений. В середине 70-х гг. был предложен подход, получивший название «средовое проектирование» [7, 20, 21]. В соответствие с данным подходом полагают, что:

1. Преступления привязаны к местам, наиболее посещаемым преступником – в терминах «средового проектирования» «узлам», к которым традиционно относят места работы, учебы, проживания и т.п. [21].

2. Совокупность мест, находящихся на маршруте передвижения потенциального нарушителя между узлами (например, остановки общественного транспорта, пешеходные дороги и т.п.) называется «тропа». Объекты, находящиеся рядом с тропами также рассматриваются как потенциальные места для совершения преступления (например, парки, магазины по пути следования потенциального нарушителя).

3. Граница минимальной области, охватывающей все «узлы» и «тропы», называется «границей среды» (далее – «граница»).

Принимая во внимание, очевидную аналогию между поведением обычного преступника и преступника, совершающего киберпреступления, можно установить следующее соответствие между ключевыми элементами «средового проектирования» в киберпространстве:

1. «Узлы» – *ip*-адреса нарушителя, прокси-серверы, форумы для получения информации об КА, объекты организации, доступ к которым был получен на успешно реализованных этапах КА, сканируемые или периодически атакуемые для проверки ИС.

2. «Тропы» – маршруты, *TCP* соединения, ИС, к которым есть доступ у нарушителя, наличие выполненных этапов *КА*.

3. «Границы» – объекты, ИС организации, находящиеся в контакте с «узлами» или «тропами». «Граница» определяет область зараженных узлов сети Интернет.

Подтверждением возможности и эффективности применения подхода «средового проектирования» для киберпространства при выявлении вероятных мест КА являются результаты [22, 23], в которых продемонстрировано, что ограничение области анализа уязвимостей ИБ поиском только уязвимых частей программного кода (например, элементов взаимодействия с внешними системами, пользовательских интерфейсов) позволяет улучшить качество прогнозирования новых уязвимостей. Таким образом, рассмотрение точек наиболее вероятного взлома ИС, позволяет улучшить качество прогноза, используемого для выявления новых уязвимостей ПО и оценок векторов КА.

В терминологии выбранного подхода («средового проектирования») правила проведения КА имеют следующие формулировки.

1. Каждый из «узлов» организации, с которым связан нарушитель, становится для него потенциальным началом «тропы» до другого «узла» – объекта КА (т.е. при успешной реализации хотя бы одного из этапов КА нарушитель при достаточности ожидаемой полезности совершит атаку).

2. Ключевым фактором выбора объекта КА является попадание объекта организации в «границы».

3. Успешная реализация КА на внешний «узел» организации предшествует успешной реализации КА на внутренний «узел» организации. Переход нарушителя с одного этапа КА на другой этап КА приводит к расширению «границ».

4. Распространение КА происходит с одного или нескольких «узлов», но не возникает из неоткуда.

5. Правило перехода от «узла» к «узлу» представляет собой или метод реализации КА, или метод получения информации об объекте КА, то есть, де-факто, определяет ключевые факторы КА.

6. Вероятность реализации КА увеличивается при увеличении числа «узлов» и «троп», известных нарушителю.

7. Начальное состояние «узлов» определяет результат реализации метода КА, выбранного нарушителем.

Для обоснования выбора математической модели, описывающей КА, сравним структуры атакуемой ИС, терминологии и правила, используемые в моделировании КА, с соответствующими структурами, терминологией и правилами, используемыми в теории клеточных автоматов [24, 25] (табл. 2).

Из табл. 2 видно, что динамика КА, действительно, подобна динамике клеточного автомата, поэтому изменение состояния отдельного узла ИС в процессе проведения КА можно характеризовать некоторым вероятностным коэффициентом – весовым коэффициентом перехода (ВКП), аналогично тому, как это реализуется в теории клеточных автоматов. Применительно, к КА данный коэффициент, как очевидно, есть ничто иное как показатель вероятности реализации КА.

4. Параметры, влияющие на возможность реализации компьютерной атаки

В [1] обоснована адекватность использования факторов КА для прогнозирования КА. Для построения функциональной зависимости удобнее использовать параметры. Основываясь на логических утверждениях, приведенных в данной статье, представим факторы КА [1] в виде параметров, которые будут определять ВКП.

1. КА может быть начата нарушителем, если:

– нарушителю известен метод КА, в том числе из сети DarkNet (количественно данный фактор можно охарактеризовать коэффициентом a_n известности метода КА, зависящего от активности обсуждений («объяснений») данного метода КА на форумах DarkNet, который есть отношение числа всех обсуждений в указанном сегменте Интернет данного метода КА к общему числу обсуждаемых методов КА);

– на объекте КА отсутствуют или недостаточны меры защиты от данной КА (количественно данный фактор можно охарактеризовать коэффициентом D_a наличия/достаточности средств защиты от данной КА, оценка значения которого может быть получена на основе анализа статистической информации о зафиксированных КА);

– на объекте КА отсутствуют или недостаточны мероприятия по мониторингу КА (количественно данный фактор можно охарактеризовать коэффициентом M_a наличия

решений по мониторингу данной КА, оценка значения которого может быть получена на основе анализа статистической информации о зафиксированных КА).

Таблица 2. Сравнение подходов к описанию динамики атакуемой ИС и клеточного автомата

Структура, термины и правила, используемые в моделировании КА	Структура термины и правила, используемые в теории клеточных автоматов
КА на ИС, состоящую из отдельных (дискретных) узлов, реализуется в соответствие со сценарием КА, предусматривающим некоторую дискретную последовательность действий атакующего (этапов сценария КА). При этом каждый следующий этап КА начинается только после окончания предыдущего этапа КА, а КА распространяется в ИС, через узлы ИС (локальной сети или сети Интернет), связанных друг с другом с помощью троп.	Клеточный автомат – дискретная динамическая систем, представляющая собой совокупность одинаковых клеток, состояние которых зависит от состояния соседних клеток.
Правила проведения КА: – «мгновенное» состояние атакуемой ИС, определяется совокупностью «мгновенных» состояний каждого из узлов ИС; – динамика атакуемой ИС описывается упорядоченной во времени последовательностью «мгновенных» состояний узлов ИС; – изменение/сохранение состояния на данном временном шаге всех узлов атакуемой ИС происходит одновременно; – изменение/сохранение состояний данного узла атакуемой ИС определяется состоянием его соседних узлов ИС (здесь под соседним узлом понимаем не физически, но логически связанные друг с другом узлы атакуемой ИС); – количество состояний каждого из узлов атакуемой ИС конечно.	**Правила изменения состояния клеточного автомата:** – «мгновенное» состояние клеточного автомата определяется совокупностью мгновенных состояний каждой из его клеток; – динамика состояния клеточного автомата описывается упорядоченной во времени последовательностью его «мгновенных состояний»; – изменение/сохранение состояния на данном временном шаге всех клеток происходит одновременно; – изменение/сохранение состояний данной клетки клеточного автомата определяется состоянием ее соседних узлов; – количество состояний каждой клетки клеточного автомата конечно.
Динамика КА полностью определяется: – наличием возможности заражения одного из узлов атакуемой ИС, обусловленной наличием уязвимости, средств защиты и т.п. (начальные условия) – правилами изменения/сохранения свойств узлов атакуемой ИС (при этом число состояний узла атакуемой ИС для разных типов КА количество состояний может быть различным); – числом узлов атакуемой ИС.	Динамика клеточных автоматов полностью определяется: – начальными условиями; – правилами изменения/сохранения свойств клеток; – числом клеток, образующими клеточный автомат.

2. КА может быть прекращена нарушителем, если:

– у нарушителя окажется недостаточно навыков, методов и инструментов для проведения успешной КА, что может быть обнаружено им на любом из этапов КА (количественно данный фактор характеризуется введенными выше коэффициентами a_n и D_a);

– КА будет обнаружена на этапе теоретической или практической подготовки к ее проведению, либо в момент достижения цели КА (количественно данный фактор можно охарактеризовать коэффициентом наличия отсутствия/наличия видимого вреда от КА S_a,

зависящим от использования методов сокрытия при реализации КА нарушителем, который может быть оценен на известности методов сокрытия в сети DarkNet S_a, а также ранее введенным коэффициентом M_a);

3. КА может быть прекращена специалистом по защите информации, если:

– КА будет обнаружена на этапе ее теоретической или практической подготовки, либо в момент достижения цели КА (количественно данный фактор можно охарактеризовать коэффициентом T – длительностью временного интервала, необходимого для обнаружения КА и разработки рекомендаций по блокировке КА и соответствующих средств защиты от КА, в частности, новых вирусных сигнатур);

– существует (либо находится в финальной стадии разработки) решение по защите от данной КА (количественно данный фактор можно охарактеризовать ранее введенным параметром D_a, а также числом узлов атакуемой ИС $У_a$, потенциально подверженных данной КА, и общим числом узлов атакуемой ИС $У$ в сети Интернет).

Таким образом, ВКП, определяющий динамику КА на ИС, является функцией, зависящей от переменных $У_a, У, T, D_a, M_a, S_a, a_a$:

$$ВКП = F\left(У_a, У, T, D_a, M_a, S_a, a_a\right). \quad (2)$$

Для подтверждения адекватности предложенных авторами подходов далее был проведен анализ КА, реализованной ВПО Petya на ИС, расположенные на территории Украины, результаты которого обсуждаются далее. Обоснование выбора конкретного типа функции $F\left(У_a, У, T, D_a, M_a, S_a, a_a\right)$ является предметом дальнейших исследований.

5. Анализ сценария компьютерной атаки, реализованной с помощью вредоносного программного обеспечения Petya

Напомним, что распространение ВПО Petya началось в апреле 2017 г. [20]. Данное ПО использовало известную на тот момент уязвимость EternalBlue, которая ранее уже эксплуатировалась для проведения КА шифровальщиком WannaCry. Это, с нашей точки зрения, является подтверждением наличия этапа «Практическая подготовка к проведению КА». Данный вывод также подтверждается результатами анализа форумов и чатов DarkNet в соответствующий период времени [18], результаты которого свидетельствуют о том, что:

– осуществлялась продажа услуг, связанных, с подготовкой поддельных файлов якобы с обновлениями или утилитами, которые размещают на взломанных или подконтрольных нарушителю организациях в 51% случаев (из всех услуг продаваемых в DarkNet);

– происходило обсуждение ВПО, связанного с Троянами-вымогатели (ransomware), к которым относится Petya (процент сообщений, связанных с этим типов ВПО составлял 12%).

В доступном описании сценария КА ВПО Petya на ИС, расположенные на территории Украины [19], в том числе сообщается.

«Заражение вирусом началось через распространение обновления для ПО M.E.Doc 27 июня 2017 г. ПО M.E.Doc широко используется для подачи бухгалтерской отчетности на Украине, по данным специалистов информационной безопасности, у фирмы на момент заражения было около 400 тысяч клиентов, что составляет порядка 90 % всех организаций страны.» [19, 20] Таким образом, об КА стало известно только 27.06.2017, а именно от организаций Украины с 27.06.2017 по 28.06.2017: «в Департамент киберполиции Украины

поступило более 1000 сообщений о вмешательстве в работу компьютерных сетей, что привело к сбоям в их работе. Из них официально с заявлениями в полицию обратились 43 компании» [7].

Полный перечень мероприятий по защите от этой КА был разработан в течение суток после обнаружения КА [25]. «28 июня 2017 г. Кабинет Министров Украины сообщил, что масштабная КА на корпоративные сети и сети органов власти была остановлена. 4 июля 2017 г. с целью немедленного прекращения распространения червя Petya принято решение о проведении обысков и изъятии программного и аппаратного обеспечения компании, с помощью которого распространялось ВПО. Обыски проведены представителями Департамента киберполиции, следователями и при участии Службы безопасности Украины. Изъяты рабочие компьютеры персонала и серверное оборудование, через которое распространялось ПО» [7].

Таким образом, КА ВПО Petya было реализовано в 3 этапа.

1. Теоретическая подготовка, состоящая в анализе сетей DarkNet и планировании данной КА.

2. Практическая подготовка, состоящая в доставке ВПО до целевой системы в период с апреля по июнь 2017 г., которая охватило порядка 90% всех узлов украинских ИС.

3. Достижение цели КА (напомним, что видимый ущерб был обнаружен 27.06.17, еще сутки потребовались для формирования перечня мероприятий по защите и еще 8 дней для окончательного блокирования КА).

Таким образом, обсуждаемая КА характеризуется:

– количеством атакованных узлов украинских ИС (90% от их общего числа) (в (2) – переменная $У_a$).

– общим количеством узлов украинских ИС в сети Интернет (в (2) – переменная У);

– временем, потребовавшимся для обнаружения КА (3 месяца) и разработки рекомендаций по его блокировке (1 день) (в (2) – переменная T);

– отсутствие/недостаточность соответствующих средств защиты на момент начала КА (в (2) – переменная D_a);

– отсутствие/недостаточность средств мониторинга данной КА (в (2) – переменная M_a);

– использование методов сокрытия КА на начальном этапе проведения (в (2) – переменная S_a);

– использованием известной уязвимости украинских систем ИБ ИС (коэффициент известности метода КА (в (2) – a_n, оказавшийся равным составил 31,5%).

Заключение

В статье на основе анализа существующих методологий Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), ФСТЭК России и ISO 27001, регламентирующих этапы и методы реализации КА, выявлены с точки зрения нарушителя следующие этапы КА:

1. Теоретическая подготовка.
2. Практическая подготовка.
3. Достижение цели КА.

Проведен сравнительный анализ математических подходов, используемых для описания динамики атакуемой ИС и клеточного автомата, результаты которого позволил

сделать обоснованный вывод о том, что динамика КА подобна динамике клеточного автомата.

Предложено использовать, аналогично тому, как это реализуется в теории клеточных автоматов, для изменения состояния отдельного узла ИС в процессе проведения КА, вероятностного коэффициента, названного весовым коэффициентом перехода, который является функцией, зависящей от обоснованно выбранных количественных показателей КА.

Достаточность перечня выбранных количественных показателей подтверждена результатами анализа сценария КА ВПО Petya на ИС, расположенные на территории Украины.

СПИСОК ЛИТЕРАТУРЫ:

1. Макарова, Ольга С., Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 6–18, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1248 (дата обращения: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
2. O. Makarova and S. Porshnev. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information, 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2020. P. 593–596. DOI: http://dx.doi.org/10.1109/USBEREIT48449.2020.9117676.
3. Макарова, Ольга С., Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе функций Безопасность информационных технологий, [S.l.], Т. 27, № 2. С. 86–96. SSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1273 (дата обращения: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.07.
4. Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, no. 11. P. 1701–1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
5. Becker G.S. The economics of crime // Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (дата обращения: 27.04.2020).
6. Бернулли Д. Опыт новой теории измерения жребия. Вехи экономической мысли. Теория потребительского поведения и спроса. Под ред. В.М. Гальперина. СПб.: Экономическая школа, 1999. Т. 1. С. 11–27.
7. Vagi KJ, Stevens MR, Simon TR, Basile KC, Carter SP, Carter SL. Crime Prevention Through Environmental Design(CPTED) characteristics associated with violence and safety in middle schools. J Sch Health. 2018. Vol. 88. P. 296–305. DOI: https://doi.org/10.1111/josh.12609.
8. Хакерские атаки на Украину (2017). URL: https://www.protectimus.com/blog/ru-conclusions-hacking-attacks-ukraine/ (дата обращения: 29.12.2020).
9. Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). DOI: https://doi.org/10.1007/s11416-019-00338-7.
10. The Cyber Kill Chain, lockheedmartin.com. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 29.12.2020).
11. Enterprise Matrix, attack.mitre.org. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 29.12.2020).
12. Scarfone, Karen & Souppaya, Murugiah & Cody, Amanda & Orebaugh, Angela. (2008). NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. URL: https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment (дата обращения: 29.12.2020).
13. Certified Ethical Hacker, eccouncil.org. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (дата обращения: 29.12.2020).
14. Методика определения актуальных угроз безопасности персональных данных при их обработке в ИС персональных данных. М.: ФСТЭК России, 2008. – 10 с.
15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). М.: ФСТЭК России, 2008. – 69 с.

16. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p.
17. Банк данных угроз БИ ФСТЭК России // FSTEC.RU/ URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2019).
18. Positive Technologies. Рынок преступных киберуслуг 2018. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf (дата обращения 11.11.2020).
19. Спецслужбы ФРГ: вирус Petya позволяет красть данные Вредоносное ПО в Германии распространялось через уязвимость в программе украинского разработчика. URL: https://tass.ru/mezhdunarodnaya-panorama/4396011 (дата обращения: 29.12.2020).
20. Разогреева А.М. Предупреждение преступлений при помощи средового проектирования: защищающее пространство и защищенное пространство / А.М. Разогреева // Всероссийский криминологический журнал. 2017. Т. 11, № 4. С. 706–716. DOI: https://doi.org/10.17150/2500-4255.2017.11(4).706-716.
21. Бауман З. Текучая современность/Пер. с англ. под ред. Ю.В. Асочакова. СПб.: Питер, 2008. – 240 с.
22. J. Stuckman, J. Walden and R. Scandariato. The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models, in IEEE Transactions on Reliability. 2017. Vol. 66, no. 1. P. 17–37. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
23. Нейман Дж. Теория самовоспроизводящихся автоматов / Дж. фон Нейман; закончено и отредактировано А. Бёрксом; пер. с англ. В. Л. Стефанюка; под ред. и с предисл. В. И. Варшавского. - Изд. 2-е. М.: URSS: Либроком, 2009. – 382 с.
24. Макарова, О. С. Моделирование непреднамеренного распространения информации пользователем / О.С. Макарова. Текст: непосредственный // Технические науки: проблемы и перспективы: материалы I Междунар. науч. конф. (г. Санкт-Петербург, март 2011 г.). СПб.: Реноме, 2011. С. 99–103. URL: https://moluch.ru/conf/tech/archive/2/136/ (дата обращения: 29.12.2020).
25. Новая эпидемия шифровальщика Petya / NotPetya / ExPetr. URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/ (дата обращения: 29.12.2020).

REFERENCES:

[1] Makarova, Olga S., Porshnev, Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.]. Vol. 27, no. 1. P. 6–18, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1248 (accessed: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[2] O. Makarova, S. Porshnev, Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information, Conference paper, 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Institute of Electrical and Electronics Engineers Inc., 2020. P. 593–596. DOI: http://dx.doi.org/10.1109/USBEREIT48449.2020.9117676.
[3] Makarova, Olga S., Porshnev, Sergey V. Assessment of probabilities of computer attacks based on function. IT Security (Russia), [S.l.]. Vol. 27, no. 2. P. 86-96, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1273 (accessed: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.07 (in Russian).
[4] Hausken K., Moxnes J.F The dynamics of crime and punishment. International Journal of Modern Physics C. 2005. Vol. 16, no. 11. P. 1701–1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
[5] G. Becker. The economics of crime, Cross Sections, Federal Reserve Bank of Richmond. Vol. 12, 1995. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (accessed: 27.04.2020).
[6] D. Bernoulli. Experience of a new theory of measurement of lots. Theory of consumer behavior and demand. Milestones of economic thought. Edited by V.M. Galperin. SPb.: Ekonomicheskaya shkola, 1999. P. 11–27 (in Russian).
[7] Vagi KJ, Stevens MR, Simon TR, Basile KC, Carter SP, Carter SL. Crime Prevention Through Environmental Design(CPTED) characteristics associated with violence and safety in middle schools. J Sch Health. 2018. Vol. 88. P. 296–305. DOI: https://doi.org/10.1111/josh.12609.
[8] Hacker attacks on Ukraine (2017). URL: https://www.protectimus.com/blog/ru-conclusions-hacking-attacks-ukraine/ (accessed: 29.12.2020) (in Russian).
[9] Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). DOI: https://doi.org/10.1007/s11416-019-00338-7.

[10] The Cyber Kill Chain, lockheedmartin.com. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed: 29.12.2020).
[11] Enterprise Matrix, attack.mitre.org. URL: https://attack.mitre.org/matrices/enterprise/ (accessed: 29.12.2020).
[12] Scarfone, Karen & Souppaya, Murugiah & Cody, Amanda & Orebaugh, Angela. (2008). NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. URL: https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment (accessed: 29.12.2020).
[13] Certified Ethical Hacker, eccouncil.org. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (accessed: 29.12.2020).
[14] Actual threats definitions method to personal data security during their processing in the information systems of personal data. M.: FSTEC Russia, 2008. – 10 p. (in Russian).
[15] The threats basic model to personal data security during their processing in personal data information systems (extract), M.: FSTEC Russia, 2008. – 69 p. (in Russian).
[16] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p.
[17] Information security threats databank of FSTEC Russia, FSTEC.RU URL: https://bdu.fstec.ru/ (accessed: 29.12.2020) (in Russian).
[18] Positive Technologies. Criminal cyber services market, ptsecurity.com. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf (accessed: 29.12.2020) (in Russian).
[19] German intelligence services: Petya virus allows data to be stolen, tass.ru. URL: https://tass.ru/mezhdunarodnaya-panorama/4396011 (accessed: 29.12.2020) (in Russian).
[20] Razogreeva A.M. Crime prevention through environmental design: defensible space and protected space. Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. 2017. Vol. 11, no. 4. P. 706–716. DOI: https://doi.org/10.17150/2500-4255.2017.11(4).706-716 (in Russian).
[21] Z. Bauman, Liquid modernity. Polity Press, 2000. – 225 p.
[22] J. Stuckman, J. Walden, R. Scandariato. The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models, in IEEE Transactions on Reliability. 2017. Vol. 66, no. 1. P 17–37. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
[23] John Von Neumann and Arthur W. Burks. Theory of Self-Reproducing Automata. University of Illinois Press, USA. 1966. – 408 p.
[24] Makarova, O.S. Modeling of unintentional dissemination of information by the user. O.S. Makarova. Text: direct. Technical sciences: problems and prospects: materials of the I International Scientific Conference (SPb., March 2011). StPb.: Renome, 2011. P. 99–103. URL: https://moluch.ru/conf/tech/archive/2/136 (accessed: 29.12.2020) (in Russian).
[25] New Petya. NotPetya. ExPetr ransomware epidemic, kaspersky.ru. URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/ (accessed: 29.12.2020) (in Russian).

Поступила в редакцию – 14 января 2021 г. Окончательный вариант – 22 марта 2021 г.
Received – January 14, 2021. The final version – March 22, 2021.

Сергей В. Дворянкин[1], Антон О. Антипенко[2]
Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский пр–кт, 49, Москва, 125167, Россия
[1]e-mail: SVDvoryankin@fa.ru, https://orcid.org/0000-0001-6908-0676
[2]e-mail: An-go-55@yandex.ru, https://orcid.org/0000-0001-8692-6637

ПРИМЕНЕНИЕ ФАЗОВЫХ ХАРАКТЕРИСТИК ГОЛОСОВЫХ ВОКАЛИЗМОВ В РЕШЕНИИ ЗАДАЧ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2021.2.02

Аннотация. В настоящее время из-за своего удобства речевые технологии приобретают всё большую популярность, в том числе применительно к системам обеспечения безопасности, однако из-за возможных проблем с безопасностью остаются сферы, в которых данная технология находит крайне ограниченное применение. **Цель** работы состоит в уточнении области применения фазовых характеристик голосовых вокализмов при решении различных задач в области защиты и обработки речевой информации. **Методы**. В работе использовались методы компьютерного и математического моделирования, цифровой обработки сигналов и изображений. **Результаты**. Предложено использовать фазовые характеристики речи в различных приложениях, в том числе для решения различных проблем безопасности, например, надёжной идентификации. **Выводы**. Представлены основные характеристики речевых сигналов. Рассмотрена Гильбертовская модель речевого сигнала, а также модель синусоидального описания речевого сигнала МакАуэля и Куатьери. Приведены области практического применения фазовых характеристик голосовых вокализмов (включая внедрение в фазограмму биометрической информации о говорящем).
Ключевые слова: голосовые вокализмы, защита речевой информации, разборчивость, речевой сигнал, фазовые характеристики, синусоидальная модель.
Для цитирования: ДВОРЯНКИН, Сергей В.; АНТИПЕНКО, Антон О. ПРИМЕНЕНИЕ ФАЗОВЫХ ХАРАКТЕРИСТИК ГОЛОСОВЫХ ВОКАЛИЗМОВ В РЕШЕНИИ ЗАДАЧ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 21–33, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1337>. Дата доступа: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.02.

Sergey V. Dvoryankin[1], Anton O. Antipenko[2]
Financial University under the Government of the Russian Federation
(Financial University),
Leningradsky prospect, 49, Moscow, 125167, Russia
[1]e-mail: SVDvoryankin@fa.ru, https://orcid.org/0000-0001-6908-0676
[2]e-mail: An-go-55@yandex.ru, https://orcid.org/0000-0001-8692-6637

Applying the phase characteristics of voice vocalisms in solving problem of protection of speech information

DOI: http://dx.doi.org/10.26583/bit.2021.2.02

Annotation. At present, due to its convenience, speech technologies are gaining increasing popularity, including in relation to security systems. However, due to possible security problems, the areas in which this technology is extremely limited still remain. **The aim** of this work is to clarify the field of application of the phase characteristics of voice vocalisms in solving various problems of protection and processing of speech information. **Methods.** The methods of computer and mathematical modeling, digital processing of signals and images are used. **Results**. It is proposed to use the phase characteristics of speech in various applications, including security problems such as a reliable identification. **Conclusion**. The major characteristics of speech signals are presented. The Hilbert model of the speech signal is considered, as well as the model of the sinusoidal description of the speech signal by MacAuel and

Quatieri. The areas of practical application of the phase characteristics of voice vocalisms (including the introduction of biometric information about the speaker into the phaseogram) are described.
Keywords: voice vocalisms, speech information protection, intelligibility, speech signal, phase characteristics, sinusoidal model.
For citation: DVORYANKIN, Sergey V.; ANTIPENKO, Anton O. Applying the phase characteristics of voice vocalisms in solving problem of protection of speech information. IT Security (Russia), [S.l.], v. 28, n. 2, p. 21–33, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1337>. Date accessed: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.02.

Введение

В настоящий момент количество сервисов, в которых могут найти применение речевые технологии, постоянно возрастает – это связано, главным образом, с лёгкостью их освоения и применения пользователями, а также сопутствующими удобствами [1]. Хорошим примером может служить внедрение функции голосовой аутентификации в приложениях дистанционного банковского обслуживания (ДБО), однако в следствие угрозы перехвата и утечки вводимой голосом ключевой информации, а также недостаточной надёжности данная технология не находит широкого применения.

Вместе с тем до настоящего времени из-за нехватки знаний о природе образования, а также сложности вычислений исследователями не уделялось должного внимания фазовым характеристикам речевого сигнала, хотя их применение позволит не только повысить надёжность голосовой аутентификации, но и решить некоторые другие прикладные задачи, связанные с речевой обработкой, а именно улучшения качества передачи голосовых сигналов в каналах речевой связи и защиты речевой информации.

1. Речевой сигнал и основные характеристики речевых вокализмов

Будем считать, что речь – это исторически сложившаяся форма общения людей посредством языковых конструкций, создаваемых на основе определённых правил [2]. Множество исследований в части разработки высокоскоростных и надёжных систем обработки речи показали, что главным фактором их успеха является применение подходящего способа представления соответствующих сигналов, а также математических моделей.

Базовым компонентом речи являются звуки, которые, благодаря распространению на некоторые, иногда весьма значительные, расстояния в различных средах, например, в воздухе или строительных конструкциях, переносят информацию, воспринимаемую далее органами слуха человека либо различными средствами приёма акустических сигналов, в том числе разведки [3]. В настоящее время выделяют и используют различные характеристики речевого сигнала, полезные для решения задач речевой обработки, из них чаще всего особо отмечают следующие:

- частотные характеристики;
- амплитудные характеристики;
- энергетические характеристики;
- временные характеристики;
- фазовые характеристики.

Амплитудные характеристики речевого сигнала находят своё отражение в громкости звука – субъективном восприятии его силы, которое во многом зависит от частоты звуковых колебаний, а также давления (интенсивности) звука, и в меньшей степени от тембра, локализации в пространстве, спектрального состава и длительности [4, 5].

В соответствии с Международной организацией по стандартизации сон является единицей абсолютной шкалы громкости. Согласно стандарту, громкостью равной 1 сон называют громкость чистого непрерывного синусоидального тона частотой в 1 кГц и создающего звуковое давление равное 2 мПа. Часто уровень звукового давления выражается не в паскалях, а в децибелах (дБ) – это отношение величины звукового давления P к некоторому пороговому значению, а именно:

$$P_0 = 2 * 10^{-5} \text{ Па},$$

$$P_{\text{дБ}} = 20 \lg \frac{P_{\text{Па}}}{P_0} \text{ дБ}.$$

Кроме того, существует ещё и относительная величина громкости звука – его уровень, выражаемый в фонах, который равен звуковому давлению в 1 дБ, создаваемому чистым непрерывным синусоидальным тоном частотой 1 кГц равногромкому измеряемому звуку.

На рис. 1 представлены изофоны – кривые равной громкости. Их значения определяются международным стандартом ISO 226 (российский аналог – ГОСТ Р ИСО 226–2009 «Акустика. Стандартные кривые равной громкости») и отражают зависимость уровня звукового давления от частоты при определённом уровне громкости. Применяя изофоны можно легко сопоставить уровень создаваемого звукового давления и уровень громкости тона определённой частоты. Допустим дана синусоидальная волна с частотой в 1000 Гц, которая создаёт звуковое давление в 20 дБ. Используя приведённые выше изофоны легко понять, что данный звук имеет громкость в 20 фон. Порог слышимости стандартного человеческого уха составляет ноль фон – на изофонах на рис. 1 он изображён пунктирной линией [6].

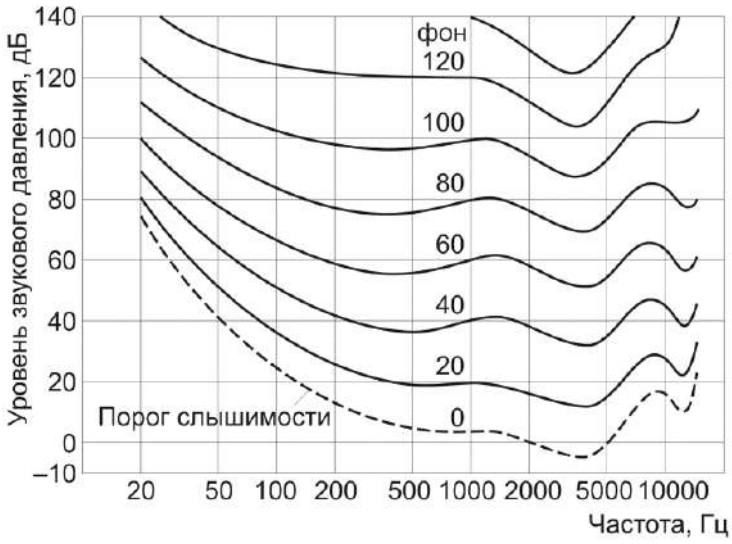

Рис. 1. Зависимость уровня громкости от звукового давления и частоты
Fig. 1. Dependence of the volume level on sound pressure and frequency

Темпом речи называется скорость произнесения элементов речи, таких как слова, слоги, звуки [7]. Эта характеристика речевого сигнала является одним из компонентов интонации и дополнительным элементом речи, при этом она сильно зависит от эмоционального состояния говорящего, его особенностей строения голосового аппарата, стиля произношения элементов речи, а также ситуации общения. Темп речи может

измеряться как средней длительностью элемента речи, так и числом произносимых элементов в момент времени [8]. Снижение темпа речи как правило достигается за счёт увеличения длительности гласных звуков, в то время как повышение осуществляется сокращением длительности и согласных, и гласных. Кроме того, темп речи используется и в качестве интонационного средства, позволяя выделить более важные моменты речи – как правило она становится более медленной, в то время как второстепенные моменты произносятся быстрее. Замедление темпа также характерно к концу высказывания, позволяя, тем самым, оформить его целостность. Вместе с тем темп можно рассматривать как характеристику степени слуховой отчётности и артикуляционной напряжённости, например, при быстром темпе речи слова обычно начинают выступать в неполных звуковых формах.

Частотный диапазон голоса человека измеряется в герцах, у мужчин он составляет от 80 до 150 Гц, у женщин от 120 до 400 Гц, у детей он сильно выше, отметим при этом, что диапазон разговорного голоса человека составляет только около 10% от общего диапазона голоса [9]. Заметим, что из-за особенностей человеческого слуха высокие голоса (с высокой частотой) воспринимаются более громко, нежели низкочастотные. Интересно, что окраска голоса, отражающаяся в его частоте, может служить индикатором не только эмоционального, но и психического состояние говорящего.

К энергетическим характеристикам речи относят интенсивность звука, а также плотность энергии. Количество энергии, проходящее в единицу времени через единицу площади, перпендикулярной к направлению распространения, называют силой звука или, по-другому, его интенсивностью, измеряется показатель в Вт/м^2. Интенсивность речевых сигналов зависит от амплитуды колебания голосовых связок человека и их напряжённости. Интенсивность звука снижается в случае уменьшения амплитуды колебаний. При этом различают несколько уровней интенсивности – от высокого до низкого. Интенсивность может быть как постоянна на отрезке времени, так и динамически меняться (плавно или резко). Под плотностью звуковой энергии подразумевают количество энергии акустических колебаний, находящейся в единице объёма (Дж/м^3).

Фазовым характеристикам речи, которые более подробно описаны в следующем разделе настоящего исследования, до настоящего времени, за исключением нескольких работ [10, 11], практически не уделялось внимания учёных, в первую очередь из-за сложности их вычисления, а также недостаточности знаний об их образовании, при этом их анализ и применение может кардинально повысить надёжность голосовой аутентификации, в том числе в приложениях дистанционного банковского обслуживания. Наибольший интерес представляет оценка фазовых характеристик на вокализованных отрезках речевого сигнала.

2. Гильбертовская модель и фаза речевого сигнала

В целях выделения характеристик речевого сигнала и последующего приведения его к подходящей форме для анализа-синтеза разработано большое количество различных математических моделей, таким образом, что каждая из моделей удобна для решения своей узкой технической задачи [12, 13]. Для целей защиты речевой информации чаще всего применяются модели искусственного моделирования начальных фазовых характеристик, а также описания вокализованных участков речи. В настоящее время преобразование Фурье играет ключевую роль в области исследования акустического сигнала и является наиболее популярным методом его представления в частотной области [13]. При этом необходимо отметить существенный недостаток многих математических

моделей речевого сигнала – зачастую они не учитывают фазовые характеристики речевого сигнала.

Для исключения вышеназванного недостатка в статье предлагается использовать преобразования Гильберта и Фурье. Например, вокализованные участки речи можно представить следующим выражением [12]:

$$S(t) = \sum_{k=1}^{\infty} a_k(t) \cos k2\pi f t,$$

где f – частота основного тона, $a_k(t)$ – амплитуда k-ой гармоники основного тона, k – номер гармоники.

При этом для невокализованных звуков используют иную формулу:

$$S(t) = \int_0^{\infty} a_\omega(t) \cos \omega t \, dt,$$

где $a_\omega(t)$ – спектральная амплитудная плотность на частоте ω.

В общем случае принято использовать другое описание речевого сигнала [13]:

$$S(t) = a(t)cos\varphi(t),$$

где $a(t)$ и $\varphi(t)$ – мгновенная амплитуда и мгновенная фаза соответственно, определяемые преобразованиями В.И. Коржикова, Гильберта или В.И. Тихонова [14].

С помощью преобразования Гильберта речь можно представить в аналитическом виде и таким образом найти значения параметров, отвечающих за разборчивость (опорных точек), однако при таком подходе фаза не является определённой по времени и частоте, что сильно усложняет вычисление начальной фазы. Таким образом традиционные модели описания речевых сигналов не подходят для решения задач вычисления и дальнейшего анализа фазовых характеристик, фактически для построения эффективного процесса верификации и распознавания голосов требуется нахождение и использование нового алгоритма.

Тем не менее речь на вокализованных участках можно представить как суперпозицию акустических узкополосных по Гильберту [12]:

$$s(t) = \sum s_i(t) = \sum A_i(t)cos\ \varphi_i(t).$$

И затем для всех обертонов речи необходимо вычислить полную фазу $\varphi_i(t)$ по Гильберту согласно формуле:

$$\varphi_i(t) = arctg\left(\frac{s_i(t)}{s_i^c(t)}\right) + 2k\pi,$$

где k – неопределённое целое число, а $s_i^c(t)$ – сопряжённая функция от $s_i(t)$ по Гильберту.

Представим полную фазу i-го обертона в виде:

$$\varphi_i(t) = \omega_i t + \theta_i(t) + \varphi_{0i},$$

где ω_i принимает кратные частоте основного тона значения, φ_{0i} – начальная фаза i-го обертона речи, $\theta_i(t)$ отвечает за нелинейную зависимость фазы от времени.

Одной из самых важных задач при исследовании фазовых характеристик голосовых вокализмов является определение зависимости изменения фазы от времени.

Для определения данной зависимости нужно взять производную второго порядка от косинуса фазы, тогда:

$$\frac{d(cos\ \varphi_i(t))}{dt} = sin\ \varphi_i(t)\frac{d\varphi_i(t)}{dt},$$

$$\frac{d^2(cos\ \varphi_i(t))}{dt^2} = -cos\varphi_i(t)\left(\frac{d\varphi_i(t)}{dt}\right)^2 + sin\varphi_i(t)\frac{d^2\varphi_i(t)}{d^2t}.$$

Результаты ранее проведённых экспериментов по нахождению второй производной от $cos\ \varphi_i(t)$ явно указывают на то, что в окрестности точек пересечения нуля, где $cos\ \varphi_i(t) \approx 1,\ sin\ \varphi_i(t) \approx 1$ значение производной стабильно, практически не изменяется на коротком промежутке времени. Таким образом нелинейная зависимость фазы от времени на коротком промежутке имеет параболический вид:

$$\theta_i(t) = \frac{\delta_i}{2}t^2,$$

где $\delta_i = \frac{d^2\varphi_i(t)}{dt^2}$.

Выявленная зависимость позволяет полную фазу каждого обертона сигнала приблизить к следующему выражению:

$$\varphi_i(t) = \omega_i t + \delta\frac{t^2}{2} + \varphi_{0i}.$$

Принимая во внимание вышеизложенное, общую формулу описания речевого сигнала на вокализованных участках можно представить в следующем виде:

$$s(t) = \sum_K A_k e^{\alpha_k t}\cos\left(\omega_k t + \delta_k\frac{t^2}{2} + \varphi_{0k}\right).$$

Эта модель хорошо показывает себя в решении задач идентификации говорящего (например, в речевых системах контроля и управления доступом) благодаря возможности оценки как потерь в речевом тракте (коэффициент α_k), так и частотно-фазовых параметров (коэффициенты $\omega_k, \delta_k, \varphi_{0k}$).

Очевидно, что главным прототипом для создания будущих эффективных информационных систем обработки и защиты речевой информации являются механизмы человеческого речевосприятия и речеобразования, вместе с тем некоторые из них так до конца и не изучены. Исследование данных механизмов позволит создавать новые функциональные модели анализа-синтеза речевой информации. Одним из примеров использования такого механизма является международный стандарт сжатия цифрового аудио и видеосигналов MPEG-4, в основу которого положен эффект скрытия энергетически слабых звуковых сигналов громкими [15]. Эти методы также могут быть приложены и к решению задач считывания, визуального представления и корректировки речевой информации.

Добавим, что к показателям, определяющим качество фиксируемой речи, относят её громкость, естественность, а также разборчивость. Показатели громкости речи уже были подробно разобраны в предыдущей части исследования, добавим лишь, что при определении качества этот показатель сравнивается с нормальным уровнем порога слышимости человеческого уха. Натуральность (естественность) речи является субъективным показателем качества, поскольку до настоящего времени надёжных математических методов оценки этого показателя не существует, однако существует

предположение, подкреплённое некоторым количеством научных работ, согласно которому этот показатель скрывается именно в фазовых характеристиках голосовых вокализмов, при этом интересна их оценка на вокализованных участках речевого сигнала, как наиболее инвариантных к различным преобразованиям в системах обработки и передачи речи. Чаще всего качество речи измеряется её разборчивостью, которая является статистической характеристикой и определяется отношением числа правильно понятых речевых конструкций (слов, звуков, слогов, фраз) к их общему переданному по каналу количеству, при этом используется среднее значение, допускающее некоторые отклонения. Для различных работ, в том числе и по защите речевой информации, чаще всего применяют слоговую разборчивость, при этом существуют и другие типы, такие как фразовая и словесная. Все они измеряются в процентах и связаны определёнными соотношениями [16].

3. Модель синусоидального описания речевого сигнала МакАуэля и Куатьери

Наиболее исчерпывающее объяснение синусоидальных моделей описания речевых сигналов, которые также включают низкие частоты, были представлены в исследованиях МакАуэля и Куатьери. Синусоидальная модель, предложенная МакАуэлем и Куатьери, представляет речь как линейную комбинацию синусоид с изменяющимися во времени амплитудами, фазами и частотами [17]:

$$S_{\widetilde{SR}}(n) = \sum_{K=1}^{L} A_k \cos(\Omega_k n + \varphi_k)$$

где *SR* обозначает синусоидальное представление.

Заметим, что число синусоид L изменяется во времени. Возможность уменьшить скорость передачи данных с использованием этой модели связана с тем, что голосовая речь как правило высокопериодична и, следовательно, она может быть представлена ограниченным набором синусоид. К тому же статическая структура (коротко-временной спектр) шёпота (глухой речи) может быть представлена синусоидальной моделью с соответственно определёнными случайными фазами. Синусоидальная модель может связана с моделью системы-источника посредством замены упрощённой модели возбуждения голосового тракта на более общую модель, содержащую зависящую от L синусоидальных компонент, состоящих из амплитуд, частот и фаз. Выход из голосовой полосы фильтра (синтетическая речь) в стационарном состоянии может быть записан в соответствии с формулой. Основным предположением является то, что параметры синусоидальной модели медленно изменяются во времени по отношению к длительности импульса голосовая тракта.

МакАуэль и Куатьери показали, что высококачественное восстановление может быть достигнуто путём использования синусоид с амплитудами, частотами и фазами, соответствующими пикам коротко-временного преобразования Фурье. Ширина окна Хемминга, равная 2,5 средним высотам, подходит и гарантирует, что синусоидальные волны хорошо определены. Более того, синусоидальная модель слабо зависит от высоты и голос начиная со средней высоты используется только для определения длины анализируемого окна.

Синусоидальная модель была представлена выше в наиболее общей форме. Основные вклады в работе МакАуэля и Куатьери лежат в анализе минимального параметра синусоидальной модели, а также в разработке алгоритма отслеживания синусоидальных параметров от фрейма к фрейму. Прежде всего, поскольку число синусоид меняется с высотой, было установлено понятие «жизни» и «смерти»

синусоидальных компонентов для обеспечения соответствия динамических параметров. В добавок к этому были разработаны новые алгоритмы интерполяции фазы и амплитуды для соответствия этим параметрам от одного фрейма к другому. Эксперименты с синусоидальной моделью показали, что целых 80 синусоид могут быть использованы для синтеза. Эти эксперименты проводились при использовании адаптированного окна Хемминга шириной в 2,5 от средней высоты, и 1024 точки быстрого преобразования Фурье, которое обновляется каждые 10 мс. Синусоидальная анализо-синтезирующая модель работает достаточно хорошо с большим количеством сигналов (несколько динамиков, музыка, биологические звуки), а также с речью в присутствии фонового шума.

Для низкочастотных приложений частоты синусоидальных волн могут быть ограничены, в итоге они получаются целыми, кратными основной частоте, то есть [17]:

$$S_{\widetilde{HR}}(n) = \sum_{k=1}^{L(\Omega_0)} \cos\left(\varphi_k + k\Omega_0 n\right) A_k,$$

где $L\left(\Omega_0\right)$ – количество гармоник интересующей речевой полосы частот (обычно 4 кГц), Ω_0 – частота основного тона, а $\widetilde{HR}$ означает гармоническое представление сигнала. Гармоническое представление обеспечивает оптимальное множество частот только для идеально звучащих сегментов. Основное предположение в голосовой речи – шаг периода постоянен в течение всего периода анализа окна. Для не голосовой речи, множество синусоид, равноудалённых по частоте, как правило сохранят статистику не голосовых сегментов. Предположение для не голосовой речи – частоты синусоид достаточно близки так что они следуют за изменениями измеряемой кратковременной спектральной плотностью.

Простой пример реконструкции сегмента голосовой речи при помощи линейной комбинации гармонических синусоид показан на рис. 2. Голосовой сегмент, сформированный с помощью 32 мс прямоугольных окон и амплитуд фаз синусоидальных волн, оценивался по пикам сегмента дискретного преобразования Фурье (рис. 3).

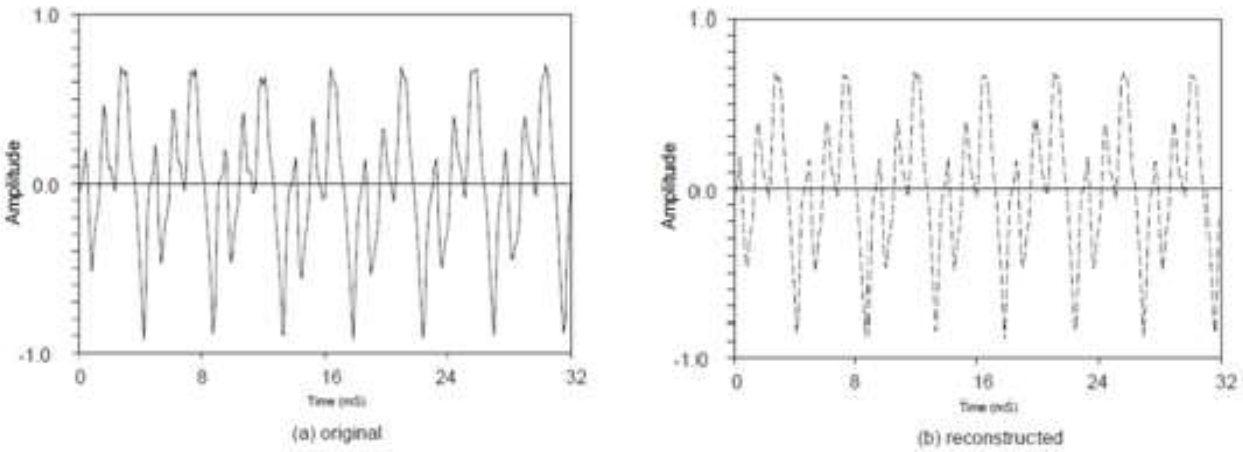

Рис. 2. Восстановление сигнала по набору гармоник
Fig. 2. Reconstruction of a signal from a set of harmonics

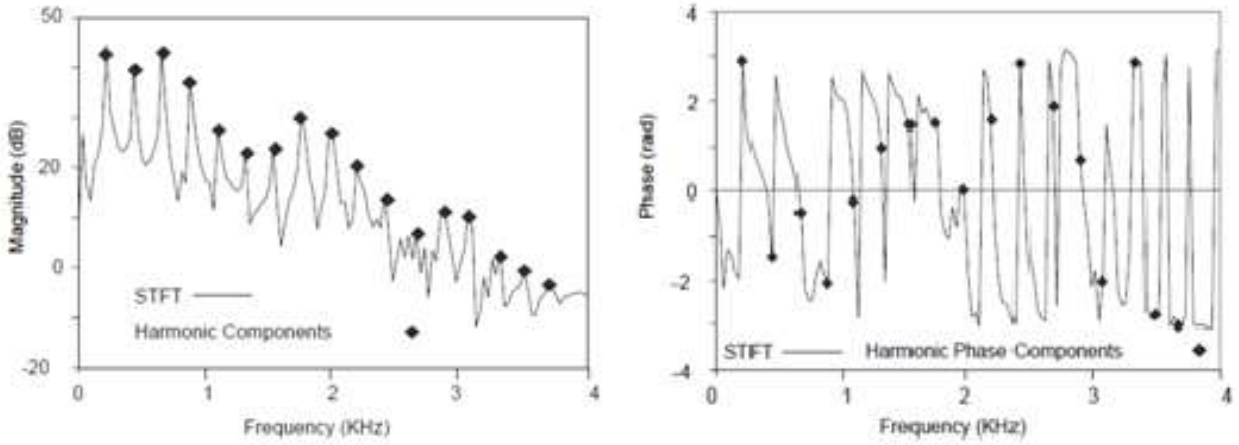

Рис. 3. Амплитуды и фазы участка речевого сигнала, выделенные с помощью дискретного преобразования Фурье
Fig. 3. Amplitudes and phases of a section of a speech signal isolated using a discrete Fourier transform

4. Области практического применения фазовых характеристик голосовых вокализмов

Из-за сложности современных информационных систем, и, вследствие этого, широчайшего спектра возможных угроз в том числе речевой информации, информационная безопасность таких систем требует от проектировщика и разработчика применения комплексного подхода к вопросам защиты информации. Перед построением системы защиты необходимо разработать модель угроз и нарушителя, при этом в общем случае закладывается предположение, что злоумышленник обладает всеми возможными ресурсами, в том числе техническими и интеллектуальными, для осуществления несанкционированного доступа к конфиденциальной информации, циркулирующей в информационной системе и каналах связи [18].

На рис. 4 приведёны некоторые методы защиты речевой информации от угроз целостности, конфиденциальной и доступности. Например, для купирования угрозы фейковых аудиозаписей (когда голосом известного человека озвучивают заранее подготовленный, обычно провокационный, текст), которые сейчас набирают популярность, можно использовать технологию речевой подписи. Для реализации данной технологии предлагается использовать фазовые характеристики голосовых вокализмов. На рис. 5 приведён пример построенной фазограммы с наложением спектрограммы, фактически это является неким графическим изображением звукового сигнала и позволяет его рассмотреть в многомерном пространстве – со стороны классической частоты и времени, а с другой стороны фазы и мощности (в градациях серого).

Кроме того, удобным такой формат представляется, в том числе, потому, что в него можно встроить биометрическую информацию о говорящем, например, рукописную подпись (рис. 6) или изображение отпечатка пальца.

Рис. 4. Методы защиты речевой информации
Fig. 4. Methods for protecting speech information

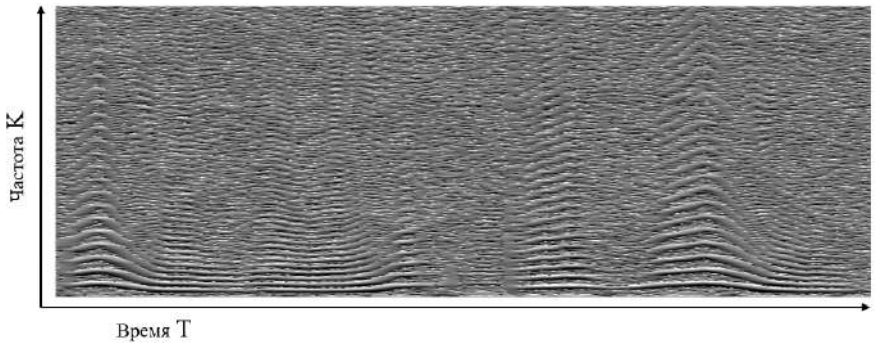

Рис. 5. Пример фазограммы с наложением спектрограммы
Fig. 5. An example of a phase chart with a spectrogram overlay

Применение фазовых характеристик речи позволит не только переосмыслить принципы использования технологии речевой подписи, но и решить некоторые другие прикладные задачи, связанные с речевой обработкой, в частности существенно повысить надёжность голосовой аутентификации и распознавания речи, а также улучшить защиту

речевого сигнала от несанкционированного доступа в выделенных защищаемых помещениях.

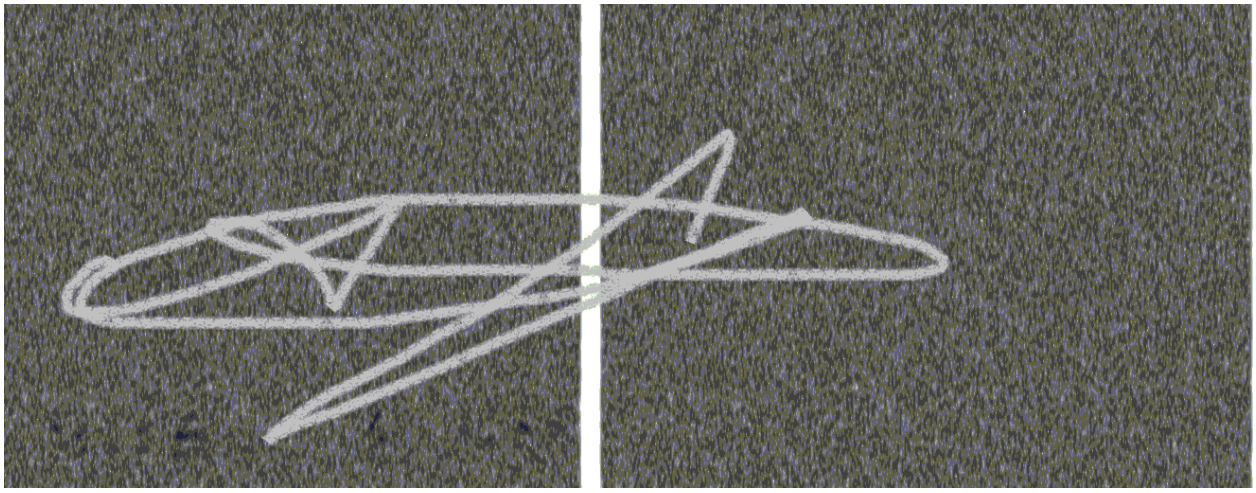

Рис. 6. Пример фазограммы с наложением рукописной подписи
Fig. 6. An example of a phasogram with overlaid handwritten signature

Заключение

В статье подробно представлены основные характеристики речевых сигналов (частотные, амплитудные, энергетические, временные и фазовые). Разобрана Гильбертовская модель речевого сигнала (в том числе для вокализованных и невокализованных звуковых сигналов) и принцип вычисления фазы по Гильберту. Выведена общая формула описания речевого сигнала на вокализованных участках. Представлена модель синусоидального описания речевого сигнала МакАуэля и Куатьери. Приведены примеры реконструкции сегмента голосовой речи при помощи линейной комбинации гармонических синусоид.

В заключение необходимо отметить, что фазовые характеристики голосовых вокализмов, а равно результаты настоящего исследования, полученные согласно поставленной цели, могут найти широкое применение при построении удобных и безопасных систем голосовой аутентификации говорящего (например, внедрение в фазограмму биометрии), а также в автоматических системах анализа, искусственного синтеза и распознавания речи.

СПИСОК ЛИТЕРАТУРЫ:

1. Федоринин М. Они нас слышат: куда развиваются речевые технологии? URL: https://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (дата обращения: 25.03.2021).
2. Жинкин Н.И. Речь как проводник информации. М.: Наука, 1982. – 159 с.
3. Хорев А.А. Технические каналы утечки акустической (речевой) информации // Специальная техника. 2009. № 5. С. 12–26. URL: https://elibrary.ru/item.asp?id=13011605 (дата обращения: 25.03.2021).
4. Дворянкин С.В., Дворянкин Н.С., Устинов Р.А. Развитие технологий образного анализа-синтеза акустической (речевой) информации в системах управления, безопасности и связи. Безопасность информационных технологий, [S.l.], Т. 26, № 1. С. 64–76, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1186 (дата обращения: 25.03.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.07.
5. Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. Принципы формирования тестовых речевых сигналов при оценках эффективности технологий шумоочистки // Вопросы кибербезопасности. 2018.

№ 3 (27). С. 9–15. URL: https://cyberleninka.ru/article/n/printsipy-formirovaniya-testovyh-rechevyh-signalov-pri-otsenkah-effektivnosti-tehnologiy-shumoochistki (дата обращения: 25.03.2021).
6. Gelfand S.A. Hearing: An introduction to psychological and physiological acoustics. 2nd edition. New York and Basel: Marcel Dekker, Inc., 1990. – 488 p.
7. Ахманова О.С. Словарь лингвистических терминов. М.: КомКнига, 2007. – 607 с.
8. Кармин Г. Презентации в стиле TED: 9 приёмов лучших в мире выступлений. М.: Альпина Паблишер, 2015. – 253 с.
9. Вартанян И.А. Звук — слух — мозг. Ленинград: Наука, 1981. – 176 с.
10. Дворянкин, Сергей В. и др. Системное моделирование речеподобных сигналов и его применение в сфере безопасности, связи и управления // Безопасность информационных технологий. [S.l.], Т. 26, № 4. С. 101–119, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1236 (дата обращения: 25.03.2021). DOI: http://dx.doi.org/10.26583/bit.2019.4.08.
11. Митянок В.В., Коновалов Л.В. Применение фазового анализа звуков речи для распознавания человека по его голосу // Техническая акустика. 2013. № 4. С. 1–10. URL: https://elibrary.ru/item.asp?id=21084028 (дата обращения: 25.03.2021).
12. Оппенгейм А.В. Применение цифровой обработки сигналов. М.: Мир, 1980. – 552 с.
13. Сергиенко А.Б. Цифровая обработка сигналов. СПб.: Питер, 2003. – 604 с.
14. Коржик В.И. Расширенное преобразование Гильберта и его применения в теории сигналов // Проблемы передачи информации. 1969. Т. 5, № 4. С. 3–18. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=1817&option_lang=rus (дата обращения: 25.03.2021 года).
15. Touradj E., Fernando P. The MPEG-4 Book. Prentice Hall Professional, 2002. – 896 p.
16. Покровский Н.Б. Расчёт и измерение разборчивости речи. М.: Связьиздат, 1962. – 390 с.
17. R. McAulay and T. Quatieri, Speech analysis/Synthesis based on a sinusoidal representation, in IEEE Transactions on Acoustics, Speech, and Signal Processing. V. 34, no. 4. P. 744–754, August 1986. DOI: http://dx.doi.org/10.1109/TASSP.1986.1164910.
18. Антипенко А.О. О методах обеспечения информационной безопасности в системах речевой связи // Modern Science. 2019. № 5–3. С. 187–195. URL: https://elibrary.ru/item.asp?id=38250230 (дата обращения: 25.03.2021).

REFERENCES:

[1] Fedorinin M. They hear us: where are speech technologies developing? URL: https://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (accessed: 25.03.2021) (in Russian).
[2] Zhinkin N.I. Speech as a conductor of information. M.: Nauka, 1982. – 159 p. (in Russian).
[3] Horev A.A. Technical channels of acoustic (speech) information leakage. Special'naja tehnika, 2009, no. 5. P. 12–26. URL: https://elibrary.ru/item.asp?id=13011605 (accessed: 25.03.2021) (in Russian).
[4] Dvoryankin, Sergey V., Dvoryankin, Nikita S., Ustinov, Roman A. Improvement of image analysis/synthesis technologies of acoustic (speech) information for the control, safety and communication systems. IT Security (Russia), [S.l.]. V. 26, no. 1. P. 64–76, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1186 (accessed 25.03.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.07 (in Russian).
[5] Kozlachkov S.B., Dvorjankin S.V., Bonch-Bruevich A.M. Principles of Formation of Test Speech Signals in Evaluating the Effectiveness of Noise Cleaning Technologies. Voprosy kiberbezopasnosti, 2018, no. 3 (27), P. 9–15. URL: https://cyberleninka.ru/article/n/printsipy-formirovaniya-testovyh-rechevyh-signalov-pri-otsenkah-effektivnosti-tehnologiy-shumoochistki (accessed: 25.03.2021) (in Russian).
[6] Gelfand S.A. Hearing: An introduction to psychological and physiological acoustics. 2nd edition. New York and Basel: Marcel Dekker, Inc., 1990. – 488 p.
[7] Ahmanova O.S. Dictionary of linguistic terms. M.: KomKniga, 2007. – 607 p. (in Russian).
[8] Karmin G. TED Presentations: 9 Tricks of the World's Best Speaking. M.: Al'pina Pablisher, 2015. – 253 p. (in Russian).
[9] Vartanjan I.A. Sound - hearing - brain. Leningrad: Nauka, 1981. – 176 p. (in Russian).
[10] Dvoryankin, Sergey V. et al. Speech-like signal system modeling and its application in the field of security, communication and control access. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 101–119, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1236. (accessed: 25.03.2021). DOI: http://dx.doi.org/10.26583/bit.2019.4.08 (in Russian).

[11] Mitjanok V.V., Konovalov L.V. Application of phase analysis of speech sounds to recognize a person by his voice. Tehnicheskaja akustika, 2013, no. 4. P. 1–10. URL: https://elibrary.ru/item.asp?id=21084028 (accessed: 25.03.2021) (in Russian).
[12] Oppengejm A.V. Digital Signal Processing Applications. M.: Mir, 1980. – 552 p. (in Russian).
[13] Sergienko A.B. Digital signal processing. SPb.: Piter, 2003. – 604 p. (in Russian).
[14] Korzhik V.I. Extended Hilbert transform and its applications in signal theory. Problems of Information Transmission, 1969. V. 5, no. 4. P. 1–14. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=1817&option_lang=rus (accessed: 25.03.2021) (in Russian).
[15] Touradj E., Fernando P. The MPEG-4 Book. Prentice Hall Professional, 2002. – 896 p.
[16] Pokrovskij N.B. Calculation and measurement of speech intelligibility. M.: Svjaz'izdat, 1962. – 390 p. (in Russian).
[17] R. McAulay and T. Quatieri, Speech analysis/Synthesis based on a sinusoidal representation, in IEEE Transactions on Acoustics, Speech, and Signal Processing. V. 34, no. 4. P. 744–754, August 1986. DOI: http://dx.doi.org/10.1109/TASSP.1986.1164910.
[18] Antipenko A.O. On methods of ensuring information security in voice communication systems. Modern Science, 2019, no. 5–3. P. 187–195. URL: https://elibrary.ru/item.asp?id=38250230 (accessed: 25.03.2021) (in Russian).

Поступила в редакцию – 29 января 2021 г. Окончательный вариант – 01 апреля 2021 г.
Received – January 29, 2021. The final version – April 01, 2021.

Александр И. Чумаков[1], Армен В. Согоян[2], Дмитрий В. Бобровский[3],
Дмитрий О. Титовец[4], Константин А. Чумаков[5], Сергей Ю. Дианков[6],
Виталий В. Хаустов[7], Олег А. Герасимчук[8], Дмитрий И. Юрков[9]
[1,2,3,4,8,9]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1,2,3,4]Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»,
Каширское ш., 31, 115409, Москва, 115409, Россия
[5]Федеральное государственное учреждение «Федеральный научный центр Научно-
исследовательский институт системных исследований Российской академии наук»,
Нахимовский пр-кт, 36, к.1, Москва, 117218, Россия
[6,7]ФГБУ 46 Центральный научно-исследовательский институт Министерства обороны
Российской Федерации,
Чукотский пр-д, д/вл 10, Москва, 129327, Россия
[1]e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-2663
[2]e-mail: avsog@spels.ru, https://orcid.org/0000-0002-9380-239X
[3]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953
[4]e-mail: dotit@spels.ru, http://orcid.org/0000-0002-4934-5945
[5]e-mail: kachumakov@mail.ru, https://orcid.org/0000-0003-2013-1350
[6]e-mail: diankov@yandex.ru, https://orcid.org/0000-0002-6399-8985
[7]e-mail: vvkhaustov@yandex.ru, https://orcid.org/0000-0003-0469-5439
[8]e-mail: oleg.gerasimchuk@bk.ru, https://orcid.org/0000-0003-2307-0848
[9]e-mail: dmitry_yurkov@mail.ru, https://orcid.org/0000-0002-4672-3007

ОСОБЕННОСТИ ОЦЕНКИ РАДИАЦИОННОЙ СТОЙКОСТИ ИНТЕГРАЛЬНЫХ СХЕМ К НЕЙТРОННОМУ ВОЗДЕЙСТВИЮ

DOI: http://dx.doi.org/10.26583/bit.2021.2.03

Аннотация. В работе проводится анализ особенностей возникновения доминирующих радиационных эффектов в современных полупроводниковых изделиях информационных, информационно-вычислительных и управляющих систем при нейтронном воздействии. Данные вопросы имеют существенное значение в свете расширения сферы практического применения в системах управления ядерными энергетическими и физическими установками микросхем повышенной степени интеграции, так как при нейтронном излучении возможно проявление всех основных доминирующих радиационных эффектов, оказывающих влияние на безопасность информационных систем. Показано, что существующие модели, основанные на оценке эквивалентности среднего энерговыделения (дозы), не в полной мере адекватно описывают эффекты от воздействия нейтронного излучения. В ряде случаев необходимо учитывать возможности проявления микродозиметрических эффектов, а в ряде случаев имеют место существенные расхождения из-за различий в процессах первичной рекомбинации избыточного заряда в окислах. Наличие сильной зависимости доли энергии, затрачиваемой на ионизацию, от энергии нейтронов приводит к отличиям в амплитудно-временных характеристиках мощности дозы и плотности потока нейтронов. Существенное уменьшение зарядов переключения в современных изделиях микроэлектроники приводит к появлению одиночных радиационных эффектов при воздействии нейтронов, что также необходимо учитывать при построении сбоеустойчивой электронной аппаратуры. Представленные результаты позволяют корректно проводить оценку стойкости полупроводниковых электронных изделий к нейтронному воздействию искусственного и естественного происхождений.

Ключевые слова: безопасность информационных систем, нейтронное излучение, доминирующие радиационные эффекты, структурные повреждения, объемная ионизация, первичная рекомбинация, одиночные эффекты.

Для цитирования: ЧУМАКОВ, Александр И. et al. ОСОБЕННОСТИ ОЦЕНКИ РАДИАЦИОННОЙ СТОЙКОСТИ ИНТЕГРАЛЬНЫХ СХЕМ К НЕЙТРОННОМУ ВОЗДЕЙСТВИЮ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 34–43, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1338>. Дата доступа: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.03.

Alexander I. Chumakov[1], Armen V. Sogoyan[2], Dmitry V. Bobrovsky[3],
Dmitry O. Titovets[4], Konstantin A. Chumakov[5], Sergey Y. Diankov[6],
Vitaly V. Khaustov[7], Oleg A. Gerasimchuk[8], Dmitry I. Yurkov[9]
*[1,2,3,4,8,9]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia*
*[1,2,3,4]Joint Stock Company "Experimental Research and Production Association
SPECIALIZED ELECTRONIC SYSTEMS"
Kashirskoe shosse, 31, Moscow, 115409, Russia*
*[5]Federal State Institution "Scientific Research Institute for System Analysis
of the Russian Academy of Sciences",
Nakhimovskiy prospekt, 36/1, Moscow, 117218, Russia*
*[6,7]46 Central Research Institute of the Russian Defense Ministry,
Chukotsky pr-d, 10, Moscow, 129327, Russia*
[1]e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-2663
[2]e-mail: avsog@spels.ru, https://orcid.org/0000-0002-9380-239X
[3]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953
[4]e-mail: dotit@spels.ru, http://orcid.org/0000-0002-4934-5945
[5]e-mail: kachumakov@mail.ru, https://orcid.org/0000-0003-2013-1350
[6]e-mail: diankov@yandex.ru, https://orcid.org/0000-0002-6399-8985
[7]e-mail: vvkhaustov@yandex.ru, https://orcid.org/0000-0003-0469-5439
[8]e-mail: oleg.gerasimchuk@bk.ru, https://orcid.org/0000-0003-2307-0848
[9]e-mail: dmitry_yurkov@mail.ru, https://orcid.org/0000-0002-4672-3007

Some aspects of IC radiation hardness evaluation when exposed to neutrons

DOI: http://dx.doi.org/10.26583/bit.2021.2.03

Abstract. Some features of dominant radiation effects in modern ICs of information, information-computing and control systems when exposed to neutrons are analysed. Occurrence of all main dominant radiation effects in ICs is possible under influence of neutrons. Thus these investigations are essential due to expanding the scope of practical application of VLSI in control systems of nuclear power and physical facilities, affecting the security of information systems. It is shown that the existing models based on the assessment of the equivalence of the average energy release (dose) do not fully adequately describe the effects of neutron radiation exposure. In some cases, there are occurrence of microdosimetric effects and significant deviations due to differences in the processes of primary recombination of excess charge in oxides. These effects should not be ignored. Ionisation energy depends on neutron energy, which leads to differences in the amplitude-time characteristics of the dose rate and the neutron flux density. A significant reduction in switching charges in modern microelectronics leads to the appearance of single event effects when exposed to neutrons, which must also be taken into account when constructing radiation-resistant electronic facilities. The presented results allow us to correctly assess the resistance of semiconductor electronic products to the neutron effects of artificial and natural origin.

Keywords: information security, neutron radiation, main radiation effects, general radiation effects, structural damage, volume ionization, primary recombination, single effects.
For citation: CHUMAKOV, Alexander I. et al. Some aspects of IC radiation hardness evaluation when exposed to neutrons. IT Security (Russia), [S.l.], v. 28, n. 2, p. 34–43, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1338>. Date accessed: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.03.

Введение

Характерной особенностью воздействия нейтронного излучения на интегральные схемы является проявление в них практически всех основных доминирующих эффектов: дефектообразование, объемная ионизация полупроводниковых структур, поверхностные и одиночные радиационные эффекты [1, 2]. Вместе с тем, оценка влияния доминирующих эффектов на отказы и сбои интегральных схем в информационно-вычислительных системах может отличаться от классических представлений, так как при нейтронном воздействии основное энерговыделение обусловлено потерями энергии в чувствительных объемах полупроводниковых элементов вторичными частицами в небольшой локальной области. Кроме того, в области энергий нейтронов до 10 МэВ потери энергии на структурные повреждения (дефектообразование) по порядку величины соизмеримы с ионизационными потерями. При энергиях выше 30…50 МэВ ощутимого различия между эффектами от протонов и нейтронов практически не наблюдается [3, 4]. Поэтому именно диапазон энергий, характерный для спектра быстрых нейтронов (0.1…15 МэВ), представляет наибольший интерес в силу наличия большого количества экспериментальных установок, работающих со спектрами ядерных реакций деления и синтеза.

1. Структурные повреждения

Данный вид радиационного повреждения наиболее изучен. Несмотря на то, что при нейтронном облучении в полупроводниковых материалах образуются разупорядоченные области [1, 2], состоящие из стабильных радиационных дефектов, считается, что структура радиационных дефектов не оказывает влияние на деградацию характеристик полупроводниковых приборов. Пересчет от одного вида излучения к другому может быть проведен по величине энергии, затрачиваемой на структурные повреждения (d-керма).

Однако такой подход может оказаться не применим в случае проявления микродозиметрических эффектов, т.е. тогда, когда среднее энерговыделение при одном взаимодействии нейтрона с веществом становится сравнимым с энергией, необходимой для отказа отдельного элемента [1, 5, 6]. Оценки показывают, что эти эффекты будут сказываться при величинах активного объема прибора V_a менее:

$$V_a \leq 100/(\Phi_n \times \Sigma_n), \quad (1)$$

где Φ_n – средний флюенс нейтронов, необходимый для отказа элемента, Σ_n – макроскопическое сечение взаимодействия нейтронов с веществом. Например, для спектра нейтронов реакции деления и при $\Phi_n = 10^{14}$ нейтрон/см^2 получим, что микродозиметрические эффекты будут влиять при величинах активного объема менее 1 мкм^3.

В настоящее время подобные эффекты проявляются в ПЗС элементах даже при создании одной разупорядоченной области внутри чувствительной области [1, 2, 7]. Увеличившийся ток утечки при вводе одной разупорядоченной области в чувствительный объем, как правило, приводит к потере одного пикселя. Очевидно, что в этом случае уже невозможно пользоваться пересчетом от эффективности воздействия одного излучения в другое по величине энергии, затрачиваемой на структурные повреждения. Задача может быть решена аналогичным образом, если вместо пороговой энергии образования точечного радиационного дефекта поставить пороговую величину образования одной разупорядоченной области.

2. Объемные ионизационные эффекты

Радиационные эффекты, вызванные объемной ионизацией импульсом быстрых нейтронов, необходимо оценивать с учетом энергетической зависимости энергии нейтронов, затрачиваемой на ионизацию. Дело в том, что эта зависимость в пределах энергий нейтронов в диапазоне 0.1…15 МэВ меняется практически на два порядка, поэтому нейтроны с малой энергией будут давать существенно меньший вклад в общую ионизацию полупроводниковой структуры. С другой стороны, из-за наличия спектральной зависимости нейтроны с разной энергией имеют различные скорости распространения в пространстве, вследствие чего длительность импульса нейтронов при удалении от источника излучения увеличивается. Эти два обстоятельства приводят к двум противоположным эффектам – увеличению длительности плотности потока нейтронов при удалении от источника нейтронов и уменьшению длительности импульса ионизации полупроводниковой структуры внутри этого импульса за счет различной эффективности ионизации при разных энергиях нейтронов. При этом последний эффект в значительной степени будет зависеть от полупроводникового материала, так как помимо энергии нейтронов коэффициент ионизационных потерь зависит от его химического состава материала [8]. Таким образом, в общем случае невозможно использовать непосредственную форму импульсов нейтронного излучения (плотности потока) для оценки объемных ионизационных эффектов в полупроводниковых структурах.

Наглядно это может быть показано при оценках эффективной мощности дозы от воздействия импульса нейтронов со спектром деления и монохроматического излучения с энергией равной 14 МэВ. Предположим, что действует комбинированный мгновенный источник нейтронов со спектром деления dN_n/dE:

$$\frac{dN_n}{dE} = k_f \cdot e^{-\frac{E}{E_o}} \cdot sh\left(\sqrt{\frac{2E}{E_o}}\right), \tag{2}$$

где E – энергия нейтронов в МэВ, E_o = 1 МэВ, а k_f – коэффициент нормировки для нейтронов деления и монохромное нейтронное излучение с энергией 14 МэВ:

$$\frac{dN_s}{dE} = k_s \cdot e^{-\left(\frac{E-E_s}{0.5E_o}\right)^2}, \tag{3}$$

где E_s = 14 МэВ, k_s – коэффициент нормировки для 14 МэВ нейтронов.

За счет того, что время пролета t_r от источника до детектора зависит от энергии

$$t_r \cong {R}\Big/{c\sqrt{2E/m_n}} \tag{4}$$

импульс растягивается во времени, где c – скорость света, m_n – масса нейтрона в МэВ (939.6 МэВ), R – расстояние от источника до детектора.

Из соотношений (2)–(4) нетрудно получить оценки плотности потока нейтронов на удалении R от источника нейтронов:

$$\frac{dN_n(t)}{dt} = k_d \cdot \exp\left(-\frac{E(t)}{E_o}\right) \cdot sh\left(\sqrt{\frac{2E(t)}{E_o}}\right) \cdot \frac{2E(t)}{t}, \tag{5a}$$

$$\frac{dN_s}{dt} = k_s \cdot e^{-\left(\frac{E(t)-E_s}{0.5E_o}\right)^2} \cdot \frac{2E(t)}{t}, \tag{5b}$$

где $E(t) = \frac{m_n}{2} \cdot \left(\frac{R}{c \cdot t_r}\right)^2$.

Умножив плотность потока на K_i – коэффициент ионизационных потерь от нейронов, получим эквивалентную мощность дозы. На рис. 1 и рис. 2 представлены

нормированные зависимости плотностей потока нейтронов и эквивалентной мощности дозы по кремнию для трех случаев. Первый случай соответствует только спектру вида (2), второй – спектру вида (3), а третий комбинация этих двух спектров, при этом вклад 14 МэВ нейтронов составляет всего 20% от общего числа нейтронов. При оценках для коэффициента ионизационных потерь от нейронов брались данные из работы [8].

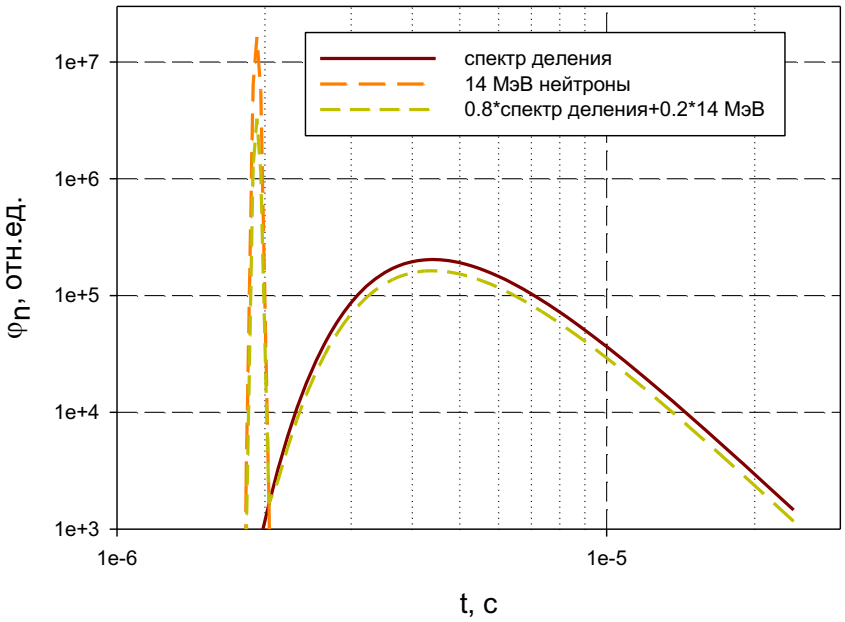

Рис. 1. Относительные значения плотности потоков нейтронов на расстоянии 100 м от точечного источника для разных спектров
Fig. 1. Relative values of the neutron flux density at a distance of 100 m from the point source for different spectra

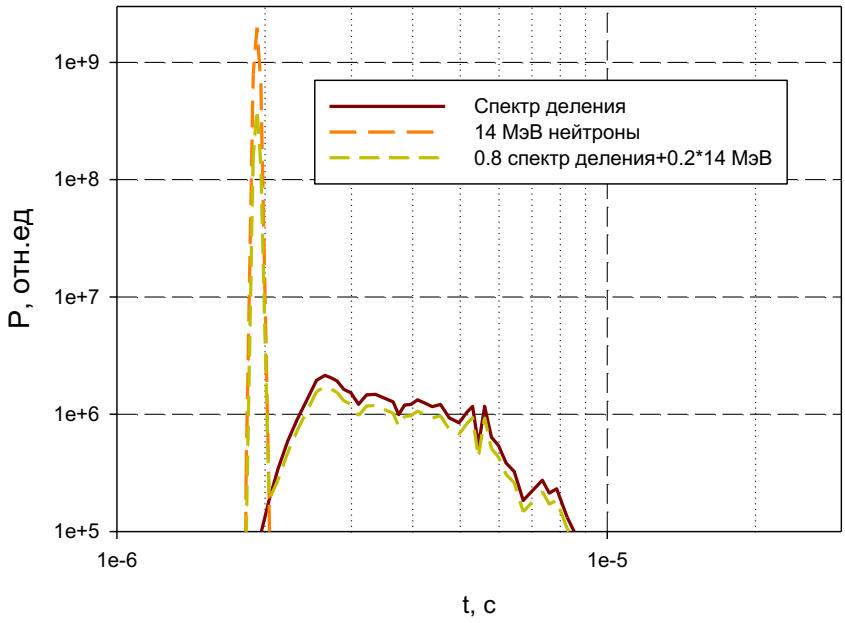

Рис. 2. Относительные значения мощности поглощенной дозы в кремнии при воздействии импульса нейтронов на расстоянии 100 м от точечного источника для разных спектров
Fig. 2. Relative values of the absorbed dose rate in silicon under the influence of a neutron pulse at a distance of 100 m from a point source for different spectra

Из сравнения представленных на рис. 1 и рис. 2 результатов можно сделать следующие выводы:

– отсутствует эквивалентность в амплитудно-временных характеристиках (АВХ) для плотности потока нейтронов и мощности поглощенной дозы. При этом при одной и той же АВХ для плотности потока нейтронов временные зависимости для мощности поглощенной дозы будут отличаться для разных материалов;

– кривые между собой близки только для монохроматичного излучения нейтронов;

– происходит существенное уменьшение длительности импульса для немонохроматичного излучения по эквивалентной мощности дозы по сравнению с плотностью потока нейтронов;

– форма импульса мощности поглощенной дозы получается неплавной из-за подобной зависимости сечений взаимодействия нейтронов с веществом;

– максимальные значения АВХ для плотности потока и мощности поглощенной дозы не совпадают по времени для немонохроматичных излучений;

– фактически максимальное значение мощности поглощенной дозы формируется нейтронами с большими энергиями;

– основные отличия в формах импульса имеют место на «хвостах», когда формируется суммарная доза. При оценках длительности импульса, например, по уровню 0.5, отличия получаются не очень значительными.

Представленные результаты свидетельствуют о том, что оценка уровней бессбойной работы и/или времени потери работоспособности невозможна, когда расчеты базируется только на АВХ плотностей потока нейтронов. Необходимо дополнительная информация о спектральных характеристиках нейтронного излучения.

В заключении следует отметить, что нейтронный спектр не является фиксированным на различных расстояниях от источника, так как имеют место потери энергии нейтронов при взаимодействии их с веществом, например, с атомами, входящими в состав атмосферы. Однако проведенные оценки на рис. 3 показывают, что на расстояниях порядка 100 м этими изменениями можно пренебречь.

3. Поверхностные ионизационные эффекты

На первый взгляд кажется, что при оценке радиационной стойкости интегральных микросхем и полупроводниковых приборов к эффектам суммарной дозы, обусловленной ионизацией, не должно быть особых проблем. На самом деле, это не так из-за того, что избыточный заряд формируется вторичными частицами – продуктами ядерного рассеяния, которые имеют относительно высокие линейные потери энергии (ЛПЭ). Вследствие этого эффективная поглощенная доза D_e будет несколько меньше суммарной поглощенной дозы за счет процессов первичной рекомбинации электронов и дырок в оксиде кремния:

$$D_e = k_\gamma \cdot K_i \cdot \Phi_n, \tag{6}$$

где k_γ – коэффициент первичной рекомбинации, величина которого в сильной степени зависит от напряженности электрического поля в оксиде и значений ЛПЭ. На рис. 4 в качестве примера представлены типовые зависимости, представленные в работе [9].

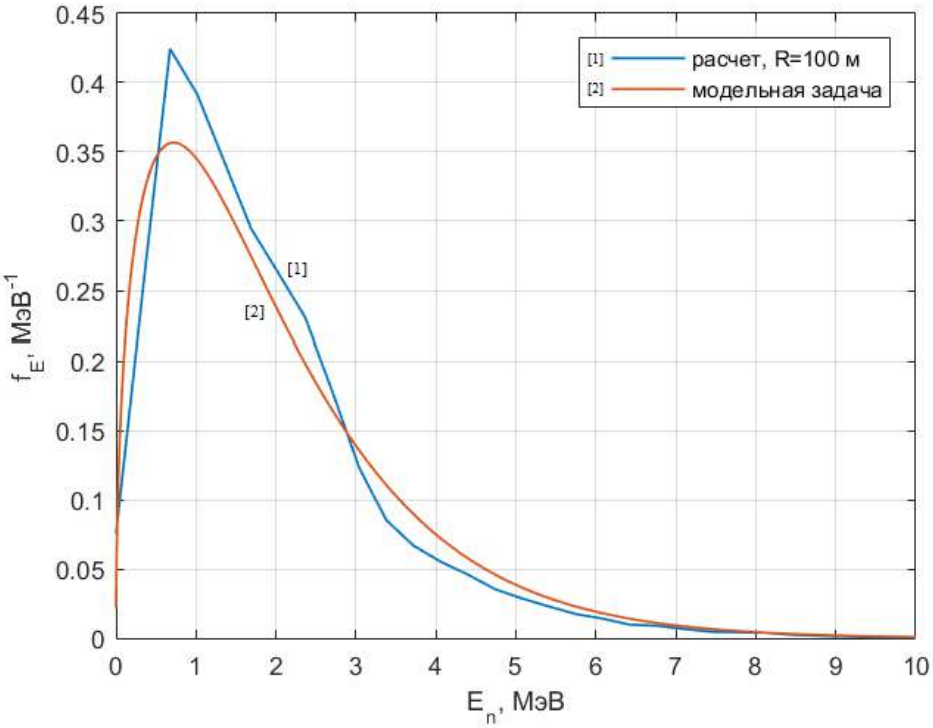

Рис. 3. Расчетные результаты по изменению спектра деления в атмосфере на расстоянии 100 м от точечного источника
(Fig. 3. Calculated results on the change in the fission spectrum in the atmosphere at a distance of 100 m from the point source)

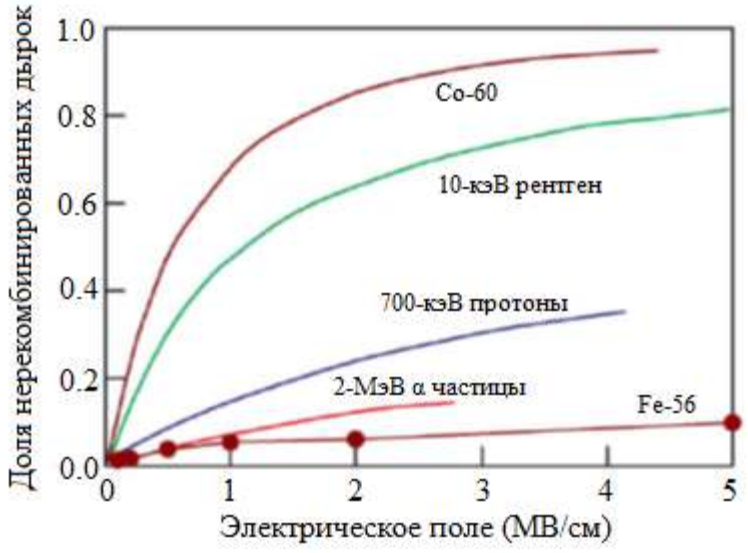

Рис. 4. Зависимости доли оставшихся дырок после процессов первичной рекомбинации от напряженности электрического поля в оксиде кремния [9]
Fig. 4. Charge yield electric field for Co-60 gamma rays, 10-keV X-rays, 700-keV protons, and 2 MeV α-particles in comparison to the charge yields for Fe ions [9]

Как видно, для получения количественных оценок необходимо определить среднее значение L_z ЛПЭ для вторичных частиц, продуктов взаимодействия нейтронов с

веществом. Достаточно грубая оценка L_z в единицах МэВ·см^2/мг может быть проведена из следующего соотношения:

$$L_z \approx 6.25 \cdot 10^4 \cdot K_i / (\Sigma_n \cdot R_s), \quad (7)$$

где Σ_n – макроскопическое взаимодействие нейтрона с веществом, R_s – средней пробег вторичной частицы.

Например, для спектра деления в кремнии $\Sigma_n \approx 0.16$ 1/см, $K_i \approx 5 \cdot 10^{-11}$ рад (Si)·нейтрон/см^2 и, положив $R_s \approx 1$ мкм, получим значение $L_z \approx 0.2$ МэВ·см^2/мг. Даже при таких достаточно грубых оценках получаем, что отличия в эффективных дозах при воздействии гамма-излучения и нейтронов при одной и той же суммарной поглощенной дозы составляет величину около порядка. Для 14 МэВ нейтронов эти различия еще будут более существенными.

С учетом того, что для спектра деления всегда присутствует сопутствующее гамма-излучение с эквивалентной мощностью дозы порядка 1 рад (Si)/с на плотность потока нейтронов с уровнем около 10^9 нейтрон/(см^2·с), можно уверенно пренебрегать вкладом нейтронного излучения в поверхностные радиационные эффекты. Только при воздействии «чистых» нейтронов синтеза этот вклад в ряде случаев надо учитывать. При этом надо иметь в виду, что эффективная суммарная доза по эффектам в оксидах кремния электронных изделий будет на два и более порядка меньше, чем следует из оценок суммарной поглощенной дозы.

4. Одиночные радиационные эффекты

Одиночные радиационные эффекты возникают в изделиях электронной техники при воздействии нейтронов за счет локального энерговыделения вторичными частицами – продуктами взаимодействия нейтронов с веществом. Проведенный анализ показывает, что в общем случае в интересующем диапазоне энергий нейтронов можно выделить три области энергий [10]:

– 0.1…2 МэВ – энерговыделение производят только первично выбитые атомы за счет упругого рассеяния нейтронов; см ВЫШЕ вначале введение …

– 2…5 МэВ – энерговыделение производят только атомы Si за счет упругого и неупругого рассеяний;

– 5…15 МэВ – энерговыделение производят атомы Si за счет упругого и неупругого рассеяний, а также тяжелые вторичные ядерные частицы – продукты ядерных реакций.

Хотя ядерные реакции и начинаются в кремнии с энергий выше 4.2 МэВ, но сечение их до 5 МэВ достаточно малое, что позволяет в этой области их не учитывать.

В современных СБИС с проектными нормами менее 90 нм используется медная металлизация, что потенциально может приводить к генерации вторичных частиц, образующихся в меди. Однако в этом случае энергетика тяжелых ядерных частиц будет достаточно низкая (менее 1 МэВ), что с учетом их малых пробегов и более значимой доли энергии, затрачиваемой на структурные повреждения, приведут к незначительному вкладу в общую чувствительность. Возможным механизмом в этом случае, приводящим к ОРЭ, будет ионизация вторичными альфа-частицами, но, по сути дела, этот механизм будет проявляться и для других более лёгких материалов (кремний, алюминий).

Оценку чувствительности к одиночным радиационным эффектам можно проводить на основе BGR функции или используя более простые полуаналитические модели [11]. В любом случае при использовании подобных подходов необходимо определение двух независимых параметров, которые могут быть оценены из независимых экспериментов.

Наиболее информативными будут эксперименты, проведенные при двух энергиях нейтронах. Анализ показывает, что наиболее подходящим вариантом является облучение моноэнергетичными нейтронами синтеза с энергиями около 2 МэВ и 14 МэВ. Подобные условия эксперимента могут быть получены на генераторах нейтронов, например, на генераторе НГ-14 или аналогичных [12].

Заключение

Представленные в настоящей работе результаты, оказывающие влияние на безопасность информационных систем, кратко можно сформулировать следующим образом:

– классический подход по оценке уровней отказов полупроводниковых изделий, основанный на эквивалентности значений энергий, затрачиваемых на структурные повреждения, не применим для изделий с активными чувствительными объемами менее 1 мкм^3;

– оценка отказов, обусловленных структурными повреждениями, вследствие создания одной разупорядоченной области в активном объеме, возможна к другим воздействиям, если пересчет проводить с учетом пороговой энергии образования разупорядоченной области;

– форма импульса мощности поглощенной дозы значительно отличается от амплитудно-временных характеристик плотности потока нейтронов из-за сильной зависимости удельных ионизационных потерь от энергии нейтронов;

– оценка уровней дозовых отказов вследствие поверхностных радиационных эффектов по эквивалентности значений суммарной поглощенной дозе приводит к очень значительным ошибкам для нейтронного воздействия из-за малых значений выхода дырок после процессов первичной рекомбинации;

– оценка чувствительности электронных изделий по одиночным радиационным эффектам при воздействии нейтронного излучения произвольного спектра может быть оценена с использованием не менее двух независимых экспериментов при разных энергиях нейтронов.

СПИСОК ЛИТЕРАТУРЫ:

1. Чумаков А.И. Действие космической радиации на ИС. М.: Радио и связь. 2004. – 320 с.
2. Радиационная стойкость изделий ЭКБ. Научное издание. /Под ред. А.И. Чумакова. М.: НИЯУ МИФИ, 2015. – 512 с.
3. Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices. JEDEC Standard No. 89A, Oct 2006, p. 84.
4. Чумаков А.И., Афонин А.В., Полунин В.А. Особенности энерговыделения в микрообъемах элементов СБИС при воздействии нейтронного излучения. Известия ВУЗов. Электроника. 5(97), 2012. С. 5–10.
5. Агаханян Т.М., Аствацатурьян Е.Р., Чумаков А.И. Особенности использования БИС и сверхБИС в аппаратуре ядерного физического эксперимента//Электронные приборы и схемы для экспериментальной физики / Под ред. Т.М. Агаханяна. М.: Энергоатомиздат, 1983. С. 3–9.
6. Agahanyan T.M., Astvacaturyan E.R., Chumakov A.I. On the possibility of controlling non-stationary annealing characteristics in a stationary environment//International Journal of Electronics. 1986. Vol. 61, no. 1. P. 73–78.
7. The Radiation Design Handbook. European Space Agency. ESTEC, Noordwijk, the Nederlands, 1993. – 444 p.
8. Bendel W. Displacement and ionization fractions of fast neutron Kerma in TLDs and Si//IEEE Trans. on Nucl. Sci., Vol. NS-24, no. 6. P. 2516–2521. December 1977. DOI: http://dx.doi.org/10.1109/TNS.1977.4329248
9. Javanainen A., Schwank J.R., Shaneyfelt M.R. et al. Heavy-Ion Induced Charge Yield in MOSFETs//IEEE Trans. on Nucl. Sci., Vol. 56, no. 6. P. 3367–3371, December 2009. DOI: http://dx.doi.org/10.1109/TNS.2009.2033687.

10. Чумаков А.И. Оценка чувствительности СБИС к одиночным радиационным эффектам при нейтронном воздействии. Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2020. № 2. С. 153–157. DOI: http://dx.doi.org/10.31114/2078-7707-2020-2-153-157.
11. Титовец Дмитрий О. и др. Использование функции генерации заряда при оценке параметров чувствительности КМОП микросхем к одиночным сбоям при воздействии нейтронов. Безопасность информационных технологий, [S.l.]. Т. 27, № 3, С. 89–97, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1295 (дата обращения: 08.09.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.08.
12. Юрков Дмитрий И. и др. Уникальный прототип радиотерапевтической установки: p53- независимый антипролиферативный эффект нейтронного облучения // Acta Naturae (русскоязычная версия). 2019. Т. 11, № 3. С. 33–36. DOI: http://dx.doi.org/10.32607/20758251-2019-11-3-99-102.

REFERENCES:
[1] Chumakov A.I., Effects of Cosmic Radiation on IC, M.: Radio i Svyaz', 2004. – 319 p. (in Russian).
[2] Radiation resistance of ECB products. /Under red. A.I. Chumakov. M.: NRNU MEPhI, 2015. – 512 p. (in Russian).
[3] Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices. JEDEC Standard No. 89A, Oct 2006, p. 84.
[4] Chumakov A.I., Afonin A.V. Polunin V.A. Features of energy release in microvolumes of VLSI elements upon the effect of neutron radiation Russian Microelectronics.Vol. 42, Issue 7, December 2013. P. 424–427.
[5] Agahanyan T.M., Astvacaturyan E.R., Chumakov A.I. Features of the use of LSI and VLSI in the equipment of a nuclear physics experiment. M.: Atomenergoizdat, 1983. P. 3–9 (in Russian).
[6] Agahanyan T.M., Astvacaturyan E.R., Chumakov A.I. On the possibility of controlling non-stationary annealing characteristics in a stationary environment//International Journal of Electronics. 1986. Vol. 61, no. 1. P. 73–78.
[7] The Radiation Design Handbook. European Space Agency. ESTEC, Noordwijk, the Nederlands, 1993. – 444 p.
[8] Bendel W. Displacement and ionization fractions of fast neutron Kerma in TLDs and Si//IEEE Trans. on Nucl. Sci., Vol. NS-24, no. 6. P. 2516–2521. December 1977. DOI: http://dx.doi.org/10.1109/TNS.1977.4329248.
[9] Javanainen A., Schwank J. R., Shaneyfelt M. R. et al. Heavy-Ion Induced Charge Yield in MOSFETs//IEEE Trans. on Nucl. Sci., Vol. 56, no. 6. P. 3367–3371, December 2009. DOI: http://dx.doi.org/10.1109/TNS.2009.2033687.
[10] Chumakov A.I. Estimation of Single Event Effect Sensitivity in VLSI to Neutron Irradiation. Problemy razrabotki perspectivnih micro- i nanoelectronnih system (MES). 2020, no. 2. P. 153–157. DOI: http://dx.doi.org/10.31114/2078-7707-2020-2-153-157 (in Russian).
[11] Titovets Dmitry O. et al. Evaluating CMOS chip sensitivity parameters to single event upsets under influence of neutrons by the burst generation rate function. IT Security (Russia), [S.l.]. Vol. 27, no. 3. P. 89–97, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1295 (accessed: 08.09.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.08 (in Russian).
[12] Yurkov D.I. et al. The unique prototype of a radiotherapy unit: p53-independent antiproliferative effect under neutron irradiation. // Acta Naturae (Russian edition). 2019. Vol. 11, no. 3. P. 33–36. DOI: http://dx.doi.org/10.32607/20758251-2019-11-3-99-102 (in Russian).

Поступила в редакцию –22 февраля 2021 г. Окончательный вариант – 05 апреля 2021 г.
Received – February 22, 2021. The final version – April 05, 2021.

Ольга В. Бойправ[1], Александр В. Потапович[2], Вадим А. Богуш[3], Леонид М. Лыньков[4]
Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, Минск, 220013, Беларусь
[1]e-mail: smu@bsuir.by, https://orcid/org/0000-0002-9987-8109
[2]e-mail: nil53@bsuir.edu.by, https://orcid/org/0000-0002-7403-9034
[3]e-mail: bogush@bsuir.by, https://orcid.org/0000-0001-7516-4841
[4]e-mail: leonid@bsuir.by, https://orcid/org/0000-0001-6578-7113

ЭКСПЕРИМЕНТАЛЬНОЕ ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛАСТИЧНЫХ И ВОЗДУХОПРОНИЦАЕМЫХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ НА ОСНОВЕ ФОЛЬГИРОВАННЫХ МАТЕРИАЛОВ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ ПЕРЕХВАТА

DOI: http://dx.doi.org/10.26583/bit.2021.2.04

Аннотация. В статье представлены результаты исследования влияния эластичных и воздухопроницаемых электромагнитных экранов на основе фольгированных материалов на уровни электромагнитного излучения в диапазоне частот 0,4…2,5 ГГц, формируемого имитаторами приемопередающих устройств несанкционированного съема информации вследствие воздействия на эти имитаторы короткими радиоимпульсами. Данное исследование проведено с целью экспериментального обоснования возможности использования указанных экранов для защиты речевой информации от утечки по прямому акустическому и параметрическому каналам. В ходе проведения исследования была применена методика, основанная на использовании аппаратно-программного комплекса «Локатор для обнаружения устройств ЛВ-2Р», предназначенного для выявления приемопередающих устройств несанкционированного съема информации по резонансным явлениям в их антенных системах и в сопутствующих фильтрующих элементах и включающего в себя автономный генераторно-приемный блок, антенну широкополосную, персональный компьютер, на котором установлено специальное программное обеспечение для детальной обработки информации, комплект соединительных кабелей и комплект имитаторов устройств несанкционированного съема информации. На основе результатов проведенного исследования установлено, что эластичные и воздухопроницаемые электромагнитные экраны на основе фольгированных материалов обеспечивают снижение уровня электромагнитного излучения, формируемого имитаторами устройств несанкционированного съема информации вследствие воздействия на них коротких радиоимпульсов, до тех величин, при которых это излучение не может быть зарегистрировано приемными антеннами. Вследствие этого сделан вывод о том, что исследованные электромагнитные экраны представляются перспективным решением для обеспечения защиты информации от утечки по прямому акустическому и параметрическому каналам. Такие экраны рекомендованы для использования в виде облицовочных модулей для стен помещений, в пределах которых циркулирует речевая информация ограниченного распространения, и внутри которых могут быть установлены или расположены устройства, предназначенные или соответственно применяемые для ее несанкционированного съема.

Ключевые слова: параметрический канал утечки речевой информации, фольгированный материал, электромагнитный экран.

Для цитирования: БОЙПРАВ, Ольга В. et al. ЭКСПЕРИМЕНТАЛЬНОЕ ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛАСТИЧНЫХ И ВОЗДУХОПРОНИЦАЕМЫХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ НА ОСНОВЕ ФОЛЬГИРОВАННЫХ МАТЕРИАЛОВ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ ПЕРЕХВАТА. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 44–53, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1339>. Дата доступа: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.04.

Olga V. Boiprav[1], Aleksandr V. Potapovich[2], Vadim A. Bogush[3], Leonid M. Lynkou[4]
Belarusian State University of Informatics and Radioelectronics,
P. Brovki str., 6, Minsk, 220013, Belarus
[1]e-mail: smu@bsuir.by, https://orcid/org/0000-0002-9987-8109
[2]e-mail: nil53@bsuir.edu.by, https://orcid/org/0000-0002-7403-9034
[3]e-mail: bogush@bsuir.by, https://orcid.org/0000-0001-7516-4841
[4]e-mail: leonid@bsuir.by, https://orcid/org/0000-0001-6578-7113

Experimental substantiation of the possibility of using the elastic and air-permeable electromagnetic shields based on foiled materials for protecting voice information from leakage

DOI: http://dx.doi.org/10.26583/bit.2021.2.04

Abstract. The paper presents the results of a study of the influence of elastic and air-permeable electromagnetic shields based on foiled materials on the levels of electromagnetic radiation in the frequency range of 0.4...2.5 GHz, generated by simulators of simulators of devices for unauthorized retrieval of information due to an exposure to these simulators by short radio pulses. This study has been carried out with the aim of experimentally substantiation the possibility of these shields use to protect speech information from leakage via the direct acoustic and parametric channels. In the course of the study, the method based on the use of the hardware and software complex “Locator for the detection of LV-2R devices”, designed to identify transceiver devices for unauthorized retrieval of information based on the resonance phenomena in their antenna systems and in associated filter elements and including an autonomous a generating and receiving unit, the broadband antenna, the personal computer on which special software for detailed information processing is installed, the set of connecting cables and the set of simulators of devices for unauthorized retrieval of information, has been applied. It has been found that elastic and air-permeable electromagnetic shields based on foiled materials reduce the level of electromagnetic radiation generated by simulators of devices for unauthorized retrieval of information due to exposure to them by short radio pulses, to those values at which this radiation can not be recorded by receiving antennas. As a result, it has been concluded that the investigated electromagnetic shields are the promising solution for ensuring the information protection from leakage via the direct acoustic and parametric channels. Such shields are recommended for use as cladding modules for rooms designed for speech information of limited distribution and where devices used for its unauthorized retrieval could be installed or located.

Keywords: parametric channel of speech information leakage, foiled material, electromagnetic shield.
For citation: BOIPRAV, Olga V. et al. Experimental substantiation of the possibility of using the elastic and air-permeable electromagnetic shields based on foiled materials for protecting voice information from leakage. IT Security (Russia), [S.l.], v. 28, n. 2, p. 44–53, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1339>. Date accessed: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.04.

Введение

В работах [1, 2] представлены результаты экспериментального обоснования перспективности использования эластичных и воздухопроницаемых электромагнитных экранов, изготовленных в соответствии со способом, описанным в [3], для маскирования наземных объектов в радиолокационном и инфракрасном диапазонах длин электромагнитных волн, или, иными словами, для защиты информации о таких объектах от утечки по комплексируемым инфракрасному и радиолокационному каналам. Такие экраны представляют собой изготовленные из трикотажного материала чехлы, заполненные фрагментами на основе фольгированных материалов. Передние и задние стенки таких чехлов соединены друг с другом путем ниточного соединения вдоль условных продольных и поперечных параллельных линий, идущих параллельно друг

другу с шагом не более 3,0 см [3]. Внешний вид одного из указанных экранов представлен на рис. 1 [1].

Рис. 1. Внешний вид эластичного и воздухопроницаемого электромагнитного экрана на основе фольгированных материалов
Fig. 1. Appearance of an elastic and air-permeable electromagnetic shield based on foil materials

В рамках работы, результаты выполнения которой представлены в настоящей статье, выполнены исследования, направленные на экспериментальное обоснование возможности использования эластичных и воздухопроницаемых электромагнитных экранов для:

– защиты речевой информации от перехвата по прямому акустическому каналу, реализуемого с помощью закладных устройств, устанавливаемых внутри помещений, в пределах которых циркулирует речевая информация ограниченного распространения [4];

– защиты речевой информации от перехвата по параметрическому каналу, реализуемого путем воздействия электромагнитным излучением радиочастотного диапазона на вспомогательные технические средства и системы, характеризующиеся «микрофонным эффектом» и расположенные внутри помещений, в пределах которых циркулирует речевая информация ограниченного распространения [5, 6].

Актуальность проведения таких исследований обусловлена рядом причин.

1. В настоящее время перехват информации ограниченного распространения чаще всего реализуется по акустическим техническим каналам утечки в связи с тем, что речевые сигналы чаще, чем электромагнитные волны, являются носителями такой информации [7].

2. Процесс перехвата речевой информации, реализуемый с помощью закладных устройств или путем воздействия электромагнитным излучением радиочастотного

диапазона на вспомогательные технические средства и системы, характеризуется большей скрытностью по сравнению с процессом перехвата аналогичной информации по акустическим техническим каналам других разновидностей. Это связано с тем, что:

– закладные устройства по сравнению с другими устройствами несанкционированного съема речевой информации характеризуются миниатюрными размерами и могут быть скрытно установлены в помещении, в пределах которого циркулирует речевая информация ограниченного распространения [8];

– воздействие электромагнитным излучением радиочастотного диапазона на вспомогательные технические средства и системы, характеризующиеся «микрофонным эффектом» и расположенные внутри помещений, в пределах которых циркулирует речевая информация ограниченного распространения, может быть реализовано за границами контролируемой зоны [9].

1. Методика проведения эксперимента

Для экспериментального обоснования возможности использования эластичных и воздухопроницаемых электромагнитных экранов на основе фольгированных материалов [1–3] для защиты речевой информации от утечки по прямому акустическому и параметрическому каналам была применена методика, основанная на использовании аппаратно-программного комплекса «Локатор для обнаружения устройств ЛВ-2Р» (далее – комплекс). Комплекс предназначен для выявления приемопередающих устройств несанкционированного съема информации по резонансным явлениям в их антенных системах и в сопутствующих фильтрующих элементах. Комплекс включает в себя следующие устройства:

– автономный генераторно-приемный блок;

– антенна широкополосная АШ 0,3–3;

– комплект комбинированный, в состав которого входят адаптер питания, кабель питания от сети переменного тока 220 В, кабель соединительный, стереонаушники, кабель USB;

– персональный компьютер, на котором установлено специальное программное обеспечение для детальной обработки информации;

– комплект из пяти имитаторов устройств несанкционированного съема информации, каждый из которых отличается определенной рабочей частотой, соответствующей либо частоте сигналов, используемых для передачи данных в системах сотовой связи, либо частоте GPS-сигналов, либо частоте, относящейся к ISM-диапазону (имитатор № 1 – 434 МГц, имитатор № 2 – 900 МГц, имитатор № 3 – 1880 МГц, имитатор № 4 – 1575 МГц, имитатор № 5 – 2,45 ГГц); в конструкцию каждого из имитаторов входят компоненты беспроводных систем: микросхема приемопередатчика, фильтры, антенна.

Автономный генераторно-приемный блок комплекса обеспечивает генерацию зондирующих сигналов и обработку принимаемых переизлученных сигналов в заданном диапазоне частот в режиме реального времени. Тип генерируемых рассматриваемым блоков сигналов – перестраиваемые по частоте гармонические короткие радиоимпульсы[1].

Внешний вид автономного генераторно-приемного блока комплекса представлен на рис. 2, 3.

[1]ГЛЮИ.464425.001 РЭ. Локатор для обнаружения устройств несанкционированного съема информации ЛВ-2Р. Руководство по эксплуатации. Минск: БГУИР, 2016. – 34 с.
[1]GLUI.464425.001 RE. Locator for detecting devices for unauthorized information retrieval LV-2R. Manual. Minsk: BSUIR, 2016. – 34 p. (in Russian).

Рис. 2. Внешний вид спереди автономного генераторно-приемного блока комплекса: 1 – разъем типа SMA для подключения приемо-передающей антенны; 2 – дисплей; 3 – клавиатура; 4 – динамик; 5 – индикатор питания
Fig. 2. Front view of the autonomous generator-receiving unit of the complex: 1-SMA connector for connecting the receiving and transmitting antenna; 2-display; 3-keyboard; 4-speaker; 5-power indicator

Рис. 3. Внешний вид сзади автономного генераторно-приемного блока комплекса: 1 – разъем для подключения внешнего источника питания; 2 – разъем USB для подключения к персональному компьютеру; 3 – разъем mini Jack Ø3,5 мм для подключения стереонаушников
Fig. 3. Rear view of the autonomous generator and receiver unit of the complex: 1-connector for connecting an external power source; 2-USB connector for connecting to a personal computer; 3-mini Jack connector Ø3. 5 mm for connecting stereo headphones

Внешний вид окна специального программного обеспечения для детальной обработки информации, установленного на персональном компьютере, представлен на рис. 4.

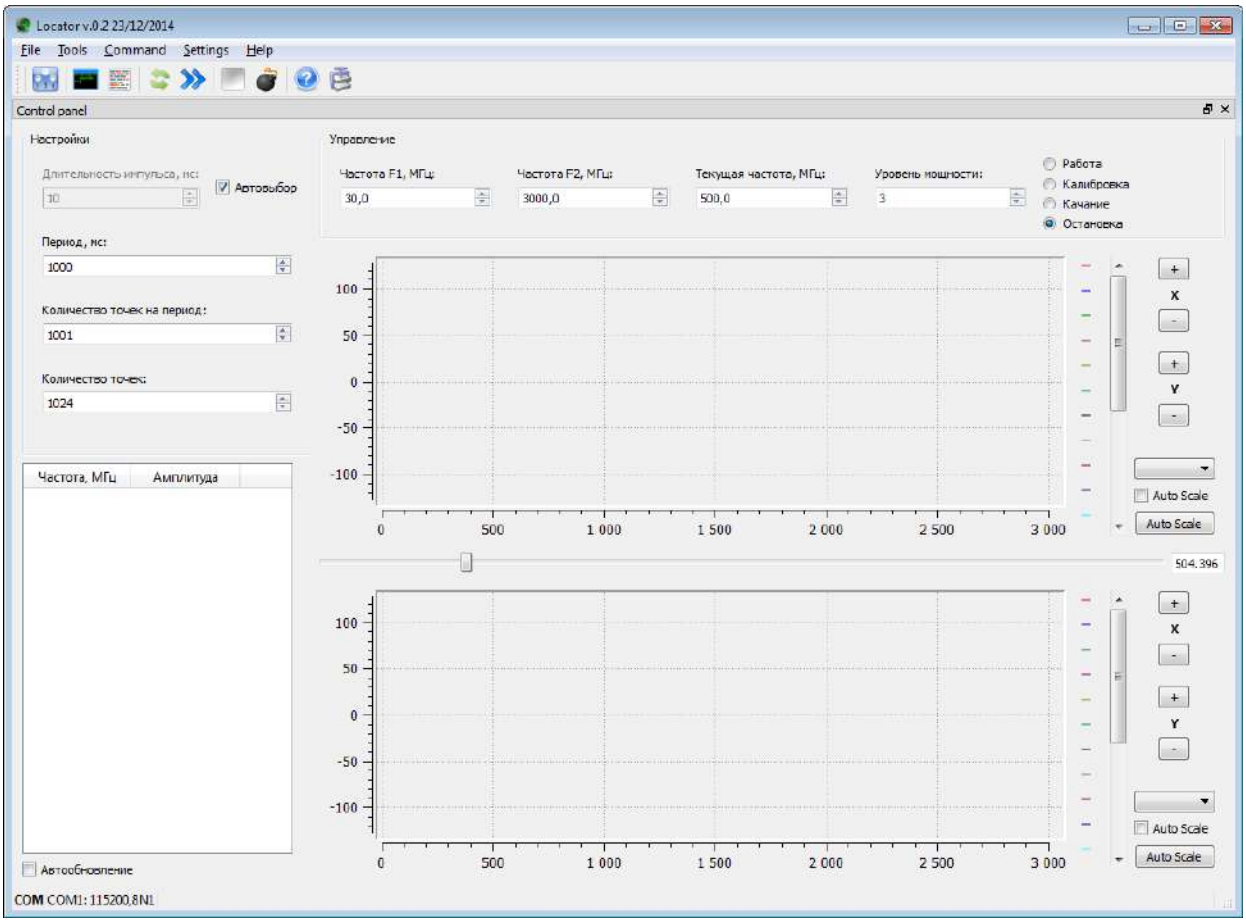

Рис. 4. Внешний вид окна программы специального программного обеспечения для детальной обработки информации
Fig. 4. Appearance of the program window of special software for detailed information processing

Внешний вид имитаторов устройств несанкционированного съема информации представлен на рис. 5.

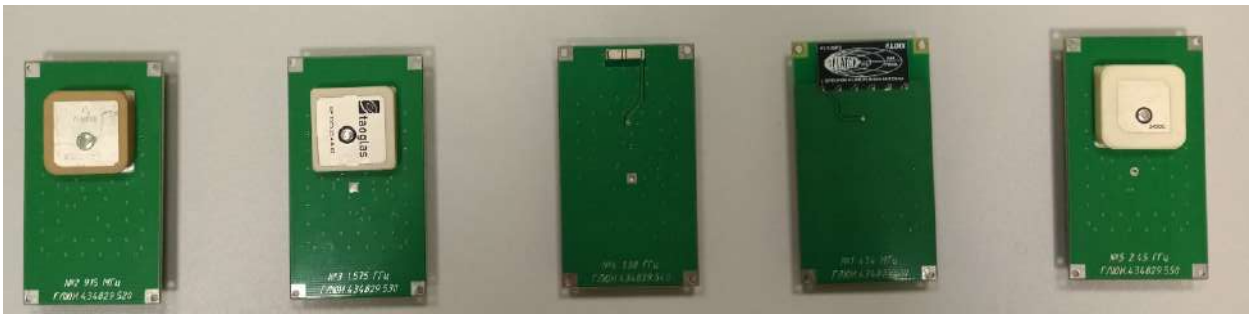

Рис. 5. Внешний вид имитаторов устройств несанкционированного съема информации
Fig. 5. Appearance of imitators of unauthorized information retrieval devices

Примененная для экспериментального обоснования методика включает следующие шаги.

Шаг 1. Соединение устройств комплекса в соответствии со схемой, представленной на рис. 6.

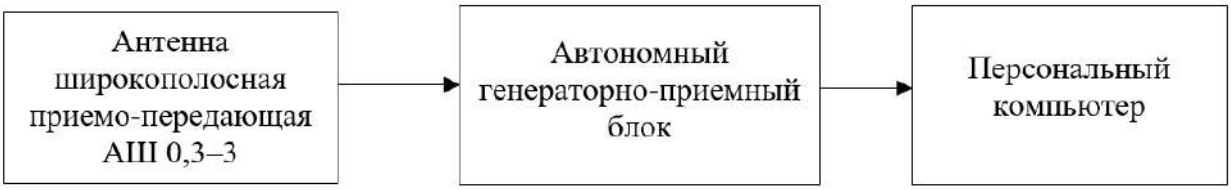

Рис. 6. Схема соединения устройств комплекса в ходе проведения экспериментального обоснования
Fig. 6. Connection diagram of the complex devices during the experimental study

Шаг 2. Размещение одного из имитаторов устройств несанкционированного съема информации на расстоянии 0,5 м от приемо-передающей антенны.

Шаг 3. Запуск автономного генераторно-приемного блока и специального программного обеспечения для детальной обработки информации, установленного на персональном компьютере с целью формирования коротких радиоимпульсов.

Шаг 4. Воздействие короткими радиоимпульсами на имитатор устройства несанкционированного съема информации.

Шаг 5. Регистрация с помощью автономного генераторно-приемного блока комплекса, подключенной к нему антенны широкополосной приемо-передающей и специального программного обеспечения для детальной обработки информации, установленного на персональном компьютере, сигнала, переизлученного имитатором устройства несанкционированного съема информации вследствие воздействия на этот имитатор короткими радиоимпульсами.

Шаг 6. Размещение исследуемого эластичного и воздухопроницаемого электромагнитного экрана поверх имитатора устройства несанкционированного съема информации.

Шаг 6. Повторная реализация шагов 4, 5.

Шаг 7. Сравнительный анализ данных, полученных в результате реализации шагов 5 и 6.

2. Результаты и их обсуждение

На рисунках 7 (a, b, c, d, e) представлены частотные характеристики сигналов, переизлученных имитаторами №№ 1–5 вследствие воздействия на них короткими радиоимпульсами, сформированными с помощью автономного генераторно-приемного блока комплекса и подключенной к нему антенны широкополосной приемо-передающей. На рисунке 7f представлена частотная характеристика сигнала, переизлученного каждым из указанных имитаторов, зарегистрированного в условиях, при которых поверх них расположен эластичный и воздухопроницаемый электромагнитный экран, изготовленный в соответствии со способом, описанным в [3].

На основе результатов сравнительного анализа характеристик, представленных на рисунках 7 (a, b, c, d, e) и характеристики, представленной на рисунке 7f установлено, что эластичный и воздухопроницаемый электромагнитный экран, изготовленный в соответствии со способом, описанным в [3], обеспечивает снижение уровня сигнала, переизлучаемого имитаторами устройств несанкционированного съема информации вследствие воздействия на него короткими радиоимпульсами, до уровней, при которых этот сигнал не может быть зарегистрирован приемной антенной.

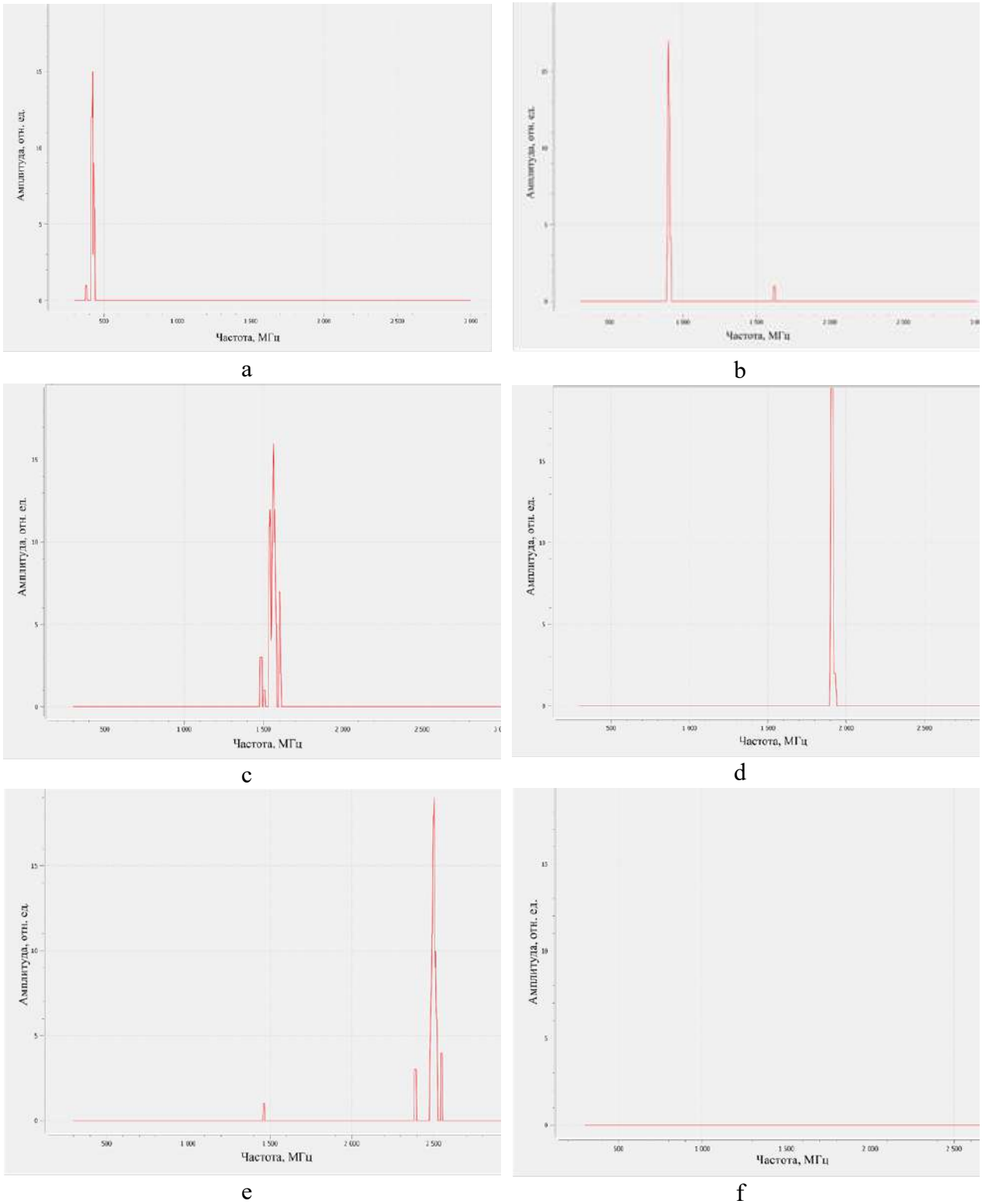

Рис.7. Частотные характеристики сигналов, переизлученных имитаторами: (a – № 1, b – № 2, c - № 3, d - № 4, e - № 5, f - №№ 1–5, поверх которых размещен электромагнитный экран)

Fig. 7. Frequency characteristics of the signal re-emitted by the simulators: (a - No. 1, b-No. 2, c - No. 3, d - No. 4, e - No. 5, f - No. 1-5, on top of which an electromagnetic shield is placed)

Заключение

На основе полученных результатов можно сделать вывод о том, что эластичные и воздухопроницаемые электромагнитные экраны, изготовленные в соответствии со способом, описанным в [3], могут быть использованы для обеспечения защиты информации от перехвата по прямому акустическому (с помощью закладных устройств) и параметрическому каналам. Для достижения обозначенной цели такие экраны следует закреплять на стенах помещений, в которых проводятся переговоры, предметом которых является информация ограниченного распространения. По сравнению с аналогами исследованные экраны характеризуются пониженной массой. Кроме того, процесс их изготовления характеризуется более низкими временными затратами по сравнению с процессом изготовления аналогов [10–14].

СПИСОК ЛИТЕРАТУРЫ:

1. Бойправ О.В., Лыньков Л.М., Аль-Машатт Е. А.А., Абдулхади Х. Д.А. Эластичные электромагнитные экраны на основе комбинированных металлосодержащих элементов // Материалы XXIII научно-практической конференции «Комплексная защита информации», Суздаль, 22–24 мая 2018 г. С. 312–315. URL: https://kzi.su/tezisy (дата обращения: 01.03.2021).
2. Бойправ О.В., Лобунов В.В., Лыньков Л.М., Аль-Машатт Е. А.А. Исследование взаимодействия электромагнитного излучения инфракрасного диапазона длин волн с радиопоглотителями на основе металлсодержащих элементов // Авиационные материалы и технологии. 2020, № 2 (59). С. 89–94. DOI: http://dx.doi.org/10.18577/2071-9140-2020-0-2-89-94.
3. Лыньков Л.М., Богуш В.А., Бойправ О.В. Способ изготовления эластичного электромагнитного экрана и электромагнитный экран, изготовленный этим способом. Патент BY 23305. Опубл. 28.02.2021.
4. Корнюшин П.Н., Костерин С.С. Информационная безопасность. Владивосток, 2003. – 155 с.
5. Зайчук А.В. Основные пути утечки информации и несанкционированного доступа в корпоративных сетях // Защита информации. 2004, № 4. С. 19–24. URL: https://docplayer.ru/32716545-Osnovnye-puti-utechki-informacii-i-nesankcionirovannogo-dostupa-v-korporativnyh-setyah.html (дата обращения: 01.03.2021).
6. Хорев А.А. Технические каналы утечки акустической (речевой) информации // Специальная техника. 2009, № 5. С. 12–26. URL: https://www.elibrary.ru/item.asp?id=13011605 (дата обращения: 01.03.2021).
7. Хорев А. А. Техническая защита информации. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. – 436 с.
8. Хорев А.А. Классификация электронных устройств перехвата информации // Спецтехника и связь. 2009. С. 46–49. URL: https://www.elibrary.ru/item.asp?id=15187727 (дата обращения: 01.03.2021).
9. Алексеев В.В., Яковлев А.В., Моисеева М.В. Классификация акустических каналов утечки информации в помещениях офисного типа // Материалы международной конференции «Информатика: проблемы, методы, технологии», Воронеж, 11–12 февраля 2016 г.
10. Heller R. Radar reflector. Patent CH 634691 A5. Publ. 15.02.1983.
11. Устименко Л.Г. Астахов М.В., Бурашова Т.И. и др. Защитное покрытие. Патент RU 2313869 C1. Опубл. 27.12.2007.
12. Арбузов О.А., Бочаров А.В., Волков А.Г. и др. Слоистый защитный материал. Патент RU 2474628 C2. Опубл. 10.02.2013.
13. Wonjun Lee, Cho Chang Min, Jun Seung Moon. Multilayer flexible electromagnetic wave absorber. Patent KR 101576070 B1. Publ. 10.12.2015.
14. Li Xiuhan, Xu Zhengshuai, Xu Wei, Guo Haiyang, Zhu Wangqiang. Net-shaped layered-structure electromagnetic wave absorbing metamaterial. Patent CN 105762531 A. Publ. 13.07.2016.

REFERENCES:

[1] Boiprav O.V., Lynkou L.M., Al-Mashatt E. A.A., Abdulhadi Kh. D.A. Elastic electromagnetic shields based on combined metal-containing elements. Materials of the XXIII scientific-practical conference “Complex information security”, Suzdal, 22–24 May 2018. P. 312–315. URL: https://kzi.su/tezisy (accessed: 01.03.2021) (in Russian).
[2] Boiprav O.V., Lobunov V.V., Lynkou L.M., Al-Mashatt E. A.A. Research of interaction of infrared wavelength range electromagnetic radiation with radio-absorbent materials based on metal-containing

elements. Belarusian State University of Informatics and Radioelectronics. P. 89–94. DOI: http://dx.doi.org/10.18577/2071-9140-2020-0-2-89-94.
[3] Lynkou L.M., Bogush V.A., Boiprav O.V. Method of manufacturing an elastic electromagnetic shield and the electromagnetic shield made by this method. Patent BY 23305. Publ. 28.02.2021 (in Russian).
[4] Kornyushin P.N., Kosterin S.S. Information security. Vladivostok, 2003. – 155 p. (in Russian).
[5] Zaichuk A.V. The main ways of information leakage and unauthorized access in corporate networks. Information Security. 2004, no. 4. P. 19–24. URL: https://docplayer.ru/32716545-Osnovnye-puti-utechki-informacii-i-nesankcionirovannogo-dostupa-v-korporativnyh-setyah.html (accessed: 01.03.2021) (in Russian).
[6] Khorev A.A. Technical channels of acoustic (speech) information leakage. Special equipment. 2009, no. 5. P. 12–26. URL: https://www.elibrary.ru/item.asp?id=13011605 (accessed: 01.03.2021) (in Russian).
[7] Khorev A. A. Technical protection of information. Vol. 1. Technical channels of information leakage. M.: SPC "Analytica", 2008. – 436 p. (in Russian).
[8] Khorev A.A. Classification of electronic devices for intercepting information. Special equipment and communication. 2009. P. 46–49. URL: https://www.elibrary.ru/item.asp?id=15187727 (accessed: 01.03.2021) (in Russian).
[9] Alekseev V.V., Yakovlev A.V., Moiseeva M.V. Classification of acoustic channels of information leakage in office-type premises. Proceedings of the international conference "Informatics: problems, methods, technologies", Voronezh, 11–12 February 2016 (in Russian).
[10] Heller R. Radar reflector. Patent CH 634691 A5. Publ. 15.02.1983.
[11] Ustimenko L.G. Astakhov M.V., Burashova T.I. et al. Protective coating. Patent RU 2313869 C1. Publ. 27.12.2007 (in Russian).
[12] Arbuzov O.A., Bocharov A.V., Volkov A.G.et al. Layered protective material. Patent RU 2474628 C2. Publ. 10.02.2013 (in Russian).
[13] Wonjun Lee, Cho Chang Min, Jun Seung Moon. Multilayer flexible electromagnetic wave absorber. Patent KR 101576070 B1. Publ. 10.12.2015.
[14] Li Xiuhan, Xu Zhengshuai, Xu Wei, Guo Haiyang, Zhu Wangqiang. Net-shaped layered-structure electromagnetic wave absorbing metamaterial. Patent CN 105762531 A. Publ. 13.07.2016.

Поступила в редакцию – 22 марта 2021 г. Окончательный вариант – 07 апреля 2021 г.
Received – March 22, 2021. The final version – April 07, 2021.

Константин Г. Когос[1], Михаил А. Финошин[2]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
[1]e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X
[2]e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645

ПЕРСПЕКТИВНЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ

DOI: http://dx.doi.org/10.26583/bit.2021.2.05

Аннотация. Целью данной статьи является анализ существующих методов обнаружения сетевых скрытых каналов по времени. Для противодействия сетевым скрытым каналам по памяти зачастую применяют превентивные меры, такие как шифрование трафика и нормализация длин передаваемых пакетов. В случае скрытых каналов по времени более предпочтительны методы, не влияющие на функционирование легитимных каналов связи, так как превентивные меры приводят к более ощутимым последствиям для работы всей системы в целом. Одной из не превентивных мер является обнаружение. Задача обнаружения функционирующих скрытых каналов в защищаемой системе сводится либо к задаче поиска закономерностей в потоке трафика, либо к задаче сравнения тестируемой выборки с «эталонной». «Эталонная» выборка — это выборка с гарантированным отсутствием функционирующего скрытого канала. В статье рассматривается вопрос места алгоритмов машинного обучения в контексте задачи обнаружения сетевых скрытых каналов. Выделяются три случая работы методов обнаружения сетевых скрытых каналов по времени, основанных на алгоритмах машинного обучения, в зависимости от знаний о защищаемой системе. Приводится общая схема работы таких методов для трех случаев. Результатом анализа существующих методов является вывод о необходимости их усовершенствования для наиболее реалистичного случая – отсутствия как «эталонного» трафика, так и трафика с гарантированным присутствием скрытого канала. Описанная проблематика показывает перспективное направление в области исследований методов противодействия утечке информации по сетевым скрытым каналам.

Ключевые слова: скрытые каналы, каналы по времени, утечка информации, обнаружение, машинное обучение.
Для цитирования: КОГОС, Константин Г.; ФИНОШИН, Михаил А. ПЕРСПЕКТИВНЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 54–61, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1340>. Дата доступа: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.05.

Благодарности. Работа выполнена при поддержке Министерства науки и высшего образования РФ (проект государственного задания № 0723-2020-0036).

Konstantin G. Kogos[1], Mihail A. Finoshin[2]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X
[2]e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645

Prospective approaches to detecting network covert channels

DOI: http://dx.doi.org/10.26583/bit.2021.2.05

Abstract. The purpose of this study is to analyze the existing timing covert channels detection methods. Preventive measures are often used to counteract storage covert channels, such as traffic encryption and transmitted packets length normalization. Methods, that do not affect the functioning of legitimate communication channels are more preferable in the case of timing covert channels, since preventive measures lead to more tangible consequences for the operation of the entire system. One of the non-preventative measures is detection. The task of detecting covert channels in the protected system is

reduced either to the task of searching for patterns in the traffic flow, or to the task of comparing the tested sample with the "reference" one. A "reference" sample is a sample with a guaranteed absence of a functioning covert channel. The machine learning algorithms in the context of the problem of network covert channels detection are discussed. There are three cases of work of methods for detecting network timing covert channels, based on machine learning algorithms. The cases differ depending on the knowledge of the protected system. The general scheme of operation of such methods for three cases is given. The result of the analysis of existing methods is the conclusion about the need to improve them for the most realistic case – the absence of both "reference" traffic and traffic with a guaranteed presence of a covert channel. The described problems show a promising direction in the field of research on methods of countering information leakage through network covert channels.
Keywords: covert channels, timing channels, information leakage, detection, machine learning.
For citation: KOGOS, Konstantin G.; FINOSHIN, Mihail A. Prospective approaches to detecting network covert channels. IT Security (Russia), [S.l.], v. 28, n. 2, p. 54–61, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1340>. Date accessed: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.05.

Acknowledgement. This work was supported by the Ministry of Science and Higher Education of the Russian Federation (draft state assignment No. 0723-2020-0036).

Введение

Понятие скрытого канала впервые использовали авторы в [1]. Согласно им, канал называется скрытым, если он не проектировался и не предназначался для передачи информации. Отечественный стандарт[1] вводит следующее определение: «скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности». Высокоскоростные сетевые технологии позволяют строить скрытые каналы с пропускной способностью, позволяющей нелегитимно передавать критичную информацию в ограниченные сроки. Существование скрытого канала в системе представляет собой серьезную угрозу безопасности, так как стандартные меры и средства сетевой защиты, такие как шифрование канала связи, межсетевые экраны и средства анализа защищенности, не способны противодействовать утечке информации по скрытым каналам.

Известны различные способы передачи информации по сетевым скрытым каналам: скрытая информация может передаваться в заголовках полей передаваемых пакетов [2, 3], посредством изменения длин передаваемых пакетов [4, 5], а также с помощью изменения длин межпакетных интервалов и скоростей передаваемых пакетов [6, 7]. Первые два способа составляют группу скрытых каналов, называемую скрытыми каналами по памяти. Вторые два способа относят к скрытым каналам по времени.

1. Подходы к противодействию утечке информации по скрытым каналам

В отношении скрытых каналов применяются различные контрмеры [8]. Общая схема противодействия утечке информации по скрытым каналам включает в себя несколько шагов:

– идентификация скрытого канала – выявление скрытых каналов, которые могут быть потенциально реализованы в исследуемой системе;

– анализ идентифицированных скрытых каналов, включающий в себя определение количества информации, которое можно передать по выявленным скрытым каналам;

[1]ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов – Введ. 2009-10-01. М.: Стандартинформ, 2009. – 13 с.

– принятие решения о контрмерах в отношении идентифицированных и проанализированных скрытых каналов.

К превентивным контрмерам относят:

– ограничение – снижение пропускной способности скрытого канала до значения, которое считается не опасным;

– подавление – архитектурные ограничения, устраняющие возможность построения скрытого канала.

На рис. 1 представлена общая схема противодействия утечке информации по скрытым каналам.

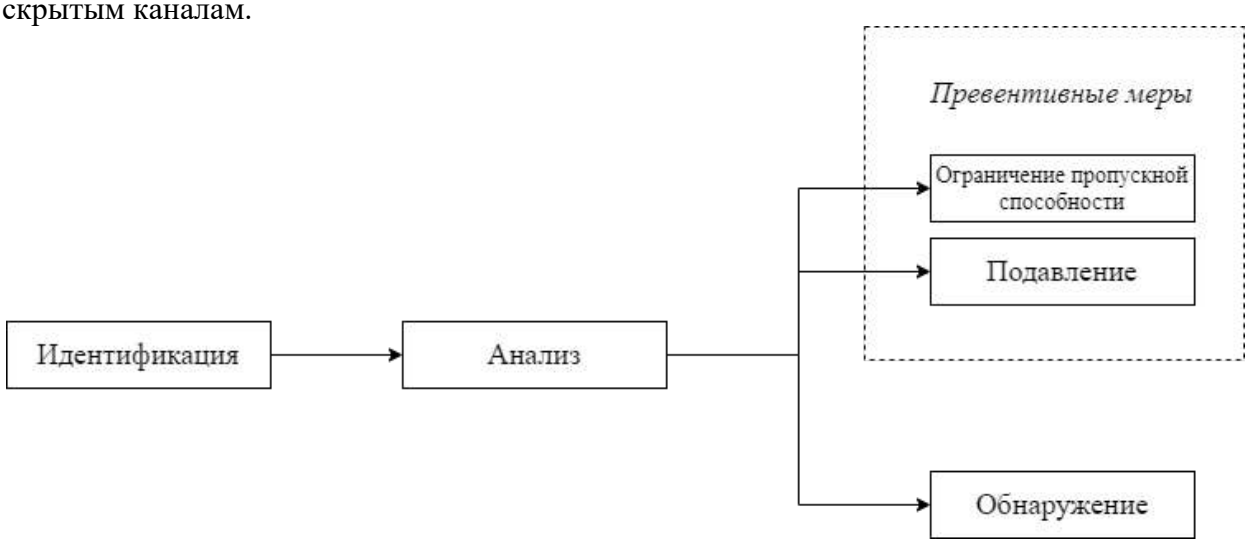

Рис. 1. Схема противодействия утечке информации по скрытым каналам
Fig. 1. The scheme of counteracting information leakage through covert channels

2. Методы обнаружения сетевых скрытых каналов по времени

Множество работ посвящено разработке и анализу статистических методов обнаружения скрытых каналов по времени [6, 10–19]. Условно данные методы можно разделить на требующие и не требующие «эталонную» выборку. Выборка получается из трафика путем извлечения длин межпакетных интервалов. Возможны три случая при снятии трафика из канала связи:

– гарантированное отсутствие скрытно передаваемой информации в трафике;

– гарантированное присутствие скрытно передаваемой информации в трафике;

– невозможность гарантировать как отсутствие, так и присутствие скрытно передаваемой информации в трафике.

Исходя из трех случаев, назовем таким образом получаемый трафик «эталонным», «скрытым» и «неизвестным» соответственно. Следовательно, выборка, получаемая из «эталонного» трафика, будет «эталонной» выборкой, аналогично для двух оставшихся случаев.

В [6] предлагается метод обнаружения скрытых каналов, основанный на изменении длин межпакетных интервалов, не требующий «эталонной» выборки. В [11] рассматриваются методы, основанные на анализе закономерностей в потоке трафика: метод на основе дисперсии, метод «ε-близости» и метод на основе Колмогоровской сложности, которые не требуют «эталонную» выборку, однако для них не оценены количественные характеристики. Кроме того, большое распространение в литературе получили методы, основанные на анализе энтропии трафика [12–14]. Данные методы требуют наличие «эталонной» выборки.

Среди методов обнаружения сетевых скрытых каналов в отдельную группу можно выделить те, которые основаны на методах математической статистики. Для методов данной группы необходимо наличие «эталонной» выборки. Например, в [12] для сравнения распределения длин межпакетных интервалов трафика в системе с аналогичным распределением в «эталонной» выборке используется критерий Колмогорова-Смирнова. Также существует возможность построения метода обнаружения на основе критерия согласия Пирсона [15, 16]. Существуют и другие статистические методы обнаружения сетевых скрытых каналов по времени [17–19].

Стоит отметить ограничения описанных выше методов. В случае параметрических методов выбор конкретных значений параметров не всегда определен, либо же определен только для конкретных типов скрытых каналов [20]. Таким образом, каждый конкретный метод можно применять для обнаружения только ограниченного спектра скрытых каналов. Очевидным недостатком многих методов является требование наличия «эталонной» выборки. В реальных условиях зачастую внедрение системы защиты происходит в уже функционирующую информационную систему, и невозможно гарантировать отсутствие скрытого канала при сборе данных для «эталонной» выборки.

В настоящее время получили развитие методы обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения. В зависимости от наличия исходных данных, применяются различные подходы на основе машинного обучения [21]: обучение с учителем, обучение без учителя и обучение с подкреплением. Обучение с подкреплением можно рассматривать как область, имеющую отношение к обучению с учителем.

Сложность задачи обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения зависит от начальных условий. Наиболее простым является случай, когда возможно получение «эталонной» и «скрытой» выборок. Общим подходом для первого случая является применение алгоритмов машинного обучения с учителем. Однако, при реализации системы защиты затруднительно получение таких выборок. Во-первых, как было отмечено выше, сбор «эталонной» выборки представляет серьезную проблему. Во-вторых, для различных типов сетевых скрытых каналов по времени «скрытые» выборки могут сильно различаться, что приводит к необходимости иметь большое число образцов трафика для каждого конкретного типа скрытого канала.

Более сложным является случай, когда имеется возможность получения только «эталонной» выборки. Для второго случая применяются алгоритмы обнаружения аномалий. Исследование первого и второго случаев широко представлено в зарубежной литературе [20, 22–26].

Наконец, наиболее сложным для исследования является случай, когда отсутствует возможность сбора «эталонной» выборки, в таком случае предлагается применять алгоритмы кластеризации.

Необходимым условием для решения задач с помощью алгоритмов машинного обучения является наличие сформированного набора признаков исследуемого объекта. Данный вектор признаков подается на вход алгоритму машинного обучения. В случае задачи обнаружения сетевых скрытых каналов по времени из трафика выделяется массив значений длин межпакетных интервалов. Признаки от данного массива могут вычисляться как на основе формул математической статистики, так и на основе отдельных параметров, анализируемых методами обнаружения сетевых скрытых каналов.

Например, в [22] используют в качестве признаков значение теста Колмогорова-Смирнова, энтропию, условную энтропию и значение теста на определение регулярности, а в качестве метода машинного обучения – метод опорных векторов. В другом случае

строится классификатор, а в качестве признаков используется автокорреляция и энтропия [23]. Классификатор также может строиться на основе Вейвлет-преобразования [20]. Построение методов обнаружения не ограничено данными способами [24–26].

Таким образом, работа метода обнаружения сетевых скрытых каналов по времени включает в себя три этапа:

– анализ трафика и выделение из него массива значений длин межпакетных интервалов;

– обработка массива значений длин межпакетных интервалов и получение на его основе вектора признаков;

– применение алгоритма машинного обучения исходя из типа трафика («эталонный», «скрытый», «неизвестный»), на основе которого принимается решение о наличии или отсутствии скрытого канала в системе.

В зависимости от одного из трех случаев наличия или отсутствия «эталонной» и «скрытой» выборок меняется алгоритм машинного обучения. Данная схема представлена на рис. 2 (где введены обозначения: ССК – сетевой скрытый канал, ДМИ – длины межпакетных интервалов).

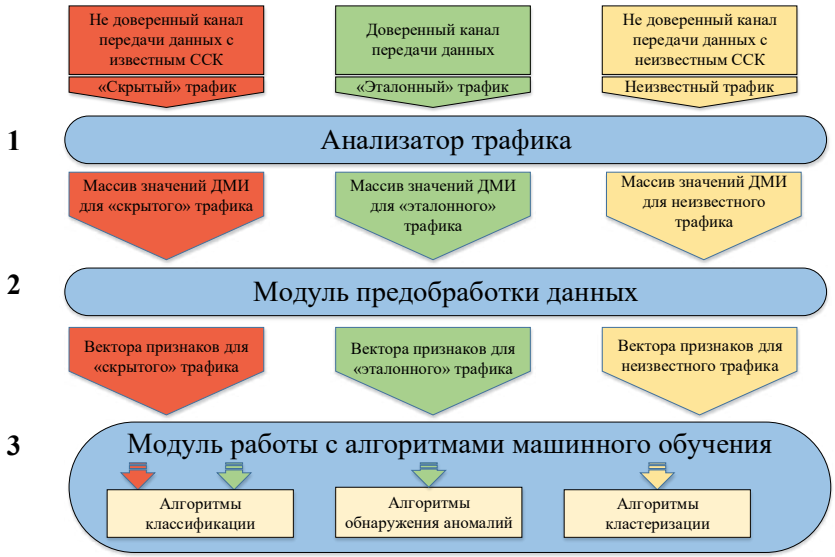

Рис. 2. Схема работы метода обнаружения скрытых каналов по времени на основе алгоритмов машинного обучения

Fig.2. Scheme of the timing covert channels detection method based on machine learning algorithms

Как было отмечено выше, исследования в настоящее время ведутся исходя из условий наличия «эталонной» выборки. Однако, зачастую невозможно гарантировать отсутствие скрытого канала в системе при проведении исследований. Таким образом, актуальной является разработка метода обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения в случае, когда отсутствует обучающая выборка. Такой метод позволит внедрять систему противодействия утечке информации по сетевым скрытым каналам по времени в уже функционирующую систему без предварительного обучения системы защиты.

Заключение

В работе приведен краткий обзор подходов к противодействию утечке информации по сетевым скрытым каналам, при этом особое внимание уделяется методам обнаружения сетевых скрытых каналов по времени. Рассматривается перспективное направление построения методов обнаружения, основанных на алгоритмах машинного обучения. Вводятся понятия «скрытого» и «эталонного» трафика, на основе которых выделяются три возможных случая работы методов обнаружения. Случаи различаются в зависимости от наличия или отсутствия «скрытого» и «эталонного» трафика. Приводится общая схема работы методов обнаружения сетевых скрытых каналов, основанных на алгоритмах машинного обучения. По результатам работы делается вывод о необходимости усовершенствования существующих методов обнаружения с целью их применения для наиболее реалистичного сценария, когда невозможно гарантировать как наличие, так и отсутствие скрытого канала в системе.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A note on the confinement problem //Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
2. Millen J.K. Security kernel validation in practice //Communications of the ACM. 1976. Vol. 19. no. 5. C. 243–250.
3. Zander, Sebastian & Armitage, Grenville & Branch, Philip. (2007). Covert channels in the IP time to live field. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (дата обращения: 01.02.2021).
4. M. Hussain and M. Hussain. A high bandwidth covert channel in network protocol. International Conference on Information and Communication Technologies, Karachi, Pakistan, 2011. P. 1–6. DOI: https://doi.org/10.1109/ICICT.2011.5983562.
5. L. Ji, H. Liang, Y. Song and X. Niu, A Normal-Traffic Network Covert Channel, 2009 International Conference on Computational Intelligence and Security, Beijing, China, 2009. P. 499–503. DOI: https://doi.org/10.1109/CIS.2009.156.
6. Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays (2005). URL: https://www.semanticscholar.org/paper/Detection-of-Covert-Channel-Encoding-in-Network-Berk-Giani/58a022c5ff528efa142c1452952c6043d916ffab (дата обращения: 01.02.2021).
7. S.H. Sellke, C. Wang, S. Bagchi and N. Shroff, TCP/IP Timing Channels: Theory to Implementation, IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009. P. 2204–2212. DOI: https://doi.org/10.1109/INFCOM.2009.5062145.
8. S. Zander, G. Armitage and P. Branch. A survey of covert channels and countermeasures in computer network protocols, in IEEE Communications Surveys & Tutorials. Vol. 9, no. 3. P. 44–57, Third Quarter 2007. DOI: https://doi.org/10.1109/COMST.2007.4317620.
9. Грушо А.А. Скрытые каналы и безопасность в компьютерных системах. Дискретная математика. 1998. Т. 10, вып. 1. С. 3–9. DOI: https://doi.org/10.4213/dm411.
10. Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels //2015 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2015. P. 1107–1111. DOI: http://dx.doi.org/10.15439/2015F88.
11. Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2004. IP covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). Association for Computing Machinery, New York, NY, USA. P. 178–187. DOI: https://doi.org/10.1145/1030083.1030108.
12. Walls R. J., Kothari K., Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55. Issue 6. P. 1217–1228.
13. Steven Gianvecchio and Haining Wang. 2007. Detecting covert timing channels: an entropy-based approach. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA. P. 307–316. DOI: https://doi.org/10.1145/1315245.1315284.
14. O. Darwish, A. Al-Fuqaha, M. Anan and N. Nasser. The role of hierarchical entropy analysis in the detection and time-scale determination of covert timing channels. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 153–159. DOI: https://doi.org/10.1109/IWCMC.2015.7289074.

15. Никулин М.С. Критерий хи-квадрат для непрерывных распределений с параметрами сдвига и масштаба, Теория вероятн. и ее примен., 18:3 (1973), С. 583–591. DOI: https://doi.org/10.1137/1118069.
16. C. Zhiyong, S. Ying and S. Changxiang. Detection of Insertional Covert Channels Using Chi-square Test. International Conference on Multimedia Information Networking and Security, Wuhan, China, 2009. P. 432–435. DOI: https://doi.org/10.1109/MINES.2009.296.
17. F. Rezaei, M. Hempel, P.L. Shrestha, S.M. Rakshit and H. Sharif. Detecting covert timing channels using non-parametric statistical approaches. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 102–107. DOI: https://doi.org/10.1109/IWCMC.2015.7289065.
18. F. Rezaei, M. Hempel and H. Sharif. Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic, in IEEE Transactions on Dependable and Secure Computing. Vol. 14, no. 3. P. 249–264, 1 May-June 2017. DOI: https://doi.org/10.1109/TDSC.2017.2656078.
19. F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. A novel Covert Timing Channel detection approach for online network traffic, 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 2015. P. 737–738. DOI: https://doi.org/10.1109/CNS.2015.7346911.
20. Archibald R., Ghosal D. A comparative analysis of detection metrics for covert timing channels //Computers & security. 2014. Vol. 45. P. 284–292.
21. Рашка С. Python и машинное обучение / С. Рашка, перевод с англ. А.В. Логунова // М.: ДМК Пресс. 2017. – 418 с.
22. P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. A Support Vector Machine-Based Framework for Detection of Covert Timing Channels, in IEEE Transactions on Dependable and Secure Computing. Vol. 13, no. 2. P. 274–283, 1 March-April 2016. DOI: https://doi.org/10.1109/TDSC.2015.2423680.
23. P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. Leveraging Statistical Feature Points for Generalized Detection of Covert Timing Channels. IEEE Military Communications Conference, Baltimore, MD, USA, 2014. P. 7–11. DOI: https://doi.org/10.1109/MILCOM.2014.10.
24. İ.G. Çavuşo˘glu, H. Alemdar and E. Onur. Covert Channel Detection Using Machine Learning. 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey, 2020. P. 1–4. DOI: https://doi.org/10.1109/SIU49456.2020.9302098.
25. M. Chourib. Detecting Selected Network Covert Channels Using Machine Learning. International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 2019. P. 582–588. DOI: https://doi.org/10.1109/HPCS48598.2019.9188115.
26. Y. Sun, L. Zhang and C. Zhao. A Study of Network Covert Channel Detection Based on Deep Learning. 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018. P. 637–641. DOI: https://doi.org/10.1109/IMCEC.2018.8469669.

REFERENCES:

[1] Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
[2] Millen J.K. Security kernel validation in practice. Communications of the ACM. 1976. Vol. 19. no. 5. P. 243–250.
[3] Zander, Sebastian & Armitage, Grenville & Branch, Philip. (2007). Covert channels in the IP time to live field. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (accessed: 01.02.2021).
[4] M. Hussain and M. Hussain. A high bandwidth covert channel in network protocol. International Conference on Information and Communication Technologies, Karachi, Pakistan, 2011. P. 1–6. DOI: https://doi.org/10.1109/ICICT.2011.5983562.
[5] L. Ji, H. Liang, Y. Song and X. Niu, A Normal-Traffic Network Covert Channel, 2009 International Conference on Computational Intelligence and Security, Beijing, China, 2009. P. 499–503. DOI: https://doi.org/10.1109/CIS.2009.156.
[6] Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays (2005). URL: https://www.semanticscholar.org/paper/Detection-of-Covert-Channel-Encoding-in-Network-Berk-Giani/58a022c5ff528efa142c1452952c6043d916ffab (accessed: 01.02.2021).
[7] S.H. Sellke, C. Wang, S. Bagchi and N. Shroff, TCP/IP Timing Channels: Theory to Implementation, IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009. P. 2204–2212. DOI: https://doi.org/10.1109/INFCOM.2009.5062145.
[8] S. Zander, G. Armitage and P. Branch. A survey of covert channels and countermeasures in computer network protocols, in IEEE Communications Surveys & Tutorials. Vol. 9, no. 3. P. 44–57, Third Quarter 2007. DOI: https://doi.org/10.1109/COMST.2007.4317620.

[9] Grusho, A.A. Covert channels and security in computer systems. Discrete mathematics. 1998. Vol. 10, issue. 1. P. 3–9. DOI: https://doi.org/10.4213/dm411 (in Russian).
[10] Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels. 2015 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2015. P. 1107–1111. DOI: http://dx.doi.org/10.15439/2015F88.
[11] Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2004. IP covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). Association for Computing Machinery, New York, NY, USA. P. 178–187. DOI: https://doi.org/10.1145/1030083.1030108.
[12] Walls R.J., Kothari K., Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping. Computer networks. 2011. Vol. 55. Issue 6. P. 1217–1228.
[13] Steven Gianvecchio and Haining Wang. 2007. Detecting covert timing channels: an entropy-based approach. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA. P. 307–316. DOI: https://doi.org/10.1145/1315245.1315284.
[14] O. Darwish, A. Al-Fuqaha, M. Anan and N. Nasser. The role of hierarchical entropy analysis in the detection and time-scale determination of covert timing channels. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 153–159. DOI: https://doi.org/10.1109/IWCMC.2015.7289074.
[15] Nikulin M.S. Chi-Square Test for Continuous Distributions with Shift and Scale Parameters. Theory Probab. Appl., 18:3 (1974). P. 559–568. DOI: https://doi.org/10.1137/1118069.
[16] C. Zhiyong, S. Ying and S. Changxiang. Detection of Insertional Covert Channels Using Chi-square Test. International Conference on Multimedia Information Networking and Security, Wuhan, China, 2009. P. 432–435. DOI: https://doi.org/10.1109/MINES.2009.296.
[17] F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. Detecting covert timing channels using non-parametric statistical approaches. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 102–107. DOI: https://doi.org/10.1109/IWCMC.2015.7289065.
[18] F. Rezaei, M. Hempel and H. Sharif. Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic, in IEEE Transactions on Dependable and Secure Computing. Vol. 14, no. 3. P. 249–264, 1 May-June 2017. DOI: https://doi.org/10.1109/TDSC.2017.2656078.
[19] F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. A novel Covert Timing Channel detection approach for online network traffic. IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 2015. P. 737–738. DOI: https://doi.org/10.1109/CNS.2015.7346911.
[20] Archibald R., Ghosal D. A comparative analysis of detection metrics for covert timing channels. Computers & security. 2014. Vol. 45. P. 284–292.
[21] Rashka, S. Python and machine learning. S. Rashka. M.: DMK Press. 2017. – 418 p. (in Russian)
[22] P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. A Support Vector Machine-Based Framework for Detection of Covert Timing Channels, in IEEE Transactions on Dependable and Secure Computing. Vol. 13, no. 2. P. 274–283, 1 March-April 2016. DOI: https://doi.org/10.1109/TDSC.2015.2423680.
[23] P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. Leveraging Statistical Feature Points for Generalized Detection of Covert Timing Channels. IEEE Military Communications Conference, Baltimore, MD, USA, 2014. P. 7–11. DOI: https://doi.org/10.1109/MILCOM.2014.10.
[24] İ.G. Çavuşo˘glu, H. Alemdar and E. Onur. Covert Channel Detection Using Machine Learning. 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey, 2020. P. 1–4. DOI: https://doi.org/10.1109/SIU49456.2020.9302098.
[25] M. Chourib. Detecting Selected Network Covert Channels Using Machine Learning. International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 2019. P. 582–588. DOI: https://doi.org/10.1109/HPCS48598.2019.9188115.
[26] Y. Sun, L. Zhang and C. Zhao. A Study of Network Covert Channel Detection Based on Deep Learning. 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018. P. 637–641. DOI: https://doi.org/10.1109/IMCEC.2018.8469669.

Поступила в редакцию – 25 марта 2021 г. Окончательный вариант – 07 апреля 2021 г.
Received – March 25, 2021. The final version – April 07, 2021.

Александр А. Козлов[1], Михаил А. Иванов[2]
[1]ООО НТЦ «Вулкан»,
ул. Ибрагимова, 31, Москва, 105318, Россия
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360
[2]e-mail: maivanov@mephi.ru, https://orcid.org/0000-0002-3204-8055

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЛИНЕЙНОГО АНАЛИЗА К ARX АЛГОРИТМАМ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ В ЗАВИСИМОСТИ ОТ ФУНКЦИИ СМЕШЕНИЯ С РАУНДОВЫМ КЛЮЧОМ

DOI: http://dx.doi.org/10.26583/bit.2021.2.06

Аннотация. ARX алгоритмы стохастического преобразования являются перспективным решением в области разработки непредсказуемых генераторов псевдослучайных чисел для низкоресурсных систем. Простота реализации ARX операций, а также их высокая энергоэффективность делают привлекательным выбор алгоритмов стохастического преобразования данных, основанных на этих операциях, для обеспечения конфиденциальности информации. Существующие исследования по возможности применения линейного анализа к ARX алгоритмам стохастического преобразования используют неточные линейные аппроксимации раундовых преобразований. Ключевой идеей линейного анализа является использование линейных статистических аналогов нелинейных функций. Линейные аппроксимации используются для выражения зависимости входа алгоритма стохастического преобразования от его выхода в виде линейной функции. Полученная линейная функция выполняется с некоторой вероятностью, зависящей от вероятности выполнения использованных линейных аппроксимаций. Единственной нелинейной операцией в ARX алгоритмах, является сложение по модулю 2^n. В данной работе проводится исследование ограничений применимости линейного подхода для анализа ARX алгоритмов стохастического преобразования. Исследование проводится для различных случаев реализации функции смешения с раундовым ключом (key mix function): использование операции сложения по модулю 2^n, операции сложения по модулю 2 и операции циклического сдвига. Для каждого из вариантов проведено исследование возможности применения линейной аппроксимации соответствующей операции ARX алгоритма для проведения его линейного анализа. Для ARX алгоритмов стохастического преобразования, использующих в качестве функции смешения с раундовым ключом сложение по модулю 2^n или сложение по модулю 2, получены оценки на число операций сложения по модулю 2^n в них, необходимое для обеспечения их устойчивости к линейному анализу.

Ключевые слова: сложение по модулю 2^n, ARX, линейный анализ, генераторы псевдослучайных чисел.

Для цитирования: КОЗЛОВ, Александр А.; ИВАНОВ, Михаил А. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЛИНЕЙНОГО АНАЛИЗА К ARX АЛГОРИТМАМ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ В ЗАВИСИМОСТИ ОТ ФУНКЦИИ СМЕШЕНИЯ С РАУНДОВЫМ КЛЮЧОМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 62–69, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1341>. Дата доступа: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.06.

Alexander A. Kozlov[1], Mikhail A. Ivanov[2]
[1]LLC Scientific and Technical Center «Vulkan»,
Ibragimova str., 31, Moscow, 105318, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360
[2]e-mail: MAIvanov@mephi.ru, https://orcid.org/0000-0002-3204-8055

The possibility of applying linear analysis to the ARX stochastic algorithms depending on round key functions

DOI: http://dx.doi.org/10.26583/bit.2021.2.06

Abstract. ARX stochastic algorithms are a promising solution in the development of unpredictable pseudo- random number generators for low-resource systems. The ease of implementation of their round operations, as well as their high energy efficiency, make the choice of such algorithms attractive for ensuring the confidentiality of information. Existing studies on the possibility of applying linear analysis to ARX stochastic algorithms use imprecise linear approximations of round functions. The key idea of linear analysis is the use of linear statistical analogs of non-linear functions. Linear approximations are used to express the inputs of the stochastic transformation algorithm by its outputs as a linear function. The resulting linear function is true with a certain probability, which depends on the probability of fulfilling the used linear approximations. The only non-linear operation in ARX algorithms is addition modulo 2^n. In this paper we study the limitations of the applicability of the linear analysis to ARX stochastic transformation algorithms. The study is carried out for various cases of the implementation of round key addition: the use of the addition modulo 2^n, the addition modulo 2, and the cyclic shift. For ARX stochastic transformation algorithms, using addition modulo 2^n or addition modulo 2 as a round key mix operation, estimates are obtained for the number of addition operations modulo 2^n needed to ensure their stability to linear analysis.

Keywords: addition modulo 2^n, ARX, linear analysis, pseudorandom number generator.
For citation: KOZLOV, Alexander A.; IVANOV, Mikhail A. The possibility of applying linear analysis to the ARX stochastic algorithms depending on round key functions. IT Security (Russia), [S.l.], v. 28, n. 2, p. 62–69, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1341>. Date accessed: 14 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.06.

Введение

Алгоритмы стохастического преобразования данных, использующие только операции сложения по модулю 2^n, циклического сдвига и сложения по модулю 2 (XOR) называются ARX (Addition-Rotate-XOR) алгоритмами, а соответствующие математические операции – ARX операциями. ARX алгоритмы относятся к типу низкоресурсных алгоритмов стохастического преобразования [1–2]. Можно выделить следующие требования к таким алгоритмам:

1. Реализация алгоритма должна иметь пониженное энергопотребление;

2. Реализация алгоритма должна использовать небольшой объем оперативной памяти.

Кроме того их производительность не должна уступать производительности не низкоресурсных алгоритмов стохастического преобразования.

ARX операции являются наиболее перспективными для построения низкоресурсных алгоритмов стохастического преобразования. Преимуществом использования этих операций является то, что они обеспечивают высокое быстродействие, как при программной, так и при аппаратной реализации. В то же время при их правильной композиции, они обладают хорошими математическими свойствами: высокой степенью нелинейности и рассеивания. Примерами алгоритмов стохастического преобразования, построенных на основе ARX операций, являются алгоритмы Salsa20 [3], PRESENT [4], SIMECK [5], SPECK [6], FEAL [7]. RC5-12 [8], Chaskey [9], SPARX [10], LEA [11], HIGHT [12].

Построенные на основе ARX операций блочные алгоритмы стохастического преобразования могут использоваться в качестве элемента непредсказуемых генераторов псевдослучайных чисел (ГПСЧ), которые могут найти широкое применение в технических областях, связанных с ограничениями в доступных вычислительных

мощностях, например в сенсорных сетях [13]. Для этого эти алгоритмы должны быть стойкими по отношению к известным методам анализа, в частности к линейному анализу [14].

Ключевой идеей линейного анализа является использование линейных статистических аналогов (линейных аппроксимаций) нелинейных функций. Линейные аппроксимации используются для выражения зависимости входа алгоритма стохастического преобразования от его выхода в виде линейной функции. Полученная линейная функция выполняется с некоторой вероятностью, зависящей от вероятности выполнения использованных линейных аппроксимаций.

Единственной нелинейной операцией в ARX алгоритмах, является сложение по модулю 2^n. В [15] представлен анализ линейных свойств операции сложения по модулю 2^n, полученные линейные аппроксимации операции сложения по модулю 2^n могут быть использованы для проведения линейного анализа ARX алгоритмов стохастического преобразования. В данной работе проводится исследование ограничений применимости линейного анализа ARX алгоритмов стохастического преобразования на основе полученных в [15] линейных аппроксимаций. Исследование проводится для различных случаев реализации функции смешения с раундовым ключом (key mix function): использование операции сложения по модулю 2^n, операции сложения по модулю 2 и операции циклического сдвига.

1. ARX алгоритмы с реализацией функции смешения с раундовым ключом на основе операции сложения по модулю 2^n

Если операция сложения по модулю 2^n используется для реализации функции смешения с раундовым ключом, то одно из входных чисел является константой (раундовым ключом). Условие фиксированного раундового ключа – это условие задачи проведения анализа конкретного экземпляра некоторого ARX преобразования. Обозначим ARX алгоритмы стохастического преобразования с реализацией функции смешения с раундовым ключом на основе операции сложения по модулю 2^n через ARX^+. Чтобы исследовать возможность применения линейного анализа для алгоритмов ARX^+ рассмотрим сложение двух n-разрядных чисел $X = (x_{n-1}, x_{n-2}, ..., x_0)$ и $K = (k_{n-1}, k_{n-2}, ..., k_0)$

$$X + K = D \mod 2^n, \quad (1)$$

где K – фиксированный раундовый ключ, $D = (d_{n-1}, d_{n-2}, ..., d_0)$, $d_i = x_i \oplus k_i \oplus p_i$, p_i – значение переноса в i-й разряд, $i = 0, 1, ..., n-1$.

Для (1) в [15] были доказаны три утверждения, представленные далее.

Утверждение 1. В выражении (1) для любого $n > 0$ и любого фиксированного раундового ключа $K = (k_{n-1}, k_{n-2}, ..., k_0)$ вероятность совпадения бита переноса p_i со значением бита входного слова x_{i-1}

$$\text{Prob}(p_i = x_{i-1}) = \frac{1}{2} + \varepsilon, \ 0 \le |\varepsilon| \le 0.5. \quad (2)$$

Утверждение 2. В выражении (1) для любого $n > 0$ и любого фиксированного раундового ключа $K = (k_{n-1}, k_{n-2}, ..., k_0)$ вероятность совпадения бита переноса p_i со значением бита раундового ключа k_{i-1}

$$\text{Prob}(p_i = k_{i-1}) = \frac{1}{2} + \varepsilon, \ 0 \le |\varepsilon| \le 0.5. \quad (3)$$

Утверждение 3. Для любого фиксированного раундового ключа, если значение вероятности (2) ниже, чем 0.75, то значение вероятности (3) обязательно выше, чем 0.75, и наоборот.

Рассмотрим некоторый ARX алгоритм $arx \in ARX^+$, $arx : X \times K -> X$, $X, K \in Z_2^m$. Обозначим через L множество ARX алгоритмов стохастического преобразования, не устойчивых к линейному анализу. Используя (1) – (3) докажем следующее утверждение.

Утверждение 4. Если $arx \in L$, то число операций сложения по модулю 2^n в arx не превышает $\frac{m-2}{3}$, $n \le m$.

Доказательство.

Рассмотрим линейные аппроксимации каждой из операций алгоритма arx.

Операция XOR линейна, аппроксимация не требуется.

Операция циклического сдвига на фиксированную величину линейна, аппроксимация не требуется.

Рассмотрим аппроксимацию выражения (1). Значение выходов соотношения (1) может быть выражено так:

$$d_i = x_i \oplus k_i \oplus x_{i-1} \quad (4)$$

$$d_i = x_i \oplus k_i \oplus k_{i-1} \quad (5)$$

В классическом методе линейного анализа используется одна единственная линейная аппроксимация алгоритма. В рассматриваемой ситуации это невозможно – так как достоверно неизвестны вероятности выполнения аппроксимации для (1). Однако можно составить несколько различных линейных аппроксимаций алгоритма arx и провести линейный анализ для каждой из них по отдельности. Из утверждения 3 следует, что либо (4), либо (5) выполняется с вероятностью выше, чем 0.75, но неизвестно какое именно. Поэтому вместо того, чтобы выразить алгоритм arx через одну линейную функцию, выполняющуюся с заданной вероятностью, выразим алгоритм arx через множество линейных функций, которое обозначим $LinArx$.

Для этого, каждую из операций сложения по модулю 2^n будем аппроксимировать, используя по отдельности выражения (4) и (5). Каждая такая аппроксимация должна рассматриваться отдельно, поэтому число линейных аппроксимаций всего алгоритма arx будет увеличиваться в два раза при каждой линейной аппроксимации операции сложения по модулю 2^n.

Если всего в алгоритме arx было t операций сложения по модулю 2^n, то получим 2^t линейных аппроксимаций. В силу того, что $LinArx$ содержит все возможные случаи линейной аппроксимации операции сложения по модулю 2^n, то согласно утверждению 3 в $LinArx$ содержится функция $f_{\max}$, все линейные аппроксимации операции сложения по модулю 2^n входящие в которую выполняются с вероятностью не меньше, чем 0.75.

Всего в $f_{\max}$ входит t линейных аппроксимаций. Каждая входит с преобладанием не меньше, чем 0.25. Отсюда, согласно лемме о накапливании [14], общее преобладание для функции $f_{\max}$ будет не меньше, чем $\frac{1}{2^{t+1}}$. Известно, что для проведения линейного анализа для некоторой аппроксимации, выполняемой с преобладанием $\frac{1}{\varepsilon}$, требуется ε^2 открытых

текстов. Тогда, для проведения линейного анализа на основе аппроксимации с преобладанием $\frac{1}{2^{t+1}}$ требуется 2^{2t+2} открытых текстов.

Чтобы точно установить функцию $f_{\max}$, нужно провести статистический подсчет согласно методу линейного анализа для всех 2^t линейных аппроксимаций. Тогда общая вычислительная сложность составит 2^{3t+2}. Всего для алгоритма arx существует 2^m открытых текстов. Отсюда получаем, что $t < \frac{m-2}{3}$.

2. ARX алгоритмы с реализацией функции смешения с раундовым ключом на основе операции сложения по модулю 2

Обозначим ARX **алгоритмы с реализацией функции смешения с раундовым ключом на основе операции** XOR через $ARX^{\oplus}$. Чтобы исследовать возможность применения линейного анализа для алгоритмов $ARX^{\oplus}$ рассмотрим сложение двух произвольных n-разрядных чисел $X = (x_{n-1}, x_{n-2}, ..., x_0)$ и $Y = (y_{n-1}, y_{n-2}, \ldots, y_0)$

$$X + Y = D \mod 2^n, \tag{6}$$

где $D = (d_{n-1}, d_{n-2}, ..., d_0)$, $d_i = x_i \oplus y_i \oplus p_i$, p_i – значение переноса в i-й разряд, $i = 0, 1, ..., n-1$.

Если операция сложения по модулю 2^n не используется для реализации функции смешения с раундовым ключом, то оба входных операнда этой операции не являются константой. Для (6) в [15] были доказаны два утверждения, представленные далее.

Утверждение 5. В выражении (6) для любого $n > 0$ и любого $0 \le i \le n$-1

$$\begin{cases} \text{Prob}(d_i = x_i \oplus y_i \oplus x_{i-1}) = 0.75 \\ \text{Prob}(d_i = x_i \oplus y_i \oplus y_{i-1}) = 0.75 \end{cases}. \tag{7}$$

Утверждение 6. В выражении (6) для любого $n > 0$ и любого $0 \le i \le n$-1

$$\text{Prob}(d_i \oplus d_{i-1} = x_i \oplus y_i \oplus 1) = 0.75. \tag{8}$$

Рассмотрим некоторый ARX алгоритм $arx \in ARX^{\oplus}$, $arx : X \times K -> X$, $X, K \in Z_2^m$. Используя (7) – (8) докажем следующее утверждение.

Утверждение 7. Если $arx \in ARX^{\oplus}$ и $arx \in L$, то число операций сложения по модулю 2^n в arx не превышает $\frac{m-2}{2}$.

Доказательство.

Рассмотрим линейные аппроксимации каждой из операций алгоритма arx.

Операция XOR линейна, аппроксимация не требуется.

Операция циклического сдвига на фиксированную величину линейна, аппроксимация не требуется.

Рассмотрим аппроксимацию выражения (6).

Соотношения выполняются с вероятностью 0.75. В [15] было доказано, что эти линейные аппроксимации являются наилучшими для операции сложения по модулю 2^n.

Если всего в алгоритме arx было t операций сложения по модулю 2^n, то для составления линейной аппроксимации алгоритма arx в лучшем случае будет использовано t линейных аппроксимаций операции сложения по модулю 2^n. Каждая из

аппроксимаций выполняется с вероятностью 0.75. Согласно лемме о накапливании [14], общее преобладание для функции линейной аппроксимации алгоритма *arx* будет не меньше, чем $\frac{1}{2^{t+1}}$. Тогда, для проведения линейного анализа на основе аппроксимации с преобладанием $\frac{1}{2^{t+1}}$ требуется 2^{2t+2} открытых текстов. Всего для алгоритма *arx* существует 2^m открытых текстов. Отсюда получаем, что $t < \frac{m-2}{2}$.

3. ARX алгоритмы с реализацией функции смешения с раундовым ключом на основе операции циклического сдвига

Обозначим через rot_r операцию циклического сдвига *n*-разрядного числа на r бит вправо

$$rot_r(X) = Y, \tag{9}$$

где $X = (x_{n-1}, x_{n-2}, ..., x_0)$, $Y = (y_{n-1}, y_{n-2}, ..., y_0)$, $y_i = x_{(i+r) \bmod n}$, $i = 0, 1, ..., n-1$.

Операция циклического сдвига *n*-разрядного числа на *r* бит влево может быть выражена как rot_{n-r}. Поэтому здесь и далее без ограничения общности будем рассматривать только операцию циклического сдвига вправо.

Если значение сдвига *r* фиксировано, то выход операции rot_r однозначно выражается через вход исходя из определения самой операции (9).

Рассмотрим случай, когда значение сдвига зависит от значения раундового ключа

$$rot_{f(k)}(X) = Y, \tag{10}$$

где $f(k)$ – некоторая функция зависимости от раундового ключа k.

В этом случае величина сдвига неизвестна, и возможны все линейные аппроксимации для некоторого выхода y_i операции циклического сдвига, $i = 0, 1, ..., n-1$:

$$y_i = x_0 \vee y_i = x_1 \vee ... \vee y_i = x_{n-1} \tag{11}$$

Величина раундового ключа является неизвестной, но фиксированной. Это означает, что среди всех возможных аппроксимаций выхода y_i в соотношении (11) верна только одна. Установить какая именно, не имея информации о значении раундового ключа, невозможно. Поэтому применение классического линейного анализа ARX алгоритмов стохастического преобразования для рассматриваемого случая невозможно.

Заключение

Получена оценка на число операций сложения по модулю 2^n в ARX алгоритмах стохастического преобразования, устойчивых к линейному анализу. Если в ARX алгоритме с длиной входного слова *m* для реализации функции смешения с раундовым ключом используется операция сложения по модулю 2^n, $n \le m$, то он устойчив к линейному анализу, если число операций сложения по модулю 2^n в нем не меньше чем $\frac{m-2}{2}$. Если для реализации функции смешения с раундовым ключом используется операция XOR, то ARX алгоритм устойчив к линейному анализу, если число операций сложения по модулю 2^n в нем не меньше чем $\frac{m-2}{3}$.

СПИСОК ЛИТЕРАТУРЫ:

1. Жуков А.Е. Легковесная криптография. Часть 1. Вопросы кибербезопасности. 2015. №1(9). С. 23–46. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_09_04.pdf (дата обращения: 20.01.2021).
2. Жуков А.Е. Легковесная криптография. Часть 2. Вопросы кибербезопасности. 2015. №2(10). С. 2–10. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (дата обращения: 20.01.2021).
3. Bernstein D.J. (2008) The Salsa20 Family of Stream Ciphers. In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol. 4986. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-68351-3_8.
4. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol. 4727. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-74735-2_31.
5. Yang G., Zhu B., Suder V., Aagaard M.D., Gong G. (2015) The Simeck Family of Lightweight Block Ciphers. In: Güneysu T., Handschuh H. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2015. CHES 2015. Lecture Notes in Computer Science, vol. 9293. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-48324-4_16.
6. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. (2015) The Simon and Speck Block Ciphers on AVR 8-Bit Microcontrollers. In: Eisenbarth T., Öztürk E. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2014. Lecture Notes in Computer Science, vol. 8898. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-16363-5_1.
7. Shimizu A., Miyaguchi S. (1988) Fast Data Encipherment Algorithm FEAL. In: Chaum D., Price W.L. (eds) Advances in Cryptology – EUROCRYPT' 87. EUROCRYPT 1987. Lecture Notes in Computer Science, vol. 304. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39118-5_24.
8. Rivest R.L. (1995) The RC5 encryption algorithm. In: Preneel B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, vol. 1008. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-60590-8_7.
9. Mouha N., Mennink B., Van Herrewege A., Watanabe D., Preneel B., Verbauwhede I. (2014) Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: Joux A., Youssef A. (eds) Selected Areas in Cryptography - SAC 2014. SAC 2014. Lecture Notes in Computer Science, vol. 8781. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-13051-4_19.
10. Dinu D., Perrin L., Udovenko A., Velichkov V., Großschädl J., Biryukov A. (2016) Design Strategies for ARX with Provable Bounds: Sparx and LAX. In: Cheon J., Takagi T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-53887-6_18.
11. Hong D., Lee JK., Kim DC., Kwon D., Ryu K.H., Lee DG. (2014) LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim Y., Lee H., Perrig A. (eds) Information Security Applications. WISA 2013. Lecture Notes in Computer Science, vol 8267. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-05149-9_1.
12. Hong D. et al. (2006) HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol. 4249. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11894063_4.
13. Варгаузин В.А. Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедия. 2005. № 6. С. 23–27. URL: http://book.itep.ru/depository/zigbee/802.15.4.pdf (дата обращения: 20.01.2021).
14. Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology – EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-48285-7_33.
15. Козлов А.А., Карондеев А.М., Силков А.А. Сложение по модулю 2n в блочном шифровании. Вопросы кибербезопасности. 2015. №3(11). С. 34–42. URL: https://cyberrus.com/wp-content/uploads/2015/09/vkb_11_4.pdf (дата обращения: 20.01.2021).

REFERENCES:

[1] Zhukov A.E. Lightweight Cryptography, Cybersecurity Issues. 2015, no. 1(9). Part 1. P. 23–46. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_09_04.pdf (accessed: 20.01.2021) (in Russian).

[2] Zhukov A.E. Lightweight Cryptography, Cybersecurity Issues. 2015, no. 2(10). P. 2–10. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (accessed: 20.01.2021) (in Russian).

[3] Bernstein D.J. (2008) The Salsa20 Family of Stream Ciphers. In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol. 4986. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-68351-3_8.

[4] Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol. 4727. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-74735-2_31.

[5] Yang G., Zhu B., Suder V., Aagaard M.D., Gong G. (2015) The Simeck Family of Lightweight Block Ciphers. In: Güneysu T., Handschuh H. (eds) Cryptographic Hardware and Embedded Systems -- CHES 2015. CHES 2015. Lecture Notes in Computer Science, vol. 9293. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-48324-4_16.

[6] Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. (2015) The Simon and Speck Block Ciphers on AVR 8-Bit Microcontrollers. In: Eisenbarth T., Öztürk E. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2014. Lecture Notes in Computer Science, vol. 8898. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-16363-5_1.

[7] Shimizu A., Miyaguchi S. (1988) Fast Data Encipherment Algorithm FEAL. In: Chaum D., Price W.L. (eds) Advances in Cryptology – EUROCRYPT' 87. EUROCRYPT 1987. Lecture Notes in Computer Science, vol. 304. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39118-5_24.

[8] Rivest R.L. (1995) The RC5 encryption algorithm. In: Preneel B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, vol 1008. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-60590-8_7.

[9] Mouha N., Mennink B., Van Herrewege A., Watanabe D., Preneel B., Verbauwhede I. (2014) Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: Joux A., Youssef A. (eds) Selected Areas in Cryptography -- SAC 2014. SAC 2014. Lecture Notes in Computer Science, vol. 8781. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-13051-4_19.

[10] Dinu D., Perrin L., Udovenko A., Velichkov V., Großschädl J., Biryukov A. (2016) Design Strategies for ARX with Provable Bounds: Sparx and LAX. In: Cheon J., Takagi T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-53887-6_18.

[11] Hong D., Lee JK., Kim DC., Kwon D., Ryu K.H., Lee DG. (2014) LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim Y., Lee H., Perrig A. (eds) Information Security Applications. WISA 2013. Lecture Notes in Computer Science, vol. 8267. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-05149-9_1.

[12] Hong D. et al. (2006) HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol. 4249. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11894063_4.

[13] Vargauzin V.A. Radioseti dlja sbora dannyh ot sensorov, monitoringa i upravlenija na osnove standarta IEEE 802.15.4, TeleMultiMedija, 2005, no. 6. P. 23–27. URL: http://book.itep.ru/depository/zigbee/802.15.4.pdf (accessed: 20.01.2021) (in Russian).

[14] Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology – EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-48285-7_33.

[15] Kozlov A.A., Karondeev A.M., Silkov A.A. Addition modulo 2^n in block ciphers. Cybersecurity Issues. 2015, no. 3(11). P. 34–42. URL: https://cyberrus.com/wp-content/uploads/2015/09/vkb_11_4.pdf (accessed: 20.01.2021) (in Russian).

Поступила в редакцию – 25 января 2021 г. Окончательный вариант – 08 апреля 2021 г.
Received – January 25, 2021. The final version – April 08, 2021.

Владимир Л. Евсеев[1], Антон С. Бураков[2], Виталий Г. Иваненко[3]
[1,2]Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский пр–кт, 49, Москва, 125993, Россия
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VLEvseev@fa.ru, https://orcid.org/0000-0003-3283-3106
[2]e-mail: anton27061999@yandex.ru, https://orcid.org/0000-0003-1380-5273
[3]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501

ИСПОЛЬЗОВАНИЕ МЕТОДОВ КЛАСТЕРНОГО АНАЛИЗА ДЛЯ ОПТИМИЗАЦИИ КАЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.2.07

Аннотация. Статья посвящена точности оценки рисков информационной безопасности. В статье обосновывается актуальность оценки рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения. Анализируется метод качественной оценки рисков информационной безопасности (метод экспертной оценки) на конкретном примере. Обосновывается применение методов кластерного анализа. На примерах показано использование методов кластерного анализа: метод ближайшего соседа, метод удаленного соседа, метод *k*-средних. Приводятся принципиальные недостатки первых двух методов: появление больших кластеров не имеющих сходств, отсутствие возможности у экспертов заранее задать желаемое количество кластеров. Обосновывается применение метода *k*-средних – наличие возможности у экспертов заранее задать желаемое количество кластеров с помощью задания начальных центров. Приводится сравнение результатов, полученных при обычной качественной оценке, с результатами полученными методами кластерного анализа. Обосновывается целесообразность использования методов кластерного анализа для повышения точности оценки рисков информационной безопасности.

Ключевые слова: оценка риска, методы кластерного анализа, метод ближайшего соседа, метод удаленного соседа, метод k-средних, степень реализации угрозы, степень влияния угрозы на актив, евклидово расстояние, определяющее расстояние, среднее внутрикластерное расстояние.
Для цитирования: ЕВСЕЕВ, Владимир Л.; БУРАКОВ, Антон С.; ИВАНЕНКО, Виталий Г. ИСПОЛЬЗОВАНИЕ МЕТОДОВ КЛАСТЕРНОГО АНАЛИЗА ДЛЯ ОПТИМИЗАЦИИ КАЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 70–82, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1345>. Дата доступа: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.07.

Vladimir L. Evseev[1], Anton S. Burakov[2], Vitaliy G. Ivanenko[3]
[1,2]Financial University under the Government of the Russian Federation (Financial University),
Leningradsky prospekt, 49, Moscow, 125993, Russia
[3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VLEvseev@fa.ru, https://orcid.org/0000–0003-3283-3106
[2]e-mail: anton27061999@yandex.ru, https://orcid.org/0000-0003-1380-5273
[3]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501

Using cluster analysis techniques to optimize the qualitative assessment of information security risk

DOI: http://dx.doi.org/10.26583/bit.2021.2.07

Abstract. The study is devoted to the accuracy of information security risk assessment. The paper substantiates the relevance of risk assessment, based on the consequences of their implementation for business and the probability of their occurrence. The method of qualitative assessment of information security risks (the method of expert assessment) is analysed on a specific example. The application of cluster analysis methods is justified. In detail, the examples show the use of cluster analysis methods: the nearest neighbor method; the remote neighbor method; the k-means method. The principal disadvantages of the first two methods are: the appearance of large clusters that do not have similarities; the lack of the ability of experts to set the desired number of clusters in advance. The application of the k-means method is justified - the ability of experts to set the desired number of clusters in advance by setting the initial centers. The results obtained with the usual qualitative assessment are compared with the results obtained by the methods of cluster analysis. The expediency of using cluster analysis methods to improve the accuracy of information security risk assessment is justified.

Keywords: risk assessment, cluster analysis methods, nearest neighbor method, remote neighbor method, k-means method, degree of threat realization, degree of threat impact on the asset, Euclidean distance, determining distance, average intra-cluster distance.

For citation: EVSEEV, Vladimir L.; BURAKOV, Anton S.; IVANENKO, Vitaliy G. Using cluster analysis techniques to optimize the qualitative assessment of information security risk. IT Security (Russia), [S.l.], v. 28, n. 2, p. 70–82, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1345>. Date accessed: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.07.

Введение

В настоящее время количество и сложность информационных систем стремительно растет. Вместе с этим возрастает и число угроз для этих информационных систем. Это ставит вопросы информационной безопасности (ИБ) в IT-технологиях на первое место.

Для того, чтобы реализация угроз ИБ для компании не стала фатальной, следует придерживаться систематического подхода к менеджменту риска ИБ, который позволяет предотвращать или, в случае реализации угрозы, минимизировать последствия [1].

В национальном стандарте РФ ГОСТ Р ИСО/МЭК 27005-2010[1] дано определение риска ИБ, как возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Процесс управления рисками ИБ состоит из нескольких этапов [2, 3]. На наш взгляд самым важным этапом является оценка риска

Существует два основных способа оценки риска ИБ – количественный [4] и качественный [5, 6]. В первом – риск определяется по формуле [7]:

$$R = P(t) * S\,, \qquad (1)$$

где R – значение риска, $P(t)$ – вероятность реализации угрозы ИБ, S – степень влияния угрозы на активы (стоимость активов).

Если в выражении (1) стоимость актива S определить достаточно просто, то точно оценить вероятность реализации угрозы $P(t)$ достаточно сложно.

Поэтому, помимо количественной оценки риска (1), для анализа и оценки рисков ИБ применяется метод качественной оценки рисков. Его суть состоит в привлечении экспертов, которые ранжируют риски ИБ по степени их реализации и степени влияния на размер наносимого (нанесенного) ущерба (либо по 10-бальной шкале, либо по 5-бальной, либо другой шкале, выбранной в этом методе). Идентификационные признаки, по которым будет проводиться кластеризация: степень реализации угрозы, значение которой может быть от 0 до 10 (где степень равная 0 имеет нулевую вероятность реализации

[1]Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст)

угрозы, а значение степени равное 10 – вероятность реализации угрозы равна 1,0), степень влияния угрозы на актив, значение которой может быть от 0 до 10 (где степень равная 10 означает полное уничтожение актива). После выставления оценок каждым из экспертов, для каждого риска находятся средние арифметические степени его реализации и степени влияния угрозы на актив (размер наносимого ущерба) Но данный метод качественной оценки рисков ИБ не лишен недостатков. Рассмотрим это на примере. Допустим, что эксперты для оценки рисков составили матрицу, в которой выделили пять областей рисков: очень низкие, низкие, средние, высокие и очень высокие (рис. 1). Экспертами была проведена оценка пяти рисков $x_1,\ldots,x_5$ информационной безопасности по 10-бальной шкале. Для каждого риска были определены средние арифметические степени реализации угрозы и степени влияния угрозы на актив (размер наносимого ущерба): $x_1 = (5{,}6;\ 5{,}6);\ x_2 = (6{,}2;\ 6{,}4);\ x_3 = (7;\ 6{,}2);\ x_4 = (8;\ 0{,}8);\ x_5 = (0{,}6;\ 7)$, рис. 1.

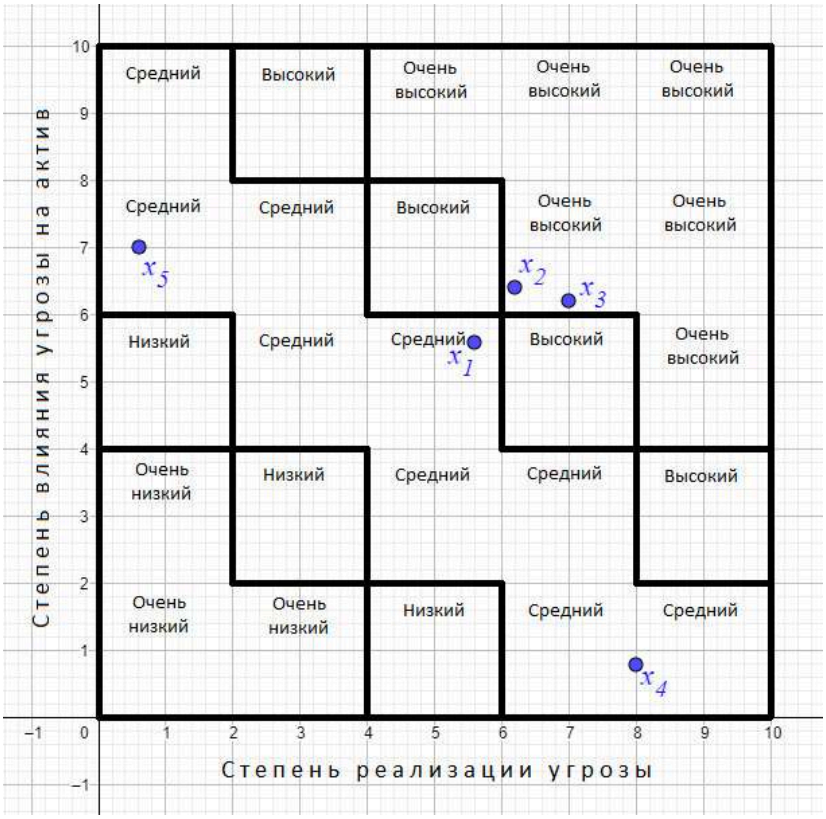

Рис. 1. Пример качественной оценки рисков
Fig. 1. Example of a qualitative risk assessment

Формально, по результатам классификации, риски x_1, x_4, x_5 должны обрабатываться специалистами по ИБ, как средние, а x_2 и x_3 – как очень высокие. Но на рис. 1 видно: риск x_1 на плоскости находится намного ближе к x_2 и x_3, поэтому его целесообразно обрабатывать, как очень высокий, или как минимум, высокий. После оценки рисков ИБ следует этап их обработки, который включает закупку и установку специалистами по ИБ средств защиты информации (СЗИ). Эффективность обработки риска зависит от результатов оценки риска.

Из-за неточности оценки рисков экспертами, они в дальнейшем могут быть обработаны некорректно, что может привести к одному из двух вариантов развития событий:

- неэффективная обработка риска, когда он относится к более низкой категории, чем реально, тогда при реализации угрозы ИБ компания понесет большие убытки;
- либо, наоборот, риск будет отнесен к более высокой категории, что приведет к значительному завышению средств на закупку и установку СЗИ, т.е. на обработку риска потратится средств больше, чем реально требуется.

Кроме того, для уменьшения общих затрат на закупку и установку СЗИ, целесообразно незначительные риски объединять в одну группу, например, области очень низкие и низкие. Для упорядочения рисков ИБ в сравнительно однородные группы целесообразно использовать математический аппарат, в частности – методы кластерного анализа.

1. Кластерные методы анализа рисков информационной безопасности

Для того, чтобы устранить недостатки, присущие качественной оценке рисков ИБ, используем кластерные методы анализа рисков [8, 9].

Преимущество использования методов кластерного анализа состоит в том, что они дают возможность проводить разбиение объектов не по одному признаку, а по целому ряду признаков. Кластеры – объединение нескольких однородных элементов, которое рассматривается как самостоятельная единица, обладающая определёнными свойствами. Суть методов кластерного анализа заключается в разбиении объектов на группы по признакам таким образом, чтобы каждый объект принадлежал только одному кластеру.

Существует множество методов кластеризации для формирования групп объектов, которые в целом схожи, но имеют разные критерии объединения в группы [10]. Будем использовать следующие методы кластерного анализа: метод ближайшего соседа, метод удаленного соседа, метод k-средних.

Алгоритмы методов кластерного анализа схожи и включают следующие шаги [11]:

1. Идентификация признаков, по которым будет проводиться кластеризация.
2. Определение выборки объектов для кластеризации.
3. Определение метрики и задание значения определяющего расстояния R между объектами, с помощью которого будет определяться сходство объектов.
4. Применение выбранного метода кластерного анализа.
5. Анализ полученных результатов.

2. Пример кластеризации рисков информационной безопасности

С целью демонстрации преимуществ методов кластерного анализа выполним группировку рисков ИБ на основе данных (2) методом обычной качественной оценки и с помощью методов кластерного анализа.

Пусть дано множество рисков ИБ, которое разобьем на группы, в которых первый параметр – степень реализации угрозы, второй – степень влияния угрозы на актив (оба параметра оцениваются экспертами по 10-бальной шкале):

$$x_1 = (5,\ 7);\ x_2 = (2,\ 1);\ x_3 = (1,\ 3);\ x_4 = (9,\ 8);\ x_5 = (5,\ 4);$$
$$x_6 = (10,\ 7);\ x_7 = (1,\ 9);\ x_8 = (8,\ 2);\ x_9 = (2,\ 8);\ x_{10} = (9,\ 3) \qquad (2)$$

Выполним группировку рисков ИБ на основе данных (2) методом обычной качественной оценки.

В результате было получено четыре группы рисков: $K_{75} = \{x_7; x_5\}$; $K_{32} = \{x_3; x_2\}$; $K_{10\,8\,1\,9} = \{x_{10}; x_8; x_1; x_9\}$; $K_{46} = \{x_4; x_6\}$. При этом, если риск находился на границе двух категорий, то он относился к более высокой группе, рис. 2.

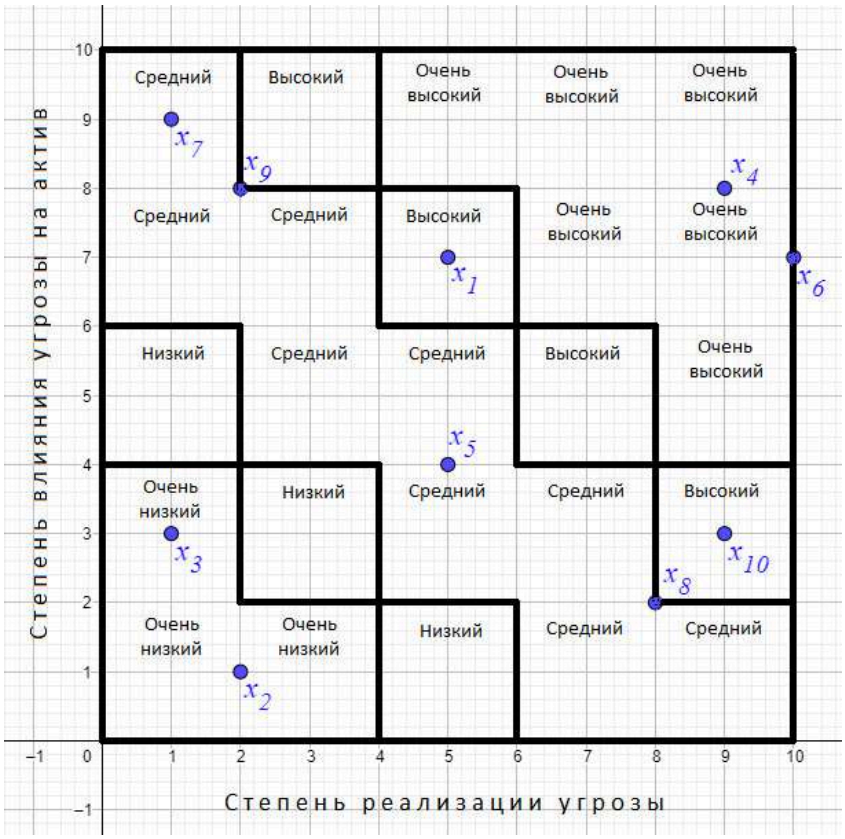

Рис. 2. Результат группирования рисков с помощью обычной качественной оценки
Fig. 2. The result of grouping risks using the usual qualitative assessment

Выполним разбиение рисков на группы с помощью методов кластерного анализа по вышеприведенному алгоритму для выбранных методов:

1. Идентификация признаков, по которым будет проводиться кластеризация.

Первый признак – степень реализации угрозы.

Второй признак – степень влияния угрозы на актив.

2. Определение выборки объектов для кластеризации.

Для сравнения с обычной качественной оценкой множество рисков ИБ берется из исходных данных (2).

Все исходные данные приводятся к единому диапазону значений (т.е. стандартизированы), что позволяет избежать некорректной кластеризации.

3. Определение метрики и задание значения определяющего расстояния R, с помощью которого будет определяться сходство объектов.

В качестве метрики выберем наиболее часто используемое для решения задач данного типа – евклидово расстояние ρ. Чем меньше это расстояние между объектами, тем они более схожи.

Задание значения определяющего расстояния R, с помощью которого будет определяться сходство объектов, выполняется лицом принимающим решение, у которого есть большой опыт в решении задач данного типа. Возьмем определяющее расстояние $R = 4$.

4. Применение выбранного метода кластерного анализа.

На данном этапе происходит применение выбранного метода кластерного анализа из трех вышеприведенных. В каждом методе свои правила формирования кластеров.

4.1. Метод ближайшего соседа [12].

В данном методе изначально каждый объект рассматривается как отдельный монокластер, например, объект x_1 образует монокластер $К_1$ и так далее. Между монокластерами рассчитывается евклидово расстояние ρ по выражению:

$$\rho_{(x_1;x_2)} = \left(\sum_{i=1}^{2}(x_{i1}-x_{i2})^2\right)^{1/2}, \quad (3)$$

где $x_1 -$ первый объект, $x_2 -$ второй объект, $i -$ признак объектов.

Если евклидово расстояние ρ между монокластерами меньше определяющего расстояния R, то они объединяются в новый кластер. Далее, находится евклидово расстояние ρ до ближайшего монокластера от ближайшего элемента новообразованного кластера.

Для упрощения решения задачи составим матрицу расстояний между монокластерами и уберём связи, где расстояние ρ больше определяющего расстояния *R*. Проведем вычисления расстояний ρ, подставив данные (2) в выражение (3). Результаты вычислений приведены в табл. 1 и табл. 2.

Таблица 1. Расстояния ρ между монокластерами

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
$К_1$	0,0	6,7	5,7	4,1	3,0	5,0	4,5	5,8	3,2	5,7
$К_2$	6,7	0,0	2,2	9,9	4,2	10,0	8,1	7,1	7,0	7,3
$К_3$	5,7	2,2	0,0	9,4	4,1	9,8	6,0	7,1	5,1	8,0
$К_4$	4,1	9,9	9,4	0,0	5,7	1,4	8,1	6,1	7,0	5,0
$К_5$	3,0	4,2	4,1	5,7	0,0	5,8	6,4	3,6	5,0	4,1
$К_6$	5,0	10,0	9,8	1,4	5,8	0,0	9,2	5,4	8,1	4,1
$К_7$	4,5	8,1	6	8,1	6,4	9,2	0,0	9,9	1,4	10,0
$К_8$	5,8	7,1	7,1	6,1	3,6	5,4	9,9	0,0	8,5	1,4
$К_9$	3,2	7	5,1	7,0	5,0	8,1	1,4	8,5	0,0	8,6
$К_{10}$	5,7	7,3	8,0	5,0	4,1	4,1	10,0	1,4	8,6	0,0

Таблица 2. Расстояния ρ между монокластерами, где расстояние ρ меньше определяющего расстояния R

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
$К_1$	0,0	0,0	0,0	0,0	3,0	0,0	0,0	0,0	3,2	0,0
$К_2$	0,0	0,0	2,2	0,0	0,0	0,0	0,0	0,0	0,0	0,0
$К_3$	0,0	2,2	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
$К_4$	0,0	0,0	0,0	0,0	0,0	1,4	0,0	0,0	0,0	0,0
$К_5$	3,0	0,0	0,0	0,0	0,0	0,0	0,0	3,6	0,0	0,0
$К_6$	0,0	0,0	0,0	1,4	0,0	0,0	0,0	0,0	0,0	0,0
$К_7$	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,4	0,0
$К_8$	0,0	0,0	0,0	0,0	3,6	0,0	0,0	0,0	0,0	1,4
$К_9$	3,2	0,0	0,0	0,0	0,0	0,0	1,4	0,0	0,0	0,0
$К_{10}$	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,4	0,0	0,0

Результаты кластеризации методом ближайшего соседа (данные табл. 2) представлены на рис. 3.

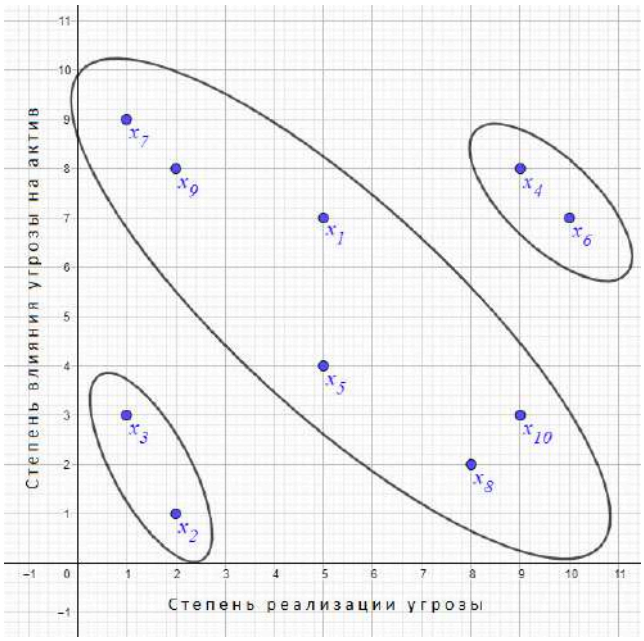

Рис. 3. Результаты кластеризации с помощью метода ближайшего соседа
Fig. 3. Results of clustering using the nearest neighbor method

4.2. Метод удаленного соседа [13].

В данном методе, по аналогии с предыдущим, каждый объект рассматривается как отдельный монокластер. Между монокластерами рассчитывается евклидово расстояние ρ по выражению (3).

Если евклидово расстояние между монокластерами ρ меньше определяющего расстояния *R*, то они объединяются в новый кластер. Разница между этим методом и предыдущим состоит в том, что на следующем этапе определяется расстояние ρ до ближайшего монокластера не от ближайшего элемента новообразованного кластера, а, наоборот, от самого дальнего.

Возьмем монокластер $К_7$ и найдем расстояние ρ до остальных монокластеров ($К_1$,…, $К_6$,) и ($К_8$, … , $К_{10}$), результаты представлены в табл. 3.

Таблица 3. Расстояние ρ от монокластера $К_7$ до остальных монокластеров

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_8$	$К_9$	$К_{10}$
$К_7$	4,5	8,1	6,0	8,1	6,4	9,2	9,9	1,4	10,0

Из анализа таблицы следует – наименьшее евклидово расстояние ρ, которое меньше определяющего расстояния R=4, – между седьмым и девятым монокластерами, которые и объединим в новообразованный монокластер $К_{79}$. Значит, кластер полностью сформирован.

Аналогично формируются остальные кластеры. Результаты кластеризации методом удаленного соседа представлены на рис. 4.

В двух примененных методах кластерного анализа нельзя с уверенностью утверждать, какое количество групп получится в итоге. При применении метода обычной качественной оценки было сформировано четыре группы, а в двух рассмотренных методах кластерного анализа – соответственно три и пять групп. Сравнению же подлежат методы, позволяющие получать одинаковое количество групп

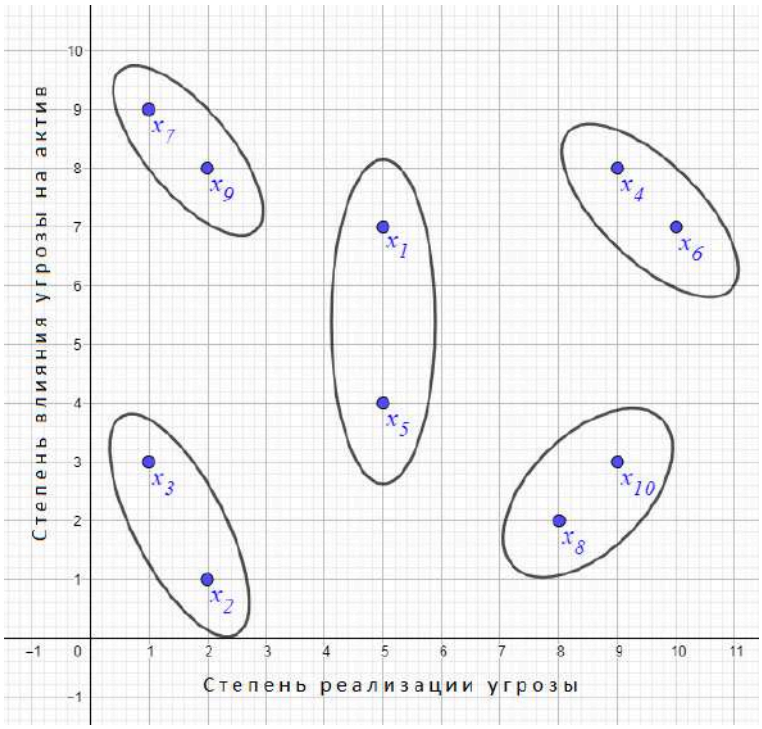

Рис. 4. Результаты кластеризации с помощью метода удаленного соседа
Fig. 4. Results of clustering using the remote neighbor method

4.3. Метод k-средних [14].

В начале данного метода задаются первоначальные центры для формирования кластеров. После этого, для каждого монокластера находится ближайший центр, который затем рассчитывается, как среднее значение параметров объектов, которые оказались ближе к нему. Процесс повторяется до тех пор, пока не будет изменений в распределении до и после.

Зададим 4 центра: $Z_1 = (2;2)$; $Z_2 = (2;8)$; $Z_3 = (8;2)$; $Z_4 = (8;8)$. Составим матрицу с расстояниями ρ от монокластеров до выбранных центров. Результаты представлены в табл. 4.

Таблица 4. Расстояния ρ между монокластерами и выбранными центрами

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
Z_1	5,8	1,0	1,4	9,2	3,6	9,4	7,1	6,0	6,0	7,1
Z_2	3,2	7,0	5,1	7,0	5,0	8,1	1,4	8,5	0,0	8,6
Z_3	5,8	6,1	7,1	6,1	3,6	5,4	9,9	0,0	8,5	1,4
Z_4	3,2	9,2	8,6	1,0	5,0	2,2	7,1	6,0	6,0	5,1

В табл. 5 оставлены только наименьшие значения расстояний ρ для каждого из монокластеров. У кластеров $К_1$ и $К_5$ есть два равноудаленных центра, выберем тот, у которого значения показателей больше.

Таблица 5. Минимальные расстояния ρ между монокластерами и выбранными центрами

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
Z_1		1,0	1,4		3,6					
Z_2	3,2						1,4		0,0	
Z_3					3,6			0,0		1,4
Z_4	*3,2*			1,0		2,2				

Получаем четыре новообразованных кластера:

$К_{79} = \{x_7; x_9\}$; $К_{32} = \{x_3; x_2\}$; $К_{10\,8\,5} = \{x_{10}; x_8; x_5\}$; $К_{461} = \{x_4; x_6; x_1\}$.

Затем рассчитаем новые центры:

$$Z_1 = \left(\frac{1+2}{2}; \frac{1+3}{2}\right) = (1{,}5; 2); \qquad Z_2 = \left(\frac{1+2}{2}; \frac{9+8}{2}\right) = (1{,}5; 8{,}5);$$
$$Z_3 = \left(\frac{5+8+9}{3}; \frac{4+2+3}{3}\right) = (7{,}3; 3); \quad Z_4 = \left(\frac{5+9+10}{3}; \frac{7+8+7}{3}\right) = (8; 7{,}3).$$

Снова найдем расстояния ρ до новообразованных центров Результаты представлены в табл. 6.

Таблица 6. Расстояния ρ от объектов до новообразованных центров

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
Z_1	6,1	1,1	1,1	9,6	4,0	9,9	7,0	6,5	6,0	7,6
Z_2	3,8	7,5	5,5	7,5	5,7	8,6	0,7	9,2	0,7	9,3
Z_3	4,6	5,7	6,3	5,3	2,5	4,8	8,7	1,2	7,3	1,7
Z_4	3,0	8,7	8,2	1,2	4,5	2,0	7,2	5,3	6,0	4,4

Оставим в табл. 6 только минимальные расстояния ρ для каждого объекта. Результаты представлены в табл. 7.

Таблица 7. Минимальные расстояния ρ между монокластерами и новообразованными центрами

	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	$К_9$	$К_{10}$
Z_1		1,1	1,1							
Z_2							0,7		0,7	
Z_3					2,5			1,2		1,7
Z_4	3,0			1,2		2,0				

Кластеры остались теми же, что и были получены по данным табл. 5, значит процесс кластеризации завершен. Итоговые результаты кластеризации с помощью метода *k*-средних представлены на рис. 5.

5. Анализ полученных результатов.

Количество кластеров и их состав, полученные разными методами кластеризации, различны. На данном этапе проводится анализ полученных кластеров, трактовка специфики отдельно взятого кластера.

5.1. С помощью кластеризации методом *ближайшего соседа* было получено три кластера: $К_{32} = \{x_3; x_2\}$; $К_{1\,5\,7\,8\,9\,10} = \{x_1, x_5, x_7, x_8, x_9, x_{10}\}$; $К_{46} = \{x_4; x_6\}$. Риски из кластера $К_{32}$ можно охарактеризовать, как риски с низким уровнем вероятности возникновения угрозы и низким потенциалом ущерба. Напротив, риски из кластера $К_{46}$ имеют высокую степень реализации угрозы, а значит обладают большим потенциалом ущерба. Самый же большой кластер $К_{1\,5\,7\,8\,9\,10}$ включает в себя риски среднего уровня.

Особенностью данного метода является близкое расположение друг к другу монокластеров, из-за чего могут появляться большие кластеры, некоторые элементы которых могут иметь мало сходств.

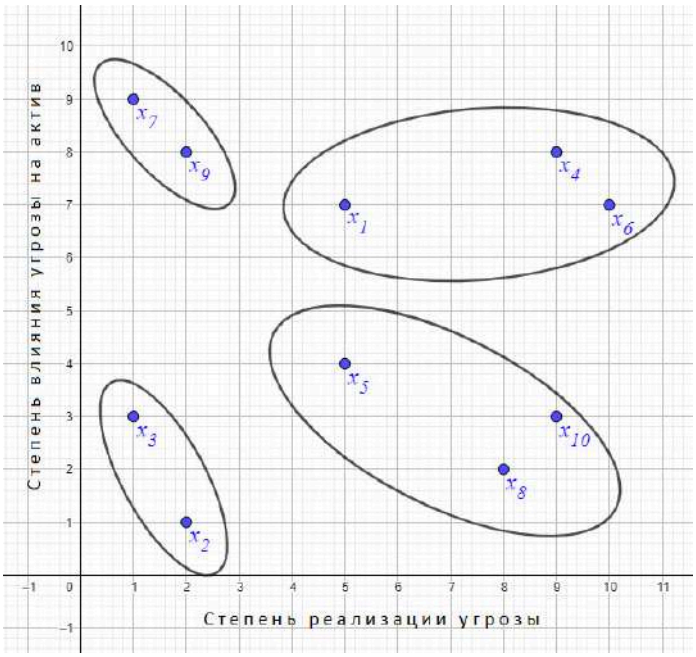

Рис. 5 Результаты кластеризации с помощью метода K-внутригрупповых средних
Fig. 5 Results of clustering using the K-intragroup mean method

5.2. С помощью кластеризации методом *удаленного соседа* было получено пять кластеров: $К_{79} = \{x_7; x_9\}$; $К_{32} = \{x_3; x_2\}$; $К_{10\,8} = \{x_{10}x_8\}$; $К_{51} = \{x_5; x_1\}$; $К_{46} = \{x_4; x_6\}$. Риски из кластера $К_{32}$ можно охарактеризовать, как очень низкие риски. Кластер $К_{10\,8}$, несмотря на высокую вероятность возникновения угрозы, включает в себя низкие риски и потенциальный ущерб небольшой. Кластер $К_{51}$ содержит средние риски. Кластер $К_{79}$ включает в себя высокие риски, у которых не очень большая степень реализации угрозы, но большой потенциальный ущерб. Кластер $К_{46}$ состоит из очень высоких рисков.

Данный метод является антиподом метода ближайшего соседа, в котором монокластеры располагаются близко друг к другу.

5.3. С помощью кластеризации методом *k-средних* были получены четыре кластера: $K_{79} = \{x_7; x_9\}$; $K_{32} = \{x_3; x_2\}$; $K_{10\,8\,5} = \{x_{10}; x_8; x_5\}$; $K_{461} = \{x_4; x_6; x_1\}$. Риски из кластера $К_{32}$ можно охарактеризовать как низкие риски. Кластер $К_{10\,8\,5}$ включает в себя средние риски, но, несмотря на высокую вероятность, потенциальный ущерб не велик. Кластер $К_{79}$ содержит высокие риски. Кластер $К_{461}$ состоит из очень высоких рисков.

Преимущество данного метода заключается в наличии возможности у экспертов заранее задать желаемое количество кластеров с помощью задания начальных центров.

Для сравнения результатов, полученных при обычной качественной оценке, с результатами, полученными методами кластерного анализа, находим среднее внутрикластерное расстояние для каждого метода, используя выражение для нахождения среднего внутрикластерного расстояния [15]:

$$d = \frac{1}{n-1}\sum_{i=1}^{n}\sum_{j=1}^{n}\rho(x_i;\ x_j), \tag{4}$$

где $\rho(x_i;\ x_j)$ – евклидово расстояние между объектами x_i и x_j, n – количество объектов в кластере.

Затем находим среднее арифметическое средних внутрикластерных расстояний для всех кластеров в каждом методе. Результаты представлены в табл. 8.

Таблица 8. Сравнение результатов оценки рисков информационной безопасности с помощью различных методов

Название метода	Количество кластеров	Среднее арифметическое средних внутрикластерных расстояний
Метод ближайшего соседа	3	13,2
Метод удаленного соседа	5	3,8
Метод *k*-средних	4	6,7
Обычная качественная оценка	4	10,6

Анализ данных табл. 8 показывает, что среднее арифметическое средних внутрикластерных расстояний значительно различаются в методах с различным количеством кластеров.

Сравнению же подлежат только те данные средних арифметических средних внутрикластерных расстояний используемых методов, у которых формируется одинаковое количество кластеров. В данном случае необходимо сравнить средние арифметические средних внутрикластерных расстояний (чем оно меньше, тем точнее определены риски), полученных при обычной качественной оценке и методом *k*-средних, так как количество получившихся кластеров у них одинаково.

Из сравнения следует, что при одинаковом количестве кластеров метод *k*-средних дает более точное решение (оценка рисков) по сравнению с обычной качественной оценкой, так как среднее арифметическое средних внутрикластерных расстояний в этом случае меньше.

Заключение

В работе проведено исследование применения в менеджменте рисков ИБ методов кластерного анализа и показано, что их использование позволяет повысить точность оценки рисков. В результате, при дальнейшей обработке рисков это позволит избежать, с одной стороны, использования недостаточного количества мер (закупка и установка СЗИ) для обработки рисков (а это может привести к реализации угроз), а с другой стороны – перерасходования средств на закупку и установку СЗИ, когда на обработку рисков затраты компании окажутся больше, чем необходимо. Кроме того, использование методов кластерного анализа позволяет структурировать угрозы ИБ по степени влияния на реализацию угроз и степени влияния угроз на активы компаний. Эффективность применения методов кластерного анализа в оценке рисков ИБ очевидна.

СПИСОК ЛИТЕРАТУРЫ:

1. Bodin L.D., Gordon L.A., Loeb M.P. Information security and risk management // Communications of the ACM. 2008. P. 64–68. URL: https://www.researchgate.net/publication/220425249_Information_security_and_risk_management (дата обращения: 15.03.2021). DOI: https://doi.org/ 10.1145/1330311.1330325.
2. Campbell T. The Information Security Manager // Practical Information Security Management. 2016. P. 31–42. URL: https://www.researchgate.net/publication/311318229_Practical_Information_Security_Management (дата обращения: 15.03.2021). DOI: https://doi.org/10.1007/978-1-4842-1685-9.
3. Козунова С.С., Кравец А.Г. Формализованное описание процедуры управления рисками информационной системы // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2018 № 2. С. 61–70. URL: https://cyberleninka.ru/article/n/formalizovannoe-opisanie-protsedury-upravleniya-riskami-informatsionnoy-sistemy (дата обращения: 15.03.2021). DOI: https://doi.org/10.24143/2072-9502-2018-2-61-70.
4. Баранова Е., Мальцева А. Анализ рисков информационной безопасности для малого и среднего бизнеса // Директор по безопасности. 2015 № 9. С. 58–63. URL: https://publications.hse.ru/articles/157681360 (дата обращения: 15.03.2021).

5. Wangen G. Information Security Risk Assessment: A Method Comparison // JOURNAL OF LATEX CLASS FILES, VOL. 6, NO. 1, JANUARY 2007. P. 1–7. URL: https://ieeexplore.ieee.org/document/7912273 (дата обращения: 15.03.2021). DOI: https://doi.org/10.1109/MC.2017.107.
6. Куркина Е.П., Шувалова Д.Г. Оценка рисков: экспертный метод // Проблемы науки. 2017 № 1 (14). С. 63–39. URL: https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod (дата обращения: 15.03.2021).
7. Винокур И.Р. Методика анализа и управления рисками. Количественная оценка рисков // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2020 № 1. С. 204–217. URL: https://cyberleninka.ru/article/n/metodika-analiza-i-upravleniya-riskami-kolichestvennaya-otsenka-riskov (дата обращения: 15.03.2021). DOI: https://doi.org/10.15593/2224-9354/2020.1.16.
8. Махрусе Н. Современные тенденции методов интеллектуального анализа данных: метод кластеризации // Московский экономический журнал. 2019 № 6. С. 359–377. URL: https://cyberleninka.ru/article/n/sovremennye-tendentsii-metodov-intellektualnogo-analiza-dannyh-metod-klasterizatsii (дата обращения: 15.03.2021). DOI: https://doi.org/10.24411/2413-046X-2019-16034.
9. Kettenring J.R. The practice of cluster analysis. Journal of Classification. 2006, 23. P. 3–30. URL: https://link.springer.com/article/10.1007/s00357-006-0002-6 (дата обращения: 15.03.2021). DOI: https://doi.org/10.1007/s00357-006-0002-6.
10. Тюрин А.Г., Зуев И.О. Кластерный анализ, методы и алгоритмы кластеризации // Вестник МГТУ МИРЭА. 2014 № 2 июнь 2014 выпуск 3. С. 86-97. URL: https://rtj.mirea.ru/upload/medialibrary/fba/09-tyurin.pdf (дата обращения: 15.03.2021).
11. Лось А.Б., Кабаов А.С., Трунцев В.И. Особенности использования кластерного анализа в системе менеджмента информационной безопасности // Промышленные контроллеры АСУ. 2013 № 8. С. 67–71. URL: https://publications.hse.ru/articles/145281528 (дата обращения: 15.03.2021).
12. Алексеева В.А., Калимуллина В.А. Применение метода ближайших соседей при моделировании кредитных рисков // Вестник Ульяновского государственного технического университета. 2014 № 3 (67). С. 54–56. URL: https://cyberleninka.ru/article/n/primenenie-metoda-blizhayshih-sosedey-pri-modelirovanii-kreditnyh-riskov (дата обращения: 15.03.2021).
13. Якимов А.И., Борчик Е.М., Башаримов В.В. Совместном использовании методов кластерного анализа многомерных данных // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2011 № 5 (59). С. 95–102. URL: https://cyberleninka.ru/article/n/sovmestnom-ispolzovanii-metodov-klasternogo-analiza-mnogomernyh-dannyh (дата обращения: 15.03.2021).
14. Осипова Ю.А., Лавров Д.Н. Применение кластерного анализа методом k-средних для классификации текстов научной направленности // Математические структуры и моделирование. 2017 № 3 (43). С. 108–121. URL: https://cyberleninka.ru/article/n/primenenie-klasternogo-analiza-metodom-k-srednih-dlya-klassifikatsii-tekstov-nauchnoy-napravlennosti (дата обращения: 15.03.2021).
15. Герасимова Н.И. Метод кластеризации многомерных данных на основе модифицированного алгоритма функционирования карт Кохонена / Н.И. Герасимова; науч. рук. С. В. Аксёнов // Молодежь и современные информационные технологии : сборник трудов XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых, г. Томск, 9-13 ноября 2015 г. : в 2 т. Томск : Изд-во ТПУ, 2016. Т. 1. С. 136–137. URL: http://earchive.tpu.ru/bitstream/11683/17107/1/conference_tpu-2015-C04-v1-059.pdf (дата обращения: 15.03.2021).

REFERENCES:

[1] Bodin L.D., Gordon L.A., Loeb M.P. Information security and risk management. Communications of the ACM. 2008. P. 64–68.
URL: https://www.researchgate.net/publication/220425249_Information_security_and_risk_management (accessed: 15.03.2021). DOI: https://doi.org/ 10.1145/1330311.1330325.
[2] Campbell T. The Information Security Manager. Practical Information Security Management. 2016. P. 31–42. URL:https://www.researchgate.net/publication/311318229_Practical_Information_Security_Management (accessed: 15.03.2021). DOI: https://doi.org/10.1007/978-1-4842-1685-9.
[3] Kozunova S.S., Kravets A.G. Formalized description of the information system risk management procedure. Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Computer Science. 2018, no. 2. P. 61–70. URL: https://cyberleninka.ru/article/n/formalizovannoe-opisanie-protsedury-upravleniya-riskami-informatsionnoy-sistemy (дата обращения: 15.03.2021). DOI: https://doi.org/10.24143/2072-9502-2018-2-61-70 (in Russian).

[4] Baranova E., Maltseva A. Analysis of information security risks for small and medium-sized businesses. Director of Security. 2015, no. 9. P. 58–63. URL: https://publications.hse.ru/articles/157681360 (accessed: 15.03.2021) (in Russian).

[5] Wangen G. Information Security Risk Assessment: A Method Comparison JOURNAL OF LATEX CLASS FILES. Vol. 6, no. 1, JANUARY 2007. P. 1–7. URL: https://ieeexplore.ieee.org/document/7912273 (accessed: 15.03.2021). DOI: https://doi.org/10.1109/MC.2017.107.

[6] Kurkina E.P., Shuvalova D.G. Risk assessment: expert method. Problems of science. 2017, no. 1 (14). P. 63–39. URL: https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod (accessed: 15.03.2021) (in Russian).

[7] Vinokur I.R. Methods of analysis and risk management. Quantitative risk assessment. Bulletin of the Perm National Research Polytechnic University. Socio-economic sciences. 2020, no. 1. P. 204–217. URL: https://cyberleninka.ru/article/n/metodika-analiza-i-upravleniya-riskami-kolichestvennaya-otsenka-riskov (accessed: 15.03.2021). DOI: https://doi.org/10.15593/2224-9354/2020.1.16 (in Russian).

[8] Mahruse N. Modern trends in data mining methods: clusterization method. Moscow Economic Journal. 2019, no. 6. P. 359–377. URL: https://cyberleninka.ru/article/n/sovremennye-tendentsii-metodov-intellektualnogo-analiza-dannyh-metod-klasterizatsii (accessed: 15.03.2021). DOI: https://doi.org/10.24411/2413-046X-2019-16034 (in Russian).

[9] Kettenring J.R. The practice of cluster analysis. J. Classif. 2006, 23. P. 3–30. URL: https://link.springer.com/article/10.1007/s00357-006-0002-6 (accessed: 15.03.2021). DOI: https://doi.org/10.1007/s00357-006-0002-6.

[10] Tyurin A.G., Zuev I.O. Cluster analysis, methods and clustering algorithms. Vestnik MGTU MIREA. 2014, no. 2, June 2014, issue 3. P. 86–97. URL: https://rtj.mirea.ru/upload/medialibrary/fba/09-tyurin.pdf (accessed: 15.03.2021) (in Russian).

[11] Los A.B., Kabov A.S., Trunci V.I. Features of using cluster analysis in the system of information security management. Industrial controllers ASU. 2013, no. 8. P. 67–71. URL: https://publications.hse.ru/articles/145281528 (accessed: 15.03.2021) (in Russian).

[12] Alekseev V.A., Kalimullina V.A. Application of the method of nearest neighbors in the modeling of credit risk. Vestnik of Ulyanovsk state technical University. 2014, no. 3 (67). P. 54–56. URL: https://cyberleninka.ru/article/n/primenenie-metoda-blizhayshih-sosedey-pri-modelirovanii-kreditnyh-riskov (accessed: 15.03.2021) (in Russian).

[13] Yakimov A.I., Borchik E.M., Basharimov V.V. Joint use of methods of cluster analysis of multidimensional data. Reports of the Belarusian State University of Informatics and Radioelectronics. 2011, no. 5 (59). P. 95–102. URL: https://cyberleninka.ru/article/n/sovmestnom-ispolzovanii-metodov-klasternogo-analiza-mnogomernyh-dannyh (accessed: 15.03.2021) (in Russian).

[14] Osipova Yu.A., Lavrov D.N. Application of cluster analysis by the k-means method for classification of scientific texts. Mathematical structures and modeling. 2017, no. 3 (43). P. 108–121. URL: https://cyberleninka.ru/article/n/primenenie-klasternogo-analiza-metodom-k-srednih-dlya-klassifikatsii-tekstov-nauchnoy-napravlennosti (accessed: 15.03.2021) (in Russian).

[15] Gerasimova N.I. Method of clusterization of multidimensional data on the basis of a modified algorithm for the functioning of Kohonen maps N.I. Gerasimova; scientific hands. S.V. Aksenov Youth and modern information technologies: proceedings of the XIII International Scientific and Practical Conference of Students, postgraduates and young scientists, Tomsk, November 9-13, 2015: in 2 vols. Tomsk: Publishing House of TPU, 2016. Vol. 1. P. 136–137. URL: http://earchive.tpu.ru/bitstream/11683/17107/1/conference_tpu-2015-C04-v1-059.pdf (accessed: 15.03.2021) (in Russian).

Поступила в редакцию – 19 марта 2021 г. Окончательный вариант – 22 апреля 2021г.
Received – March 19, 2021. The final version – April 22, 2021.

Владимир Д. Колычев[1], Николай А. Буданов[2]
Национальный исследовательский ядерный университет «МИФИ»
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VDKolychev@mephi.ru, https://orcid.prg/0000-0002-8616-9354
[2]e-mail: NABudanov@mephi.ru, https://orcid.prg/0000-0002-9714-2915

КОМПЛЕКСНАЯ МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКОМ БАНКЕ

DOI: http://dx.doi.org/10.26583/bit.2021.2.08

Аннотация. В данной статье рассматриваются методы увеличения защищенности информационной системы коммерческого банка. Предметом исследования является комплексная методика оценки информационной безопасности, используемая для определения уровня защищенности и риска информационной безопасности автоматизированной системы на основе прогнозных оценок и специализированного программного инструментария. Целью исследования и проводимого в работе анализа является повышение эффективности принимаемых решений при выполнении работ по оценке и управлению рисками в коммерческом банке. Результаты, представленные в рамках разработанной методики, могут быть использованы для решения задач увеличения надежности автоматизированной информационной системы в различных сферах и секторах деятельности, включая и организации промышленного сектора, а также коммерческие организации. Основные подходы, используемые при разработке комплексной методики оценки рисков, относятся к методам экспертного оценивания, теории случайных Марковских процессов, методам и моделям математической статистики и теории вероятностей, методам прикладного системного анализа и прогнозирования.

Ключевые слова: оценка рисков, информационные технологии, коммерческий банк, информационная система, средства защиты информации, автоматизированная информационная система.
Для цитирования: КОЛЫЧЕВ, Владимир Д.; БУДАНОВ, Николай А. КОМПЛЕКСНАЯ МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКОМ БАНКЕ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 83–97, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1346>. Дата доступа: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.08.

Vladimir D. Kolychev[1], Nikolay A. Budanov[2]
National research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VDKolychev@mephi.ru, https://orcid.prg/0000-0002-8616-9354
[2]e-mail: NABudanov@mephi.ru, https://orcid.prg/0000-0002-9714-2915

Development of a comprehensive methodology for assessing information security risks in a commercial bank

Abstract. This paper discusses the methods of improving the security of the information system of a commercial bank. The subject of the study is a comprehensive methodology for assessing information security used to determine the level of security and risk of information security of an automated system based on predictive estimates and specialized software tools. The purpose of the study and the carried out analysis are to improve the effectiveness of decisions made when performing work on risk assessment and management in a commercial bank. The results presented in the framework of the developed methodology can be used to solve the problems of increasing the reliability of an automated information system in various fields and sectors of activity, including organizations of the industrial sector, as well as commercial organizations. The main approaches used in the development of a comprehensive risk assessment methodology relate to the methods of expert assessment, the theory of random Markov processes, methods and models of mathematical statistics and probability theory, methods of applied system analysis and forecasting.

Keywords: risk assessment, information technology, commercial bank, information system, information security tools, automated information system.
For citation: KOLYCHEV, Vladimir D.; BUDANOV, Nikolay A. Development of a comprehensive methodology for assessing information security risks in a commercial bank. IT Security (Russia), [S.l.], v. 28, n. 2, p. 83– 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1346>. Date accessed: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.08.

Введение

Задачи исследования информационной безопасности (ИБ) в сфере корпоративных банковских информационных систем остаются по-прежнему актуальными, особенно в связи с ростом объема обрабатываемых массивов данных, повышения требований к надежности и отказоустойчивости программно-аппаратных комплексов технических средств [1].

Используемая система защиты корпоративных информационных систем на предприятии включает в качестве составных компонентов технические и программно-аппаратные средства защиты, организационно-методическое обеспечение, а также подсистемы гарантирующие надежность и высокую степень безопасности обрабатываемых данных.

Например, в [1] «предметом исследования является комплексная оценка системы информационной безопасности, предоставляющая возможность определения уровня защищенности информационной системы на основе прогнозных оценок. Объектом исследования является набор методов, обеспечивающих информационную безопасность корпоративных информационных систем, а также методика анализа рисков».

В отличие от [1], в данной статье дается описание разработки комплексной методики оценки и управления рисками информационной безопасности коммерческого банка на основе прогнозирования инцидентов информационной безопасности, вызванных субъективными и объективными дестабилизирующими факторами.

1. Разработка моделей бизнес-процессов комплексной оценки рисков в коммерческом банке

Динамика внедрения проектов развития информационных систем в банковской сфере и сокращение числа коммерческих банков свидетельствует о необходимости повышения требования к защищённости информационных системы, повышению надежности и отказоустойчивости их функционирования, обеспечения целостности, доступности, конфиденциальности и качества обработки информации. На рис. 1 представлена динамика изменения количества коммерческих банков [2], причем тенденция к сокращению их числа будет сохраняться и в дальнейшем[1].

Таким образом, наиболее финансово устойчивые коммерческие структуры в банковском секторе обладают высокотехнологичными информационными системами и сервисами, построенными на принципах комплексной защиты информации и предотвращения утечек персональных данных клиентов в связи с участившимися в последнее время фактами мошенничества.

[1]Количество банков в России по годам. URL: http://fincan.ru/articles/53_kolichestvo-bankov-v-rossii-po-godam/#:~:text=Динамика%20количества%20банков%20в%20России.,2018%20г.%20–%20уже%2057 (дата обращения: 14.04.2021)

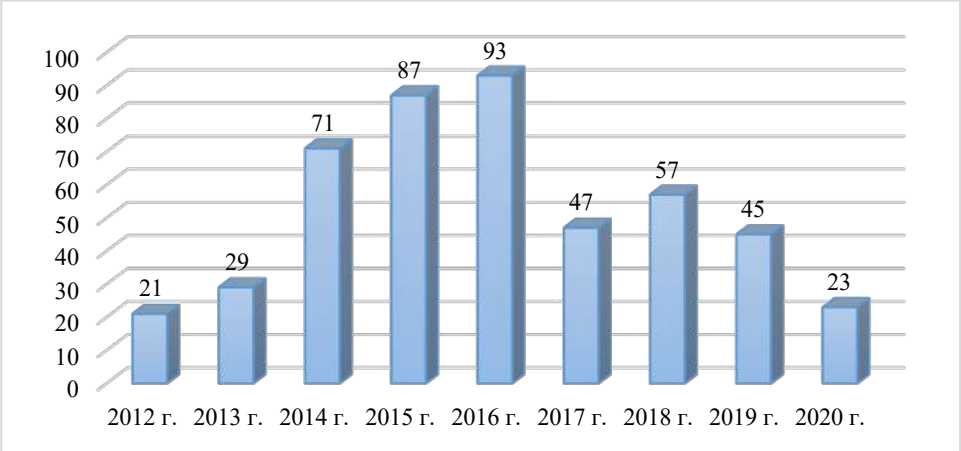

Рис. 1. Динамика отзыва лицензий у коммерческих банков на территории РФ [2]
Fig. 1. Dynamics of revocation of licenses from commercial banks in the Russian Federation [2]

В настоящее время в связи с использованием процессного подхода разрабатываются требования к формированию системы информационной безопасности коммерческого банка, которая определяется как состояние безопасности целей предприятия в условиях угроз для информационной среды [3].

Работы по обеспечению информационной безопасности коммерческого банка, в силу определенной специфики, оказывают непосредственное влияние на функционирование организации посредством:

- документации, регламентирующей информационную безопасность, в том числе и аффилированных структурных подразделений;
- методов контроля информационной безопасности, основываясь на статистических данных об инцидентах и угрозах, данных мониторинга информационной и аудита безопасности информационной системы;
- комплексного характера интересов и целей бизнес-деятельности предприятия в области информационного контроля, с учетом деятельности структурных подразделений предприятия [4].

Разработанная авторами схема оценки рисков информационной безопасности на предприятии представлена на рис. 2. В разработанной модели бизнес-процесса представлен подход к обеспечению безопасности информационной системы, включая следующие основные элементы: идентификация угроз, общее описание анализа мер обеспечения безопасности, позволяющее проводить детализированное исследование в рамках конкретной информационной системы. При этом необходимо определение комплекса защитных мер (технических, организационных, административных или технологических) для противостояния внешним угрозам [5, 6].

Следует при этом отметить, что деятельность в области анализа информационной безопасности представлена следующими этапами: идентификация и оценка характеристик угроз информационной безопасности, оценка защищенности компонентов, оценка ценности привлекаемых и используемых инфраструктурных ресурсов, документирование результатов, включая комплекс разработанных мероприятий по обеспечению информационной безопасности [6].

2. Обзор нормативно-методического инструментария оценки рисков в коммерческом банке

В основу комплексной методики заложены методы прикладного системного анализа информационной безопасности коммерческого банка, включающие применение интегрированных средств защиты информации.

В качестве нормативно-методического инструментария при разработке комплексной методики оценки рисков использован ряд отечественных[2] и зарубежных стандартов в сфере информационной безопасности: Международный стандарт ISO/IEC 1779-2005, стандарт Cobit 4 Edition (США), NIST 800-30, стандарт BS ISO 27002:2005 (Великобритания).

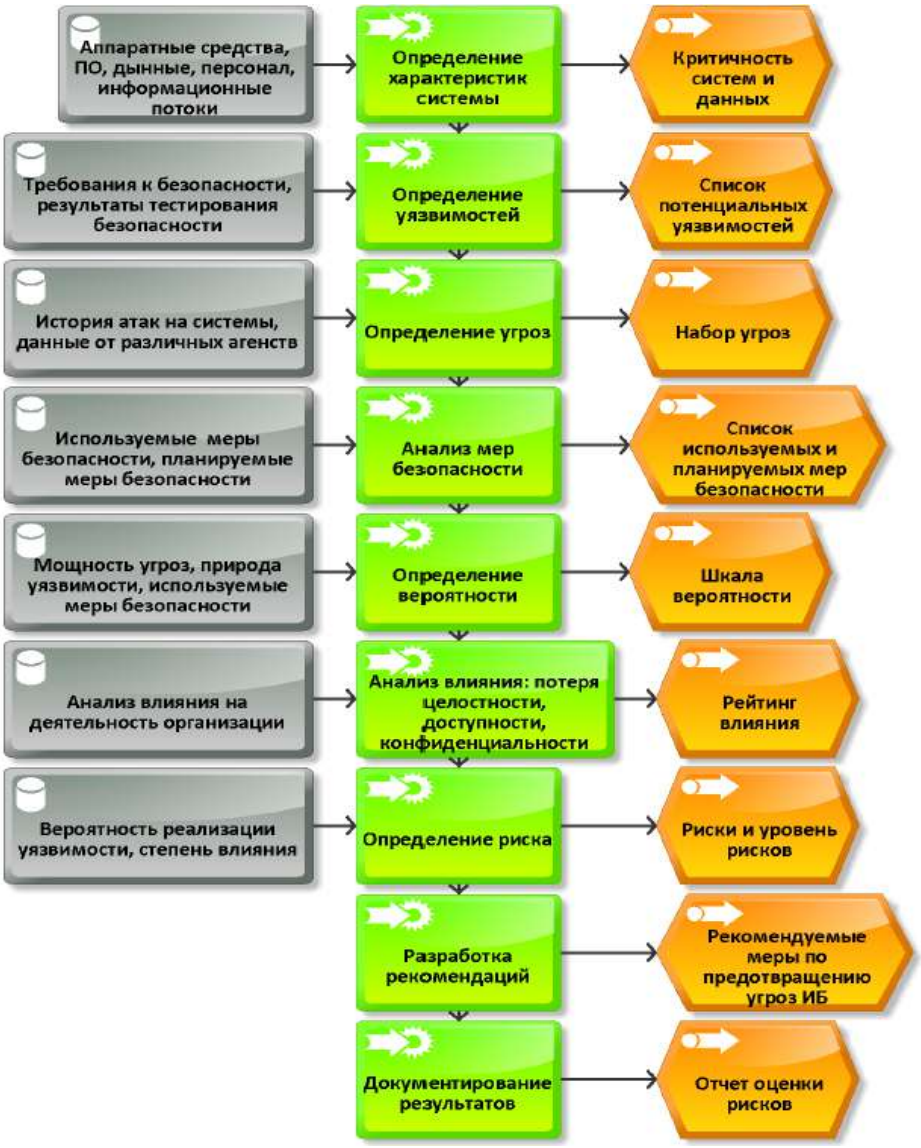

Рис. 2. Схема оценки рисков информационной безопасности
Fig. 2. Information security risk assessment scheme

[2]ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»

Согласно действующим российским и международным нормативным документам идентификация угроз информационной безопасности проводится на основе сформированного перечня угроз, принимая во внимание частоту их возникновения, используя для исследования и анализа формат реестра или базы данных. Среди факторов, оказывающих существенное влияние на процесс анализа рисков информационной безопасности, следует выделить: наличие и доступность ресурсов коммерческого банка, кадровый состав, информационную инфраструктуру, нормативно-методическое обеспечение и рабочую документацию, аппаратные средства и программное обеспечение, оборудование для обеспечения связи.

Результатом оценивания рисков является список оцененных рисковых ситуаций по каждому отдельному инциденту информационной безопасности, включая также дополнительные факторы, связанные с разграничением прав доступа, модификацией и разрушением информационной инфраструктуры коммерческого банка (нарушением функционирования сервисов и подсистем) [7, 8].

Разработанная с учетом действующих стандартов схема деятельности по обеспечению информационной безопасности и оценке рисков представлена на рис. 3.

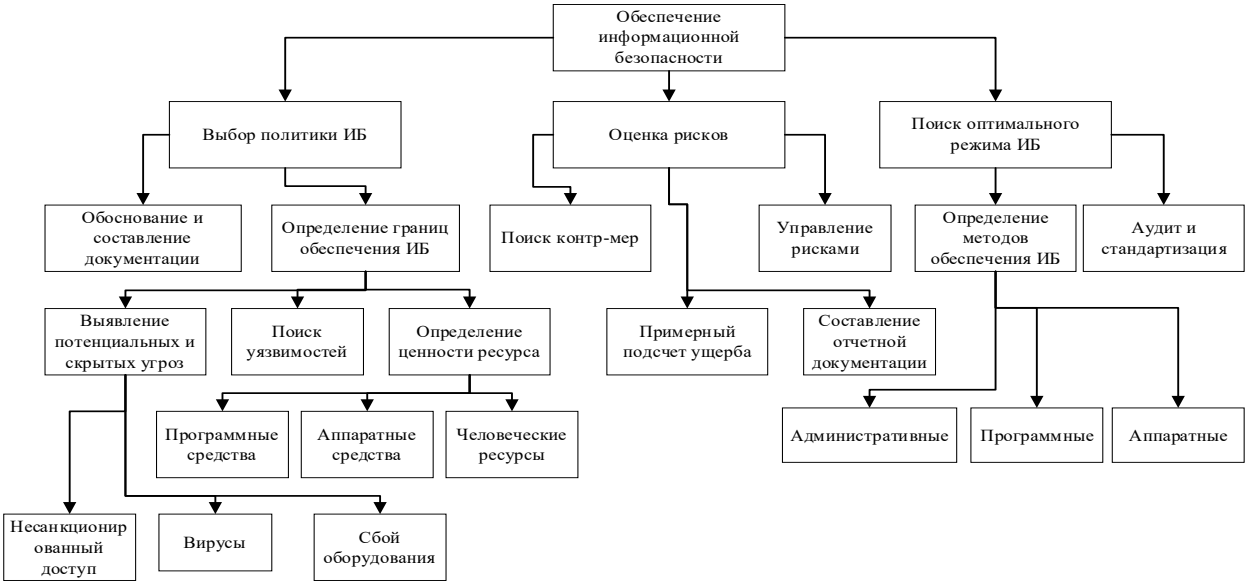

Рис. 3. Схема деятельности по обеспечению информационной безопасности и оценке рисков
Fig. 3. Outline of information security and risk assessment activities

Большинство методик[3] и стандартов[4] оценки информационной безопасности выстраивается на основе моделирования состава объектов, обобщённая модель структуры комплекса программно-технических средств, представлена на рис. 4.

Автоматизированная информационная система (АИС) коммерческого банка включает следующие компоненты:

- Сервер обработки, с помощью которого обрабатываются данные;
- Маршрутизатор для объединения внутренней сети Intranet с внешней Internet;

[3]Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)
[4]Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399)

- Сервер БД, выполняющий обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиента к информации;

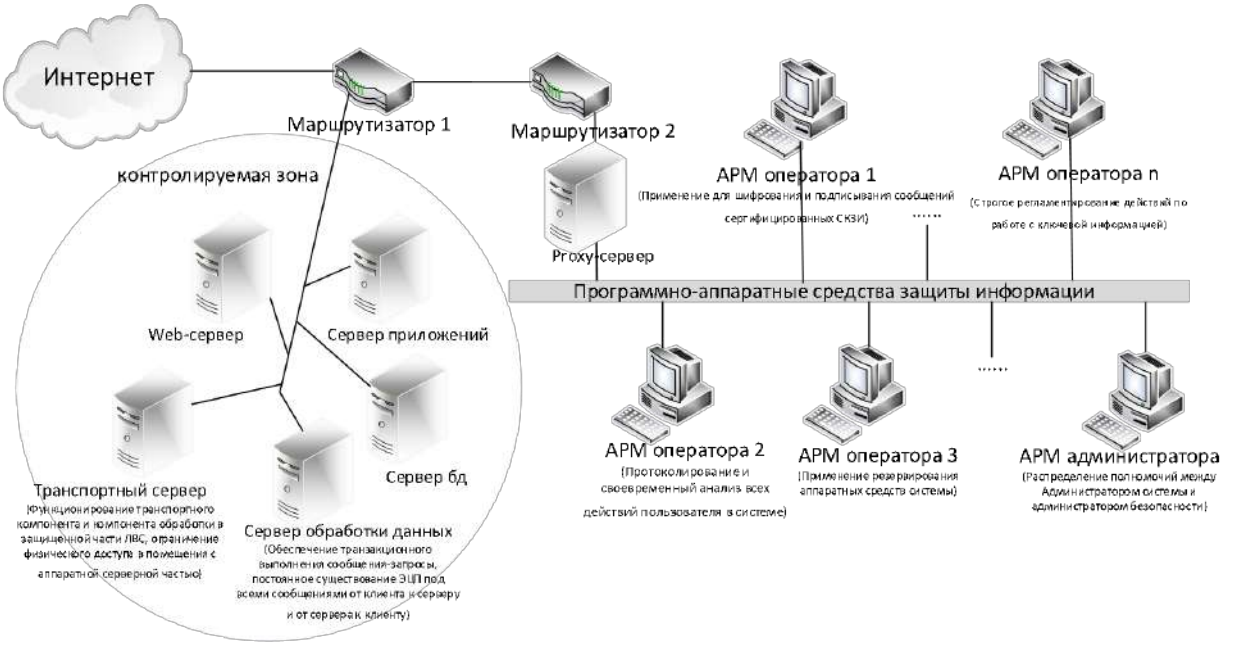

Рис. 4. Обобщенная структура комплекса программно-технических средств информационной системы

Fig. 4. Generalized structure of the complex of software and hardware tools of the information system

- Транспортный сервер, осуществляющий перенаправление информационных потоков;
- Proxy-сервер, осуществляющий мониторинг действий пользователей вне локальной сети;
- Сервер приложений, предназначенный для эффективного исполнения процедур (программ, скриптов), на которых построены приложения, а также для идентификации пользователей посредством разработанных приложений;
- Веб-сервер, предназначенный для получения доступа к внутренним информационным ресурсам организации;
- Администраторский АРМ для управления системой;
- Множество АРМ пользователей – операторов.

3. Разработка методики и реализация алгоритмов оценки рисков информационной безопасности в коммерческом банке

На основе принципов [9, 10] и стандартов информационной безопасности, разработана комплексная методика оценки рисков информационной безопасности в коммерческом банке, состоящая из следующих этапов: описание характеристик информационной системы (включая выделенные компоненты), формирование моделей нарушителя и угроз, ранжирование и оценивание важных угроз (с использованием методов экспертной оценки), оценка и прогнозирование инцидентов в соответствии с субъективными дестабилизирующими факторами (с использованием экспертных методов), оценка инцидентов в соответствии с субъективными дестабилизирующими факторами (с использованием экспертных методов), формирование отчетов,

направленных на принятие мер по совершенствованию или построению системы по защите информации [11].

На стадии описания характеристик информационной системы определяется множество объектов информационной системы (ИС), которые формально представляются в вид $s_i \in \{S\}$, где S – общее количество компонентов информационной системы, $i \in 1 \ldots n$, а n – общее количество компонентов информационной безопасности. На основе разработанных моделей по обеспечению информационной безопасности и оценке угроз были разработаны компоненты модели объекта, на который направлены угрозы. Модель объекта включает следующие атрибуты: инфраструктура, различные виды коммуникационных информационных сетей, компоненты систем передачи данных, база данных, стандартное ПО и др.

В свою очередь, модель угроз для информационной системы включает две выделенные категории угроз: объективные и субъективные, которые в свою очередь подразделяются на внешние и внутренние угрозы.

Для информационной системы коммерческого банка модель нарушителя основывается на трех категориях нарушителей в соответствии с правами доступа в контролируемую зону: внешние (хакеры), внутренние (партнеры) и внутренние (персонал). Внутренние нарушители разделяются на уровни согласно правам доступа в интегрированную АИС предприятия, также выделяют внешних нарушителей согласно их уровню осведомленности о параметрах информационной системы – клиенты, партнеры, контрагенты, поставщики и др.

Важными компонентами модели нарушителя являются общедоступное и специализированное программное обеспечение, включая программные компоненты, разработанные злоумышленниками, находящиеся в сети интернет в свободном доступе, использующие известные уязвимости («черви», вирусы, exploit, сканеры безопасности и др.). Как правило, злоумышленникам становится доступной следующая информация об объекте атаки: юридический и нормативно-правовой статус, сфера деятельности и технологии безопасности, сведения о топологических характеристиках корпоративной вычислительной сети, сведения о доступных для атаки портах рабочих станций и на сервере, используемое ПО, идентификационные пользовательские данные, методы защиты конфиденциальной информации и др.

Для оценки числа инцидентов, ранжирования и оценивания важных угроз информационной безопасности в АИС используются методы экспертной оценки [11, 12] в соответствии со следующим алгоритмом:

1. Формируется множество (пул) экспертов из числа компетентных специалистов в области информационной безопасности и сфере ИТ, создается анкета для оценивания уровня компетентности и вероятностей реализации угрозы, возможности восстановления системы после возникновения угрозы;
2. Оценивается профессионализм каждого эксперта (специалиста);
3. Эксперт заполняет предложенную анкету, в которой следует отметить количество инцидентов, которые, могут произойти на протяжении одного периода (как правило, месяца) в автоматизированной банковской информационной системе;
4. Проводится оценка согласованности мнения экспертов в соответствии с дисперсионным коэффициентом конкордации W и оценивается уровень значительности коэффициента, согласно критерию Пирсона χ^2;
5. Определяется результирующее (итоговое) значение инцидентов в сфере ИБ $r_i = \frac{\sum_{j=1}^{m} r_{ij}}{K_j}$, учитывая коэффициент компетентности каждого эксперта, где параметр

r_{ij} – оценка, принадлежащая *j*-му эксперту *i*-му фактору, $i \in 1..n$, $j \in 1..m$, (*n* – общее число экспертов, а *m* – число факторов), *K* – расчетный параметр компетентности *j* – го эксперта, т.е. его компетентность.

Определение степени компетентности экспертов реализуется на основе следующего алгоритмического подхода:

1. Специалист (компетентный эксперт) заполняет анкету, отвечая на предложенные вопросы;

2. Ответы на анкетные вопросы со стороны эксперта сохраняются в БД, проводится расчет, и получают коэффициент компетентности каждого опрошенного эксперта K_i;

3. Рассчитанные показатели нормируются $K_j = \frac{K_j}{\sum_j^1 K_j}$ и затем используются при расчете количества инцидентов информационной безопасности.

С целью определения числовой оценки согласованности экспертов, используется коэффициент конкордации *W*, рассчитываемый на основе следующего соотношения: $W = \frac{12S}{m^2(n^3-n)-m\sum_{j=1}^{m} T_j}$, где *S* – сумма квадратов отклонений, $S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} r_{ij} - \bar{r}\right)^2$, $\bar{r} = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}$, T_j – индикатор связанных рангов при ранжировании *j*-го эксперта, $T_j = \sum_{K=1}^{H_j} h_k^3 - h_k$, где h_k – количество совпадающих рангов в *k*-й группе связанных рангов; H_j – количество групп совпадающих рангов в ранжировании *j*-го эксперта.

Коэффициент конкордации *W* численно изменяется в диапазоне $0 \le W \le 1$. Верхняя граница обозначает, одинаковые оценки информативности факторов, которые проставили эксперты, нижняя граница отображает отсутствие связи между оценками, которые получены от разных экспертов [12, 13].

Оценка значимости коэффициента конкордации *W* выполняется в соответствии с критерием Пирсона χ^2 с применением соотношения: $\chi^2 = \frac{12S}{mn(n+1)-\frac{1}{n-1}\sum_{j=1}^{m} T_j}$.

Вычисленное значение критерия χ^2 сопоставляется с пороговым значением $\chi^2_{кр}(a, n-1)$ по степени значимости α, а также и по количеству степеней свободы *n* – 1. В том случае, если выполняется соотношение $\chi^2 \ge \chi^2_{кр}$, экспертные оценки считаются согласованными. Вероятность осуществления угроз информационной безопасности для автоматизированной системы определяется на основе соотношения: $P(t) = 1 - e^{-\lambda t}$, где λ – интенсивность осуществления угрозы ИБ, *t* – общее количество времени функционирования банковской информационной системы.

Для выделенных экспертами угроз информационной безопасности вычисляется значение P_{X_j} по расчетным вероятностям согласно шкалам оценки вероятностей.

Оценивание степени воздействия угроз информационной безопасности в коммерческом банке реализуется посредством следующего подхода:

1. Администратор безопасности знакомится с предлагаемой шкалой оценки степени воздействия угроз информационной безопасности в коммерческом банке;

2. Администратор безопасности заполняет предлагаемую анкету по оценке степени воздействия L_{X_j} любой угрозы на информационную систему коммерческого банка.

Оценивается вероятность восстановления по окончанию выполнения угроз ИБ посредством следующего алгоритма:

1. Экспертам представляется для ознакомления шкала оценки вероятности возобновления АИС;

2. Экспертам предлагается оценить вероятность возобновления работоспособности АИС после реализации набора реализованных угроз информационной безопасности;

3. Оценивается согласованность специалистов в соответствии с дисперсионным коэффициентом конкордации *W*, а также оценивается уровень значимости расчетного коэффициента, согласно критерию Пирсона χ^2.

4. Определяется результирующее значение вероятности возобновления функционирования АИС после реализации набора угроз, учитывая коэффициент компетентности каждого специалиста. При этом оценка значимости угроз ИБ, считается необходимой, с целью идентификации угроз ИБ, которые являются наиболее опасными.

В качестве результирующих данных используют вероятность осуществления угроз P_{X_j}, с множеством допустимых значений *P* = [0,1] и множеством базовых значений *Tp* = {очень высокая, высокая, средняя, низкая, очень низкая}= $\{a_{X_1}, a_{X_2}, a_{X_3}, a_{X_4}, a_{X_5}\}$ и уровнем воздействия угроз ИБ L_{X_j} с областью допустимых значений *L* = [0,1] и множеством базовых значений T_L = {разрушительное воздействие, критическое воздействие, тяжелое воздействие, умеренное воздействие, легкое воздействие}[1].

Уровень значимости угрозы ИБ F_{X_j} с областью допустимых значений *F* = [0,1] и множеством базовых значений T_F = {разрушительное, большое, среднее, малое, несущественное} = $\{a_{V_1}, a_{V_2}, a_{V_3}, a_{V_4}, a_{V_5}\}$, считается выходным параметром модели.

Таким образом, на основе существующих методов оценивания и предлагаемых алгоритмов оценки определяется:

- множество значительных угроз, которые способен осуществить нарушитель в ИС $x_{ij} \in \{X\}$, где $i \in 1 \ldots kj \in 1 \ldots m$, *m* – общее количество угроз ИБ, *k* – общее количество нарушителей ИБ;
- множество важных угроз ИБ для любого из объектов $x_{js_i} \in \{X\}$ и для любого из нарушителей $x_{i,js_i} \in \{X\}$;
- множество важных угроз ИБ для любого объекта и для любого нарушителя, которые относятся к классам: конфиденциальности $\{K\} - k_{js_i}, k_{i,js_i} \in \{K\} \subset \{X\}$; целостности $\{C\} - c_{js_i}, c_{i,js_i} \in \{C\} \subset \{X\}$; доступности $\{D\} - d_{js_i}, d_{i,js_i} \in \{D\} \subset \{X\}$.

После оценки уровня воздействия угроз ИБ, значения значимых угроз нормируются для: всех важных угроз ИБ $P_{норм}(x_j) = \frac{P(x_j)}{\sum_{j=1}^{m} P(x_j)}$; любого объекта ИС $P_{норм}(x_{js_i}) = \frac{P(x_{js_i})}{\sum_{j=1}^{m} P(x_{js_i})}$; любого объекта ИС по доступности, целостности и конфиденциальности $P_{норм}(k_{js_i}) = \frac{P(k_{js_i})}{\sum_{j=1}^{m} P(k_{js_i})}$; $P_{норм}(c_{js_i}) = \frac{P(c_{js_i})}{\sum_{j=1}^{m} P(c_{js_i})}$. Аналогичным образом нормируют вероятности неполного или частичного возобновления функций.

Далее определяется абсолютная вероятность осуществления угроз ИБ для любого объекта, нарушителя и абсолютная вероятность осуществления угроз для любого объекта ИС по трем категориям угроз: доступности, целостности и конфиденциальности [1]. Разработанная схема модели оценки рисков информационной безопасности в коммерческом банке представлена на рис. 5. Основное задачей создания методики оценки информационной безопасности является оценивание возможности использования выходных данных модели, с целью их применения в качестве входных для разработки рекомендаций для увеличения степени безопасности в автоматизированной ИС коммерческого банка.

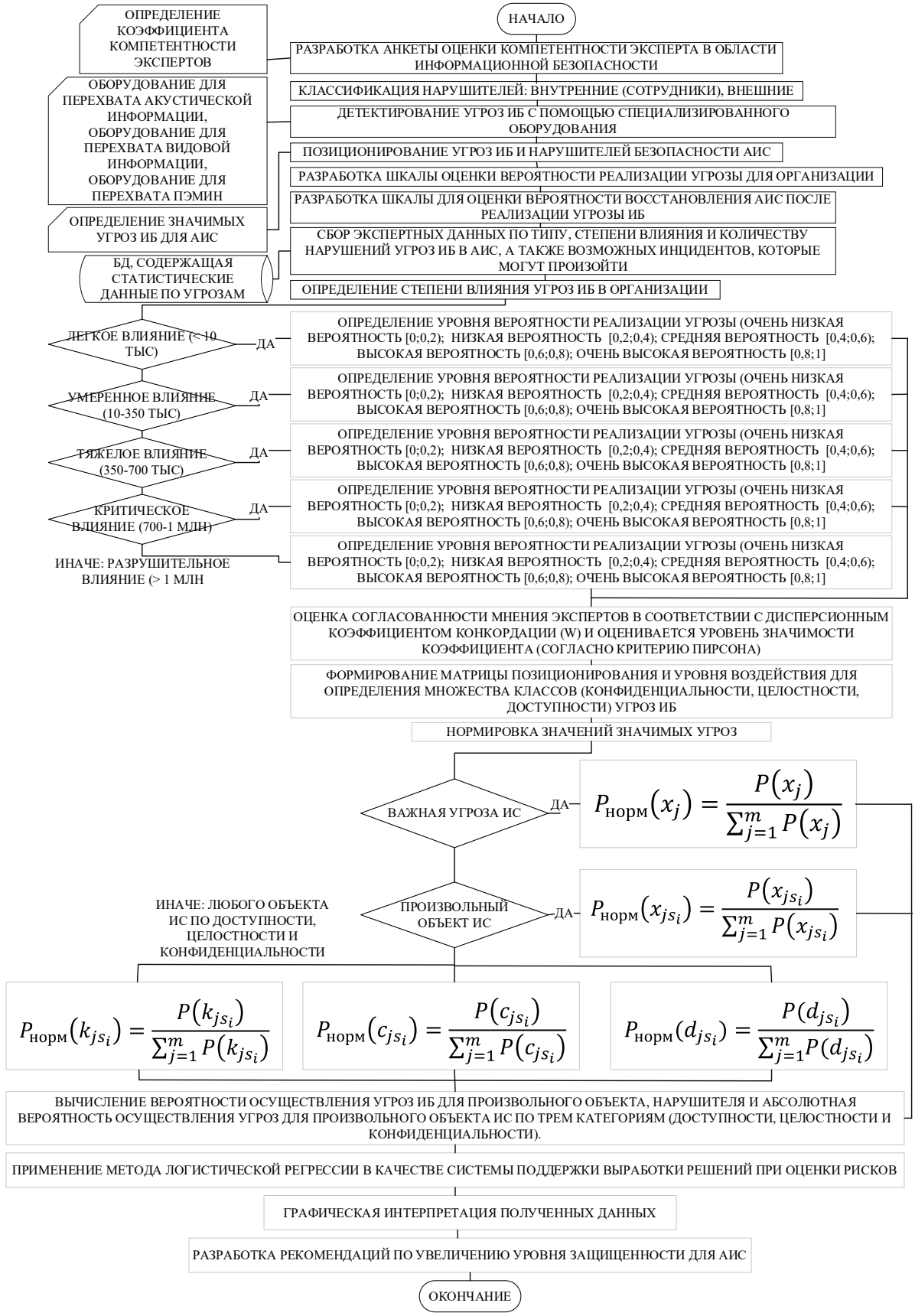

Рис. 5. Схема модели оценки рисков информационной безопасности в коммерческом банке
Fig. 5. Diagram of the information security risk assessment model in a commercial bank

С целью оценивания количества случаев нарушения ИБ коммерческого банка, была сформирована группа экспертов, проведена проверка согласованности их мнения, осуществлен сбор экспертных данных по типу, степени влияния угроз ИБ в АИС на основе разработанных шкал оценки, полученные результаты были занесены в разработанную базу данных, выполнено вычисление вероятности осуществления угроз ИБ, использованием метода логистической регрессии реализована проверка качества данных.

На рис. 6–11 представлены рассчитанные с использованием разработанной модели вероятности реализации и восстановления после реализации выделенного набора угроз информационной безопасности для компонент АИС коммерческого банка.

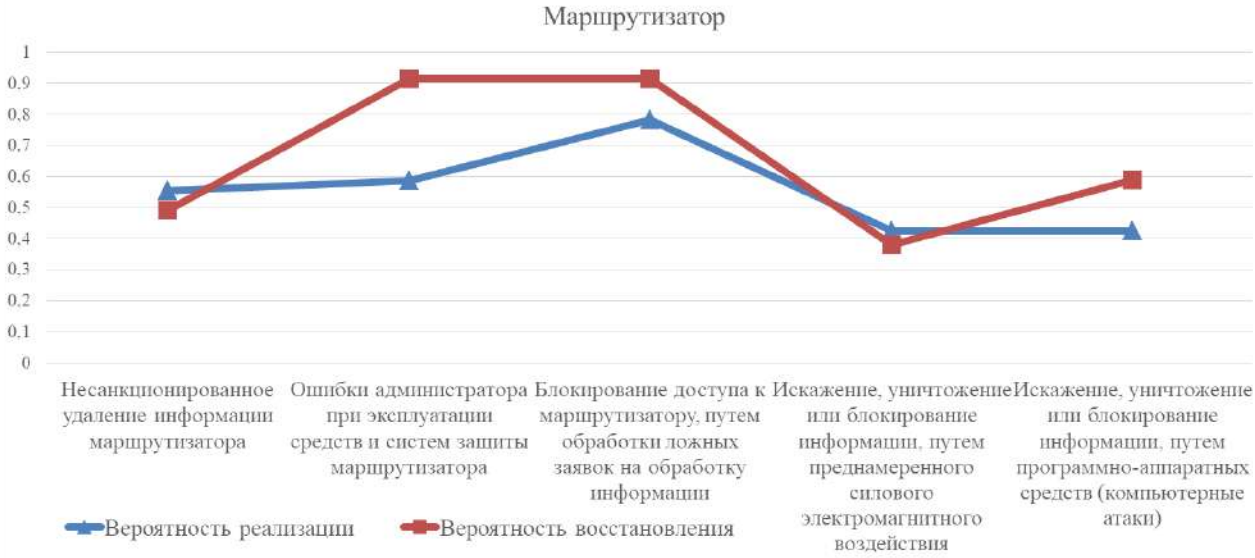

Рис. 6. Вероятности реализации и восстановления после реализации набора угроз для маршрутизатора

Fig. 6. Probabilities of implementation and recovery after a threat set to the router

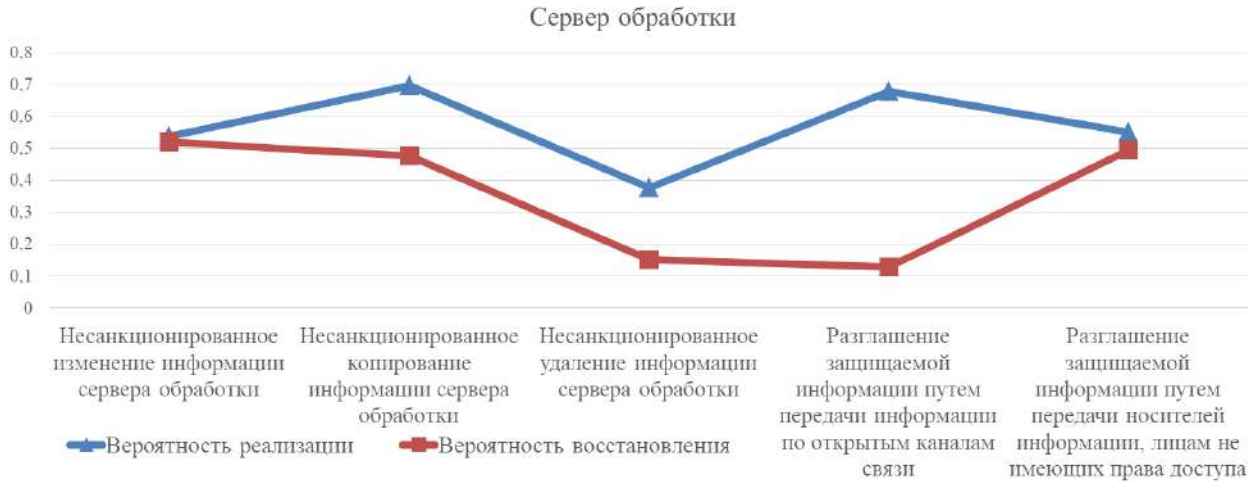

Рис. 7. Вероятности реализации и восстановления после реализации набора угроз для сервера обработки

Fig. 7. Probabilities of implementation and recovery after a threat set to the processing server

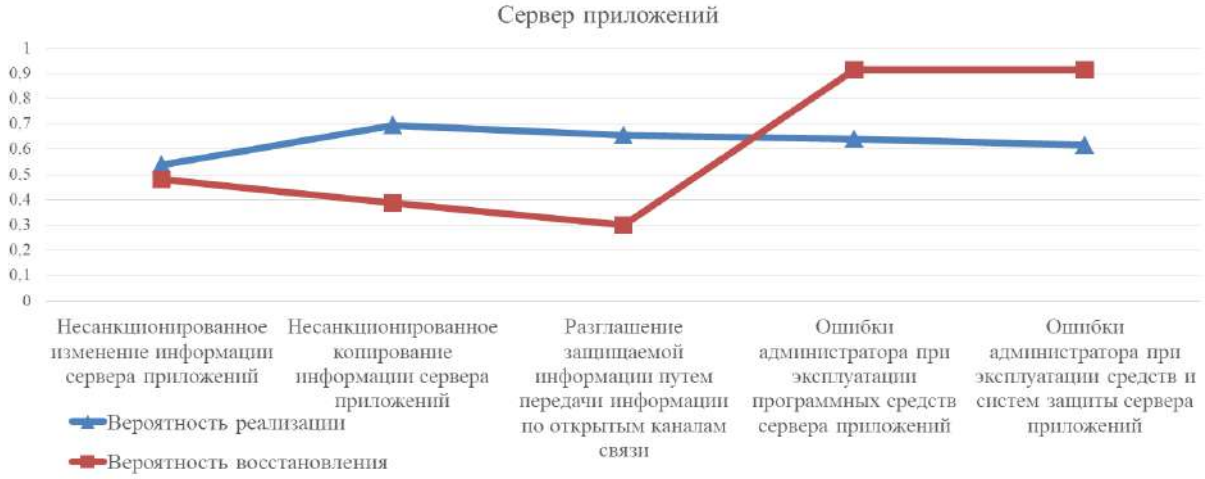

Рис. 8. Вероятности реализации и восстановления после реализации набора угроз для сервера приложений

Fig. 8. Probabilities of implementation and recovery after a threat set to the application server

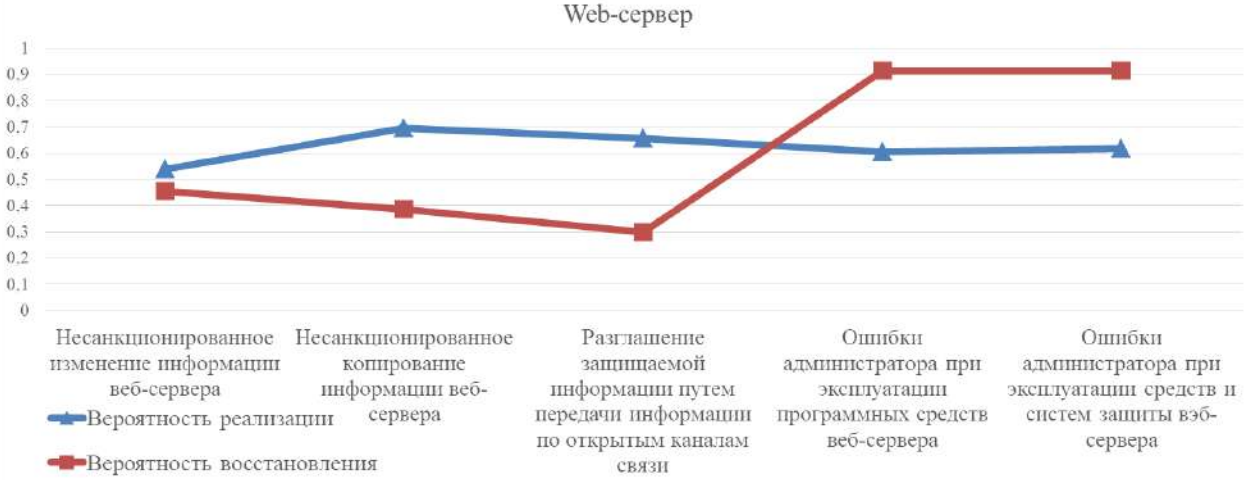

Рис. 9. Вероятности реализации и восстановления после реализации набора угроз для веб-сервера

Fig. 9. Probabilities of implementation and recovery after a threat set to the web server

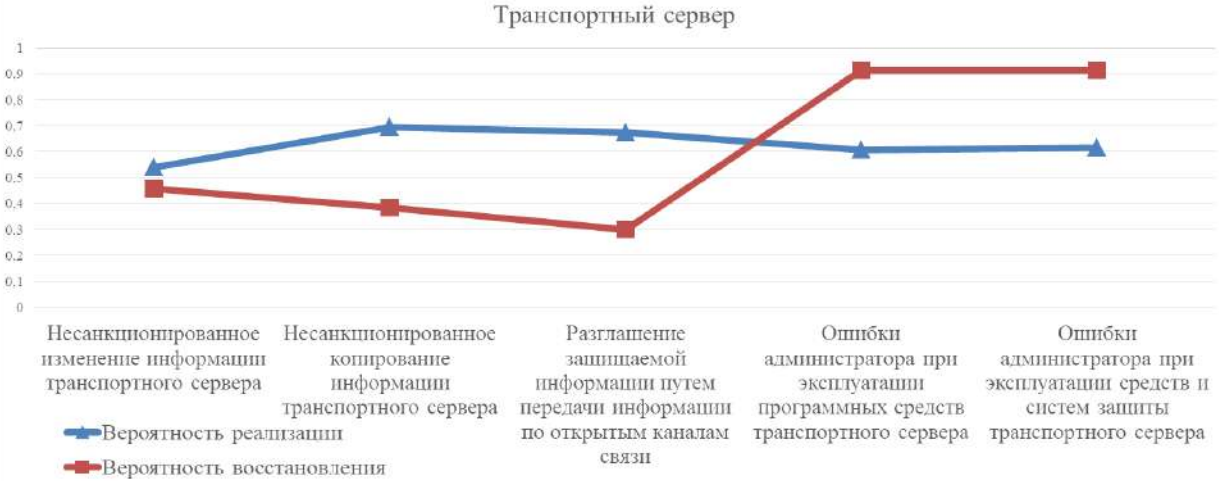

Рис. 10. Вероятности реализации и восстановления после реализации набора угроз для транспортного сервера

Fig. 10. Probabilities of implementation and recovery after a threat set to the transport server

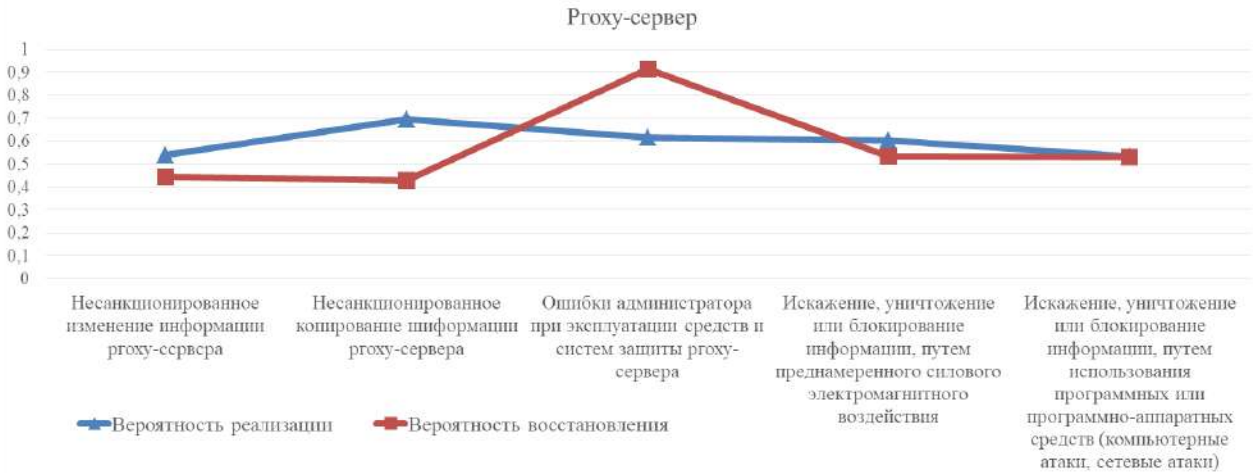

Рис. 11. Вероятности реализации и восстановления реализации набора угроз для Proxy-сервера
Fig. 11. Probabilities of implementation and recovery after a threat set to the Proxy server

Заключение

Решение задач повышения надежности средств защиты информации автоматизированной информационной системы коммерческого банка является комплексной проблемой, требующей своевременного и оперативного решения особенно в условиях увеличивающегося объема обрабатываемой информации и возрастающего количества атак злоумышленников на кредитные организации.

В данной статье выполнен анализ действующих стандартов в сфере информационной безопасности. Результаты проведенного анализа показывают, что большая часть стандартов регламентируют требования безопасности, не включая количественного подхода к оценке рисков. Выполнено моделирование бизнес-процессов комплексной оценки рисков в организации, разработана схема деятельности по обеспечению информационной безопасности и оценке рисков. Разработана архитектура системы информационной безопасности коммерческого банка с учетом структуры комплекса программно-технических средств.

С использованием методов экспертных оценок, статистического анализа данных, инструментальных средств создания баз данных разработана комплексная методика оценки рисков информационной безопасности в коммерческом банке. Разработан алгоритм вычисления вероятностей восстановления информационной системы после реализации набора угроз информационной безопасности, принимая во внимание факторы и уровни значимости и важности реализации угроз с учетом технических и эксплуатационных характеристик компонентов автоматизированной информационной системы.

Результаты тестирования комплексной модели оценки рисков информационной безопасности свидетельствуют об устойчивости получаемых значений вероятностей с точки зрения надежности функционирования информационной инфраструктуры коммерческого банка. Полученные вероятности позволят скорректировать политики информационной безопасности и повысить защищенность информационной системы за счет принятия системы мер, направленных на совершенствование комплекса программно-технических средств, а также информационных сервисов предприятия.

Предлагаемая методика может быть использована для оценки рисков информационной безопасности на предприятиях и в организациях различных сфер деятельности, ориентированных на финансово-банковский сектор.

СПИСОК ЛИТЕРАТУРЫ:

1. Ерохин С.С. Методика аудита информационной безопасности объектов электронной коммерции. Автореферат диссертации на соискание ученой степени кандидата технических наук. Томск. 2010. URL: https://www.elibrary.ru/item.asp?id=19323991 (дата обращения: 14.04.2021).
2. Балашев Н.Б., Ушаков А.И. Динамика формирования кредитной системы РФ // Научно-методический электронный журнал «Концепт». 2020. № 04 (апрель). С. 113–124. URL: http://e-koncept.ru/2020/203007.htm. DOI: https://doi.org/10.24411/2304-120X-2020-13007 (дата обращения: 14.04.2021).
3. Leonova N.M., Modyaev A.D., Kolychev V.D. Visualization of a product's life cycles in the common information space on the basis of project management methods. Scientific Visualization, 2016, 8(5). С. 26–40. URL: http://sv-journal.org/2016-5/03/en/index.php?lang=ru (дата обращения: 14.04.2021).
4. Kulik S.D. Model for evaluating the effectiveness of search operations. Journal of ICT Research and Applications. Vol. 9, Issue 2, 2015. P. 177–196. DOI: https://doi.org/10.5614/itbj.ict.res.appl.2015.9.2.5.
5. Miloslavskaya N., Furnell S. (2021) Network Security Intelligence Centres for Information Security Incident Management. In: Samsonovich A.V., Gudwin R.R., Simões A.S. (eds) Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol 1310. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-65596-9_34.
6. Miloslavskaya N., Tolstaya S. (2020) On the Assessment of Compliance with the Requirements of Regulatory Documents to Ensure Information Security. In: Rocha Á., Adeli H., Reis L., Costanzo S., Orovic I., Moreira F. (eds) Trends and Innovations in Information Systems and Technologies. WorldCIST 2020. Advances in Intelligent Systems and Computing, vol 1160. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-45691-7_74.
7. Нестерова Д.А. Риски информационной безопасности коммерческих банков в условиях новой экономической и технологической реальности. Инновации и инвестиции, 2020, № 5. С. 144–150. URL: https://www.elibrary.ru/item.asp?id=43066036 (дата обращения: 14.04.2021).
8. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга. Вопросы кибербезопасности №1(25), 2018. С. 28–38. DOI: https://doi.org/10.21681/2311-3456-2018-1-28-38.
9. Melnikov D.A., Durakovsky A.P., Dvoryankin S.V. and Gorbatov V.S. Concept for Increasing Security of National Information Technology Infrastructure and Private Clouds. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
10. Korsakov I.A., Durakovskiy A.P. (2020) About the Security Assessment of Embedded Software in Automated Process Control System. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_46.
11. Будзко В.И., Ядринцев В.В., Соченков И.В., Королёв В.И., Беленков В.Г. Формирование в системах интенсивного использования данных маркеров конфиденциальности в условиях высокой неопределенности при их использовании. В сборнике: Информационные технологии и математическое моделирование систем 2020. Труды международной научно-технической конференции. 2020. С. 81–89. DOI: https://doi.org/10.36581/CITP.2020.11.36.020.
12. Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security, 2017, vol. 65. P. 77–89. DOI: https://doi.org/10.1016/j.cose.2016.10.009.
13. Попов Г.А., Попов А.Г. Результирующая оценка при наличии нескольких вариантов оценивания на примере задач информационной безопасности. Вестник астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. № 1. С. 48–61. URL: https://www.elibrary.ru/item.asp?id=28147036 (дата обращения: 14.04.2021).

REFERENCES:

[1] Erokhin S.S. Methodology of audit of information security of electronic commerce objects. Abstract of the dissertation for the degree of Candidate of Technical Sciences. Tomsk. 2010. URL: https://www.elibrary.ru/item.asp?id=19323991 (accessed: 14.04.2021) (in Russian).
[2] Balashev N.B., Ushakov A.I. Dynamics of the credit system formation in the Russian Federation. Saentific and methodological electronic journal “Koncept”, 2020. No. 04. P. 113–124. URL: http://e-koncept.ru/2020/203007.htm. DOI: https://doi.org/10.24411/2304-120X-2020-13007 (accessed: 14.04.2021) (in Russian).

[3] Leonova N.M., Modyaev A.D., Kolychev V.D. Visualization of a product's life cycles in the common information space on the basis of project management methods. Scientific Visualization, 2016, 8(5). P. 26–40. (in Russian).
[4] Kulik S.D. Model for evaluating the effectiveness of search operations. Journal of ICT Research and Applications. Vol. 9, Issue 2, 2015. P. 177–196. DOI: https://doi.org/10.5614/itbj.ict.res.appl.2015.9.2.5.
[5] Miloslavskaya N., Furnell S. (2021) Network Security Intelligence Centres for Information Security Incident Management. In: Samsonovich A.V., Gudwin R.R., Simões A.S. (eds) Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol 1310. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-65596-9_34.
[6] Miloslavskaya N., Tolstaya S. (2020) On the Assessment of Compliance with the Requirements of Regulatory Documents to Ensure Information Security. In: Rocha Á., Adeli H., Reis L., Costanzo S., Orovic I., Moreira F. (eds) Trends and Innovations in Information Systems and Technologies. WorldCIST 2020. Advances in Intelligent Systems and Computing, vol 1160. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-45691-7_74.
[7] Nesterova D.A. Risks of information security of commercial banks in the new economic and technological reality. Innovation and investment, 2020, no. 5, P. 144–150. URL: https://www.elibrary.ru/item.asp?id=43066036 (accessed: 14.04.2021) (in Russian).
[8] Berdyugin A.A. Risk management of information security violation in conditions of electronic banking. Voprosy Kiberbezopasnosti, No 1(25) – 2018. P. 28-38. DOI: https://doi.org/10.21681/2311-3456-2018-1-28-38 (in Russian).
[9] Melnikov D.A., Durakovsky A.P., Dvoryankin S.V. and Gorbatov V.S. Concept for Increasing Security of National Information Technology Infrastructure and Private Clouds 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
[10] Korsakov I.A., Durakovskiy A.P. (2020) About the Security Assessment of Embedded Software in Automated Process Control System. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_46.
[11] Budzko V.I., Yadrentsev V.V., Sochenkov I.V., Korolev V.I., Belenkov V.G. Formation of privacy markers in systems of intensive use of data under conditions of high uncertainty when using them. In the collection: Information Technologies and mathematical modeling of systems 2020. Proceedings of the International Scientific and Technical Conference. 2020. P. 81–89. DOI: https://doi.org/10.36581/CITP.2020.11.36.020 (in Russian).
[12] Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security, 2017, vol. 65. P. 77–89. DOI: https://doi.org/10.1016/j.cose.2016.10.009.
[13] Popov G.A., Popov A.G. The final grade if there are several evaluation options using the example of information security problems. Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Computer Science. 2017. No. 1. P. 48–61. URL: https://www.elibrary.ru/item.asp?id=28147036 (accessed: 14.04.2021).

Поступила в редакцию – 24 февраля 2021 г. Окончательный вариант – 29 апреля 2021 г.
Received – February 24, 2021. The final version – April 29, 2021.

Максим О. Таныгин[1], Юлия А. Будникова[2], Андрей С. Булгаков[3], Михаил А. Марченко[4]
[1,2]Юго-Западный государственный университет,
ул. 50 лет октября, 94, Курск, 305040, Россия
[3,4]Национальный исследовательский университет «Московский институт электронной техники»,
площадь Шокина, 1, Зеленоград, Москва, 124498, Россия,
[1]e-mail: tanygin@yandex.com, https://orcid.org/0000-0002-4099-1414
[2]e-mail: juli-budni19ok@mail.ru, https://orcid.org/0000-0002-1010-5709
[3]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[4]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

МОДЕЛЬ ОЦЕНКИ УЩЕРБА ОТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.2.09

Аннотация. Любая информационная система в процессе эксплуатации требует резервирования определённого объёма средств на ликвидацию последствий инцидентов информационной безопасности в случае их возникновения. Для оценки величины ущерба использовались многомодальные законы распределения плотностей вероятностей ущерба в единичном инциденте информационной безопасности, а инциденты информационной безопасности рассматриваются как события пуассоновского потока. В работе определены зависимости между интенсивностью возникновения событий информационной безопасности, характеристиками распределения плотностей вероятностей ущерба и необходимой величиной резервируемых средств. Представленная модель оценки ущерба от инцидентов информационной безопасности позволяет более точно подходить к оценке требуемого объем резервируемых средств. Показано, что экономия средств достигает 40-50% в сравнении с подходом, основанным на оценке ущерба исходя только из среднего числа инцидентов и среднего ущерба от единичного инцидента информационной безопасности.

Ключевые слова: инциденты информационной безопасности, угрозы информационной безопасности, плотность вероятности распределения ущерба, оценка величины ущерба, ликвидация последствий инцидентов информационной безопасности.

Для цитирования: ТАНЫГИН, Максим О. и др. МОДЕЛЬ ОЦЕНКИ УЩЕРБА ОТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 98–106, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1347>. Дата доступа: 13 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

Maxim O. Tanygin[1], Yulia A. Budnikova[2], Andrey S. Bulgakov[3], Mikhail A. Marchenko[4]
[1,2]South-West State University,
50 Let Oktyabrya str., 94, Kursk, 305040, Russia
[3,4]National Research University of Electronic Technology,
Shokin Square, 1, Zelenograd, Moscow, 124498, Russia
[1]e-mail: tanygin@yandex.com, https://orcid.org/0000-0002-4099-1414
[2]e-mail: juli-budni19ok@mail.ru, https://orcid.org/0000-0002-1010-5709
[3]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[4]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

A model for assessing information security incidents damage

DOI: http://dx.doi.org/10.26583/bit.2021.2.09

Abstract. Any information system requires the funds reservation for the elimination of the consequences of information security incidents in the event of their occurrence. To estimate the amount of damage, we used multi-modal probability densities distribution laws for the damage in a single information security incident, while the information security incidents are considered as Poisson flow events. The paper defines the relationships between the intensity of information security events, the characteristics of the

distribution of probability densities of damage, and the required amount of reserved funds. The presented model of damage assessment from information security incidents allows a more accurate approach for estimation of the required amount of reserved funds. It is shown that the cost saving reaches 40-50% in comparison with the damage assessment approach using only on the average number of incidents and the average damage from a single incident of information security.
Keywords: information security incidents, information security threats, probability density of damage distribution, damage assessment, elimination of consequences of information security incidents.
For citation: TANYGIN, Maxim O. et al. A model for assessing information security incidents damage. IT Security (Russia), [S.l.], v. 28, n. 2, p. 98–106, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1347>. Date accessed: 13 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

Введение

Инциденты информационной безопасности (ИИБ), происходящие в информационной системе, требуют от владельца информационной системы (ИС) затрат на ликвидацию их последствий. Это могут быть затраты на закупку вышедшего из строя оборудования, оплату труда специалистов, ликвидирующих последствия инцидентов, компенсация расходов, связанных с потерей системой работоспособности и прочее [1, 2]. Ущерб, понесенный владельцем, можно всегда оценить в денежном эквиваленте. Организация должна зарезервировать некоторый объём денежных средств, которые расходуются в случае реализации угрозы информационной безопасности [3, 4]. При этом способ резервирования этих средств должен позволять использовать их непосредственно после возникновения ИИБ [5, 6], что подразумевает снижение их стоимости в результате инфляции. Таким образом, перед владельцем ИС стоит задача, с одной стороны, обеспечения возможности компенсации затрат на ликвидацию последствий ИИБ, а с другой стороны – минимизировать объём средств, задепонированных с этой целью [7]. Величина ущерба, понесённого владельцем ИС в результате ИИБ, является случайной величиной, а наступление самого ИИБ – случайное событие. Для определения целесообразного объёма резервируемых средств необходимо выполнить оценку вероятности ущерба, исходя из истории ИИБ.

1. Модель оценки ущерба

При оценке величины ущерба от единичного ИИБ важной характеристикой является плотность распределения вероятности ущерба $p(U)$, где U – величина ущерба от инцидента информационной безопасности, выраженная в некоторых условных единицах (рублях, человеко-часах и пр.). Статистика ИИБ и аналитические материалы позволяет утверждать, что нормальный закон распределения ущерба не подходит для описания функции $p(U)$ из-за того, что частота возникновения инцидентов, ущерб от которых неформально можно классифицировать как «незначительный», «средний», «значительный» отличается несущественно [8]. Поэтому нельзя пренебречь вкладом ни одной из указанных категорий ИИБ в общий размер ущерба. И при этом величина ущерба, которая позволяет отнести ИИБ к категории «значительный», может на порядки превышать величину ущерба, классифицируемого как «незначительный» [9]. Таким образом, функция распределения $p(U)$ имеет так называемый «тяжелый конец» (англ. – heavy-tailed distribution) [10].

Использованное для моделирования ущерба логнормальное распределение [11] также является одномодальным, что не позволяет адекватно моделировать ущерб. Причиной этого является то, что объектами угроз являются конкретные компоненты информационных систем. Ущерб, нанесенный в результате таких угроз, обычно лежит в

узком диапазоне, число же таких компонент, подверженных атакам в реальных системах, невелико [12]. Такая особенность обуславливает применение многомодальных распределений плотностей вероятностей ущерба [13].

Модель оценки ущерба предполагает представление функции распределения ущерба в единичном ИИБ, рассматриваемом исходя из двух неравновероятных нормальных распределений $p_1(U)$ (условно, инциденты с малым ущербом) и $p_2(U)$ (инциденты с большим ущербом) с различными математическими ожиданиями ущерба μ_1 и μ_2 ($\mu_1 < \mu_2$) и дисперсиями σ_1 и σ_2 соответственно:

$$p^1(U) = k_1\, p_1(U) + k_2 \cdot p_2(U), \tag{1}$$

где k_1 и k_2 – веса двух распределений ($k_1 > k_2$). Они определялись исходя из параметра модели K – отношения весов двух распределений и условия нормировки:

$$K = k_1 / k_2,$$
$$\int_{-\infty}^{\infty} \left(k_1 p_1(U) + k_2 p_2(U)\right) dU = 1. \tag{2}$$

Соотношения между параметрами μ_1 и μ_2 рассматриваемой модели выбирались в диапазоне от 7 до 12, исходя из имеющихся данных по величине ущерба информационной безопасности от различных угроз [14, 15]. Значения среднеквадратических отклонений σ_i, i = 1,2 выбирались в диапазоне 0.3…0.7 μ_i. Следует отметить, что в рамках модели значения имели именно отношения между данными параметрами, а не их абсолютные значения, так как изначально единица измерения величины ущерба U выбирается, исходя из особенностей каждой моделируемой ИС.

Отдельно стоит рассмотреть интервал модельного времени. Для получения более точных результатов интервал должен быть таким, чтобы среднее число λ инцидентов в нем лежало в диапазоне от 0.5 до 4.0. В противном случае, при числе ИИБ большем 4, расчет ущерба, выполняемый, как будет показано в дельнейшем, путём многократного нахождения численными методами значений двойного интеграла на бесконечном интервале численных методов будет сопряжен с большим объемом вычислений. Помимо факториального роста времени расчёта, это даст значительную погрешность из-за накапливаемой в каждой итерации ошибки вычислений. Если число ИИБ в течение интервала времени, выбранного за единицу модельного времени, выходит из указанного диапазона, то для получения более точных оценок ущерба единицу модельного времени следует изменить. Например, если среднее число ИИБ в течение года будет слишком велико, то следует считать среднее число ИИБ в квартал и т.д. На практике это будет означать переход от годового планирования к поквартальному [16].

Так как число инцидентов информационной безопасности в интервале модельного времени является случайной величиной, необходимо определить функцию распределения $p^{(n)}(U)$ плотностей вероятностей ущерба от n инцидентов ИБ. Для нахождения $p^{(n)}(U)$ будем использовать рекуррентную формулу:

$$p^{(n)}(U) = \frac{\int_0^U p^{(n-1)}(U-u) \cdot p^1(u)\, du}{\int_0^\infty \int_0^\infty p^{n-1}(u_1) \cdot p^1(u_2)\, du_1 du_2}, \tag{3}$$

где знаменатель введен для выполнения условия: $\int_0^\infty p^{(n)}(U)dU = 1$, а в числителе подынтегральное выражение – это плотность распределения вероятности события, при котором величина от одного ИИБ равна u, а от оставшихся $(n-1)$ ИИБ – $(U-u)$.

2. Результаты моделирования

На рис. 1 в качестве примера приведены полученные для одного набора параметров $\{K, \mu_1, \mu_2, \sigma_1, \sigma_2\}$ зависимости плотностей вероятностей ущерба для одной, двух, трёх и четырех угроз ИИБ. Значения параметров выбраны таким образом, чтобы проиллюстрировать возникновение второго локального максимума, значительно отличающегося по высоте от первого, на графике плотности распределения вероятностей.

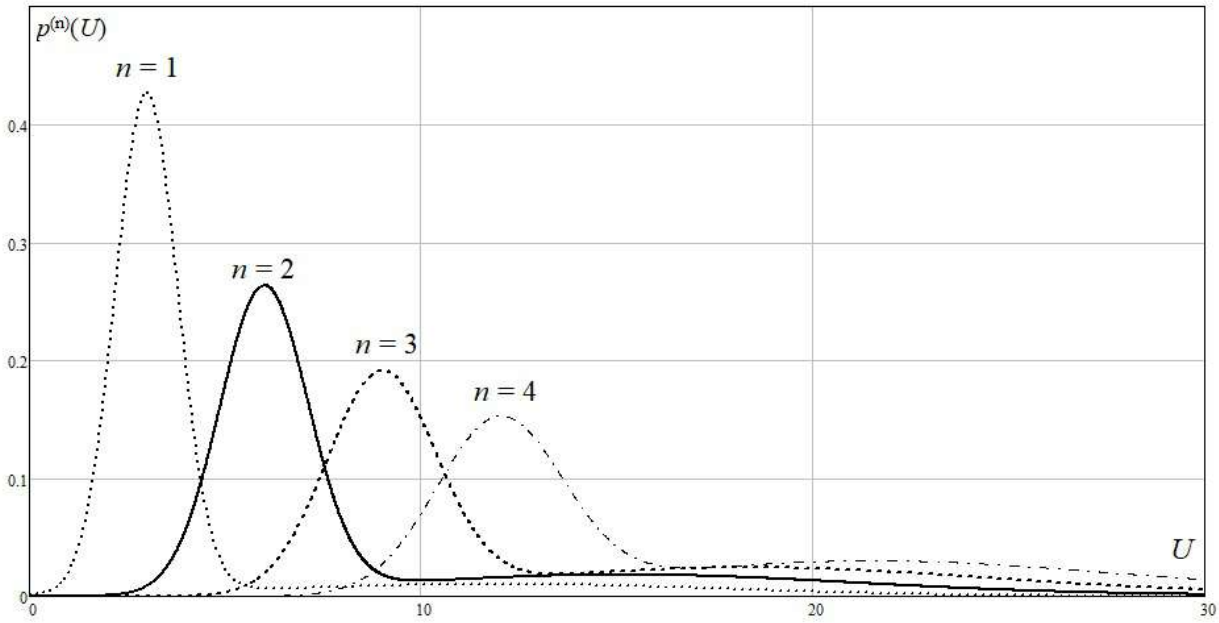

Рис. 1. Зависимость плотности вероятностей ущерба при K=6, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8 и числе инцидентов n

Fig. 1. The probability density distribution of damage at K=6, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, and number of incidents n

Влияние каждого из параметров математической модели на характер зависимости различно. С увеличением соотношения между весами распределения второй локальный максимум в правой части графиков становится менее значительным, рост отношения μ_2/μ_1 сдвигает позицию второго локального максимума вправо, делая сам максимум более заметным на фоне значений, даваемых распределением $p_1(U)$. Увеличение дисперсии σ_1 делает второй максимум, наоборот, менее заметным в правой части графика. С ростом числа n инцидентов информационной безопасности (при n=5, 6 …) влияние так называемого «тяжелого конца» в функции распределения плотностей вероятности ущерба от единичного инцидента растет. Форма кривой $p^{(n)}(U)$ становится более пологой, первый локальный максимум в окрестности $U = n \cdot \mu_1$ становится менее значительным, значение плотности вероятностей в окрестности второго локального максимума ($U = n \cdot \mu_2$) растет, как и растёт значение плотности вероятностей между максимумами (при $n \to \infty$ график выродится в одномодальный график с математически ожиданием $k_1 \cdot \mu_1 + k_2 \cdot \mu_2$).

Результирующая плотность вероятности распределения ущерба определяется по формуле:

$$p(U) = \sum_{i=1}^{\infty} p_{sl}(i) \cdot p^{(i)}(U), \quad (4)$$

где $p_{sl}(i)$ – вероятность возникновения i инцидентов информационной безопасности в течение интервала модельного времени.

Если исходить из предположения, что инциденты информационной безопасности порождаются множеством независимых субъектов, активность которых не зависит друг от друга, то для нахождения вероятности числа инцидентов будем использовать распределение Пуассона с интенсивностью λ [15] равной среднему наблюдаемому числу инцидентов информационной безопасности в течение исследуемого интервала:

$$p_{sl}(i) = \frac{\lambda^i}{i!} e^{-\lambda}, \quad (5)$$

График плотности вероятности ущерба при разных значениях интенсивностей приведен на рис. 2.

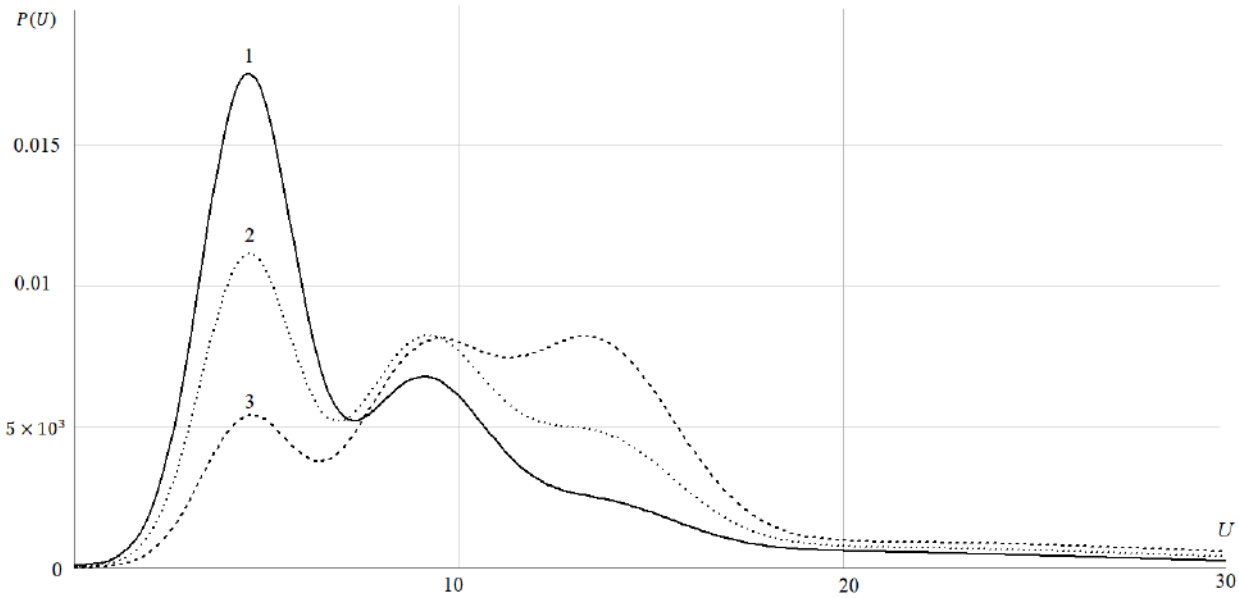

Рис. 2. Графики плотности распределения вероятностей ущерба при K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8: 1) λ = 1.0;2) λ = 2.0;3) λ = 4.0

Fig. 2. Graphs of the probability distribution density of damage at K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8: 1) λ = 1.0;2) λ = 2.0;3) λ = 4.0

Из формы графиков видно, что, увеличение интесивности возникновения инцидентов смещает вправо области наиболее вероятных значений, делая более заметным влияние «тяжелого конца» исходного распределения (1). При этом, в исследуемых диапазонах изменения параметра λ наблюдается незначительный рост функции распределения вероятностей при $U > 10 \cdot \mu_2$ (значения функции плотности ущерба близко к нулю). Последний факт создает предпосылки к игнорированию таких ситуаций с высоким суммарным ущербом от ИИБ как маловероятных [17, 18].

3. Прогнозирование величины затрат на устранение последствий инцидентов информационной безопасности

Так как начальная задача исследования формулировалась как определение величины необходимых депонируемых средств для нейтрализации угроз, а размер максимального ущерба неограничен, то необходимо ввести параметр D – доля угроз, на нейтрализацию которых задепонированных средств будет достаточно [19]. Эта доля определится как значение функции распределения вероятностей ущерба $p(U)$ (см. формулу (4)) при $U = U^{\max}$:

$$D = \int_0^{U^{\max}} \left[\sum_{i=1}^{\infty} p_{sl}(i) \cdot p^{(i)}(U) \right] dU, \qquad (6)$$

где $U^{\max}$ – величина ущерба, которую с вероятностью D не превысит суммарный ущерб от всех ИИБ в течение единицы модельного времени. На основании зависимости (6) определяется $U^{\max}$ как функция всех описанных выше параметров модели, а также параметра D.

График зависимости размера резервируемых средств от интенсивности возникновения ИИБ приведен на рис. 3, линии 1 и 2.

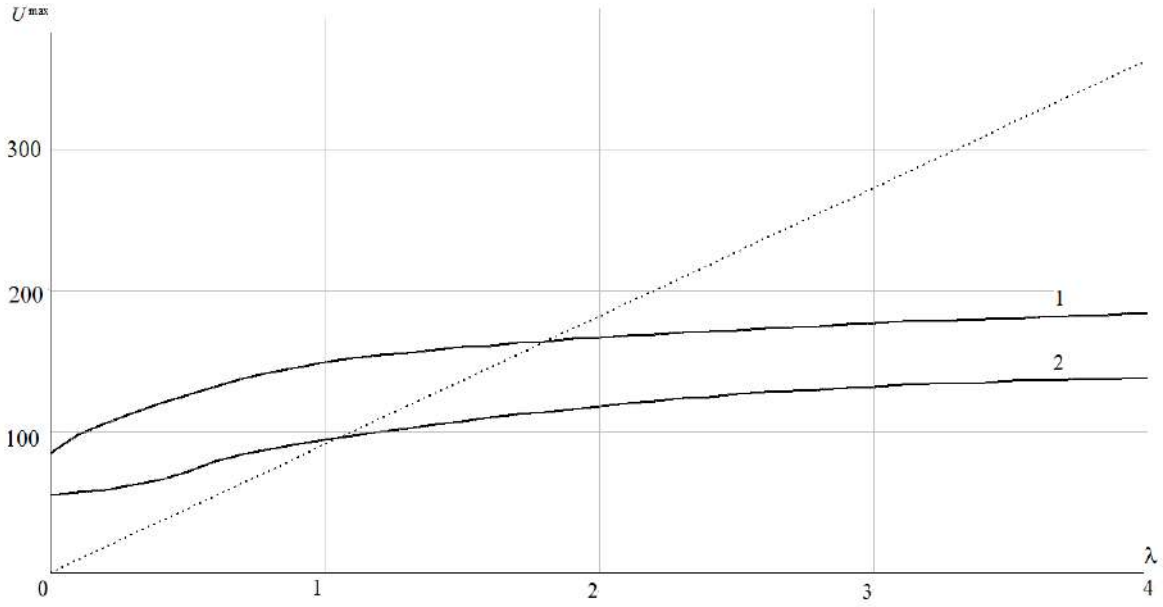

Рис. 3. График зависимости размера резервируемых средств U^{max} от интенсивности возникновения инцидентов λ
1) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.9;
2) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.7
Fig. 3. Graph of the reserved funds amount U^{max} dependence on the incidents occurrence intensity λ
1) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.9;
2) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.7

В качестве эталона была взята модель определения величины ущерба как произведение среднего ущерба от единичного ИИБ на среднее число таких же λ инцидентов с аналогичной долей D от полученного значения величины депонированных средств (зависимость показана пунктирной линией на рис. 3). Сравнение эталонных значений необходимого объёма депонированных средств $U^{\max}$ и значений, полученных на рассматриваемой в статье модели, показало, что последняя даёт более точную оценку

величины ущерба за счёт учёта вероятности возникновения ИИБ с высоким ущербом. Это позволяет резервировать на 40–50% меньше средств при больших ($\lambda>3$) значениях среднего числа ИИБ в выбранную единицу времени по сравнению с простым анализом средних значений ущерба (правая часть графиков). При небольшой же интенсивности инцидентов разработанная модель дает больший объем резервируемых средств, что позволяет ликвидировать последствия ИИБ в более полном объеме.

Заключение

Предложенная в настоящей статье математическая модель прогнозирования затрат на устранения последствий ИИБ основывается на представлении плотности распределения вероятностей ущерба от единичного инцидента в виде многомодального распределения. Исходя из рассчитанной величины ущерба от нескольких ИИБ, получены численные зависимости требуемого объема средств от среднего числа ИИБ в единицу модельного времени. В практическом плане это позволит, основываясь на истории понесенных затрат, более точно прогнозировать объём резервируемых на ликвидацию последствий ИИБ средств и оценивать максимальные затраты на внедрение и обслуживание дополнительных подсистем обеспечения ИБ.

Кроме того, получена зависимость требуемого объема средств от планируемой доли инцидентов, последствия которых удастся компенсировать или ликвидировать. Рассмотренная модель позволяет снизить размер депонируемых средств в некоторых случаях на 40–50% по сравнению с моделями, основанными исключительно на математических ожиданиях ущерба и числа инцидентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Hui P. Construction of Information Security Risk Assessment Model in Smart City / 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2020. P. 393–396. DOI: http://dx.doi.org/10.1109/TOCS50858.2020.9339614.
2. Белов В.М., Пестунов А.И., Пестунова Т.М. Методика оценки рисков информационной безопасности бизнес-процессов // ОмГТУ. 2016. №1. С. 158–161. URL: https://www.elibrary.ru/item.asp?id=27410988 (дата обращения: 01.03.2021).
3. Xiaoqian Wu, Yongjun Shen, Guidong Zhang, & Hua Zhi. Information security risk assessment based on D-S evidence theory and improved TOPSIS. 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2016. P. 153–156. DOI: http://dx.doi.org/10.1109/icsess.2016.7883037.
4. Станиславчик Е.Н. Риск-менеджмент на предприятии. Теория и практика. М.: «Ось-89». 2002. – 80 с.
5. Wangen, G. An initial insight into information security risk assessment practices / Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. 2016. Vol. 8. P. 999–1008. DOI: http://dx.doi.org/10.15439/2016F158.
6. Luo H., Shen Y., Zhang G., & Huang L. Information security risk assessment based on two stages decision model with grey synthetic measure. 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing, China, 2015. P. 795–798. DOI: http://dx.doi.org/10.1109/icsess.2015.7339176.
7. Репин М.М., Сакулина А.В., Пшехотская Е.А. Построение модели оценки экономической эффективности системы информационной безопасности // Научно-методическое обеспечение оценки качества образования. 2017. №2 (3). С. 80–84. URL: https://cyberleninka.ru/article/n/postroenie-modeli-otsenki-ekonomicheskoy-effektivnosti-sistemy-informatsionnoy-bezopasnosti (дата обращения: 01.03.2021).
8. Голубинский А.Н., Алехин И.В. Анализ распределений ущербов при реализации угроз в информационно-технических системах // Вестник ВИ МВД России. 2016. №3. С. 24–32. URL: https://www.elibrary.ru/item.asp?id=26683939 (дата обращения: 01.03.2021).
9. Andress Jason, Leary Mark. Building a Practical Information Security Program // Syngress. 2017. – 192 p.
10. Klebanov L. Heavy Tailed Distributions. Matfyzpress, Prague, 2003. – 176 p. ISBN: 80-86732-02-9.

11. Казакова А.В. Модель угроз информационной безопасности промышленных предприятий // Проблемы совершенствования организации производства и управления промышленными предприятиями: Межвузовский сборник научных трудов. 2011. № 1. С. 88–96. URL: https://www.elibrary.ru/item.asp?id=20405652 (дата обращения: 01.03.2021).
12. Wangen G. (2019) Quantifying and Analyzing Information Security Risk from Incident Data. In: Albanese M., Horne R., Probst C. (eds) Graphical Models for Security. GraMSec 2019. Lecture Notes in Computer Science, Vol. 11720. Springer, Cham. P. 129–154. DOI: http://dx.doi.org/10.1007/978-3-030-36537-0_7.
13. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука. 2001. – 295 с.
14. Peter H. Gregory Risk assessment in audit planning / Peter H. Gregory. 2018. – 46 p.
15. Peter H. Gregory CISM Certified Information Security Manager All-in-One Exam Guide» // Peter H. Gregory. 2018. – 1104 p.
16. Репин М.М. Пшехотская Е.А. Методика расчета показателя эффективности противодействия информационным угрозам в платёжной системе // Научно-методический журнал «Научно-методическое обеспечение оценки качества образования» – ГБУ ДПО РЦОКИО. 2018. №2(5). С. 141–148. URL: https://cyberleninka.ru/article/n/metodika-rascheta-pokazatelya-effektivnosti-protivodeystviya-informatsionnym-ugrozam-v-platezhnoy-sisteme (дата обращения: 01.03.2021).
17. Арсеньев В.Н., Силантьев С.Б., Ядренкин А.А. Использование априорной информации для коррекции модели потока событий в сложной системе // Изв. ВУЗов. Приборостроение. 2017. Т. 60. № 5. С. 391–397. DOI: http://dx.doi.org/10.17586/0021-3454-2017-60-5-391-397.
18. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие. СПб: Университет ИТМО. 2015. – 93 с.
19. Пугин В.В. Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // T-Comm – Телекоммуникации и Транспорт. 2012. Т. 6, № 6. С. 54–57. URL: https://www.elibrary.ru/item.asp?id=18848583 (дата обращения: 01.03.2021).

REFERENCES:

[1] Hui P. Construction of Information Security Risk Assessment Model in Smart City. 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2020. P. 393–396. DOI: http://dx.doi.org/10.1109/TOCS50858.2020.9339614.
[2] Belov V.M., Pestunov A.I., Pestunova T.M. Metodika ocenki riskov informacionnoj bezopasnosti biznes-processov. OmGTU. 2016. №1. P. 158–161. URL: https://www.elibrary.ru/item.asp?id=27410988 (accessed: 01.03.2021) (in Russian).
[3] Xiaoqian Wu, Yongjun Shen, Guidong Zhang, & Hua Zhi. Information security risk assessment based on D-S evidence theory and improved TOPSIS. 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2016. P. 153–156. DOI: http://dx.doi.org/10.1109/icsess.2016.7883037.
[4] Stanislavchik E.N. Risk-menedzhment na predpriyatii. Teoriya i praktika. M.: «Os'-89». 2002. – 80 p. (in Russian).
[5] Wangen, G. An initial insight into information security risk assessment practices. Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. 2016. Vol. 8. P. 999–1008. DOI: http://dx.doi.org/10.15439/2016F158.
[6] Luo H., Shen Y., Zhang G., & Huang, L. Information security risk assessment based on two stages decision model with grey synthetic measure. 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing, China, 2015. P. 795–798. DOI: http://dx.doi.org/10.1109/icsess.2015.7339176.
[7] Repin M.M., Sakulina A.V., Pshekhotskaya E.A. Postroenie modeli ocenki ekonomicheskoj effektivnosti sistemy informacionnoj bezopasnosti. Nauchno-metodicheskoe obespechenie ocenki kachestva obrazovaniya. 2017. №2 (3). S. 80–84. URL: https://cyberleninka.ru/article/n/postroenie-modeli-otsenki-ekonomicheskoy-effektivnosti-sistemy-informatsionnoy-bezopasnosti (accessed: 01.03.2021) (in Russian).
[8] Golubinskij A.N., Alekhin I.V. Analiz raspredelenij ushcherbov pri realizacii ugroz v informacionno-tekhnicheskih sistemah. Vestnik Voronezhskogo instituta MVD Rossii, 2016. no. 3. S. 24–32. URL: https://www.elibrary.ru/item.asp?id=26683939 (accessed: 01.03.2021) (in Russian).
[9] Andress Jason, Leary Mark. Building a Practical Information Security Program. 2017. – 192 p.
[10] Klebanov L. Heavy Tailed Distributions. Matfyzpress, Prague, 2003. – 176 p. ISBN: 80-86732-02-9.

[11] Kazakova A.V. Model' ugroz informacionnoj bezopasnosti promyshlennyh predpriyatij. Problemy sovershenstvovaniya organizacii proizvodstva i upravleniya promyshlennymi predpriyatiyami: Mezhvuzovskij sbornik nauchnyh trudov, 2011. no. 1. S. 88–96. URL: https://www.elibrary.ru/item.asp?id=20405652 (accessed: 01.03.2021) (in Russian).

[12] Wangen G. (2019) Quantifying and Analyzing Information Security Risk from Incident Data. In: Albanese M., Horne R., Probst C. (eds) Graphical Models for Security. GraMSec 2019. Lecture Notes in Computer Science, Vol. 11720. Springer, Cham. P. 129–154 DOI: http://dx.doi.org/10.1007/978-3-030-36537-0_7.

[13] Vadzinskij R.N. Spravochnik po veroyatnostnym raspredeleniyam. SPb.: Nauka. 2001. – 295 s. (in Russian).

[14] Peter H. Gregory Risk assessment in audit planning. Peter H. Gregory. 2018. – 46 p.

[15] Peter H. Gregory CISM Certified Information Security Manager All-in-One Exam Guide. 2018. – 1104 p.

[16] Repin M.M., Pshekhotskaya E.A. Metodika rascheta pokazatelya effektivnosti protivodejstviya informacionnym ugrozam v platyozhnoj sisteme. Nauchno-metodicheskij zhurnal «Nauchno-metodicheskoe obespechenie ocenki kachestva obrazovaniya» – GBU DPO RCOKIO. 2018, no. 2 (5) S. 141–148. URL: https://cyberleninka.ru/article/n/metodika-rascheta-pokazatelya-effektivnosti-protivodeystviya-informatsionnym-ugrozam-v-platezhnoy-sisteme (accessed: 01.03.2021) (in Russian).

[17] Arsenyev V.N., Silantyev S.B., Yadrenkin A.A. Using a priori information for correction of the events stream model in complex system. 2017. Vol. 60, no. 5. P. 391–397. DOI: http://dx.doi.org/10.17586/0021-3454-2017-60-5-391-397 (in Russian).

[18] Shcheglov A.Yu., Shcheglov K.A., Matematicheskie modeli i metody formal'nogo proektirovaniya sistem zashchity informacionnyh sistem. Uchebnoe posobie. SPb: Universitet ITMO, 2015. – 93 s. (in Russian).

[19] Pugin V. V. Gubareva O. YU. Obzor metodik analiza riskov informacionnoj bezopasnosti informacionnoj sistemy predpriyatiya. T-Comm – Telekommunikacii i Transport. 2012. T. 6, no. 6. S. 54–57. URL: https://www.elibrary.ru/item.asp?id=18848583 (accessed: 01.03.2021) (in Russian).

Поступила в редакцию – 09 апреля 2021 г. Окончательный вариант – 12 мая 2021 г.
Received – April 09, 2021. The final version – May 12, 2021.

Виктор Ю. Кадыков[1], Алла Б. Левина[2]
[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Кронверский пр-т, 49, Санкт-Петербург, 197101, Россия
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
ул. Профессора Попова, 5, Санкт-Петербург, 197376, Россия
[1]e-mail: pflyers@rambler.ru, https://orcid.prg/0000-0002-6896-3802
[2]e-mail: alla_levina@mail.ru, https://orcid.prg/0000-0003-4421-2411

СОЗДАНИЕ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА В РЕДУЦИРУЮЩЕМ ГОМОМОРФНОМ ШИФРОВАНИИ ДЛЯ КЛАССА КОНГРУЭНТНЫХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2021.2.10

Аннотация. В настоящее время в области информационной безопасности особое внимание уделяется системам с гомоморфным шифрованием. В данной статье рассмотрены системы гомоморфного шифрования, использующие решетки идеалов. Решетки идеалов, как математический примитив, позволяют достичь существенной производительности по сравнению с основными стандартами шифрования. Также системы гомоморфного шифрования на решетках идеалов являются перспективными за счет устойчивости к атакам с применением квантовых компьютеров. Для класса конгруэнтных систем шифрования получен параметр шума как отношение параметров отображения шифртекста на различных классах сравнений или, в рассматриваемых случаях, на операциях взятия по модулю. В зависимости от параметров, задающих указанные классы, получены условия корректной расшифровки шифртекста. Установлено, что секретные ключи участников системы шифрования могут быть объединены в общий секретный ключ с помощью факторизации целых чисел. Результаты работы могут быть использованы для модификации существующей системы NTRU (Nth-degree TRUncated polynomial ring) и для дополнения ее гомоморфным операциями, свойства которых для указанного класса систем были открыты относительно недавно. В статье используются положения теории множеств, вводится понятие конгруэнтного перехода, выводится необходимое условие вероятностной системы шифрования. Полученная математическая модель позволяет осуществлять обобщение на системы шифрования с большей размерностью или большим количеством участников, определяя эти параметры через выражение для общего секретного ключа, которое в свою очередь представлено как запись групповых операций на идеалах, используемых при построении структуры шифртекста. В настоящее время проводятся исследования по улучшению вычислительной эффективности полностью гомоморфных систем шифрования.

Ключевые слова: гомоморфное шифрование, решетки идеалов, секретный ключ, теория множеств, информационная безопасность.
Для цитирования: КАДЫКОВ, Виктор Ю.; ЛЕВИНА, Алла Б. СОЗДАНИЕ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА В РЕДУЦИРУЮЩЕМ ГОМОМОРФНОМ ШИФРОВАНИИ ДЛЯ КЛАССА КОНГРУЭНТНЫХ СИСТЕМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 107–117, apr. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1352>. Дата доступа: 25 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.10.

Victor Y. Kadykov[1], Alla B. Levina[2]
[1]Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,
Kronverksky prospect, 49, bldg. A, St. Petersburg, 197101, Russia
[2]Saint Petersburg Electrotechnical University "LETI",
Professora Popova str., 5, 197376, Saint-Petersburg, Russian
[1]e-mail: pflyers@rambler.ru, https://orcid.prg/0000-0002-6896-3802
[2]e-mail: alla_levina@mail.ru, https://orcid.prg/0000-0003-4421-2411

Creating a joint secret key in reducing homomorphic encryption for a class of congruent systems

DOI: http://dx.doi.org/10.26583/bit.2021.2.10

Abstract. Today special attention is paid to homomorphic encryption in the field of information security. Systems of homomorphic encryption represent such systems that allow arbitrary operations over ciphertext that are homomorphic to algebraic operations with plaintext. Some of such systems with ciphertext constructed over ideal lattices are reviewed in the paper. Ideal lattices, in turn, are promising mathematical primitives that allow achieving significant performance as compared to existing encryption systems. In addition, they are resistant to attacks based on quantum computer algorithms. The analysis of sets transforms in the reviewed systems showed that local dependencies and patterns exist between relations of its elements. For congruential encryption class systems, the relation between decryption conditions and noise levels is found. Moreover the private keys of encryption system participants can be hidden in a joint private key which is constructed with the factorial difficulty of recovery. The results can be used for modifying the existing NTRU encryption system and its complementation with homomorphic operations properties discovered recently. The study uses the provisions of set theory, introduces the concept of congruent transition, and deduces the necessary condition for a probabilistic encryption system. The obtained mathematical model is quite simple and allows a generalization of joint private key construction for arbitrary known number operations on a ciphertext. Research is underway to improve the computational efficiency of fully homomorphic encryption systems.

Keywords: Homomorphic Encryption, Ideal Lattices, Joint Private Key, Sets Theory, Information Security.

For citation: KADYKOV, Victor Y.; LEVINA, Alla B. Creating a joint secret key in reducing homomorphic encryption for a class of congruent systems. IT Security (Russia), [S.l.], v. 28, n. 2, p. 107–117, apr. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1352>. Date accessed: 25 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.10.

Введение

В настоящее время активно исследуется возможность обработки и изменений зашифрованных данных без знания секретного ключа и предварительного расшифровывания этих данных. Данная идея составляет основу процесса гомоморфного шифрования и может быть реализована, например, в механизме работы облачных технологий. Так, для гомоморфного шифрования справедливы соотношения:

$$\mathrm{C}_{+}(\psi_1, \psi_2) = \mathrm{Enc}(\pi_1 + \pi_2)$$

$$\mathrm{C}_{*}(\psi_1, \psi_2) = \mathrm{Enc}(\pi_1 \cdot \pi_2),$$

где π_1, π_2 – передаваемые сообщения, $Enc()$ – функция шифрования, $\psi_1 = Enc(\pi_1)$, $\psi_2 = Enc(\pi_2)$ – шифртекст, C – некоторые операции над шифртекстом, которые часто можно представить композицией различных групповых операций в пространстве шифртекста $C = c_1 \circ c_2 \circ c_3 \circ \ldots$. В представленных формулах операции C_+, C_* обеспечивают алгебраический гомоморфизм между шифртекстом и открытым текстом.

Первоначальная идея гомоморфного шифрования была предложена Джефри Хоффштейном в [1]. В тот момент существовали системы, поддерживающие гомоморфизм лишь для одной алгебраической операции, либо способные производить ограниченное количество вычислений – так называемые системы с частичным гомоморфизмом. Получение полного алгебраического гомоморфизма – задача, решение которой долгое время не было известно. Только в 1991 г. появилось формализованное определение гомоморфного шифрования [2], а затем была получена первая полностью гомоморфная система шифрования [3]. В качестве основы предложенной системы использовались решетки идеалов.

Данная идея продолжала совершенствоваться, и на протяжении нескольких поколений появились системы полностью гомоморфного шифрования и их модификации, пригодные для применения в различных областях, например, для сбора медицинских данных [4–6]. Новые системы были более практичными – менее требовательными к вычислительным ресурсам при неизменной длине ключа. Это удалось достичь за счет усложнения схем шифрования, однако, основная проблема произвольного увеличения размера шифртекста при вычислительных операциях до сих пор занимает центральное место в области гомоморфного шифрования. Проблему увеличения размера шифротекста связывают с накоплением шума после каждой операции, наличие которого обусловлено необходимостью внесения случайного параметра для защиты от атак на основе подобранного шифртекста, т.е. необходимостью построения вероятностной системы шифрования. Так, в [7, 8] было представлено доказательство того, что безопасность детерминированной системы может быть скомпрометирована при проведении атаки по выбранному шифртексту. В результате современные системы гомоморфного шифрования строятся вокруг операции динамического снижения шума и сильно зависят от нее, поскольку она занимает на несколько порядков больше вычислительных ресурсов, чем сами гомоморфные операции.

Другой проблемой для полностью гомоморфного шифрования является обеспечение криптостойкости, при наличии у атакующего множества из наборов выбранных шифртекстов. Данный вопрос не изучен в достаточной мере и в общем случае анализ стойкости системы сводится к оценке эффективности алгоритмов редукции базиса решетки в применяемой математической модели, например, алгоритмом Ленстры-Ленстры-Ловаса (LLL) или блочным алгоритмом Коркина-Золотарёва [9, 10].

В настоящее время подавляющее большинство работ, исследующих полностью гомоморфное шифрование, сосредоточено на улучшении эффективности систем последнего поколения построенных на основе математических примитивов использующих решетки идеалов и изучении свойств систем для снижения шума. Прежде всего, это обусловлено стойкостью решеток к атакам, использующим вычислительные алгоритмы на основе квантовой архитектуры компьютеров, в частности, использующим алгоритм Шора. Это создает впечатление, что решетки идеалов могут оказаться единственным примитивом, способным обеспечить полностью гомоморфное шифрование [11].

В данной работе исследуется структура шифртекста для конгруэнтной системы шифрования [12], в том числе структура шумовой составляющей. Вводится понятие конгруэнтного перехода, свойства которого используются при построении шифртекста. Показано, какое воздействие он оказывает на шумовую составляющую, и каким образом он может использоваться для формирования общего секретного ключа для гомоморфного шифрования с известным количеством операций.

Отличительной особенностью систем шифрования на решётках идеалов является то, что структура шифртекста поддерживает некоторый гомоморфизм изначально – на основе групповых операций и без дополнительных конструкций. В качестве практических результатов используется обобщение на реальную систему шифрования, использующую решетки идеалов – систему на усеченных полиноминальных кольцах, $N^{th\text{-}degree}$ TRUncated polynomial ring system или NTRU [13]. Эта система дополнена гомоморфными операциями, и в статье отображено каким образом шумовая составляющая оказывает влияние на корректность расшифровывания.

1. Теоретические сведения

В общем случае негомоморфная симметричная система шифрования может быть представлена набором элементов (Π, Ψ, P, E, D), где Π - множество открытых текстов, Ψ – множество шифртекстов, P – множество ключей, E – функция шифрования, D – функция дешифрования, т.е. для фиксированного ключа $p \in P$, открытого текста $\pi \in \Pi$, шифртекста $\psi \in \Psi$ имеют место отображения:

$$E: P \to (\Pi, \Psi); E_p: \pi \to \psi;$$

$$D: P \to (\Psi, \Pi); D_p: \psi \to p.$$

В рассматриваемом случае множества открытого текста Π и шифртекста Ψ представляют собой идеалы, и для формирования необходимой структуры шифртекста Π и Ψ должны принадлежать одному решетчатому пространству (или решетке, обозначается $\lhd \mathcal{L}$):

$$\mathcal{L} = L(B) = \{\bar{v} \times B \,|\bar{v} \in \mathbb{Z}^N\},$$

где $L(B)$ – отображение решетки на базисе векторов B, N – размерность решетки, B – некоторый базис $B = \left(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_N\right) \in \mathbb{R}^N$, состоящий из линейно независимых векторов, $\bar{v}$ – элементы множества векторов, построенные с использованием выбранного базиса. Таким образом, решетка представляет собой все линейные комбинации базисных векторов с целочисленными коэффициентами.

Корректность шифрования обеспечивается соотношением:

$$\Pi, \Psi \lhd \mathcal{L}: D_p\left(E_p(\pi)\right) = \pi^*,$$

где π – шифруемое сообщение, а π^* – сообщение, полученное после дешифрования. Условие выполняется для всех элементов подмножества открытого текста, входящего в пространство решетки. Любой идеал, как подмножество решетки, можно определить классом сравнений вида $\mathcal{L}/x$, и, таким образом, задать решетку, элементы которой порождаются заданными идеалами. Все это предполагает их использование в количестве отличном от одного. Предметом исследования данной работы выступают конгруэнтные классы идеалов, то есть классы, определяющие различные множества усеченных колец в пределах общего пространства решетки.

Зададим два класса идеалов для набора элементов системы:

$$(\mathcal{L}/q\ , \mathcal{L}/p, P, E, D); p \in P: E \to \mathcal{L}/q, D \to \mathcal{L}/p,$$

где $\mathcal{L}/q$ и $\mathcal{L}/p$ представляют смежные классы (числовые кольца) по модулю $q \in Z$ и $p \in Z$ соответственно.

Согласно [7] детерминированные системы шифрования не являются стойкими для вычислений с применением компьютеров на квантовой архитектуре. Поэтому целесообразно будет рассматривать систему шифрования с вероятностной составляющей, тогда набор элементов системы преобразуется к виду:

$$(\mathcal{L}/q\ , \mathcal{L}/p, P, E, D, R);$$

$$E: P \to (\Pi \times R, \Psi), E \to \mathcal{L}/q;$$

$$D: P \to (\Psi, \Pi), D \to \mathcal{L}/p,$$

где R представляет собой множество случайных значений.

Чтобы акцентировать внимание на вопросах безопасности, допустим, что система шифрования является абсолютно стойкой, т.е. выполнено следующее равенство:

$$\Pr(\Pi = \pi \,|\Psi = \psi) = \Pr(\Pi = \pi),$$

где $\pi \in \Pi$ – элемент множества открытого текста, $\psi \in \Psi$ – элемент множества шифртекста.

Введем понятие конгруэнтного перехода.

Определение. Отображение между подмножествами $\mathcal{L}/q$ и $\mathcal{L}/p$ называется конгруэнтным переходом от одного идеала к другому.

Подобный переход можно обеспечить построением системы линейных уравнений, взятых по модулю, для которой согласно следствию из китайской теоремы об остатках существует биективное отображение между $\mathcal{L}$ и вектором значений $\{\mathcal{L}/q, \mathcal{L}/p\}$. Кроме этого, биективным является также отображение гомоморфной алгебры над шифртекстом по отношению к соответствующей ей алгебре над открытым текстом, причем как по модулю q, так и по модулю p.

Согласно теореме Шеннона для абсолютно стойкой системы шифрования [14] чтобы такое отображение было возможным необходимо соблюдать непересечение множеств $\mathcal{L}/p$ и $\mathcal{L}/q$, что определяется параметрами p и q, соответственно. Эти значения также являются ключевой информацией и составляют весь или часть секрета $(p, q) \subseteq P$. При этих условиях можно рассматривать выстраиваемую математическую модель с допущениями, которые не затрагивают вопросы исходных данных (семплирования).

При $p = q$ открытый текст однозначно отображается в множество шифртекстов и ключом выступает сама схема преобразования, что не удовлетворяет принципу Кегрофсса.

При $p > q$ шифртекст не может быть однозначно расшифрован из-за возможных коллизий соответствующих множеств.

Выполнение неравенства $p < q$ является необходимым условием для построения вероятностной системы шифрования. В этом случае $|\Pi| < |\Psi|$ и, соответственно, отображение происходит без коллизий. Кроме этого, $|\Psi| < |\mathcal{L}|$, то есть одному и тому же шифртексту может соответствовать несколько различных элементов в $\mathcal{L}$ при фиксированном ключе, где Π – множество открытых сообщений, $\pi \in \Pi$.

Конгруэнтный переход позволяет отделить в некотором множестве счетную часть множества от несчетной части, для ясности, например, ту часть, которую нельзя представить в виде линейной комбинации базисных векторов. В качестве основного способа может быть применена теорема арифметики о делении для случая целых чисел, используемых к качестве математического примитива для решетки $\mathcal{L}$. Таким способом можно выделить вероятностную составляющую шифртекста с целью дальнейшего преобразования значащей части.

2. Конгруэнтная система шифрования

Рассмотрим как работает описанный выше метод на примере конгруэнтной системы шифрования. Условия выбора параметров, при которых работает данная система, следующие:

$$\pi^* = Decrypt_p(\psi) = D(\pi, r, q, f, p), \begin{cases} \pi, r, q, f, p \in \mathbb{Z} \\ p < q, f < \sqrt{q/2} \\ \exists f^{-1}\ mod\ q = f_q^{-1} \\ \gcd(f, p) = 1 \end{cases}.$$

Процесс получения расшифрованного сообщения π^* представляет собой функцию D от пяти параметров соответственно: ψ – зашифрованный текст, π – передаваемое сообщение, r – случайное целое число, q, p – параметры системы, и f, p – секретные значения.

После выбора параметров системы участник выбирает значение секрета f и вычисляет f_q^{-1}. В этом обозначении нижний индекс указывает на то, что обратное значение вычисляется по модулю q:

$$f \cdot f_q^{-1} = 1 \, mod \, q.$$

Далее, для шифрования сообщения вычисляется ключ шифрования h, выбирается случайное значение r и происходит формирование шифртекста по описанной выше структуре, включающей объединение двух идеалов [16]:

$$h = \left(p \cdot f_q^{-1}\right) mod \, q;$$

$$\psi = \big((\pi + h \cdot r)\big) mod \, q.$$

Так как, исходя из условий системы, значение $\pi + h \cdot r$ может быть гораздо больше q, то после взятия по модулю злоумышленнику необходимо перебрать весь диапазон возможных случайных значений r даже при известном ключе шифрования h, что и составляет верхнюю границу стойкости системы.

Расшифровывание сообщения происходит в два этапа. На первом этапе сообщение домножается на секретный ключ f, известный лишь участникам системы:

$$\psi \cdot f = \left((\pi + h \cdot r) \cdot f\right) mod \, q;$$

$$\psi \cdot f = \left(\pi \cdot f + p \cdot r \cdot ①_q\right) mod \, q.$$

Символом $①_q$ для удобства обозначена локальная единица по модулю q. То есть, это некоторое число, не равное единице, но при этом удовлетворяющее соотношению:

$$①_q = (k \cdot q + 1) \, mod \, q, \text{при } k \in \mathbb{Z}.$$

Соответственно, для успешного осуществления данного перехода необходимым является выполнение условия:

$$\pi \cdot f + p \cdot r < q.$$

После взятия по модулю получаем:

$$\psi \cdot f = \pi \cdot f + p \cdot r.$$

На втором этапе результат домножается на величину обратную f, но уже по модулю p. Существование подобной величины определено условием взаимно простых чисел:

$$\gcd(f, p) = 1;$$

$$(\psi \cdot f) \cdot f_p^{-1} = \left(\pi \cdot f \cdot f_p^{-1} + p \cdot r \cdot f_p^{-1}\right) mod \, p;$$

$$(\psi \cdot f) \cdot f_p^{-1} = \left(\pi \cdot ①_p + p \cdot r'\right) mod \, p.$$

И при выполнении условия $\pi < p$ получаем после взятия модуля расшифрованное сообщение:

$$(\psi \cdot f) \cdot f_p^{-1} = \pi.$$

3. Построение общего секретного ключа

Подход к построению систем шифрования, при котором используются свойства конгруэнтного перехода, позволяет не только выделить шумовую составляющую, но и получить возможность объединения ключей участников системы при гомоморфном шифровании в один общий секретный ключ.

Покажем это на примере системы NTRU [13], схема шифрования которой представляет собой аналогичную схему для конгруэнтного шифрования за исключением использования усеченных полиноминальных колец вида $\mathbb{Z}_q/(x^N+1)$ (при вычислении используются, соответственно, вектора размерности N) вместо целых чисел. Это повышает эффективность в вычислительном плане, так при использовании циклотомического (кругового) полинома групповая операция умножения преобразуется в операцию свертки, которая реализуется существенно более быстрым алгоритмом.

Отличительной особенностью рассматриваемых систем является то, что структура шифртекста поддерживает гомоморфную алгебру без дополнительных конструкций [15].

Перейдем непосредственно к системе шифрования по аналогии с рассматриваемой выше конгруэнтной системой шифрования. Вычисление ключей шифрования и построение шифртекста теперь происходит непосредственно для двух участников системы, которых обозначим с помощью индексов a и b:

$$h_a = \left(p \cdot f_{a_q}^{-1}\right) \ mod\ q;$$

$$h_b = \left(p \cdot f_{b_q}^{-1}\right) \ mod\ q;$$

$$\psi_a = \left((\pi_a + h_a \cdot r_b)\right) mod\ q;$$

$$\psi_b = \left((\pi_b + h_b \cdot r_b)\right) mod\ q.$$

При сложении и умножении шифртекст сохраняет свою структуру. Далее рассматривается случай для сложения:

$$\psi_a + \psi_b = \left((\pi_a + \pi_b + h_a \cdot r_a + h_b \cdot r_b\ )\right) mod\ q.$$

Для расшифрования необходимы секреты f_a и f_b, на основе которых можно построить общий секретный ключ:

$$f_{ab} = (f_a \cdot f_b)\ mod\ q.$$

Далее, домножая результат сложения на общий секретный ключ, получаем возможность выделения шумовой составляющей за счет конгруэнтного перехода:

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + h_a \cdot f_a \cdot f_b \cdot r_a + h_b \cdot f_a \cdot f_b \cdot r_b\right) mod\ q;$$

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + p \cdot f_{a_q}^{-1} \cdot f_a \cdot f_b \cdot r_a + p \cdot f_{b_q}^{-1} \cdot f_a \cdot f_b \cdot r_b\right)\ mod\ q;$$

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + p \cdot ①_a^q \cdot f_b \cdot r_a + p \cdot ①_b^q \cdot f_b \cdot r_b\right)\ mod\ q;$$

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + p \cdot \left(①_a^q \cdot f_b \cdot r_a + ①_b^q \cdot f_b \cdot r_b\right)\right)\ mod\ q;$$

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + p \cdot r'_{ab}\right)\ mod\ q.$$

При условии, что:

$$(\pi_a + \pi_b) f_a \cdot f_b + p \cdot r'_{ab} < q,\ r'_{ab} = p \cdot (f_b \cdot r_a + f_b \cdot r_b),$$

после взятия по модулю получаем промежуточное значение:

$$(\psi_a + \psi_b) \cdot f_{ab} = \left((\pi_a + \pi_b) f_a \cdot f_b + p \cdot r'_{ab}\right).$$

Для расшифрования необходима величина обратная значению общего секретного ключа:

$$f_{ab_p}^{-1} = \left(f_{a_p}^{-1} f_{b_p}^{-1}\right)\ mod\ p;$$

$$(\psi_a + \psi_b) \cdot f_{ab} \cdot f_{ab_p}^{-1} = \left((\pi_a + \pi_b) \cdot ①_{ab}^{p} + p \cdot f_{ab_p}^{-1} \cdot r'_{ab}\right) mod\ p;$$

$$(\psi_a + \psi_b) \cdot f_{ab} \cdot f_{ab_p}^{-1} = \left((\pi_a + \pi_b) \cdot ①_{ab}^{p} + p \cdot r''_{ab}\right) mod\ p.$$

Далее, при выполнении условия $\pi_a + \pi_b < p$ получаем расшифрованное сообщение:

$$(\psi_a + \psi_b) \cdot f_{ab} \cdot f_{ab_p}^{-1} = \pi_a + \pi_b.$$

Аналогичные построения можно выполнить и для операции умножения:

$$\psi_a \cdot \psi_b \cdot f_{ab} \cdot f_{ab_p}^{-1} = \pi_a \cdot \pi_b.$$

Кроме этого, построение можно обобщить на произвольное выражение с оператором $\odot$ для групповой операции, получив следующую закономерность для известного числа операций n:

$$(\psi_1 \odot \psi_2 \odot \ldots \odot \psi_n) \otimes f_n \otimes f_{n_p}^{-1} = \pi_1 \odot \pi_2 \odot \ldots \odot \pi_n.$$

Отличия будут заключаться в различных условиях для корректности расшифрования под модулем q и p соответственно. Условием полностью гомоморфного шифрования будет наличие операции F с понижением уровня шума, при которой нарушается свойство ассоциативности в пространстве решетки $\mathcal{L}$:

$$(\psi_1 \odot_F \psi_2) \odot_F \psi_3 \neq \psi_1 \odot_F (\psi_2 \odot_F \psi_3).$$

Для оценки практической значимости шифрования на идеалах приведем сравнение для систем шифрования RSA, являющейся полностью гомоморфной относительно операции умножения, и NTRU, рассмотренной выше. В [17] приводится следующий анализ для ассиметричных систем:

Стойкость	Размер открытого ключа (длина в битах)		
	NTRU	ECC	RSA
2^{80}	2008	160	1024
2^{112}	3033	224	2048
2^{128}	3501	256	3072
2^{160}	4383	320	4096
2^{192}	5193	384	7680
2^{256}	7690	521	15360

Система	Стойкость (MIPS-год)	Размер открытого ключа (биты)	Время создания ключа (мс)	Шифрование (блок/сек)	Расшифрование (блок/сек)
RSA 512	$4.00 \cdot 10^5$	512	260	2441	122
NTRU 167	$2.08 \cdot 10^6$	1169	4.0	5941	2812
RSA 1024	$3.00 \cdot 10^{12}$	1024	1280	932	22
NTRU 263	$4.61 \cdot 10^{14}$	1841	7.5	3676	1619
RSA 2048	$3.00 \cdot 10^{21}$	2048	4195	310	3
RSA 4096	$2.00 \cdot 10^{33}$	4096	-	-	-
NTRU 503	$3.38 \cdot 10^{35}$	4024	17.3	1471	608

Как можно заметить в сравнении, NTRU неоднозначно можно сравнить с RSA по необходимому объему данных: для коротких ключей NTRU значительно уступает RSA и

выигрывает при относительно большой длине ключа. Однако по производительности NTRU существенно выигрывает RSA, так как требование к вычислительным ресурсам растет линейно по отношению к длине ключа. Тем не менее, методы атаки на системы, использующие решетки, и стойкость систем изучены в значительно меньшей степени, чем для систем использующих факторизацию целых чисел. На данный момент в академическом сообществе существуют дискуссии на этот счет, и для сегодняшнего состояния вычислительных средств принято считать эквивалентную стойкость перебора 2^{256} достаточной и NTRU способна ее обеспечить при лучших скоростях создания ключа, шифрования и расшифрования, чем RSA.

Заключение

В данной статье рассмотрены конгруэнтные системы шифрования, построенные с использованием решёток идеалов, показано, что использование идеалов позволяет создать вложенную структуру шифртекста, где для каждого уровня соблюдаются определенные общие закономерности.

Особенностью таких систем является то, что структура шифртекста поддерживает гомоморфную алгебру без дополнительных конструкций, и в схеме их работы можно выделить конгруэнтный переход, который позволяет реализовать однонаправленную функцию. Однако это же приводит к увеличению вероятности ошибки при дешифровании, что обусловлено шумовой составляющей при формировании шифртекста. Накопление шума происходит после каждой групповой операции с идеалами в пространстве шифртекста. В работе прослеживается вложенная структура шума, что может быть использовано при разработке схемы понижения шума.

Выделение значащих частей происходит с использованием конгруэнтного перехода. Этот способ позволяет построить общий секретный ключ, скрывающий часть информации об участниках системы шифрования. Встречной задачей выступает выбор параметров системы для поддержки допустимого количества операций.

Практическая значимость гомоморфного шифрования заключается в возможности делегировать алгоритм вычислений третьей стороне, не разглашая структуру самого алгоритма. К сожалению, в современных схемах полностью гомоморфного шифрования наличие шифрования, происходящее после выполнения каждой групповой операции, ведет к полиноминальному снижению производительности в зависимости от длины цепочки вычислений. При этом на практике реализация таких алгоритмов требует их низкоуровневого представления в виде булевых функций, что также может приводить к чрезвычайно большим арифметическим схемам.

В качестве дальнейшего направления исследований можно предложить реализацию качественно других арифметических схем, представленный в данной работе метод конгруэнтного перехода может найти широкое применение на практике.

СПИСОК ЛИТЕРАТУРЫ:

1. Rivest R.L., Adleman L., Dertouzos M.L., et al. On data banks and privacy homomorphisms. Foundations of secure computation. Vol. 4, no. 11, 1978. P. 169–180. URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf (дата обращения: 01.02.2021).
2. Feigenbaum J. Distributed computing and cryptography: proceedings of a DIMACS Workshop, October 4–6, 1989. American Mathematical Soc., 1991. – 262 p.
3. Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09). Association for Computing Machinery, New York, NY, USA, 169–178. DOI: https://doi.org/10.1145/1536414.1536440.

4. Brakerski Z. and Vaikuntanathan V. Efficient Fully Homomorphic Encryption from (Standard) LWE. IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011. P. 97–106, DOI: https://doi.org/10.1109/FOCS.2011.12.
5. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ACM Trans. Comput. Theory 6, 3, Article 13. July 2014. – 36 p. DOI: https://doi.org/10.1145/2633600.
6. Brakerski Z., Gentry C., Halevi S. (2013) Packed Ciphertexts in LWE-Based Homomorphic Encryption. In: Kurosawa K., Hanaoka G. (eds) Public-Key Cryptography – PKC 2013. PKC 2013. Lecture Notes in Computer Science. Vol. 7778. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-36362-7_1.
7. Maurer U., Raub D. Black-box extension fields and the inexistence of field-homomorphic one-way permutations //International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2007. P. 427–443. DOI: https://doi.org/10.1007/978-3-540-76900-2_26.
8. Boneh D. and Lipton R. Searching for Elements in Black-Box Fields and Applications. In Crypto' 96, LNCS 1109. P. 283–297. Springer-Verlag, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.4296 (дата обращения: 01.02.2021).
9. Li J., Nguyen P.Q. A complete analysis of the bkz lattice reduction algorithm. – Cryptology ePrint Archive, Report 2020/1237, 2020. URL: https://eprint.iacr.org/2020/1237 (дата обращения: 01.02.2021).
10. Korkine A., Zolotareff G. Sur les formes quadratiques. Math. Ann. 6, 366–389 (1873). DOI: https://doi.org/10.1007/BF01442795.
11. Бабенко Л.К. и др. Полностью гомоморфное шифрование (обзор) //Вопросы защиты информации. 2015. №. 3. С. 3–26. URL: https://elibrary.ru/item.asp?id=24833959 (дата обращения: 01.02.2021).
12. Silverman J.H., Pipher J., Hoffstein J. An introduction to mathematical cryptography. Springer, New York, NY, 2008. – 524 p. DOI: https://doi.org/10.1007/978-0-387-77993-5.
13. Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science. Vol. 1423. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/BFb0054868.
14. Smart N.P. Cryptography: an introduction. New York: McGraw-Hill, 2004. – 433 p. ISBN: 9780077099879.
15. Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. 51, 4, Article 79. September, 2018. – 35 p. DOI: https://doi.org/10.1145/3214303.
16. Кадыков В.Ю., Левина А.Б. Гомоморфные операции в системах шифрования с применением решеток идеалов // Вестник компьютерных и информационных технологий. 2020. Т. 17. №. 11. С. 40–46. URL. https://www.elibrary.ru/item.asp?id=44421628 (дата обращения: 01.02.2021).
17. Mersin A. The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems. İzmir Institute of Technology, Master's thesis, 2007. URL: https://core.ac.uk/download/pdf/324140901.pdf (дата обращения: 01.02.2021).

REFERENCES:

[1] Rivest R.L., Adleman L., Dertouzos M.L., et al. On data banks and privacy homomorphisms. Foundations of secure computation. Vol. 4, no. 11, 1978. P. 169–180. URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf (accessed: 01.02.2021).
[2] Feigenbaum J. Distributed computing and cryptography: proceedings of a DIMACS Workshop, October 4-6, 1989. American Mathematical Soc., 1991. – 262 p.
[3] Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09). Association for Computing Machinery, New York, NY, USA, 169–178. DOI: https://doi.org/10.1145/1536414.1536440.
[4] Brakerski Z. and Vaikuntanathan V. Efficient Fully Homomorphic Encryption from (Standard) LWE. IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011. P. 97–106, DOI: https://doi.org/10.1109/FOCS.2011.12.
[5] Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ACM Trans. Comput. Theory 6, 3, Article 13. July 2014. – 36 p. DOI: https://doi.org/10.1145/2633600.
[6] Brakerski Z., Gentry C., Halevi S. (2013) Packed Ciphertexts in LWE-Based Homomorphic Encryption. In: Kurosawa K., Hanaoka G. (eds) Public-Key Cryptography – PKC 2013. PKC 2013. Lecture Notes in Computer Science. Vol. 7778. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-36362-7_1.
[7] Maurer U., Raub D. Black-box extension fields and the inexistence of field-homomorphic one-way permutations. International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2007. P. 427–443. DOI: https://doi.org/10.1007/978-3-540-76900-2_26.

[8] Boneh D. and Lipton R. Searching for Elements in Black-Box Fields and Applications. In Crypto' 96, LNCS 1109. P. 283–297. Springer-Verlag, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.4296 (дата обращения: 01.02.2021) (accessed: 01.02.2021).
[9] Li J., Nguyen P.Q. A complete analysis of the BKZ lattice reduction algorithm, tech. rep. Cryptology ePrint Archive, Report 2020/1237, 2020. URL: https://eprint.iacr.org/2020/1237 (accessed: 01.02.2021)
[10] Korkine, A., Zolotareff G. Sur les formes quadratiques. Math. Ann. 6, 366–389 (1873). DOI: https://doi.org/10.1007/BF01442795.
[11] Babenko L.K. u dr. Polnost'ju gomomorfnoe shifrovanie (obzor) [Fully Homomorphic Encryption (review)], Information security questions (ISQ), 2015, no. 3. P. 3–26. URL: https://elibrary.ru/item.asp?id=24833959 (accessed: 01.02.2021) (in Russian).
[12] Silverman J.H., Pipher J., Hoffstein J. An introduction to mathematical cryptography. Springer, New York, NY, 2008. – 524 p. DOI: https://doi.org/10.1007/978-0-387-77993-5.
[13] Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science. Vol. 1423. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/BFb0054868.
[14] Smart N.P. Cryptography: an introduction. New York: McGraw-Hill, 2004. – 433 p. ISBN: 9780077099879.
[15] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. 51, 4, Article 79. September, 2018. – 35 p. DOI: https://doi.org/10.1145/3214303.
[16] Kadykov V.Yu., Levina A.B. (2020). Homomorphic Operations in Encryption Systems Using Ideal Lattices. Vestnik komp'yuternyh i informatsionnyh tekhnologiy. Vol. 17, no. 11. P. 40–46. URL. https://www.elibrary.ru/item.asp?id=44421628 (accessed: 01.02.2021) (in Russian).
[17] Mersin A. The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems. İzmir Institute of Technology, Master's thesis, 2007. URL: https://core.ac.uk/download/pdf/324140901.pdf (accessed: 01.02.2021).

Поступила в редакцию – 10 апреля 2021 г. Окончательный вариант – 23 мая 2021 г.
Received – April 10, 2021. The final version – May 23, 2021.

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;

– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами, кегель 12); далее сведения об авторах – организация с почтовым адресом, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив, кегель 11); затем название статьи (по центру, ПРОПИСНЫМИ буквами, кегель 12), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом, кегель 11) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив, кегель 11); аннотация (100 – 250 слов, по ширине, строчными буквами – см. **правила оформления аннотации**);

– далее повторяются все сведения о статье **на английском языке.**

– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;

– в статью включают **Введение** и **Заключение**, а также вводятся **Разделы** с их нумерацией (прописные по центру, полужирно, кегль 12);

– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы литературы (по ширине, строчные, кегль 10), оформленный в соответствии с действующими стандартами и указанием идентификатора DOI (как правило, не менее 15 наименований в научной статье и 50 в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные авторов и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации на латиницу.

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).

Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи**:**

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.

Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи

и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (файл *.doc) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

The articles submitted to the editors must meet the following requirements:

– the topic of the article should be relevant, have scientific or practical significance and be published by the authors for the first time;

– the manuscript should be formatted only in * .doc or pdf format, A4 strip, size 12, TimesNewRoman font, one-and-a-half interval;

– in the beginning of the article there are information about the article in English: I.O. Name of authors (centered, lower case); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– further information on the article is in Russian: I.O. The authors' surname (for jubilus, lower case letters); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– then the text of the article is in Russian or English, size 12, interval one and a half, the recommended total volume of the article should not exceed 10 pages, including tables, illustrations;

– at the end of the article the LIST OF LITERATURE is given, in which the bibliographic list of sources of literature is indicated, drawn up in accordance with the current standards (as a rule, not less than 15 titles);

– after the list of literature is REFERENCES, in which these bibliographic sources should be written in Latin (ie Latin letters).

Rules to write a scientific abstract

Abstract is a source of information about the content of the paper and its research results. The structure of the abstract should correspond to the structure of the paper and should be not less than 100 words, but not more than 250 words.

The abstract includes the following aspects of the paper:

- subject and purpose of the paper;
- method or methodology described in the paper;
- results;
- discussion.

The abstract plays the following role:

- allows you to establish the main content of the paper, determine its relevance and decide whether to read the full text of the paper;
- provides information about the paper and eliminates the need to read the full text of the paper if the paper is of secondary interest to the reader;
- used in information systems, including automated ones, to search for documents and information (title, abstract and keywords are translated into English, and foreign readers judge the content of the paper by them).

The abstract should be informative (not contain general wordings) and original. The information contained in the title of the paper should not be repeated in the text of the abstract. The text of the abstract should not contain an interpretation of the content of the paper, criticisms and the author's point of view, as well as information that is not included in the paper. You should avoid unnecessary introductory phrases (for example, " the author is considering..."). Historical references, if they do not constitute the main content of the paper, the description of previously published works and well-known provisions are not given in the abstract.

The text of the abstract should use syntactic constructions peculiar to the language of scientific and technical documents, avoid complex grammatical structures.

The text of the abstract should use significant (key) words from the text of the paper.

The method or methodology of the work should be described if they are new or of interest from the point of view of this work. In the abstract of the paper describing the experimental work, indicate the data sources and the specific features of their processing.

The results are described very accurately and informative. The main theoretical and experimental results, actual data, discovered interrelations and regularities are presented. At the same time, preference is given to new results and data of long-term importance, important discoveries, conclusions that refute existing theories, as well as data that, in the author's opinion, have practical value.

Conclusions may be accompanied by recommendations, assessments, suggestions, hypotheses described in the paper.

Terms of publication of the article

– the article should be sent by e-mail;

– the editorial board of the journal follows the ethical standards adopted in the international scientific community, relying on the recommendations of the Ethics Committee of scientific publications that do not contradict the norms of Russian legislation in the field of regulation of the activities of the media and copyright;

– articles that do not meet the requirements for presentation and processing are not considered or published;

– in one issue of the journal, as a rule, only one author's article is published, including co-authors;

– authors should provide only original works, if text or graphic information obtained from other persons is used, references to the relevant publications or the author's written permission are necessary;

– the decision to publish the manuscript is made by the editorial board on the basis of the result of peer review and expert evaluation by qualified specialists in the field of information security;

– in the case of receipt of the manuscript for publication, the author must promptly give answers to editorial questions related to comments on the article;

– in case of refusal to publish, the editorial board should provide the author with a copy of the review and justification for refusing the publication;

– submitting an article to more than one journal is simultaneously regarded as unethical behavior and is unacceptable;

– articles are published for free.

Rules for publication of texts

1. Articles must be submitted electronically (* .doc or * .rtf) with a printout (or a file in * .pdf format) - to avoid inaccuracies in reading the formulas.
2. Pictures, graphics, photographs and other types of illustrations should, if possible, not only be included in the text, but also separate files in the original format (not integrated into the Word document).
3. Abbreviations and abbreviations, which are not on the list of abbreviations, should be disclosed (in parentheses or in a footnote).
4. By providing links to formulas, expressions or restrictions in the text of the article, please make sure that the relevant objects in the article are numbered and numbered.
5. References to the literature should be given in the text in square brackets, in the case of citations, with pages.
6. When preparing a list of literature, it is desirable to pay attention to the availability of output data of works and to avoid repeated instructions of the same work under different numbers.
7. References to laws, regulations, confessions and so on should be indicated in the prescribed form: the Law of the Russian Federation "__" of x month xxxx, No. ___. Art. ___.
8. Foreign words, terms and surnames, the spelling of which allows variants, please write within the same article the same way.

Submission Preparation Checklist

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the "About the journal" page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Privacy Statement

The names and email addresses entered in this journal site page will be used exclusively for the purposes specified by this journal and will not be used for any other purposes or will not be given over to another individuals and organizations.

СПИСОК СОКРАЩЕНИЙ, ПРИНЯТЫХ В ЖУРНАЛЕ

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
БЧ – блокчейн
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КПО – комплекс программного обеспечения
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОКСО – Общероссийский классификатор специальностей по образованию
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СБЧ – система блокчейн
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись
ФГОС – федеральный государственный образовательный стандарт
ФУМО ИБ – федеральное учебно-методическое объединение по образованию в области информационной безопасности

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 8277

Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 8277
E-mail: BIT@mephi.ru
Сайт журнала: https://bit.mephi.ru

Периодичность выхода – 4 раза в год / Periodicity – 4 times a year

Подписка на журнал
производится в почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Ответственный редактор И.М. Ядыкин
Технический редактор П.А. Золотухина

Подписано в печать _____Формат 60x84 1/8
Печ. л. 15,5. Уч.-изд. л. 15,5. Тираж 500 экз. Изд. № 002 – 3

Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»
(АО «ЭНПО СПЭЛС»)
Каширское ш., 31, строение 44, этаж 3, пом. IV, ком.4, Москва, 115409, Россия

Joint Stock Company «Experimental Scientific and Production Association
SPECIALIZED ELECTRONIC SYSTEMS»
(JSC «ENPO SPELS»)
Kashirskoe shosse, 31, building 44, floor 3, pom. IV, room 4, Moscow, 115409, Russia

Типография ООО «ТИПОГРАФИЯ»
ул. Кантемировская, 60, Москва, 115477, Россия