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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

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

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

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

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников
05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки),
05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки), по которым журнал входит в этот перечень.

Основные тематические направления журнала:

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

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

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

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

Papers in Russian and English are equally welcome.

Focus topics:

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

СОДЕРЖАНИЕ

CONTENT

ВЛАДИМИР ИГОРЕВИЧ БУДЗКО
(к 75-летию со дня рождения)

14 августа исполнилось 75 лет со дня рождения доктору технических наук, профессору Будзко Владимиру Игоревичу, члену редколлегии журнала «Безопасность информационных технологий».

В 1962 году Владимир Игоревич поступил, а в 1968 году окончил кафедру ЭВМ Московского инженерно-физического института по специальности «Вычислительные машины, комплексы, системы и сети», получив квалификацию «инженер-электрик».

С 2001 года – заместитель директора по научной работе Института проблем информатики Российской академии наук (ИПИ РАН). Владимир Игоревич известный российский ученый разработавший принципы создания современных крупномасштабных катастрофоустойчивых информационно-телекоммуникационных систем различного назначения. Под его руководством сформировалось новое научное направление теоретических исследований – «Построение информационно-телекоммуникационных систем высокой доступности».

Владимир Игоревич – автор более 100 научных работ, авторитетный педагог для студентов и аспирантов. Он обладает большим опытом организатора научной работы, направляющего усилия большого коллектива ученых и практиков на создание высокозащищенных автоматизированных систем органов государственной власти Российской Федерации, Национальной платежной системы России. В течение 10 лет входил в состав советов ВАК России, был членом Рабочей группы по банкам данных при Комитете по науке и технике СССР. Будзко В.И. член-корреспондент Академии криптографии РФ, Лауреат Премии Правительства РФ в области науки и техники за 2010 год.

Редколлегия журнала «Безопасность информационных технологий», коллеги и друзья Владимира Игоревича от всей души поздравляют его с юбилеем и желают крепкого здоровья, благополучия и дальнейшей плодотворной научной и педагогической деятельности.

ОЛЕГ БОРИСОВИЧ МАКАРЕВИЧ
(к 85-летию со дня рождения)

13 сентября исполнилось 85 лет со дня рождения доктору технических наук, профессору Макаревичу Олегу Борисовичу, члену редколлегии журнала «Безопасность информационных технологий».

В 1956 г. Олег Борисович поступил, а в 1961 г. окончил Таганрогский государственный радиотехнический институт с дипломом инженера-электрика. С 1962 г. работает в ТРТИ, где прошел путь от ассистента до заведующего кафедрой Безопасности информационных технологий, заведующего проблемной лабораторией цифровых интегрирующих машин, заведующего отделом многопроцессорных систем НИИ МВС, директора Южно-Российского регионального центра по проблемам информационной безопасности в системе высшей школы.

О.Б. Макаревич известный ученый в области многопроцессорных вычислительных систем и информационной безопасности. Под его руководством создана научно-педагогическая школа "Интеллектуальные системы защиты информации на базе нейросетевых технологий", он является одним из создателей образовательных программ для подготовки специалистов в области «Информационной безопасности».

Олег Борисович – автор более 300 научных работ, в том числе 75 изобретений и 6 монографий. Он был главным конструктором вычислительного комплекса ЕС-2703 (16-ти компьютерной вычислительной системы) и разработчиком серии интегральных микросхем К-502 (цифровых интеграторов). Участник выполнения грантов РФФИ и Минобразования. За личный вклад в укрепление государственной системы защиты информации и оказание содействия в решении задач, возложенных на Гостехкомиссию России в Южном федеральном округе Макаревич О.Б. награжден медалью «За укрепление государственной системы защиты информации II степени». О.Б. Макаревич – «Заслуженный деятель науки РФ», «Заслуженный изобретатель Российской Федерации» академик Международной академии информатизации.

Редколлегия журнала «Безопасность информационных технологий», коллеги и друзья Олега Борисовича от всей души поздравляют его с юбилеем и желают крепкого здоровья, благополучия и дальнейшей плодотворной научной и педагогической деятельности.

Наталья И. Касперская[1], Василий В. Кузьменко[2], Дмитрий А. Мананников[3],
Рустем Н. Хайретдинов[4], Андрей Ю. Щербаков[5]
[1, 2, 4] Группа компаний InfoWatch,
Верейская ул., 29, стр. 134, г. Москва, 121357, Россия
[1]Московский институт электроники и математики им. А.Н.Тихонова НИУ ВШЭ
Таллинская ул., 34, г. Москва, 123458, Россия
[2]ООО КБ «Нэклис-Банк»
Никитская Б. ул., 17, стр. 2, г. Москва, 125009, Россия
[3]Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
Проспект Вернадского, 84, г. Москва, 119571, Россия
[5]Центр развития криптовалют и цифровых финансовых активов ВИНИТИ
Усиевича ул., 20, г. Москва, А-190, 125190, Россия
[1]e-mail: natalya.kaspersky@infowatch.com, https://orcid.org/0000-0002-5205-679X
[2]e-mail: vasily.kuzmenko@infowatch.com, https://orcid.org/0000-0002-5042-2012
[3]e-mail: dmitriy@manannikov.ru, https://orcid.org/0000-0003-1116-7028
[4]e-mail: rustem.khairetdinov@infowatch.com, https://orcid.org/0000-0002-3391-7646
[5]e-mail: a.shcherbakov@c3da.org, https://orcid.org/0000-0002-1593-6704

К ПРОБЛЕМЕ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ КОРРЕКТНОСТИ БИЗНЕС-ПРОЦЕССОВ

DOI: http://dx.doi.org/10.26583/bit.2019.3.01

Аннотация. В современных условиях можно констатировать, что классические методы обеспечения информационной и технологической безопасности, связанные с формулированием политики безопасности для разрабатываемой и внедряемой информационной системы, утрачивают ценность и эффективность, поскольку отстают от развития собственно информационных технологий, не вписываются в скорости обновления программного обеспечения и изменение потребностей пользователей. Для решения этих проблем рассмотрено понятие бизнес-процесса как целевой функции, реализованной информационной (компьютерной) системой, введено понятие корректности («здоровья») бизнес-процесса. На основе субъектно-объектной модели компьютерной системы предложена математическая модель здорового бизнес-процесса как траектории или семейства желательных траекторий в состоянии информационной системы. На основе данной модели предложены непротиворечивые практические реализации платформы обеспечения здоровья бизнес-процесса как совокупность интерфейса, отображающего показатели здоровья бизнес-процесса, отчеты, оповещения, предикты (предсказатели или экстраполяторы в виде формальных выражений), коррелятора – ядра платформы, контролирующего логику и содержащее в себе информационные модели, паттерны (образцы траекторий), правила реагирования на события, базы хранения данных бизнес-процесса и коннектора, осуществляющего нормализацию данных бизнес-процесса. С точки зрения системно-аналитического подхода эта платформа представляет собой информационно-аналитическую систему, формирующую новое свойство – здоровье бизнес-процесса, направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне процесса, а также формирования контрольной среды бизнес-процесса. Приведен практический пример обеспечения здоровья бизнес-процесса для логистической системы. Предложен новый универсальный методологический подхода к оценке и обеспечению корректности функционирования бизнес-процессов на основе новой парадигмы доверия (корректности) субъектно-объектной модели бизнес-процесса и понятия здоровья бизнес-процесса, предложена концепция платформы обеспечения здоровья бизнес-процесса. Результаты работы могут широко использоваться для проектирования и оценки систем технологического и финансового профиля.

Ключевые слова: бизнес-процесс, доверие, модель бизнес-процесса, здоровье бизнес-процесса, контрольная точка, зрелость, платформа, метрика здоровья бизнес-процесса, субъектно-объектная модель, логистика, информационные артефакты.
Для цитирования: КАСПЕРСКАЯ, Наталья И. et al. К ПРОБЛЕМЕ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ КОРРЕКТНОСТИ БИЗНЕС-ПРОЦЕССОВ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 8-21, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1213>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.01.

Natalya I. Kasperskaya[1], Vasily V. Kuzmenko[2], Dmitry A. Manannikov[3],
Rustem N. Khairetdinov[4], Andrey Yu. Shcherbakov[5]
[1, 2, 4]Group of companies InfoWatch,
Vereyskaya str., 29, building 134, Moscow, 121357, Russia
[1]Moscow Institute of electronics and mathematics. A. N. Tikhonov HSE
Tallinn str., 34, Moscow, 123458, Russia
[2]Bank "Neklis-Bank"
Nikita Big str., building 17, Moscow, 125009, Russia
[3]RANEPA - National School of Public and Business Administration
Prospect Vernadskogo, 84, Moscow, 11957, Russia
[5] Center for development of cryptocurrency and digital of financial assets VINITI
Usievich str., 20, Moscow, A-190, 125190, Russia
[1]e-mail: natalya.kaspersky@infowatch.com, https://orcid.org/0000-0002-5205-679X
[2]e-mail: vasily.kuzmenko@infowatch.com, https://orcid.org/0000-0002-5042-2012
[3]e-mail: dmitriy@manannikov.ru, https://orcid.org/0000-0003-1116-7028
[4]e-mail: rustem.khairetdinov@infowatch.com, https://orcid.org/0000-0002-3391-7646
[5]e-mail: a.shcherbakov@c3da.org, https://orcid.org/0000-0002-1593-6704

To the problem of assessing and ensuring the correctness of business processes

DOI: http://dx.doi.org/10.26583/bit.2019.3.01

Abstract. In modern conditions, it can be stated that the classical methods of information and technological security related to the formulation of security policy for the developed and implemented information system lose value and efficiency, because they lag behind the development of information technology itself, do not fit into the speed of software updates and changing user needs. To solve these problems, the concept of the business process as a target function implemented by the information (computer) system is considered, the concept of correctness ("health") of the business process is introduced. Based on the subject-object model of a computer system, a mathematical model of a healthy business process as a trajectory or a family of desirable trajectories in the state of an information system is proposed. Based on this model, we propose consistent practical implementation of the platform to ensure the health of the business process as a set of interface that displays indicators of the health of the business process, reports, alerts, predicates (predictors or extrapolators in the form of formal expressions), the correlator – the core of the platform that controls the logic and contains information models, patterns (sample trajectories), the rules of response to events, the database storage of the business process and the connector that normalizes the data of the business process. From the point of view of the system-analytical approach, this platform is an information-analytical system that forms a new property – the health of the business process, aimed at reducing resource losses by identifying and preventing violations (in particular, cybercrime and fraud) at the process level, as well as the formation of the control environment of the business process. There is also a practical example of ensuring the health of the business process for the logistics system. Thus, a new universal methodological approach to assessing and ensuring the correct functioning of business processes on the basis of a new paradigm of trust (correctness) of the subject-object model of the business process and the concept of health of the business process is proposed, the concept of a platform for ensuring the health of the business process is proposed.

The results of the work can be widely used for the design and evaluation of systems of technological and financial profile.
Keywords: the business process, the trust model of the business process, the health of the business process, a reference point, the maturity of the platform, the metric of the health of the business process, subject-object model, logistics, information artifacts.
For citation: KASPERSKAYA, Natalya I. et al. To the problem of assessing and ensuring the correctness of business processes. IT Security (Russia), [S.l.], v. 26, n. 3, p. 8-21, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1213>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.01.

Введение

Современная организация бизнеса построена на использовании информационных технологий, систем и сервисов. От их эффективного использования в бизнес-процессе зависят в первую очередь его ключевые показатели. Сегодня очевидна тенденция – эффективность бизнес-процессов зависит не только от нормального функционирования информационно-телекоммуникационной инфраструктуры, на которой они реализованы, но и от того, насколько правильно процесс выстроен с точки зрения безопасности, ведь несовершенство состояния безопасности, равно как и отклонения от стандартного выполнения операционной деятельности, может привести к ущербу для организации.

Современные подходы к организации безопасных и доверенных бизнес-процессов (термины «безопасность» и «доверенность» будут раскрыты и формализованы ниже) испытывают определенный кризис [1]. Это в первую очередь связано с тем, что классические подходы к реализации свойств безопасности и доверенности основаны либо на методиках аудита (когда изучается алгоритмика бизнес-процесса и сравнивается с некоторым внешним эталоном), либо на методиках соответствия регламентам или политиках безопасности (в этом случае бизнес-процесс проверяется на соответствие некой априорно заданной политике безопасности).

Причины кризиса данных подходов объясняются следующими факторами:

- высокой изменчивостью и динамичностью развития, как самих бизнес-процессов, так и платформ, на которых они реализованы;
- отставанием формальных моделей обеспечения доверенности и безопасности от реальности;
- недостаточным осознанием управляющим персоналом и пользователями проблемы безопасности бизнес-процесса как системно-аналитической сущности.

Таким образом, можно сделать вывод, что подходы «статического» плана, когда заранее формулируется безопасная модель или регламент бизнес-процесса, вступают в диалектическое противоречие с реальностью, не успевают ни за изменчивостью бизнес-процесса, ни за изменением его целей.

Следовательно, необходимо переходить к динамической модели обеспечения безопасности и доверенности бизнес-процесса, когда оцениваются понятия и показатели его изменчивости в некоторые моменты времени и отклонения от некоторых нормальных или «здоровых» состояний. Данный подход апеллирует к опыту построения безопасных технических систем, например, газотурбинных установок, когда мерами безопасности бизнес-процесса в его технологическом понимании является сохранение набора параметров, гармоничных для технической системы и тесно связанных с понятиями технологического смысла и эффективности (температура, давление, вибрации).

Используя понятия ведомственного стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации [2], перечислим базовые определения, касающиеся безопасности бизнес-процессов.

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Актив – все, что имеет ценность для организации и находится в ее распоряжении.

К активам организации могут относиться:

- работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации – платежная, финансово-аналитическая, служебная, управляющая, персональные данные и др.;
- бизнес-процессы и технологические процессы;
- продукты и услуги, предоставляемые клиентам.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации либо находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Объект среды информационного актива – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

Ресурс – актив организации, который используется или потребляется в процессе выполнения некоторой деятельности.

Точка (область) риска – область с высокой вероятностью совершения инцидента безопасности и нарушения операционной деятельности предприятия.

В качестве методической основы для повышения эффективности бизнес-процессов, обеспечения их доверенности и безопасности используются методические материалы по реагированию на инциденты информационной безопасности (ИБ) [2].

1. Понятие бизнес-процесса

Приведем два определения бизнес-процесса (далее – БП или бизнес-процесс).

1. Бизнес-процесс – несколько связанных работ или процедур, в совокупности реализующих конкретную цель текущей деятельности в рамках существующей организационной структуры [3].

2. Бизнес-процесс в информационной системе – совокупность информационных потоков и данных, реализующая заданный и описанный внешними регламентациями бизнес-процесс.

Существуют три основных вида бизнес-процессов – управляющие, операционные и поддерживающие.

Управляющие – БП, которые управляют функционированием системы. Примером управляющего процесса может служить корпоративное управление и стратегический менеджмент.

Операционные – БП, которые составляют основной бизнес компании и создают основной поток доходов. Примеры операционных бизнес-процессов: снабжение, производство, маркетинг, продажи.

Поддерживающие – БП, которые обслуживают основной бизнес. Например, бухгалтерский учет, подбор персонала, техническая поддержка, административно-хозяйственный учет, аналитика.

Бизнес-процесс начинается с фиксации спроса потребителя в материальной форме и заканчивается его удовлетворением.

С точки зрения системного анализа можно изобразить схему бизнес-процесса в виде «черного ящика» с тремя входами и одним выходом (рис.1).

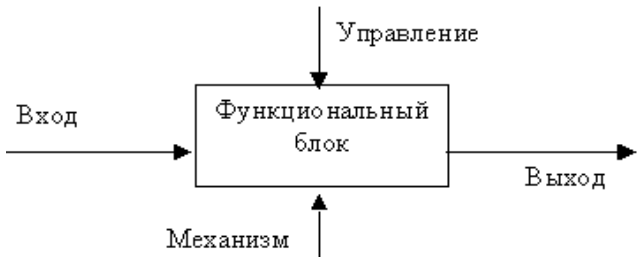

Рис. 1. Схема бизнес-процесса
(Fig. 1. Business process diagram)

БП может быть декомпозирован на несколько подпроцессов, процедур и функций, имеющих собственные атрибуты, но при этом направленных на достижение цели основного БП. Такой анализ бизнес-процессов обычно включает в себя составление карты БП и его подпроцессов, разнесенных между определенными уровнями активности.

Бизнес-процессы должны быть построены таким образом, чтобы создавать стоимость и ценность для потребителей (владельцев, создателей) данных бизнес-процессов, а также исключать любые необязательные или лишние активности [4-7]. На выходе «правильно» построенных бизнес-процессов увеличивается ценность товаров и услуг для потребителя и рентабельность (за счет уменьшения себестоимости производства товара или услуги).

БП могут подвергаться различному анализу в зависимости от целей моделирования. Например, при бизнес-моделировании, функционально-стоимостном анализе, формировании организационной структуры, реинжиниринге бизнес-процессов, автоматизации технологических процессов.

Один из методов анализа текущей деятельности – составление модели бизнес-процесса «как есть» (*as is*), т.е. описание последовательности действий по определенному выбранному направлению деятельности. Полученная модель БП подвергается критическому изучению или обрабатывается специальным программным обеспечением. По результатам анализа формируется модель бизнес-процесса «как будет» (*to be*) и план мероприятий по внедрению необходимых изменений.

Существует несколько нотаций, применяемых для описания и моделирования бизнес-процессов, например:

BPMN (*Business Process Model and Notation* – нотация и модель бизнес-процессов) – служит для отображения функциональной последовательности работ в виде диаграмм бизнес-процессов, понятных бизнес-аналитикам, техническим специалистам и другим бизнес-пользователям;

EPC (*Event-driven process chain* – событийная цепочка процессов) – блок-схема, представляющая упорядоченную логически взаимосвязанную событийную последовательность действий для получения желаемого результата;

IDEF0 (*Integration Definition for Process Modelling* – функциональное моделирование бизнес-процессов) – графическая нотация, описывающая функции системы и логические связи между ними и внешней средой.

Описание бизнес-процесса – это фиксация последовательности действий при его выполнении с целью их анализа и оптимизации, а также улучшения свойств БП (в частности, безопасности и доверенности) и повышения его качества [8, 9].

2. Математическая модель компьютерной системы и бизнес-процесса. Понятие здоровья бизнес-процесса

В современной информатике **модель компьютерной системы** (КС) чаще всего рассматривается в виде **совокупности элементов**, которые можно разделить на два подмножества: множество **объектов** и множество **субъектов** [9-12].

В любой системе с точки зрения системного анализа выделяются существенные для ее качественной определенности части, подсистемы или компоненты. В случае компьютерной системы компонентами будут субъекты и объекты. Разделение компонент на субъекты и объекты в компьютерной системе основывается на свойстве компонента «быть активным» или «получить управление», т.е. субъектами в компьютерной системе являются программы, а объектами – данные.

Передача или поток информации от одного объекта к другому происходит по инициативе субъекта, поэтому в соответствии с [9] введем формальное определение. **Потоком информации** между объектом O_m и объектом O_j называется произвольная операция над объектом O_j, реализуемая в субъекте S_i и зависящая от O_m.

Обозначения: $\boldsymbol{Stream}(S_i, O_m) \rightarrow O_j$ – поток информации от объекта O_m к объекту O_j.

Изменение и порождение новых объектов компьютерной системы (т.е. появление в компьютерной системе новых программ) производится субъектом как активной компонентой, управляемой пользователем через органы управления.

Соответственно вводится понятие порождения субъекта [9] $\boldsymbol{Create}(S_j, O_i) \rightarrow S_k$ – из объекта O_i порожден субъект S_k при активизирующем воздействии субъекта S_j. ***Create*** назовем операцией порождения субъектов.

Тогда с точки зрения субъекто-объектной модели **бизнес-процесс** представляет собой последовательность матриц состояний декартова произведения множества субъектов на множество объектов $<S,O>t$, где t – моменты времени или контрольные точки бизнес-процесса, т.е. такие моменты времени, в которых матрица состояний подвергается сравнению с заданными эталонными значениями либо проверяется на выполнение некоторых свойств. В данном случае полагаем, что бизнес-процесс реализован в рамках компьютерной системы.

Введем также следующее определение. Бизнес-процесс является доверенным (корректным) или здоровым, когда последовательность матриц состояний не выходит за пределы априорно установленных значений для всех моментов времени или в контрольных точках, а потоки в моменты t обусловлены логикой бизнес-процесса. Например, процесс увеличения кредитного лимита в банке выполняется каждым субъектом на своем шаге – приемщиком заявки, кредитным оператором, администратором смены; появление потока от субъекта не своего шага является недоверенным (нездоровым).

Этим определением задается также методология установления здоровья бизнес-процесса:

- бизнес-процесс есть совокупность изменения объектов субъектами в некоторые моменты времени;
- его текущий ход (траектория БП) описывается матрицей состояний $<S,O>t$;
- матрица состояний может быть проверена на соответствие некоторым внешним и/или внутренним правилам, и эта проверка позволяет сделать вывод о здоровье или нездоровье бизнес-процесса (можно сформулировать эквивалентное положение о том, что матрица состояний должна соответствовать желательной траектории).

Итак, мы перешли от статичной модели к динамической, которая ниже будет проиллюстрирована конкретным примером. В первую очередь бизнес-процесс должен

быть обследован на предмет формирования матрицы его состояний в удобном для восприятия и последующей реализации виде. Задача обследования направлена на выявление угроз безопасности индивидуально для каждого БП, на определение оценки эффективности обеспечения его здоровья и безопасности, выявление «точек риска» (областей с высокой вероятностью совершения инцидента безопасности и нарушения операционной деятельности).

Работы по обследованию включают в себя анализ информационных активов бизнес-процессов на предмет выявления чувствительной информации и определения критериев ее легитимной обработки, изучение основного функционала и ролей доступа в используемых информационных системах и сервисах, построение информационных моделей бизнес-процессов с выделением проблемных областей – «точек риска», моделирование в них угроз безопасности и нарушения операционной деятельности, подготовку мероприятий по их устранению за счет формирования непрерывной контрольной среды.

Второй важный момент наряду с обследованием бизнес-процесса – формулирование технического механизма контроля, предусматривающего в первую очередь накопление данных, а затем их анализ исходя из результатов обследования.

Для обеспечения непрерывного контроля безопасности функционирования бизнес-процессов предлагается создание системы, осуществляющей агрегацию, корреляцию и анализ собранных на этапе обследования данных для определения отклонения бизнес-процесса от описанной информационной модели (возникновение нестандартных событий, которые могут указывать на потенциальное киберпреступление, внутреннее мошенничество или другие бизнес-риски). Делается это с целью обозначения отклонения траектории бизнес-процесса от желаемой. Разработка такой системы направлена на автоматизированное непрерывное обеспечение контрольной среды, выявление и мониторинг девиантных состояний, потенциально свидетельствующих о возможных нарушениях внутри контролируемого бизнес-процесса.

3. Цели обеспечения здоровья бизнес-процессов

Основная цель обеспечения здоровья бизнес-процесса заключается в снижении потерь (т.е. в предотвращении снижения коэффициента эффективности или полезного действия бизнес-процесса) в его рамках, как прямых – в случае реализации инцидентов информационной безопасности и внутреннего мошенничества, так и косвенных – в случаях отхождения бизнес-процесса от описанной модели (снижение доверенности, качества, эффективности) за счет обеспечения прозрачности информационных потоков бизнес-процессов, выявления, сквозного контроля или устранения всех «точек риска» в каждом из функционирующих в организации бизнес-процессов.

Согласно [13], **доверие** – свойство системы, объективно, обоснованно и документально выраженное основание того, что элемент системы (в терминах стандартов – изделие информационных технологий, информационный продукт, информационно-телекоммуникационная система, ее компоненты, бизнес-процесс в целом) отвечает априорно заданной (регламентациями высшего уровня) целевой функции на всем протяжении своего жизненного цикла и во всех режимах функционирования. Исходя из этого определения, понятие доверия включают в понятие здоровья.

По уровню защищенности разделим бизнес-процессы на: базово-защищенные – безопасность поддерживается на необходимом базовом уровне за счет применения штатных средств обеспечения информационной безопасности; уверенно-защищенные – безопасность поддерживается на необходимом уверенном уровне за счет применения

отечественных средств обеспечения информационной безопасности; высокозащищенные – безопасность поддерживается на необходимом высоком уровне за счет применения отечественных сертифицированных (рекомендованных, аттестованных) средств. По уровню доверенности бизнес-процессы можно разделить на базово-доверенные, среднедоверенные и высокодоверенные.

Высокая защищенность и доверенность подразумевают использование средств обеспечения информационной безопасности отечественной разработки, собственное управление ими (отсутствие аутсорсинга), проведение аудита и аттестации.

4. Платформа обеспечения здоровья бизнес-процесса

Для решения задачи обеспечения здоровья бизнес-процесса рассмотрим понятие платформы обеспечения здоровья БП.

С точки зрения системно-аналитического подхода платформа обеспечения здоровья БП представляет информационно-аналитическую систему, формирующую новое рассмотренное выше свойство – «здоровье БП», направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне бизнес-процесса, а также формирования его контрольной среды.

Архитектура такой платформы включает компоненты:

- интерфейс – визуальный компонент платформы, отображающий показатели здоровья БП, отчеты, оповещения, предикты (предсказатели или экстраполяторы в виде формальных выражений);
- коррелятор – ядро платформы, контролирующее логику БП и содержащее в себе информационные модели, паттерны (образцы траекторий), правила реагирования;
- БД – базу хранения данных бизнес-процесса;
- коннектор – пассивный компонент, осуществляющий нормализацию и парсинг данных бизнес-процесса. Может принудительно запрашивать данные БП, не вмешиваясь в его логику и/или его данные.

Платформа через коннекторы к компьютерной системе и сервисам собирает весь объем информационных артефактов, используемых в рамках БП. Информационные артефакты приводятся к единому формату, сохраняются в базе данных и индексируются для обеспечения возможности онлайн-поиска и запросов. Коррелятор (в соответствии с загруженными в него информационными моделями БП) выполняет наложение паттернов процессов на базу информационных артефактов и фиксирует все возможные отклонения. Интерфейс системы формирует отчеты и оповещения об отклонениях, а также поддерживает процедуры обеспечения безопасности.

Измеряемыми результатами внедрения платформы являются: существующие индикаторы эффективности бизнес-процесса и его «здоровья», БП – индикатор, определяющий устойчивость к нарушениям в рамках этого БП.

Методология обеспечения безопасности бизнес-процесса базируется на обоснованных утверждениях:

- нарушением в БП является любое отклонение от заданной логики (желательной траектории БП);
- БП существует на уровне событий информационных систем независимо от степени формализации заданной логики;
- правила, устанавливаемые заданной логикой БП, однозначно идентифицируются набором взаимосвязанных событий и данных в информационных системах.

Приведенные утверждения лежат в основе построения информационной модели бизнес-процесса – фундаментальной задачи в рамках обеспечения его безопасности, решаемой платформой обеспечения здоровья БП.

Информационная модель является частью платформы и представляет совокупность трех уровней информационной модели БП. Первый уровень информационной модели БП – логический. Служит для фиксации заданной логики БП: взаимосвязи этапов, процедур, логических событий и т.д. Исходно логика БП может быть задана как формализовано – в рамках утвержденного документа в формате одной из существующих международных схем, так и не формализовано – в виде каких-либо инструкций и общепринятых правил.

Второй уровень – информационный. Определяет совокупность событий и данных в информационных системах (с учетом временных интервалов создания этих событий), отвечающих заданной логике БП – паттерн информационных артефактов, соответствующий траектории в виде событий информационной системы (выше говорили о совокупности потоков и порождений субъектов). Поскольку одним из основных и неотъемлемых ресурсов бизнес-процессов является человек – пользователь соответствующих информационных систем, среди паттернов информационных артефактов выделяются паттерн БП и паттерн пользователя. Паттерн БП не зависит от конкретного пользователя и является общим для процесса. Паттерн пользователя соответствует конкретному пользователю, выполняющему процесс (процесс соответствует субъекту). Информационный уровень напрямую связан с логическим и формируется на основе анализа логов информационных систем, которые генерируются каждым отдельным логическим событием БП (зафиксированным на первом уровне).

Третий уровень – корреляционный. Определяет перечень и состав контрольных точек БП.

Контрольная точка – взаимосвязь логических блоков БП, правил их выполнения и требований к результатам, а также соответствующий им набор событий и данных в информационных системах, являющихся частью паттерна информационных артефактов. Совокупность контрольных точек БП и взаимосвязанных с ними логических блоков и правил, событий и данных в информационных системах формируют модель корреляции – один из основных элементов, входящих в состав информационной модели БП.

Метод обеспечения безопасности бизнес-процессов на основе построенной информационной модели базируется на возможности выявлять нарушения в процессах по их следам в информационной инфраструктуре. Опишем его суть.

- Нарушения выявляются сравнением фактической логики выполнения БП (т.е. отдельной итерации) с заданной логикой.
- Так как заданная логика однозначно определяется паттерном информационных артефактов, то наложение паттерна на их текущую базу покажет отклонения фактической логики выполнения бизнес-процесса (отдельной итерации) от заданной. В зависимости от необходимой степени детализации в качестве паттерна информационных артефактов можно использовать либо паттерн БП, либо паттерн пользователя БП. В последнем случае следует более точно задать границы логики, соответствующие выполнению бизнес-процесса определенным пользователем с учетом особенностей его работы в конкретных информационных системах, и тем самым выявлять нарушения, связанные с подменой пользователя.
- Использование модели корреляции при наложении паттерна БП/пользователя БП на текущую базу информационных артефактов позволяет на уровне логов информационных систем сформировать предикты (выражения, описывающие экстраполяцию состояний) по возможным отклонениям и, соответственно, предотвратить

нарушения в бизнес-процессе – реализовать контрольную среду. Информационная модель БП позволяет автоматизировать выявление и предотвращение нарушений на основе платформы обеспечения здоровья БП: информационный и корреляционный уровни формируют логику работы платформы, логический уровень — является интерфейсом между внутренней логикой работы платформы и оператором/пользователем платформы.

Алгоритм обеспечения безопасности БП представляет непрерывный цикл, включающий указанные выше три шага. Непрерывность этого цикла обеспечивается, с одной стороны, функционирующей платформой обеспечения здоровья БП, с другой – процессом обеспечения безопасности БП, реализуемым в компании.

Численным показателем здоровья бизнес-процесса служит метрика, отражающая отсутствие отклонений от заданной логики и определяемая отношением количества итераций БП, выполненных без нарушений, к общему числу итераций БП за определенный интервал времени.

Другим эквивалентным показателем здоровья бизнес-процесса будет отношение количества его итераций (шагов) без нарушений за заданный период к общему количеству итераций БП за тот же период.

Предложенная метрика здоровья БП может быть уточнена. Возможна, например, такая ситуация, что будет иметь место одно отклонение из ста, но очень серьезное, которое приведет к существенному нарушению на выходе (простой пример – вброс в финансовую систему платежного документа задним числом. При этом очевидное, лежащее на поверхности, решение – добавить в метрику коэффициент серьезности отклонения, который формируется заказчиком по анкете – «несерьезное», «среднее», «серьезное» [14-15].

Архитектура платформы является универсальной для любого бизнес-процесса и не зависит от перечня и количества поддерживаемых им информационных систем. С точки зрения архитектуры на базе одной платформы можно реализовать (масштабировать) контрольную среду и устойчивое к мошенничеству состояние для неограниченного количества БП.

5. Пример применения платформы обеспечения здоровья бизнес-процесса

Представим бизнес-процесс на двух уровнях – уровне логики и уровне информации [16-17].

Уровень логики

1. Клиент отгружает логистической компании товар для последующей доставки конечным покупателям. При этом груз приходит одной машиной, например, в 10 000 товарных мест. С грузом идет одна товарно-транспортная накладная (ТТН), в которой описан весь груз.

2. Склад принимает груз, деконсолидирует его для отправки в сортировочные центры, где его деконсолидируют до уровня единицы груза.

3. Склад сортирует единицы груза и создает на каждую единицу груза – единицу накладной. Вносит в нее дополнительную стоимость, например, сумму страховки.

4. Склад выдает единицу груза курьеру для доставки.

5. Курьер осуществляет доставку, принимает денежные средства, выписывает (пробивает) кассовый чек, сдает деньги в бухгалтерию.

6. Бухгалтерия консолидирует суммы, полученные от курьеров, и отправляет их на счет клиента.

7. Клиент осуществляет сверку стоимости отгруженного товара (ТТН из п. 1) и полученной суммы (п. 6), в случае расхождения сумм клиент выставляет претензию, а логистическая компания ее оплачивает.

Уровень информации (представление процесса на уровне событий в информационной сети логистической компании)

1. По электронной почте клиент отправляет логистическому оператору сообщение, содержащее количество единиц товара и сумму. После утверждения этих данных в переписке клиент отправляет на интерфейс логистического оператора файл-реестр с содержанием количества единиц груза, стоимостью каждой единицы и адресом доставки

2. Логистический оператор принимает файл-реестр и конвертирует его в формат, понятный системе обработки документов логистического оператора, которая разбивает общий реестр на логические единицы, соответствующие единицам груза, и по признакам адреса определяет правила их пересылки и обработки на складах.

3. Система обработки документов создает электронную накладную для каждой единицы груза, присваивая дополнительные поля по совокупности признаков (например, наложенный платеж, сумма страховки или надбавка за срочную доставку по просьбе клиента).

4. Электронная накладная загружается в коммуникатор курьера. Формируется маршрутный лист.

5. Курьер ставит признак «доставлено», коммуникатор передает информацию на мобильную кассу, печатающую чек, в котором общая сумма платежа разбита по различным секциям учета.

6. Бухгалтерская система консолидирует платежную информацию. По всем счетам проводит зачисления и формирует платежные поручения для банка в пользу клиента.

7. Происходит обмен реестрами по электронной почте.

Может показаться, что бизнес-процесс довольно прост. Однако на практике в нем постоянно происходят инциденты. Базовые нарушения при конвертации реестров на интерфейсе логистического оператора, такие как некорректные символы, дополнительные поля и т.д., приводят к тому, что значения в системе обработки документов отличаются от значений в файле-реестре. В результате значение суммы не соответствует фактическому и делятся на два типа – недостаточная сумма/недостаточные условия доставки и избыточная сумма/избыточные условия доставки. Первый тип ошибок выясняется на этапе сверки с клиентом. Инциденты второго типа вызывают конфликт с конечным получателем, который не готов платить больше. Эти инциденты выясняются сразу по мере возникновения. Для их обработки существует процесс коррекции сумм в накладных, однако он не автоматизирован, а количество накладных с потенциальной ошибкой может исчисляться в тысячах единиц. При этом создаются ошибки второго уровня – ошибки ввода оператором новых значений. Помимо репутационных потерь логистический оператор теряет на подобных коллизиях до 2% от всей выручки (суммы, которые он получает в счет оплаты груза от конечного получателя).

Уровень корреляции в данном случае работает по принципу вычисления сверки общей суммы и последующего вычисления суммы всех значений логических единиц, которые появляются после обработки реестра в режиме реального времени на всех этапах процесса, включающего работу операторов по корректировке. В том случае, если сумма перестает совпадать с эталоном, система блокирует дальнейшие действия с накладными до успешной корректировки.

На рис. 2 показана схема, иллюстрирующая описанный процесс внутреннего контроля в логистике и обеспечение здорового логистического бизнес-процесса.

Рис. 2. Внутренний контроль накладных в логистике (обеспечение здорового логистического бизнес-процесса)
(Fig. 2. Internal control of invoices in logistics (ensuring a healthy logistics business process))

Заключение

Статические методы корректировки бизнес-процессов перестают работать в условиях быстро развивающейся среды. Нужны динамические методы анализа и корректировки бизнес-процессов (БП). Для решения этой задачи был предложен подход формирования модели здоровья БП, на основании которого можно строить платформу обеспечения здоровья БП.

С точки зрения системно-аналитического подхода эта платформа представляет собой информационно-аналитическую систему [20], формирующую новое свойство – здоровье бизнес-процесса, направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне процесса, а также формирования контрольной среды БП.

Целью внедрения платформы обеспечения здоровья БП является снижение потенциальных потерь (как прямых, так и косвенных), связанных с нарушениями в БП, посредством формирования контрольной среды – предиктивности (предсказательности) к нарушениям и обеспечения качества и стабильности БП (отсутствия нарушений).

Ключевые преимущества платформы: повышение качества результата бизнес-процесса и формирование устойчивости к его отклонениям.

СПИСОК ЛИТЕРАТУРЫ:

1. Колин К.К. Эволюция информатики //Информационные технологии. – 2005. №1. С. 2–16.
2. Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения". – СТО БР ИББС-1.0-2014" (введен в действие Распоряжением Банка России от 17.05.2014 №Р-399). URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (дата обращения: 12.08.2019).
3. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств". – СТО БР ИББС-1.3-2016". URL: https://www.cbr.ru/content/document/file/46920/st-13-16.pdf (дата обращения: 12.08.2019).
4. Биктимиров М.Р., Щербаков А.Ю. Избранные главы компьютерной безопасности. – Казань: Изд-во Казанского матем. общества, 2004. – 372 с.
5. Абдеев Р.Ф. Философия информатизационной цивилизации. – М.: ВЛАДОС, 1994. – 336 с.
6. Gloning T., Fritz G. (Hrsg.): Digitale Wissenschaftskommunikation – Formate und ihre Nutzung. 2011. Gießen: Gießener elektronische Bibliothek. Abgerufen am 27. Mai 2014.
7. Voshmgir Sh. Blockchains, smart contracts und das dezentrale Web. 2016. Technologie Stiftung Berlin.
8. Михайлов А.И., Черный А.И., Гиляревский Р.С. Основы информатики. – М.: Наука, 1968. – 756 с.
9. Михайлов А.И., Черный А.И., Гиляревский Р.С. Научные коммуникации и информатика. – М.: Наука, 1976. – 435 с.
10. Колин К.К. Природа информации и философские основы информатики. Открытое образование. 2005. №2. С. 43–51.
11. Эпштейн В.Л. Антропоцентрическое информационное взаимодействие (вопросы терминологии)// Проблемы управления. 2003. № 1. С. 28–33.
12. Шемакин Ю.И. Семантика самоорганизующихся систем. – М.: Академический проект, 2003. – 176 с.
13. Правиков Д.И., Щербаков А.Ю. Новая парадигма информационной безопасности: взгляд основоположников //Актуальные вопросы науки и техники. Вып. 5. Сборник научных трудов по итогам международной научно-практической конференции (11 апреля 2018 г.), Самара, 2018.
14. Mainelli M., von Gunten C. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. 2014. A Long Finance report prepared by Z/Yen Group.
15. McKinsey & Company. Beyond the Hype: Blockchains in Capital Markets.
16. Hagenhoff S., Seidenfaden L., Ortelbach B., Schumann M. Neue Formen der Wissenschaftskommunikation. Eine Fallstudienuntersuchung. Göttingen, 2007, S. 5f.
17. Dernbach B., Kleinert C., Münder H. (Hrsg.): Handbuch Wissenschaftskommunikation. Wiesbaden, 2012.
18. Codd E.F. A Relational Model of Data for Large Shared Data Banks. Communications of the ACM, v. 13, n. 6, June, 1970.
19. Schlatt V., Schweizer A., Urbach N., Fridgen G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
20. Рязанова А.А. Технология блокчейн в научно-информационной деятельности // Научно-техническая информация. Сер.1. – 2018. № 4. С. 8–12.

REFERENCES:

[1] Kolin K.K. the Evolution of computer science. Information technology. - 2005. №1. P. 2–16 (in Russian).
[2] Standard of The Bank of Russia "Information security of organizations of the banking system of Russian Federation. Generalities" - STO BR IBBS-1.0-2014" (introduced by the order of the Bank of Russia from 17.05.2014 №P-399). URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (accessed: 12.08.2019) (in Russian).
[3] Standard of The Bank of Russia “Collection and analysis of technical data in response to information security incidents in the implementation of money transfers”. - STO BR IBBS-1.3-2016. URL: https://www.cbr.ru/content/document/file/46920/st-13-16.pdf (accessed: 12.08.2019) (in Russian).
[4] Biktimirov M.R., Shcherbakov A.Yu. Elected heads of computer security. – Kazan: publishing House of Kazan Matem. societies, 2004. – 372 p. (in Russian).
[5] Abdeev R.F. Philosophy of civilization.– M.: VLADOS, 1994. – 336 p. (in Russian).
[6] Gloning T., Fritz G. (Hrsg.): Digitale Wissenschaftskommunikation – Formate und ihre Nutzung. 2011. Gießen: Gießener elektronische Bibliothek. Abgerufen am 27. Mai 2014.
[7] Voshmgir Sh. Blockchains, smart contracts und das dezentrale Web. 2016. Technologie Stiftung Berlin.
[8] Mikhailov A.I., Chernyi A.I., Gilyarevskyi R.S. Foundations of computer science. – M.: Publishing house "Science". 1968. – 756 p. (in Russian).
[9] Mikhailov A.I., Chernyi A.I., Gilyarevskyi R.S. Scientific communications and Informatics. – M.: Publishing house "Science". 1976. – 435 p. (in Russian).

[10] Colin K.K. Nature of information and philosophical foundations of Informatics. Open education. 2005. №2. P. 43–51 (in Russian).
[11] Epstein V.L. Anthropocentric information interaction (questions of terminology). Problems of management. 2003. № 1. P. 28–33 (in Russian).
[12] Shemakin Yu.I. Semantics of self-organizing systems. – M.: Academic project, 2003. – 176 p. (in Russian).
[13] Pravikov D.I., Shcherbakov, A.Yu. A new paradigm to information security: a view of the founders of the Topical issues of science and technology. Issue. 5. Collection of scientific papers on the results of the international scientific-practical conference (April 11, 2018), Samara, 2018 (in Russian).
[14] Mainelli M., von Gunten C. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. 2014. A Long Finance report prepared by Z/Yen Group.
[15] McKinsey & Company. Beyond the Hype: Blockchains in Capital Markets.
[16] Hagenhoff S., Seidenfaden L., Ortelbach B., Schumann M. Neue Formen der Wissenschaftskommunikation. Eine Fallstudienuntersuchung. Göttingen, 2007. S. 5f.
[17] Dernbach B., Kleinert C., Münder H. (Hrsg.): Handbuch Wissenschaftskommunikation. Wiesbaden, 2012.
[18] Codd E.F. A Relational Model of Data for Large Shared Data Banks. Communications of the ACM, v. 13, n. 6, June, 1970.
[19] Schlatt V., Schweizer A., Urbach N., Fridgen G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
[20] Ryazanova A. A. Blockchain Technology in scientific and information activities. Scientific and technical information. Ser.1. – 2018. № 4. P. 8–12 (in Russian).

Поступила в редакцию – 06 июня 2019 г. Окончательный вариант – 15 августа 2019 г.
Received – Juny 06, 2019. The final version – August 15, 2019.

Татьяна М. Каннер
ЗАО «ОКБ САПР»,
2-й Кожевнический пер., 12, Москва, 115114, Россия
e-mail: tatianash@okbsapr.ru, https://orcid.org/0000-0002-3210-2090

ОСОБЕННОСТИ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2019.2.02

Аннотация. В статье рассматривается программа повышения квалификации, позволяющая слушателям получить знания и навыки в области обеспечения безопасности критической информационной инфраструктуры (КИИ). Программа разъясняет действия государственных органов, учреждений и других организаций при реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Целью статьи является описание особенностей реализации предлагаемой программы повышения квалификации. Приводится состав программы, формы проведения, типы занятий, состав итоговой аттестации, типы документов о прохождении повышения квалификации. Описываются особенности требований к образованию слушателей, поступающих на обучение, а также особенности преподавания программы и взаимодействия со слушателями в рамках курса. Особое внимание уделяется содержащимся в программе практическим вопросам, связанным с организацией защищенной сетевой коммуникации между элементами критической информационной инфраструктуры с применением микрокомпьютеров «m-TrusT». В результате успешного освоения программы слушатели получают удостоверения установленного образца, применяя полученную на курсе информацию, могут организовывать работы по категорированию своих объектов КИИ и реализации требований ФЗ №187 к ним.

Ключевые слова: критические информационные инфраструктуры, КИИ, повышение квалификации по технической защите информации, повышение квалификации в области обеспечения безопасности КИИ, микрокомпьютер «m-TrusT».
Для цитирования: КАННЕР, Татьяна М. ОСОБЕННОСТИ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 22-31, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1214>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.02.

Tatiana M. Kanner
"OKB SAPR",
2nd Kozhevnichesky lane, 12, Moscow,115114, Russia
e-mail: tatianash@okbsapr.ru, https://orcid.org/0000-0002-3210-2090

Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2019.2.02

Abstract. The article considers the program of professional development that allows to gain the necessary knowledge and abilities in the field of safety of the critical information infrastructure (CII). This program explains actions of public authorities, institutions and other organizations for fulfilling the requirements of the Federal law of July 26, 2017 No. 187 "About safety of critical information infrastructure of the Russian Federation". The purpose of the article is to describe the features of implementation of the offered program for advanced training. The structure of the program, the form and types of advanced training, structure of the final assessment, types of qualification documents are given. The article also

describes the educational requirements for students entering and features of teaching the program and interaction with students within a course. Special attention is paid to the practical issues contained in the program related to the organization of secure network communication between elements of the critical information infrastructure using “m-TrusT” microcomputers. As a result of successful mastering of the program, students receive standard certificates and with information obtained on the course could organize works on categorization of the objects of the CII’s and fulfill the requirements of Federal Law No. 187 for them.

Keywords: critical information infrastructure, CII, advanced training in the field of technical information security, advanced training in the field of ensuring safety for CII, “m-TrusT” microcomputers.

For citation: KANNER, Tatiana M. Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure. IT Security (Russia), [S.l.], v. 26, n. 3, p. 22-31, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1214>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.02.

Введение

В настоящее время все большую актуальность набирает необходимость получения дополнительного профессионального образования в области критических информационных инфраструктур (КИИ) путем повышения квалификации по данному направлению. Это связано с вступлением в силу 1 января 2018 г. Федерального закона (ФЗ) от 26 июля 2017 г. ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1]. Данный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (РФ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В приведенном законе к объектам КИИ отнесены [1]:

- информационные системы;
- информационно-телекоммуникационные сети;
- автоматизированные системы управления технологическим процессом субъектов КИИ.

А к субъектам отнесены государственные органы, государственные учреждения, российские юридические лица и/или индивидуальные предприниматели, которым на правах собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в 13 сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности, химической промышленности, а также – российские юридические лица и/или индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [1].

В рассматриваемом ФЗ №187 действия субъектов КИИ относительно их объектов описаны достаточно подробно. Также в настоящее время издан ряд дополняющих данный закон нормативных документов, которые уточняют все требуемые действия. При этом необходимо отметить, что для большинства организаций КИИ, приведенные в данных документах действия, представляются трудными для внедрения в процесс обеспечения безопасности своих объектов критических информационных инфраструктур. Например, в соответствии с требованиями закона, субъекты КИИ должны определить относятся ли их объекты к объектам КИИ, после чего сообщить об этом во ФСТЭК России. Это значит, что субъекты КИИ должны либо присвоить одну из категорий значимости своим объектам, либо не присвоить ни одну из категорий, если объект КИИ не соответствует

критериям значимости. Используемые для этого правила категорирования объектов КИИ утвержденны постановлением Правительства РФ от 8 февраля 2018 года №127 [2]. Данные правила позволяют провести категорирование объектов КИИ. Однако в этих правилах множество различных показателей определения категории, что усложняет выбор правильного варианта [3].

Помимо этого, в соответствии с данным ФЗ необходимо интегрироваться в ГосСОПКА – государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. В законе не приводятся действия субъектов КИИ по обеспечению встраивания в ГосСОПКА. Эту информацию можно получить из приказов ФСБ России №367 и №368 от 24 июля 2018 г. [4, 5], регламентирующих перечень и порядок предоставления информации субъектами КИИ в ГосСОПКА, а также порядки обмена информацией о компьютерных инцидентах субъектами КИИ (в том числе иностранными учреждениями и организациями) и получения ими информации о средствах и способах проведения компьютерных атак и методах их предупреждения и обнаружения. Однако данные документы содержат множество специализированных нюансов, доступных только специалистам в области обеспечения безопасности КИИ [3].

Также, следуя закону ФЗ №187, субъекты КИИ должны соблюдать требования по обеспечению безопасности значимых объектов КИИ, утвержденные Приказом ФСТЭК России от 21 декабря 2017 г. №235 [6]. В требованиях рассматриваются этапы обеспечения безопасности значимых объектов КИИ, включающие планирование, разработку, реализацию необходимых мероприятий, контроль состояния и совершенствование их безопасности. Несмотря на то, что данные требования достаточно конкретные, начинающему специалисту в области КИИ сложно определить, например, какие именно средства защиты подходят для его системы. Понимание данных вопросов можно приобрести путем изучения примеров различных объектов КИИ, разбора требований к их средствам обеспечения безопасности и выбора конкретного средства защиты в каждом случае.

Из рассмотренного выше видно, что большинству субъектов критических информационных инфраструктур, даже после изучения соответствующих приказов и постановлений, в связи с наличием множества вопросов будет достаточно сложно самостоятельно провести категорирование объектов КИИ, организовать работы по интеграции в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и обеспечению безопасности объектов КИИ в соответствии с требованиями федерального закона №187. Получить соответствующие знания, навыки и умения, которые могут ответить на все эти вопросы, позволяет прохождение курса повышения квалификации в области обеспечения безопасности критических информационных инфраструктур [3].

В связи с этим ОКБ САПР совместно с Московским физико-техническим институтом (МФТИ) реализует программу повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

В данной статье рассматриваются особенности предлагаемой программы повышения квалификации специалистов по обеспечению безопасности значимых объектов КИИ, связанные с ее реализацией в соответствии с требованиями ФСТЭК России к программам повышения квалификации, а также с приобретением дополнительных компетенций, необходимых при реализации этих требований на реальных объектах критических информационных инфраструктур.

Основная часть

Одной из важных особенностей реализации предлагаемой «ОКБ САПР» совместно с МФТИ программы повышения квалификации является ее разработка в соответствии с «Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации», утвержденными ФСТЭК России 16 апреля 2018 г., и примерной программой повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры», утвержденной ФСТЭК России 17 декабря 2018 г. Разработка программы в соответствии с приведенными документами от ФСТЭК означает, что все положения, модули и темы программы утверждены регуляторами и соответствуют законодательству РФ. Поэтому полученные в рамках курса знания могут быть на законном основании применены субъектами КИИ для реализации требований ФЗ №187 в действительности.

Помимо этого, следует обратить внимание на особенность, связанную с необходимостью планового/внепланового прохождения курсов повышения квалификации. Слушатели могут пройти обучение при появлении потребности совершенствования или получения новых компетенций в области обеспечения безопасности КИИ, или при плановом повышении квалификации специалистов, ответственных за обеспечение технической защиты информации. Необходимость планового повышения квалификации через определенный период, как известно, связана с правилами, приведенными в постановлении Правительства РФ от 6 мая 2016 г. №399 «Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса» [7]. В соотвествии с данными правилами все федеральные государственные органы, органы государственной власти субъектов РФ, органам местного самоуправления, организациям с государственным участием и организациям оборонно-промышленного комплекса должны проходить повышение квалификации через определенный период времени.

Перед подачей заявки на зачисление на курс необходимо обратить внимание на немаловажную особенность проведения программы – достаточно высокие требования к квалификации поступающих на курс слушателей. Предполагается обучение только тех специалистов, которые имеют высшее образование или диплом о профессиональной переподготовке в области информационной безопасности. Однако это оправдано, так как для освоения рассматриваемого в программе материала они уже должны обладать базовыми знаниями в области информационной безопасности. В этом случае при успешном завершении курса слушатели получают удостоверение МФТИ установленного образца о повышении квалификации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. При этом необходимо отметить, что слушатель, не имеющий требуемого образования, также может пройти обучение, но под свою персональную ответственность, так как в процессе обучения, не обладая требуемыми знаниями в области информационной безопасности, он должен будет получить их самостоятельно с целью понимания преподаваемого материала. В этом случае по завершении обучения слушатели получают справку с подтверждением прохождения курса, а не удостоверение как слушатели с требуемым образованием.

Еще одной важной особенностью реализации рассматриваемой программы повышения квалификации является ее состав. Предлагаемая программа включает три базовых модуля, рассматривающих основы обеспечения безопасности значимых объектов КИИ, организацию работ по обеспечению безопасности значимого объекта КИИ и контроль за обеспечением безопасности значимого объекта КИИ. При этом в состав программы также входит четвертый специализированный модуль. В этом модуле рассматривается организация защищенной сетевой коммуникации между элементами КИИ с применением разработанных «ОКБ САПР» микрокомпьютеров «m-Trust» [8, 9] – одноплатных компьютеров Новой гарвардской архитектуры [10, 11]. Данный модуль включает большое количество практических и лабораторных работ, что позволит слушателям ознакомиться и научиться применять указанные средства защиты информации (СЗИ) для организации защищенной сетевой коммуникации своих объектов КИИ.

В рамках четвертого модуля рассматривается понятие резидентного компонента безопасности (РКБ) [12, 13], идея которого заложена в «m-Trust». Разбираются ключевые характеристики РКБ, применение РКБ для обеспечения доверенной загрузки операционной системы средства вычислительной техники [14], реализации криптографических алгоритмов (шифрование и подпись), защищенного хранения неизвлекаемых криптографических ключей, ведения неперезаписываемых журналов событий [15, 16], генерации случайных последовательностей. Рассматривается понятие интеграционной платформы «МК-И». Описываются типовые характеристики и параметры микрокомпьютеров «m-TrusT». Приводятся варианты интерфейсных плат, позволяющих коммутировать микрокомпьютер «m-TrusT» в «разрыв» между подконтрольными объектами различного назначения и каналом связи. Большое внимание уделяется особенностям построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT», а также разбираются примеры построения такой коммуникации.

Наличие данного модуля дает возможность слушателям в результате освоения рассматриваемой программы повышения квалификации приобрести новые компетенции, связанные с применением микрокомпьютеров «m-TrusT» для организации защищенного сетевого взаимодействия между элементами КИИ. Такие компетенции являются дополнительными к базовым, определенным в одноименной примерной программе, утвержденной ФСТЭК России, и получаемым в ходе обучения на первых трех модулях рассматриваемой программы. Так, в рассматриваемой программе повышения квалификации к базовым компетенциям добавляются следующие:

а) к общепрофессиональным – способность пользоваться документацией на микрокомпьютеры «m-TrusT»;

б) к профессиональным:

- в организационно-управленческой деятельности:

– способность планировать и разрабатывать мероприятия по обеспечению безопасности сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– способность реализовывать (внедрять) мероприятия по организации защищенной сетевой коммуникации между элементами КИИ при помощи микрокомпьютеров «m-TrusT»;

- в проектной деятельности – способность разрабатывать предложения по построению защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

- в эксплуатационной деятельности – способность устанавливать, настраивать и осуществлять администрирование микрокомпьютерами «m-TrusT».

При этом в результате освоения данной программы повышения квалификации, обучающиеся должны получить знания, умения и навыки, также являющиеся дополнительными к базовым, определенным в одноименной примерной программе.

Освоившие четвертый модуль должны:

а) знать:

– основы понятия резидентного компонента безопасности: концепцию корректного старта и путь ее развития в истории эволюции средств вычислительной техники и средств защиты информации;

– характеристики и возможности резидентного компонента безопасности;

– характеристики, особенности настройки и применения микрокомпьютеров «m-TrusT»;

– характеристики интерфейсных плат для подключения микрокомпьютеров «m-TrusT» к различным подконтрольным объектам и каналообразующей аппаратуре;

– особенности построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– примеры построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– особенности работы и обновления ключевой системы микрокомпьютеров «m-TrusT»;

б) уметь:

– определять тип необходимой для конкретного подконтрольного объекта и каналообразующей аппаратуры интерфейсной платы подключения микрокомпьютера «m-TrusT»;

– определять необходимый в конкретной ситуации состав программного обеспечения активной части «m-TrusT»;

– применять микрокомпьютеры «m-TrusT» для построения защищенной сетевой коммуникации между элементами КИИ;

– работать с ключевой системой «m-TrusT» и уметь ее обновлять;

в) владеть навыками установки, настройки и применения микрокомпьютеров «m-TrusT» для обеспечения защищенного сетевого взаимодействия между элементами КИИ.

Первые три модуля программы обеспечивают формирование базового уровня знаний, умений, навыков и компетенций у слушателей, необходимых им для профессиональной деятельности в области обеспечения безопасности значимых объектов КИИ. Однако в базовых модулях уделяется внимание обеспечению безопасности объектов КИИ в общем, без рассмотрения конкретных средств защиты, которые можно применять для данной цели. Четвертый модуль включает ряд семинаров, практических и лабораторных занятий, позволяющих познакомиться со средством защиты сетевого взаимодействия между элементами КИИ (микрокомпьютером «m-TrusT») в действительности и получить практический опыт его применения. За счет этого приобретаемые на курсе знания, навыки и умения позволяют слушателям получить всестороннее представление об обеспечении безопасности значимых объектов КИИ в целом, а также освоить практическую сторону данного вопроса. Тем самым наличие дополнительного, четвертого модуля в программе позволяет обеспечить полноту компетенций, необходимых слушателям в области обеспечения безопасности значимых объектов КИИ.

Особенностью реализации программы также является наличие различных форм ее проведения. В базовом варианте рассматриваемая программа построена по очно-заочному принципу с применением электронного обучения и дистанционных образовательных технологий.

Взаимодействие со слушателями по теоретическим вопросам курса (лекции, занятия в режиме круглого стола) осуществляется дистанционно с помощью системы управления образовательным процессом на базе Moodle (СДО – система дистанционного образования). Как правило, при проведении обучения лекции чередуются с занятиями в режиме круглого стола – в конце каждой лекции преподаватель выдает самостоятельные задания (изучить литературу/написать небольшой реферат на одну из тем лекций или вообще на не затронутую на лекции тему/решить какую-то задачу/выполнить какие-либо практические действия), а на занятиях в режиме круглого стола проверяет выполнение задания, отвечает на возникшие вопросы, обсуждает ошибки, особенности, правильное решение и тому подобное.

Взаимодействие со слушателями курса по практическим вопросам курса (семинары, практические занятия, лабораторные работы) осуществляется в виде аудиторных занятий. Аудиторные занятия проходят в рамках нескольких очных сессий, которые, как правило, назначаются на длинные выходные, выпадающие на праздничные дни (например, на новогодние каникулы или праздники в феврале, марте или мае). На таких занятиях преподаватель в том числе демонстрирует рассматриваемые в рамках курса СЗИ на практике и предоставляет возможность поработать с ними самостоятельно, отвечает на возникшие вопросы и помогает решить поставленные задачи.

При отсутствии возможности принять участие в очной сессии слушатели могут проходить практические и лабораторные занятия удаленно, под контролем преподавателя. Для этого «ОКБ САПР» заранее выдает слушателям во временное пользование все необходимое для участия в занятиях программное обеспечение и оборудование. На очных занятиях такие слушатели присутствуют удаленно (через Skype) и принимают в них полноценное участие.

Важно отметить, что как при заочном взаимодействии во время лекций и занятий в режиме круглого стола, так и при вынужденном удаленном выполнении практических и лабораторных работ возможности взаимодействия слушателя и преподавателя достаточно хорошо приближены к очной форме, так как при использовании системы дистанционного обучения слушатели видят преподавателя, использующего веб-камеру, на своих экранах, слышат – через гарнитуру, могут задавать вопросы как голосом (при наличии аналогичной гарнитуры), так и письменно в специально предназначенном для этого в СДО форуме. Для проведения занятий преподаватели могут использовать:

– презентации;

– электронную доску (писать маркером на белом электронном листе, аналогично тому, как это можно сделать в графическом редакторе рисунков);

– белый лист бумаги с дополнительной веб-камерой, транслирующей в реальном времени то, что пишет преподаватель на этом листе при помощи обычной ручки или карандаша (как замена магнитно-маркерной доски);

– предоставление слушателям общего доступа к компьютеру преподавателя («расшаривание» рабочего стола) для демонстрации практической части занятий.

Описанная форма проведения занятий предполагает обучение слушателей без отрыва от основной работы. Однако при необходимости, по желанию организации, возможно проведение очного обучения, с полным отрывом слушателей от работы – очная форма обучения. В этом случае сократится длительность обучения, и слушатели освоят

программу за более короткий срок. Как видно из вышеописанного, слушатели могут принять участие в обучении в любой удобной для них форме.

По завершении занятий «ОКБ САПР», вне зависимости от выбранной формы проведения занятий, выполняет итоговое тестирование слушателей по изученному материалу. В случае успешного прохождения итогового тестирования, слушатели, как уже было указано выше, получают удостоверение МФТИ установленного образца о повышении квалификации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры (либо справку о прохождении курса, при отсутствии требуемого образования).

Заключение

Предлагаемая «ОКБ САПР» совместно с МФТИ Программа повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» разработана в соответствии с официальными требованиями ФСТЭК России, изложенными в методических рекомендациях по разработке программ повышения квалификации и соответствующей примерной программой повышения квалификации. То есть в содержании программе разбираются все требования ФЗ №187 и все дополняющие его нормативные документы, а ее положения, модули и темы утверждены ФСТЭК России. Поэтому полученные на курсе знания позволяют субъектам КИИ применять их для своих объектов КИИ без колебаний относительно корректности с точки зрения регулятора.

Программа содержит высокие требования к квалификации поступающих на курс слушателей – они должны иметь высшее образование или диплом о профессиональной переподготовке в области информационной безопасности. В результате обучения после успешного прохождения итогового тестирования слушатели получают удостоверение МФТИ установленного образца. Слушатели, не имеющие такого образования, также могут пройти обучение и итоговое тестирование, но без получения такого удостоверения (выдается справка с подтверждением прохождения курса).

Предлагаемая программа включает четыре модуля, три базовых с основными знаниями в области безопасности КИИ и один специализированный. Последний в основном состоит из практических и лабораторных работ, позволяющих научиться организовывать и обеспечивать защищенные сетевые коммуникации объектов КИИ с применением микрокомпьютеров «m-TrusT» производства «ОКБ САПР». Наличие такого модуля дает возможность слушателям в результате освоения рассматриваемой программы повышения квалификации помимо базовых также приобрести новые знания, умения и навыки и получить новые компетенции, связанные с применением микрокомпьютеров «m-TrusT» для организации защищенного сетевого взаимодействия между элементами КИИ. В связи с этим в результате обучения слушатели получают всестороннее представление об обеспечении безопасности значимых объектов КИИ в целом, в том числе и практической стороне данного вопроса.

При реализации программы предусмотрено несколько форм ее проведения (очно-заочная, очная). При очно-заочной форме возможно удаленное прохождение практических и лабораторных занятий. Слушатели в зависимости от наличия/отсутствия возможности и желания полного отрыва от работы могут принять участие в обучении в любой удобной для них форме.

Подводя итог статьи, необходимо отметить, что актуальность рассматриваемой программы основана на необходимости повышения квалификации в области безопасности

критических информационных инфраструктур, понятие которых появилось в РФ совсем недавно при вступлении в силу Федерального закона № 187-ФЗ. Предлагаемая программа повышения квалификации позволяет получить как базовые, так и дополнительные знания, навыки и умения в области обеспечения безопасности критической информационной инфраструктуры, подтвержденные удостоверением МФТИ установленного образца. А на основании полученной на курсе информации – организовать работы по категорированию своих объектов КИИ и реализации требований ФЗ №187 к ним.

СПИСОКЛИТЕРАТУРЫ:

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ// Государственная дума. 2017. – 20 с.
2. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства Российской Федерации от 8 февраля 2018 г. №127 // Правительство Российской Федерации. 2018. – 11 с.
3. Каннер Т.М. Повышение квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры // Материалы XXIV научно-практической конференции «Комплексная защита информации», Витебск: ВГТУ, 21–23 мая, 2019. С. 186–191.
4. Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА: Приказ ФСБ Российской Федерации от 24 июля 2018 г. №367 // ФСБ Российской Федерации. 2018. – 10 с.
5. Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения: Приказ ФСБ Российской Федерации от 24 июля 2018 г. №368 // ФСБ Российской Федерации. 2018. – 7 с.
6. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ ФСТЭК России от 21 декабря 2017 г. № 235 // ФСТЭК России. 2017. – 10 с.
7. Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса: Постановление Правительства Российской Федерации от 06 мая 2016 г. №399 // Правительство Российской Федерации. 2016. – 2 с.
8. Конявская С.В. Защищенные сетевые коммуникации не требуют «зоопарка» // Национальный банковский журнал. 2018. № 10. С. 92–93.
9. Конявская С.В. Защита сетевой коммуникации: «зоопарк» с человеческим лицом // Инсайд. Защита информации. 2018. № 5. С. 38–41.
10. Конявский В.А. Иммунитет как результат эволюции ЭВМ // Инсайд. Защита информации. 2017. № 4. С. 46–52.
11. Конявский В.А., Конявская С.В. Доверенные информационные технологии: от архитектуры к системам и средствам. Москва: URSS, 2019. – 264 с.
12. Конявский В.А. Доверенные системы как средство противодействия киберугрозам. Базовые понятия // Information Security/Информационная безопасность. 2016. № 3. С. 40–41.
13. Алтухов А.А. Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности // Материалы XX научно-практической конференции «Комплексная защита информации», Минск, 19–21 мая, 2015. С. 53–55.
14. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с.
15. Конявская С.В. Неперезаписываемый журнал событий: лайфхак для аудитора // Information Security/Информационная безопасность. 2018. № 1. С. 37.
16. Андреев В.М., Давыдов А.Н. Безопасное хранение журналов работы СЗИ // Материалы XX научно-практической конференции «Комплексная защита информации», Минск, 19 – 21 мая, 2015. С. 49–52.

REFERENCES:

[1] O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Federal'nyj zakon ot 26 ijulja 2017 № 187-FZ. Gosudarstvennaja duma. 2017. – 20 s. (in Russian).

[2] Ob utverzhdenii Pravil kategorirovanija ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnja pokazatelej kriteriev znachimosti ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij: Postanovlenie Pravitel'stva Rossijskoj Federacii ot 8 fevralja 2018 g. №127. Pravitel'stvo Rossijskoj Federacii. 2018. – 11 s. (in Russian).

[3] Kanner T.M. Povyshenie kvalifikacii specialistov, rabotayushchih v oblasti obespecheniya bezopasnosti znachimyh ob'ektov kriticheskoj informacionnoj infrastruktury [Professional development of the expert working in the field of security of significant objects of critical information infrastructure]. Materialy XXIV nauchno-prakticheskoj konferencii «Kompleksnaya zashchita informacii», Vitebsk: VGTU, 21–23 maya, 2019 [Proceedings of the scientific and practical conference "Complex Information Security", Vitebsk: VGTU, 21–23 May 2019]. Vitebsk, 2019. S. 186–191 (in Russian).

[4] Ob utverzhdenii Perechnja informacii, predstavljaemoj v GosSOPKA i Porjadka predstavlenija informacii v GosSOPKA: Prikaz FSB Rossijskoj Federacii ot 24 ijulja 2018 g. №367 FSB Rossijskoj Federacii. 2018. – 10 s. (in Russian).

[5] Ob utverzhdenii Porjadka obmena informaciej o komp'juternyh incidentah i Porjadka poluchenija sub#ektami KII informacii o sredstvah i sposobah provedenija komp'juternyh atak i o metodah ih preduprezhdenija i obnaruzhenija: Prikaz FSB Rossijskoj Federacii ot 24 ijulja 2018 g. №368. FSB Rossijskoj Federacii. 2018. – 7 s. (in Russian).

[6] Ob utverzhdenii trebovanij k sozdaniju sistem bezopasnosti znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i obespecheniju ih funkcionirovanija: Prikaz FSTJeK Rossii ot 21 dekabrja 2017 g. № 235. FSTJeK Rossii. 2017. – 10 s. (in Russian).

[7] Ob organizacii povyshenija kvalifikacii specialistov po zashhite informacii i dolzhnostnyh lic, otvetstvennyh za organizaciju zashhity informacii v organah gosudarstvennoj vlasti, organah mestnogo samoupravlenija, organizacijah s gosudarstvennym uchastiem i organizacijah oboronno-promyshlennogo kompleksa: Postanovlenie Pravitel'stva Rossijskoj Federacii ot 06 maja 2016 g. №399. Pravitel'stvo Rossijskoj Federacii. 2016. – 2 s. (in Russian).

[8] Konyavskaya S.V. The protected network communications do not demand "zoo". Nacional'nyj bankovskij zhurnal [The National bank magazine]. 2018, n. 10. S. 92–93 (in Russian).

[9] Konyavskaya S.V. Protection of network communication: "zoo" with a human face. Insajd. Zashhita informacii [Insider. Information security], 2018, n. 5. S. 38–41 (in Russian).

[10] Konyavskiy V. A. Immunity as result of evolution of the COMPUTER. Insajd. Zashhita informacii [Insider. Information security], 2017, n. 4. S. 46–52 (in Russian).

[11] Konyavskiy V.A., Konyavskaya S.V. The entrusted information technologies: from architecture to systems and tools. Moscow: URSS, 2019. – 264 s. (in Russian).

[12] Konyavskiy V.A. The entrusted systems as tools of counteraction to cyberthreats. Basic concepts. Information Security. 2016, n. 3. S. 40–41 (in Russian).

[13] Altukhov A.A. Neatomarnyj vzgljad na RKB kak na kompoziciju perehvata upravlenija i kontrolja celostnosti [Not atomic view of a SRC as on composition of interception of management and control of integrity]. Materialy XX nauchno-prakticheskoj konferencii «Kompleksnaja zashhita informacii», Minsk, 19–21 maya 2015 [Proceedings of the scientific and practical conference "Complex Information Security", Minsk 19–21 May 2015]. Minsk, 2015. S. 53–55 (in Russian).

[14] Konyavskiy V.A. Upravlenie zashhitoj informacii na baze SZI NSD «Akkord» [Management of information security on the basis of Accord-TSHM]. Moscow, Radio i svjaz' [Radio and communication], 1999. – 325 s. (in Russian).

[15] Konyavskaya S.V. Not re-recorded log: life hack for the auditor. Information Security. 2018. n. 1. P. 37 (in Russian).

[16] Andreev V.M. Davidov V.M. Bezopasnoe hranenie zhurnalov raboty SZI [Safe storage of DST work logs]. Materialy XX nauchno-prakticheskoj konferencii «Kompleksnaja zashhita informacii», Minsk, 19–21 maya 2015 [Proceedings of the scientific and practical conference "Complex Information Security", Minsk 19–21 May 2015]. Minsk, 2015. P. 49–52 (in Russian).

Поступила в редакцию – 10 июня 2019 г. Окончательный вариант – 16 августа 2019 г.
Received – June 10, 2019. The final version – August 16, 2019.

Роман А. Шарапов
Московский физико-технический институт,
Институтский пер., 9, г. Долгопрудный, 141701, Россия
e-mail: sharapov.roman@gmail.com, https://orcid.org/0000-0002-2378-0260

ХОЛОДНЫЙ МУЛЬТИВАЛЮТНЫЙ КОШЕЛЕК НА ПЛАТФОРМЕ МКТ

DOI: http://dx.doi.org/10.26583/bit.2019.2.03

Аннотация. В настоящей статье исследуется концепт реализации защищённого мультивалютного холодного кошелька на базе микрокомпьютера с динамически изменяемой архитектурой МКТ. Данное устройство создано на базе новой гарвадской архитектуры, модификации классической гарвардской архитектуры, с использованием неизменяемой памяти (для обеспечения целостности и неизменяемости операционной системы) и блоков сеансовой памяти (для обеспечения корректной работы программного обеспечения). В статье описывается механизм работы блокчейна и блокчейн-транзакций, рассмотрены основные принципы хранения криптовалют. Рассмотрена имплементация в систему алгоритма офлайн-подписи транзакций и протоколов, обеспечивающих иерархическую генерацию ключей по технологии HD Wallet. Предложено разделение функционала мультивалютного кошелька на две группы, предназначенные для исполнения либо в операционной системе, доступной только для чтения либо — доступной и для чтения, и для записи. Расписан сценарий исполнения рабочего цикла спроектированной системы.
Ключевые слова: Новая гарвардская архитектура, динамически изменяемая архитектура, блокчейн, офлайн-подпись транзакций, HD wallet.
Для цитирования: ШАРАПОВ, Роман А. ХОЛОДНЫЙ МУЛЬТИВАЛЮТНЫЙ КОШЕЛЕК НА ПЛАТФОРМЕ МКТ. Безопасность Информационных Технологий, [S.l.], v. 26, n. 3, p. 32-44, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1215>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.03.

Roman A. Sharapov
Moscow Institute of Physics and Technology,
Insitutskyy per., 9, Dolgoprudnyy, 141701, Russia
e-mail: sharapov.roman@gmail.com, https://orcid.org/0000-0002-2378-0260

Cold multi-currency wallet on the platform MKT

DOI: http://dx.doi.org/10.26583/bit.2019.2.03

Abstract. The paper is exploring the concept of implementing multi-currency secure cold wallet on the basis of the microcomputer with dynamically variable architecture MKT. This device is based on the new Harvard architecture, a modification of the classic Harvard architecture, using immutable memory (to ensure the integrity and immutability of the operating system) and session memory blocks (to ensure the correct operation of the software). The paper describes the work mechanism of blockchain and blockchain transactions, the basic principles of cryptocurrency storage. The implementation of the system algorithm for offline signing of transactions and protocols that provide a hierarchical key generation based on HD Wallet technology are reviewed. It is proposed to divide the functionality of the multi-currency wallet into two groups intended for execution either in the operating system that is read-only or available both for reading and writing. The scenario of execution of the working cycle of the designed system is described.
Keywords: New Harward architecture, dynamically variable architecture, blockchain, offline transaction signature, HD wallet.
For citation: SHARAPOV, Roman A. Cold multi-currency wallet on the platform MKT. IT Security (Russia), [S.l.], v. 26, n. 3, p. 32-44, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1215>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.03.

Введение

При использовании горячих криптовалютных кошельков из-за постоянного контакта с Сетью, повышается риск компрометации ключей, поэтому для более безопасного хранения криптовалюты и совершения транзакций используют холодные криптовалютные кошельки [1].

Холодный кошелек не имеет постоянного соединения с интернетом и блокчейном и как следствие менее подвержен атакам злоумышленников. Однако рано или поздно появляется необходимость произвести транзакцию с применением закрытых ключей, хранящихся в холодном кошельке, при этом возникают следующие проблемы:

- во-первых, нет гарантии, что операция проводится на доверенном компьютере;
- во-вторых, для выполнения транзакции кошельку необходимо обновить блокчейн, то есть за продолжительное время ему необходимо скачать большой объем информации, и в данных условиях снова повышается риск компрометации ключей, так как за время закачки необходимой информации в систему может скачаться и начать исполняться вредоносный код.

Таким образом, возникает противоречие между потенциальными уязвимостями при хранении ключей и проведении транзакций из горячих и холодных кошельков и потребностями общества в безопасном хранении ключей и безопасном проведении транзакций.

Данное противоречие можно разрешить, если в качестве доверенной исполняемой среды использовать облачный микрокомпьютер с динамически изменяемой архитектурой МКТ, который позволяет размещать ПО в памяти с физически устанавливаемым доступом read-only [2], что исключает ее искажение и обеспечивает неизменность среды функционирования.

В настоящей работе предложен концепт решения этой задачи и рассмотрена реализация локального холодного кошелька на платформе МКТ.

1. Хранение криптовалюты и совершение транзакций

Рассмотрим механизм работы блокчейна и блокчейн-транзакций.

В блокчейн имплементирована программа с внутренним хранилищем в которой хранится реестр монет, который представляет собой массив ассоциаций аккаунтов с суммами. Полный доступ к данному реестру имеет только эта программа, она же предоставляет всем желающим возможности просматривать суммы на аккаунтах и переводить сумм между аккаунтами, предварительно выполнив проверку на наличие у обратившегося доступа к тому аккаунту, с которого он пытается передать деньги, а также на не превышение суммы на балансе этого аккаунта. Проверка доступа основывается на проверке закрытого ключа из классической пары шифрования с открытым ключом. Если проверка прошла, то запрос на транзакцию будет отослан в Сеть, после чего запрос будет принят или отвергнут на основании алгоритма консенсуса, принятого в данном блокчейне [6].

Перечислим ключевые тезисы, на которые будем опираться при построении защищенной системы:

- Криптовалюта как деньги — это не более чем счетчик, записанный в реестре валют блокчейн-программы [3].
- Криптовалюта хранится не в кошельке, а в реестре валюты в блокчейне [3].
- У кого есть закрытый ключ от аккаунта, на котором лежат деньги, тот может переводить деньги в независимости от мнения оригинального владельца пары ключей.

- В случае кражи ключей, и вывода денег, злоумышленника вычислить крайне трудно, практически невозможно.
- Хранить криптовалюту в безопасности означает хранить в безопасности закрытые ключи.
- Неважно, откуда или с какого типа кошелька идет перевод денег, важно, чтобы программа получила из блокчейна корректную идентификационную информацию [4].
- «Холодный кошелек» означает, что кошелек не требует постоянного подключения к интернету. А горячий, соответственно, требует подключения к сети, что делает его более уязвимым для атак, так как каналы связи или сервера могут быть скомпрометированы [1].
- Холодные кошельки в пассивном режиме (без соединения с интернетом и без совершения транзакций) являются безопасными, при условии, что компьютер, на котором хранятся закрытые ключи, является доверенным, и мы можем гарантировать, что у злоумышленников нет к нему доступа.
- Пока не проведен ни один платеж с холодного кошелька (ни разу не использован приватный ключ) — холодный криптокошелек будет столь же надежен, как и аппаратный или бумажный.
- Проверять получение платежей на свой адрес можно на сторонних сервисах контроля блокчейна по запросу на открытый ключ пользователя.
- После проведения первой транзакции с холодного кошелька, кошелек перестает быть холодным в чистом виде (из пассивного режима на короткий период переходит в активный), и возрастает риск компрометации ключа. Чем больше хранимая сумма — тем больше риск.
- После совершения транзакции и отключения интернета риск компрометации ключа снижается, но остается, так как злоумышленники, применяя аналитические методы и вредоносное программное обеспечение, все равно могут получить доступ к закрытым ключам.
- В большинстве криптовалют действует система, аналогичная биткойну: каждая транзакция должна быть потрачена полностью. То есть если у Алисы на аккаунте есть 5 BTC и она хочет перевести Бобу 1 BTC, то она должна сделать транзакцию с двумя выходами: один для Боба (1 BTC) и второй для «сдачи» для Алисы на ее собственный адрес (4 BTC) [5].
- Послетранзакционный риск можно нивелировать, если использовать одноразовые ключевые пары и после каждой транзакции переводить «сдачу» на свой другой, только что созданный аккаунт. В такой схеме аккаунты (открытые ключи и ключевые пары) являются одноразовыми, и после первой же произведенной транзакции больше не используются.

Снижение и ликвидация риска компрометации ключа во время соединения с интернетом являются основными задачами этой работы.

2. Офлайн-подпись транзакций

Офлайн-подпись транзакций — это модификация метода холодного хранения, которая применяется для уменьшения риска компрометации в момент совершения транзакции:

- Система состоит из двух компьютеров, один из них всегда отключен от интернета, второй — подключен к сети

- На первом компьютере с помощью кошелька создаем пару ключей, импортируем открытый ключ на второй компьютер. После чего на этот адрес можно перевести необходимую сумму для хранения.
- Когда возникает необходимость в переводе, то на втором компьютере создается неподписанная транзакция (указываются адреса отправителя и получателя, а также объём средств), которая затем копируется на съемный носитель и импортируется на первый компьютер, неподключенный к интернету.
- На первом компьютере транзакция подписывается после чего точно также на съемном носителе импортируется на первый компьютер и отсылается в Сеть.

Ошибочно считается, что этот метод является абсолютно безопасным, потому что Интернет и закрытые ключи никогда не контактируют. Однако при импорте транзакции на носитель, даже при соблюдении всех мерах безопасности, все равно остается вероятность загрузки исполняемого вредоносного кода и на съемный носитель, и на сам компьютер, что может привести к подмене данных в транзакции, краже или повреждению закрытого ключа.

3. Иерархическая генерация ключей

Рассмотрим технологию, позволяющую удобным образом реализовать одноразовые ключевые пары.

Deterministic wallet — это кошелек, особенность которого состоит в том, что есть возможность из одного секрета (master seed) породить сколько угодно пар ключей для электронной подписи [6]. Это позволяет использовать новые адреса для каждого входящего платежа и сдачи, при этом все порожденные из основного секрета личные ключи друг с другом никак не связаны, то есть нельзя проследить связь между порожденными адресами (определить, что все они принадлежат одному пользователю), а имея порожденный личный ключ, нельзя восстановить изначальный общий секрет. Стандартизированный подход к кодированию основного секрета расписан в протоколах семейства BIP (Bitcoin Improvement Protocol) [7].

Детерминистические кошельки бывают двух типов:

- Простой детерминистический кошелек: Основной секрет здесь конкатенируется с индексом дочернего ключа, который мы хотим получить, после чего конкатенированные данные хешируются, с помощью хеш-функции SHA-256. Кошелек имеет некоторый seed, из которого напрямую генерируется множество личных ключей. Их количество может быть ограничено только размерностью индекса, который конкатенируется к секрету перед хешированием. Обычно это 4 байта, а это около 4 миллиардов уникальных ключей.
- Иерархически детерминистический кошелек (hierarchical deterministic wallets, HD wallets): На каждом уровне иерархии узел порождения имеет три объекта: личный ключ (private key), открытый ключ (public key) и код цепочки (chain code), который используется для порождения следующего уровня иерархии. Ключ, из которого порождают, называется родительским (parent), а порожденный ключ называется дочерним (child). Генерации ключей происходят по стандарту BIP32, в котором определены принципы работы этих кошельков [3].

Стоит отметить, что получение из родительского открытого ключа дочернего личного невозможно. То есть в данных системах можно выполнить следующие операции по развертыванию ключа:

- Master seed --> master key.
- Private parent key --> private child key.
- Private parent key --> public child key.

- public parent key --> public child key.

Рассмотрим следующий подход — hardened derivation. Это метод, не позволяющий рассчитывать дочерние открытые ключи из соответствующего родительского открытого ключа [7]. От обычного порождения отличается тем, что в обычном в качестве сообщения функции HMAC используется конкатенация сериализованной точки на эллиптической кривой, в качестве родительского открытого ключа, а в hardened derivation используют сериализацию родительского личного ключа. Если использовать этот подход, то злоумышленник, имея на руках родительский открытый ключ, не сможет рассчитать дочерние открытые ключи, и, следовательно, он не сможет вычислить адреса и их связь с полученным родительским ключом, что гарантирует дополнительный уровень анонимности.

Перечислим основные протоколы из семейства BIP, активно применяемые при проектировании криптовалютных кошельков с применением технологии HD Wallet:

- **BIP32** (hierarchical deterministic wallets) [8].

BIP32 — это протокол, определяющий иерархические ключи и способы их внутренней организации, в виде древовидной структуры. Также в этом протоколе описан способ разделения ключей на те, что будут использоваться для основных транзакций, и на те, что нужны для возвращения сдачи.

- **BIP39** (mnemonic code for generating deterministic keys) [9].

Данный протокол применяется при развертывании ключей. Он представляет собой кодирование основного секрета в мнемоническую фразу — набор обычных слов, который легко запомнить. При этом при вводе и выводе фразы есть возможность проверить контрольную сумму, то есть с большой вероятностью выявить ошибку, если такая имеется.

- **BIP43** (Purpose Field for Deterministic Wallets) [6] и **BIP44** (Multi-Account Hierarchy for Deterministic Wallets) [10].

BIP43 предполагает запись в первый уровень иерархии ключа номера улучшения, которое предлагает новый путь порождения или улучшения (m/bip_number'/*). BIP44, использует особенность предыдущего предложения, то есть для первого уровня иерархии записывается индекс 44, а в индексе второго уровня записывается определенное значение, которое будет соответствовать типу монеты, которую мы используем для данного кошелька. Теперь в одном кошельке могут разворачиваться и использоваться ключи для разных валют, то есть кошелек становится мультивалютным.

Таким образом, технология HD Wallet с применением метода hardened derivation позволяет оперировать очень большим (до 4 млрд) количеством аккаунтов в разных блокчейн-системах, сохраняя полную анонимность платежей, при этом сохраняя удобство и возможность автоматически посылать сдачу от транзакций на новые адреса. При этом от пользователя требуется всего лишь знать один мастер-ключ (или мнемоническая фраза, при использовании стандарта BIP39). Решение является очень удобным для пользователя и эффективным с точки зрения эффективности и безопасности, кроме того, оно обеспечивает мультивалютность кошелька.

4. МКТ и новая гарвардская архитектура

Вспомним классические подходы при построении архитектуры компьютерных систем:

- Архитектура фон Неймана – реализована практически во всех настольных компьютерах: Команды и данные не разделяются, а передаются по единому общему каналу.

• Гарвардская архитектура – реализована практически во всех планшетных компьютерах и телефонах: потоки команд и данных параллельны и независимы, что требует более сложной организации процессора, но обеспечивает более высокое быстродействие.

Данные классические архитектуры уязвимы, так как в них есть возможность изменения последовательности команд и данных независимо от того, размещены они в одной памяти или разделены [12]. Как следствие – возможность для несанкционированного вмешательства в логику работы с помощью вредоносного программного обеспечения.

Запись в долговременную память можно заблокировать, если использовать механизмы контроля целостности данных, причем проверка целостности должна идти до загрузки операционной системы. То есть атаки можно заблокировать с помощью механизмов контроля запуска задач (процессов, потоков) [13].

Чтобы предотвратить эти атаки, необходимо добавить неизменяемую память, разделить потоки команд и данных, исполнить контрольные процедуры в доверенной среде до запуска ОС. В гарвардской архитектуре уже есть разделение потоков команд и данных, поэтому если сделать память неизменяемой и разрешить движение данных и команд только по направлению к процессору, то ВРПО не будет фиксироваться и исполняться на компьютере, однако в этом случае не сможет исполняться и часть обычных программ, которым необходима запись данных в память для нормальной работы [13-14].

Эти противоречия разрешает новая гарвардская архитектура – модификация гарвардской архитектуры с использованием неизменяемой памяти (что избавляет от необходимости использовать сложные механизмы контроля целостности программ и данных до запуска ОС) и блоков сеансовой памяти (для возможности исполнения программ, для большей части которых необходима возможность записи) [13-14].

Есть целая ветка семейства компьютеров с вирусным иммунитетом на базе новой гарвардской архитектуры [12] — компьютеры МКTrusT, которые позволяют работать в одном из двух режимов — защищенном (read only) или незащищенном (read and write) [15]. Работа в этих режимах производится в разных ОС, загружающихся из разных, физически разделенных разделов памяти (то есть взаимовлияние ОС исключено технологически, как исключен и их одновременный запуск). Переключение режимов работы производится с помощью физического переключателя, расположенного на корпусе устройства, то есть необходимый режим выбирает пользователь, и не может выбрать хакер, так как невозможно программное воздействие на выбор режима. Для совершения транзакции пользователю понадобится выйти в интернет, и в таком случае ОС может перестать быть доверенной. Поэтому выход в интернет осуществляется только со второй, незащищенной, ОС.

5. Использование особенностей МКТ для устранения известных уязвимостей

Перечисленные выше ключевые особенности МКТ позволяют решить ряд проблем при работе с криптовалютными кошельками:

1. Офлайн-подпись транзакций: если в качестве офлайн-компьютера использовать МКТ в защищенном read only режиме, то можно гарантировать, что даже при попадании вредоносного ПО в систему, оно не сможет исполниться и таким образом транзакция не будет скомпрометирована.

2. Использование U2F для подписи транзакций: используя защищенную ОС МКТ в качестве доверенной среды, можно быть уверенным, что на входе и выходе U2F устройства будет именно та транзакция, которая нужна

3. Хранение ключей: если устанавливать кошелек в защищенную ОС МКТ, то при создании аккаунта в этом кошельке, можно выбрать опцию сохранения закрытых ключей в постоянную память, и не бояться, что эти ключи будут скомпрометированы.

Кроме того, особенности архитектуры МКТ позволяют часть функционала кошелька исполнять в защищенной среде и часть — в не защищенной. Чтобы эффективно использовать эту опцию, необходимо понять, какую часть функционала кошелька необходимо исполнять в каждой из ОС. Для этого введем два класса операций:

1. Операции, которые необходимо проводить в защищенной (RO) ОС.
2. Операции, которые необходимо проводить в незащищенной (RW) ОС.

К первому классу отнесем все функции, где так или иначе задействованы закрытые ключи или персональные данные пользователя, так как эти данные являются наиболее ценными и, как следствие, наиболее вероятными целями для хакеров, и поэтому для этих функций необходимо обеспечить максимально возможную безопасную среду исполнения.

Ко второму классу отнесем те функции, для исполнения которых необходима запись данных в постоянную память (так как в этом классе применяется read and write ОС), а также необходим интернет (соединение с которым повышает вероятность атаки на систему, а поэтому не желательно оперировать ценными данными в этой ОС).

Проведем следующий анализ функционала:

- опишем каждую функцию;
- укажем, нужен ли интернет для ее корректной работы;
- укажем, есть ли потенциальные уязвимости (если применять функцию на обычном компьютере) и какие;
- на основе предыдущих трех пунктов решим — к какому классу причислить эту функцию.

Результаты анализа занесем в табл. 1.

Перечислим операции, необходимые для работы проектируемой системы, и разделим их на два класса:

- **Операции, которые необходимо проводить в защищенной (RO) ОС:**
  - Генерация ключей, мастер-ключа или мнемонической фразы.
  - Развертывание ключей из мастер-ключа или мнемонической фразы.
  - Создание нового аккаунта в кошельке.
  - Подпись транзакции через интерфейс кошелька.
  - Подпись транзакции через U2F.
  - Хранение ключей в постоянной памяти.
  - Аутентификация через U2F.
- **Операции, которые необходимо проводить в незащищенной (RW) ОС:**
  - Чтение баланса из скачанного блокчейна.
  - Скачивание и обновление блокчейна.
  - Чтение баланса из блокчейна в интернете.
  - Создание транзакции.
  - Трансляция транзакции в блокчейн-сеть.

Выполнение этих операций в соответствующих ОС поможет минимизировать риски компрометации.

Таблица. 1 Сравнительный анализ функционала кошелька

Название функции	**Описание**	**Есть ли потенциальные уязвимости?**	**Класс функции**
Генерация ключей, мастер-ключа или мнемонической фразы	Генератор псевдослучайных чисел выдает на выходе, в зависимости от выбранного режима, либо ключевую пару, либо seed, из которого дальше по протоколу BIP32 будут развернуты остальные ключевые пары и по протоколу BIP39 этот seed будет представлен в виде мнемонической фразы	Если среда и приложение доверенные — то нет	Класс 1
Развертывание ключей из мастер-ключа или мнемонической фразы	Пользователь вводит ключ или мнемоническую фразу, а кошелек на основе введенных данных выдает список всех ключевых пар пользователя, после чего ими можно пользоваться	Если среда и приложение доверенные — то нет	Класс 1
Создание нового аккаунта в кошельке	После генерации и развертывания ключей, на выбор пользователя будет создан файл аккаунта в кошельке. В этом файле будет записано, что за данным пользователем закреплены соответствующие открытые ключи, и этот же файл будет хранить историю операций.	Хранить историю операций и открытые ключи в постоянной памяти компьютера — это потенциально не безопасное решение, так как если среда недоверенная, то при компрометации такого файла злоумышленник может узнать, например, что определенный набор открытых ключей принадлежит одному человеку	Класс 1
Чтение баланса из скачанного блокчейна	Идет чтение из блокчейна, расположенного в постоянной памяти. По завершению операции на выходе получаем баланс адреса на момент последнего обновления блокчейна	Если исключить вероятность наличия вредоносного кода в скачанном блокчейне, то сама операция чтения не является уязвимой	Класс 2
Скачивание обновление блокчейна	Обновление блокчейна, для последующего совершения транзакции или чтения баланса аккаунта	Из интернета в течение продолжительного времени качается большой объем данных (в случае если блокчейн не обновлялся достаточно давно), поэтому есть вероятность закачки вредоносного кода	Класс 2
Чтение баланса из блокчейна в интернете	Чтобы не скачивать гигабайты данных, идет чтение из блокчейна, расположенного в интернете, то есть идет обращение к серверам или соседним узлам. По завершению операции на выходе получаем баланс аккаунта на момент последнего обновления блокчейна	За время соединения с интернетом в систему может попасть вредоносный код. Также есть вероятность чтения данных из ложных источников в случае компрометации каналов связи	Класс 2

Название функции	**Описание**	**Есть ли потенциальные уязвимости?**	**Класс функции**
Создание транзакции	Пользователь вводит адрес отправителя, адрес получателя и количество валюты, которую нужно перевести. В случае если сумма переводится не полностью, то необходимо добавить адрес для возвращения сдачи. Также в транзакцию необходимо добавить ряд служебной информации, включая адреса и хэши транзакций, с которых были получены средства. Для корректной работы этого этапа необходимо обновить блокчейн до актуального состояния. На выходе получаем сформированную, но не подписанную транзакцию	Есть возможность того, что злоумышленник может подменить данные в транзакции на ложные. С учетом того, что этому этапу предшествовал этап обновления блокчейна, в системе мог оказаться вредоносный код	Класс 2
Подпись транзакции через интерфейс кошелька	Чтобы подписать транзакцию, пользователю необходимо ввести закрытый ключ в соответствующее поле (или идет чтение из файла, в котором в зашифрованном виде хранятся закрытые ключи), после чего система произведет все необходимые операции и вычисления	Подмена транзакции на ложные данные. Компрометация закрытого ключа	Класс 1
Трансляция транзакции в блокчейн-сеть	Подписанная транзакция посылается в Сеть, на ближайший доступный узел	Злоумышленник может послать в Сеть, подписанную в предыдущем пункте транзакцию с ложными данными. Остальные атаки зависят от надежности канала связи и узлов, на которые идет распространение информации	Класс 2
Аутентификация через U2F	В случае если был создан кошелек с двухфакторной аутентификацией, для входа в свой аккаунт пользователь должен вставить в компьютер U2F устройство	Если среда и приложение доверенные, то нет	Класс 1
Подпись транзакции через U2F	На вход в U2F устройство посылается сформированная и неподписанная транзакция. U2F устройство посылает в компьютер подписанную транзакцию	На вход устройству может послаться транзакция с фальшивыми данными или с вредоносным кодом	Класс 1
Хранение ключей	Закрытые ключи хранятся на жестком диске в зашифрованном виде	Ключи лучше не хранить в постоянной памяти, но если возникает такая необходимость, то делать это можно только в защищенной ОС	Класс 1

6. Сценарий работы системы

Опишем работу системы на верхнем логическом уровне. Начало работы с мультивалютным кошельком выглядит следующим образом:

- Заходим в защищенную ОС и создаем кошелек.
- Импортируем необходимые открытые ключи для последующего применения в не защищенной ОС.
- Заходим в незащищенную ОС и импортируем созданные в предыдущем пункте открытые ключи в кошелек.
- Когда возникает необходимость совершить транзакцию с одного из адресов, то система в незащищенной ОС должна:
  - Обновить блокчейн.
  - Сформировать транзакцию.
  - Экспортировать сформированную транзакцию на отчуждаемый носитель.
- Сформированная в предыдущем пункте транзакция на отчуждаемом носителе импортируется в защищенную ОС.
- В защищенной ОС транзакция подписывается одним из вариантов:
  - С помощью U2F устройства.
  - С помощью закрытого ключа, хранимого в зашифрованном виде в файле в постоянной памяти.
  - С помощью закрытого ключа, введенного пользователем вручную в соответствующее поле интерфейса.
- После этого подписанная транзакция экспортируется через отчуждаемый носитель обратно в незащищенную ОС.
- В незащищенной ОС подписанная транзакция транслируется в Сеть

Схема рабочего цикла кошелька приведена на рис. 1

Таким образом, мы получаем систему, в которой все операции, производимые с закрытыми ключами, проводятся в отдельной защищенной операционной системе с постоянной памятью, доступной только чтения. Благодаря технологии иерархически детерминированного кошелька все ключевые пары являются одноразовыми, то есть после каждой транзакции закрытый ключ больше не используется, причем, даже если злоумышленник перехватит все использованные ключи, он не сможет вычислить остальные.

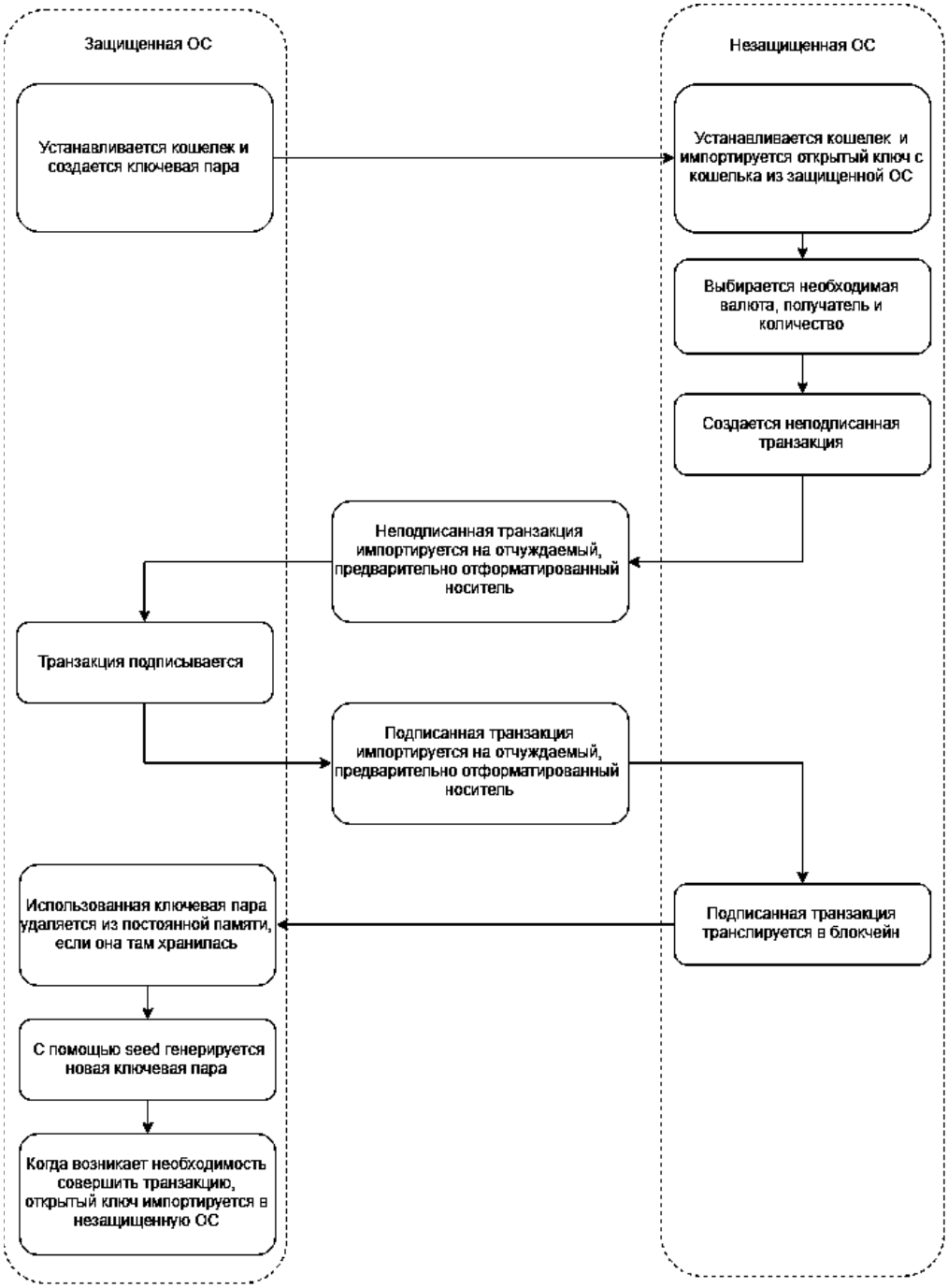

Рис. 1. Схема работы проектируемой системы
(Fig. 1 Working scheme of the designed system)

Заключение

В данной статье рассмотрена одна из возможных реализаций холодного мультивалютного кошелька на базе компьютера с динамически изменяемой архитектурой МКТ: были рассмотрены ключевые аспекты системы, выбран алгоритм развертки ключей, предложен вариант разделения функционала мультивалютного холодного кошелька на

две группы, каждая из которых предназначена для исполнения в своей среде, и описан цикл работы системы на логическом уровне.

СПИСОК ЛИТЕРАТУРЫ:

1. Cold storage [Электронный ресурс]. — Электрон. текстовые дан. — URL: https://en.bitcoinwiki.org/wiki/Cold_storage, свободный (дата обращения: 20.06.19).
2. Конявский, В.А. Компьютер с «вирусным иммунитетом» [Электронный ресурс]. В.А. Конявский. — Электрон. текстовые дан. — URL: http://www.okbsapr.ru/konyavskiy_2015_2.html, свободный (дата обращения: 20.06.19).
3. Bitcoin in a nutshell — Blockchain [Электронный ресурс]. — Электрон. журн. — URL: https://habr.com/ru/post/320176/ (дата обращения: 20.06.19).
4. Как на самом деле работает протокол Биткоин [Электронный ресурс]. — Электрон. журн. — URL: https://habr.com/ru/post/222493/ (дата обращения: 20.06.19).
5. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. Satoshi Nakamoto. — Электрон. журн. — URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 20.06.19).
6. Hierarchical deterministic Bitcoin wallets that tolerate key leakage [Электронный ресурс]. Gus Gutoski. — Электрон. журн. — URL: https://eprint.iacr.org/2014/998.pdf (дата обращения: 20.06.19).
7. Иерархическая генерация ключей [Электронный ресурс]. — Электрон. текстовые дан. — URL: https://habr.com/company/distributedlab/blog/413627/, свободный (дата обращения: 20.06.19).
8. bip-0032 [Электронный ресурс]. — Электрон. текстовые дан. — URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, свободный (дата обращения: 20.06.19).
9. bip-0039 [Электронный ресурс]. — Электрон. текстовые дан. — URL: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, свободный (дата обращения: 20.06.19).
10. bip-0043 [Электронный ресурс]. — Электрон. текстовые дан. — URL: https://github.com/bitcoin/bips/blob/master/bip-0043.mediawiki, свободный (дата обращения: 20.06.19).
11. bip-0044 [Электронный ресурс]. — Электрон. Текстовые дан. — URL: https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki, свободный (дата обращения: 20.06.19).
12. Конявский В.А. Компьютер с вирусным иммунитетом. Информационные ресурсы России. 2015. № 6. С. 31–34.
13. Конявский В.А. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.
14. Конявский В.А. Защищенный микрокомпьютер МК-TRUST — новое решение для ДБО. Национальный банковский журнал. — 2014. — № 3. — С. 105.
15. Работа с одного рабочего места в двух разных контурах защищенности [Электронный ресурс]. — Электрон. текстовые дан. — URL: http://www.okbsapr.ru/sol17.html, свободный (дата обращения: 20.06.19).

REFERENCES:

[1] Cold storage [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://en.bitcoinwiki.org/wiki/Cold_storage, svobodnyj (accessed: 20.06.2019) (in Russian).
[2] Konjavskij, V.A. Komp'juter s «virusnym immunitetom» [Jelektronnyj resurs] V.A. Konjavskij. — Jelektron. tekstovye dan. — URL: http://www.okbsapr.ru/konyavskiy_2015_2.html, svobodnyj (accessed: 20.06.2019) (in Russian).
[3] Bitcoin in a nutshell — Blockchain [Jelektronnyj resurs]. — Jelektron. zhurn. — URL: https://habr.com/ru/post/320176/ (accessed: 20.06.2019) (in Russian).
[4] Kak na samom dele rabotaet protokol Bitkoin [Jelektronnyj resurs]. — Jelektron. zhurn. — URL: https://habr.com/ru/post/222493/ (accessed: 20.06.2019) (in Russian).
[5] Bitcoin: A Peer-to-Peer Electronic Cash System [Jelektronnyj resurs]. Satoshi Nakamoto. — Jelektron. zhurn. — URL: https://bitcoin.org/bitcoin.pdf (accessed: 20.06.2019) (in Russian).
[6] Hierarchical deterministic Bitcoin wallets that tolerate key leakage [Jelektronnyj resurs]. Gus Gutoski. — Jelektron. zhurn. — URL: https://eprint.iacr.org/2014/998.pdf (accessed: 20.06.2019) (in Russian).
[7] Ierarhicheskaja generacija kljuchej [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://habr.com/company/distributedlab/blog/413627/, svobodnyj (accessed: 20.06.2019) (in Russian).
[8] bip-0032 [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, svobodnyj (accessed: 20.06.2019) (in Russian).

[9] bip-0039 [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, svobodnyj (accessed: 20.06.2019) (in Russian).
[10] bip-0043 [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://github.com/bitcoin/bips/blob/master/bip-0043.mediawiki, svobodnyj (accessed: 20.06.2019) (in Russian).
[11] bip-0044 [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki, svobodnyj (accessed: 20.06.19).
[12] Konjavskij V.A. Komp'juter s virusnym immunitetom. Informacionnye resursy Rossii. 2015. № 6. S. 31–34 (in Russian).
[13] Konjavskij V.A. Mobil'nyj komp'juter s apparatnoj zashhitoj doverennoj operacionnoj sistemy: Patent na poleznuju model' № 147527. 10.11.2014. Bjul. № 31 (in Russian).
[14] Konjavskij V.A. Zashhishhennyj mikrokomp'juter MK-TRUST — novoe reshenie dlja DBO. Nacional'nyj bankovskij zhurnal. — 2014. — № 3. — S. 105 (in Russian).
[15] Rabota s odnogo rabochego mesta v dvuh raznyh konturah zashhishhennosti [Jelektronnyj resurs]. — Jelektron. tekstovye dan. — URL: http://www.okbsapr.ru/sol17.html, svobodnyj (in Russian).

Поступила в редакцию – 25 июня 2019 г. Окончательный вариант – 17 августа 2019 г.
Received – Juny 25, 2019. The final version – August 17, 2019.

Сергей В. Дуга[1], Алексей Г. Себякин[2], Андрей И. Труфанов[3], Людмила Л. Носырева[4]
[1,2] Экспертно-криминалистический отдел, следственное управление Следственного комитета Российской Федерации по Иркутской области,
Клары Цеткин ул., 9а, г. Иркутск, 664039, Россия
[3,4] Иркутский национальный исследовательский технический университет,
Лермонтова ул., 83, г. Иркутск, 664074, Россия
[1]e-mail: siber@list.ru, https://orcid.org/0000-0002-5894-9855
[2]e-mail: quattro.sa@yandex.ru, https://orcid.org/0000-0002-4858-2703
[3]e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[4]e-mail: nll@list.ru, https://orcid.org/0000-0001-8145-1126

КОНЦЕПЦИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ

DOI: http://dx.doi.org/10.26583/bit.2019.2.04

Аннотация. Предлагается основанная на разработанной сетевой онтологии предметной области «Предварительное следствие», концептуальная модель системы информационно-аналитической поддержки принятия решений как ответ на вызов всё более возрастающей необходимости анализа «больших данных» в ходе расследования преступлений. На основе проведенного анализа сетевого взаимодействия фигурантов 12 уголовных дел демонстрируется важность автоматизированного сбора и обработки всего многообразия сведений, полученных в ходе производства отдельных следственных действий.

Ключевые слова: информатизация расследования, уголовное дело, СППР, сетевая онтология, комплексные сети, большие данные, сетевой анализ.
Для цитирования: ДУГА, Сергей В. et al. КОНЦЕПЦИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 45-57, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1216>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.04.

Sergey V. Duga[1], Aleksey G. Sebyakin[2], Andrey I. Trufanov[3], Lyudmila L. Nosyreva[4]
[1, 2]Investigation Department, Investigative Committee of the Russian Federation Irkutsk Region,
K. Tsetkin str., 9a, Irkutsk, 664039, Russia
[3, 4]Irkutsk National Research Technical University,
Lermontova str., 83, Irkutsk, 664074, Russia
[1]e-mail: siber@list.ru, https://orcid.org/0000-0002-5894-9855
[2]e-mail: quattro.sa@yandex.ru, https://orcid.org/0000-0002-4858-2703
[3]e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[4]e-mail: nll@list.ru, https://orcid.org/0000-0001-8145-1126

The concept of decision support system in preliminary investigation

DOI: http://dx.doi.org/10.26583/bit.2019.2.04

Abstract. Based on the developed network ontology of the subject area "Preliminary investigation" a conceptual model of the information and analytical decision support system is proposed as a response to the challenge of the increasing need for the analysis of "big data" in the course of a crime investigation. It is demonstrated the importance of automated collection and processing of a variety of information obtained during the individual investigations based on the analysis of network interaction of persons involved in 12 criminal cases.

Keywords: investigation informatization, criminal case, DSS, network ontology, complex networks, big data, network analysis.
For citation: DUGA, Sergey V. et al. The concept of decision support system in preliminary investigation. IT Security (Russia), [S.l.], v. 26, n. 3, p. 45-57, 2019. ISSN 2074-7136. Available at:

<https://bit.mephi.ru/index.php/bit/article/view/1216>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.04.

Введение

В прошлом значительная часть активности правоохранительных органов была сосредоточена на физическом наблюдении, «бумажных следах» и прослушивании телефонных разговоров. В настоящее время правоохранители также имеют дело с широким спектром информации, содержащейся в электронных письмах, в текстовых, голосовых и графических сообщениях, в интернет-мессенджерах, на компьютерных жестких дисках и других устройствах памяти, в т.ч. на планшетах и мобильных телефонах.

Уже сейчас можно говорить, что работа следственных органов становится все более информационно емкой — все большую часть рабочего дня занимает обработка цифровой информации и ее анализ с помощью современных информационных технологий. Этот информационно-интенсивный способ работы привносит как преимущества, так и дополнительные сложности, в частности, большой объем информации, который необходимо проанализировать при расследовании преступлений.

В современных реалиях правоохранительные органы напрямую сталкиваются с «большими данными» (Big Data) — термином, под которым понимается качественно иной огромный объем как структурированных, так и неструктурированных данных.

С одной стороны, как отмечается в [1], «электронные следы — различные виды компьютерной информации, содержащейся на электронных носителях, — все чаще используются в качестве доказательств по уголовным делам о преступлениях различных видов». С другой, непомерный рост объема информации, хранящейся на цифровых устройствах, уже сейчас ставит перед следователем непростую задачу — охватить этот объем и провести его анализ. Даже с привлечением специалиста в области информационных технологий этот процесс может занять весьма продолжительное время и привести к значительным трудозатратам.

Другая проблема, с которой сталкиваются следователи, — невозможность или сложность проанализировать имеющуюся в рамках расследуемого уголовного дела (УД) информацию с учетом полученных ранее данных по другим уголовным делам. Например, для анализа информации о соединении абонентов, полученной как от операторов связи, так и из данных, полученных в ходе осмотров мобильных телефонов, следователем назначается информационно-аналитическая экспертиза. Как правило, на экспертизу представляются сведения только по одному – текущему расследуемому УД, а информация по другим уголовным делам откладывается в сторону, в том числе важная, в связи с чем анализ носит весьма ограниченный характер.

Другой проблемой является такой трудоемкий процесс, как проверка материалов уголовного дела. Проверке, в частности, подлежат следующие вопросы: правильно ли записаны фамилия, имя, отчество обвиняемого, время и место его рождения; были ли обеспечены подозреваемый, обвиняемый помощью адвоката-защитника во всех предусмотренных законом случаях, в том числе в случаях обязательного участия защитника, разрешены ли ходатайства обвиняемого и его защитника; вынесены ли все необходимые постановления; допрошены ли все упомянутые в протоколах, рапортах, объяснениях; проведены ли все необходимые осмотры, освидетельствования; все ли необходимые экспертизы проведены; имеются ли в наличии все вещественные доказательства, документы, ценности, указанные в протоколах как изъятые; определена ли судьба не имеющих отношения к делу личных вещей и документов, изъятых у подозреваемого, обвиняемого, иных лиц [2, 3]. Но даже после такой проверки, которая,

несомненно, отнимает большое количество времени и сил, не гарантировано отсутствие мелких технических и процессуальных ошибок, что чревато неблагоприятными последствиями.

Как нам видится, одним из важнейших факторов тенденции развития органов предварительного следствия является развитие потенциала информационных технологий в области оперативной обработки больших объемов информации, а также создание высокоэффективной информационной среды в работе следователя.

1. Родственные работы

Для создания современной информационной среды в работе следователя традиционно используются системы информационно-аналитической поддержки принятия решений (СППР). Существуют различные определения СППР [4-7]. В работе мы придерживались определения СППР, данного в [8]: «СППР — в большинстве случаев – это интерактивная автоматизированная система, которая помогает пользователю использовать данные и модели для идентификации, решения задач и принятия решений».

На сегодняшний день исследования в области применения СППР в борьбе с преступностью наблюдается во всем мире [9-12]. В частности, полиция Эдмонтона (Канада) строит первую в Канаде корпоративную цифровую полицейскую платформу, предлагая новые способы управления и анализа множеством данных из всех своих операций [13]. К началу 2019 года планировалось запустить новую платформу с базовым уровнем функциональности. Европейские правоохранители также используют те преимущества, что обеспечивают СППР [14].

Аналогичные работы ведутся и в России [15-18].

В последние годы онтологии успешно используются в системах СППР для обоснования и развития ряда этапов процесса принятия решений, а иногда и для всего контента, обрабатываемого и создаваемого при ответах на запросы [19-22]. Несмотря на то, что, как считают многие [23], в отличие от медицины, техники или психологии, право не является «онтологически» обоснованным, онтологические платформы нашли свое отражение и в правоохранительной деятельности [24].

Недавний пример онтологии [25] представляет семантическую информацию об уголовном и процессуальном праве в США, а также о применяемых правовых нормах.

2. Онтология и модель

В качестве базового подхода исследования двух вышеуказанных проблем использовалось представление на основе комплексных сетей. Ключевое математическое описание комплексной сети/сложной сети (англ. complex networks) — граф с достаточно большим числом вершин (ассоциируемых с узлами сети – участниками взаимодействия) одной и той же природы, характеризуемых в том числе многомерным кортежем признаков и динамически изменяющимся набором ребер (связей). Распределение признаков узлов и характеристик связей может быть описано вероятностной моделью (многомерным распределением) [19]. Характерно, что топологические свойства этих сетей, рассматриваемые отвлеченно от их физической природы, но существенно определяющие функционирование сетей, и составляют предмет исследования комплексных сетей. Подход к анализу сложных систем на основе комплексных сетей оказался весьма эффективным практически во всех научных областях, например, в социологии, биологии, технике и т.д. [26], и особенно междисциплинарных [27].

3. Характеристики комплексных сетей

Для описания структуры комплексных сетей используются различные характеристики. Перечислим некоторые из них [28].

Степень узла (число связей, инцидентных данному узлу).

Среднее расстояние между узлами. Минимальное число связей, которое необходимо преодолеть, чтобы попасть из узла в узел, называется расстоянием между узлами. Усредненное расстояние между всеми парами узлов сети, для которых существует путь перехода из одного в другой, называется средним расстоянием между узлами d.

Распределение узлов по числу связей P(q) – вероятность того, что случайно выбранный узел в случайной сети имеет степень *q*:

где - среднее число узлов степени *q* в сети, причем усреднение берется по всему статистическому ансамблю, *N* – количество узлов сети. При этом подразумевается, что суммарное число узлов у всех членов этого ансамбля одинаковое.

Коэффициент кластеризации узла - вероятность того, что два ближайших соседа узла *i* сами есть ближайшие соседи:

где q – число ближайших соседей узла *i*, *t* – число связей между ними.
Коэффициент кластеризации сети характеризует статистику циклов в сети.

Центральность (англ. Centrality): центральность относится к группе метрик, целью которых является определение «значительности» или «влияния» (в различных значениях) определённого узла (или группы) в сети. Примерами общих методов измерения «центральности» являются: определение центральности по посредничеству, центральность по близости, центральности собственного вектора, альфа центральности и центральности по степени [29].

4. Программные инструменты

Для графического представления использовалась платформа для визуализации графов Gephi [30]. В зависимости от настроек в Gephi есть возможность отображения вершин, ребер, меток (вершин и ребер), по необходимости можно менять их величину и расцветку, масштабировать изображение с различной степенью детализации, просматривать списки вершин и ребер, ранжировать их. В числе аналитических возможностей Gephi автоматическое вычисление таких характеристик, как диаметр графа, плотность графа, модулярность, средняя длина пути между любыми двумя вершинами, метрики авторитетности вершин HITS и PageRank, центральность по собственному вектору (eigenvector centrality), средний коэффициент кластеризации и пр. [31].

5. Данные

В подтверждение важности более общего подхода при анализе информации о соединении абонентов была рассмотрена задача сетевого взаимодействия фигурантов двенадцати уголовных дел. Используемые в задаче данные были получены в ходе осмотров мобильных телефонов с участием экспертов экспертно-криминалистического отдела СУ СК России по Иркутской области в рамках расследования различных уголовных дел экономического и коррупционного характера. Подготовлен пример, для которого выбраны сведения о контактах из «записной книжки» 36 мобильных телефонов.

6. Основные результаты

В качестве социальной сети был построен неориентированный граф, вершинами которого являются записи о телефонных номерах, а ребрами – наличие взаимной записи в двух различных телефонных аппаратах. Каждому узлу был добавлен атрибут,

соответствующий номеру уголовного дела. В результате был получен граф, состоящий из 12084 вершин и 12752 ребер. После того как были отфильтрованы «листы» (вершины с единичной степенью), в графе осталось 606 вершин и 1274 ребер. Далее, посредством алгоритма «Betweeness Centrality» программного инструмента Gephi, был проведен анализ центральности, после чего, в соответствии с данной метрикой, задавался визуальный размер каждой вершины. Также граф был раскрашен в соответствующий цвет для каждого уголовного дела (рис.1).

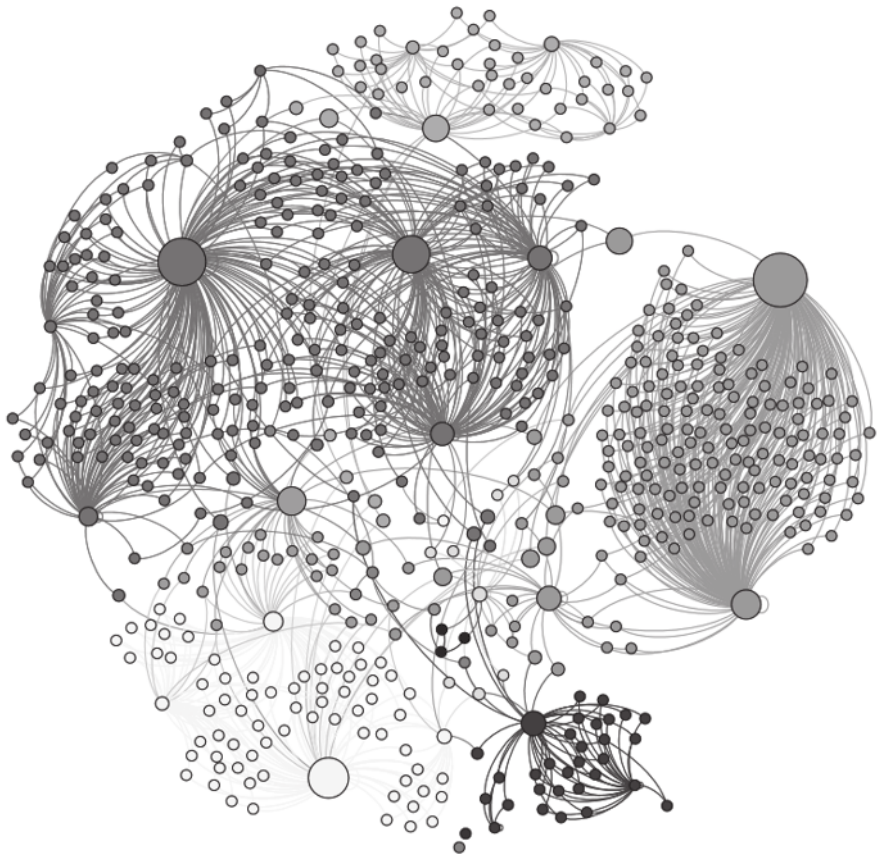

Рис. 1. Пример сетевого взаимодействия фигурантов 12 уголовных дел
(Fig. 1. Example of network interaction of persons involved in twelve criminal cases)

Проведенный анализ указывает на тесную связь между фигурантами различных уголовных дел одновременно и на присутствие автономных компонентов связности.

Таким образом, пример демонстрирует то, что анализ информации о соединении абонентов, ограниченный рамками отдельного уголовного дела, не дает полной картины о сетевых структурах криминальных сообществ и, соответственно, не может выявить ключевых или неочевидных фигурантов.

Далее, подобно [14], на абстрактном уровне были выделены три этапа в процессе принятия решений:

1. Постановка задачи принятия решения.
2. Сбор, хранение и объединение данных, имеющих отношение к данной проблеме.
3. Обоснование данных, необходимых для принятия решения.

Для поддержки реализации такого процесса в СППР разумно включить следующие три основных модуля [21]:

- диалоговый или пользовательский модуль, который поддерживает взаимодействие пользователя с системой, чтобы сформулировать проблему и получить на выходе результат СППР;
- модуль данных, который позволяет хранить данные, собранные и обработанные СППР;
- модуль модели, который реализует стратегию поддержки принятия решений.

Необходимо отметить, что в целом использование онтологии предметной области может помочь в моделировании данных и переносе модели в данные, фактически в СППР. Онтология, в том числе и сетевая, – это общая терминология, которая фиксирует свойства и отношения между объектами и событиями. Онтологии могут обеспечить: (а) общее понимание области знаний, которая может передаваться агентам и прикладным системам, и (б) явную концептуализацию, которая описывает семантику данных. Считается, что онтологии имеют решающее значение для того, чтобы позволить программным средствам осмысленно взаимодействовать между собой [22], и не только программным средствам, но и специалистам конкретной предметной области, более того экспертам, представляющим разные области знаний и практики. Нельзя не согласиться с утверждением, что онтология является средством междисциплинарного переноса знаний между разными предметными областями [32].

Для онтологического слоя, в зависимости от необходимой степени концептуализации, возможны следующие два вида онтологий:

1. Онтологии метауровня. Содержат понятия, являющиеся метапонятиями, и с таким уровнем абстракции, чтобы с их помощью можно было описать понятия прикладных онтологий.
2. Прикладные онтологии. Создаются для решения конкретной задачи предметной области. Используются для одной предметной области (напр. правоохранительная деятельность, авиация, медицина, и т.д.).

Общий вид структуры онтологии составляют такие компоненты, как:

- Понятия (классы), атрибуты, аксиомы, экземпляры (объекты);
- Классы (понятия): Акторы – Следы – Действия, процессы.
- Атрибуты: роль в деле, анкетные данные – улики, отпечаток, свидетельство (предмет, текст, аудио, фото, видео... – состоялось, произошло, дата, место, масштаб…).
- Аксиомы – именно аксиомы устанавливают то, каким образом понятия или их атрибуты взаимодействуют друг с другом. Полагаем, что Законы науки о сетях, проявляющиеся в свойствах комплексных сетей, – это аксиомы онтологий предварительного следствия. Данными законами определяются основные положения, структура и масштаб онтологии.
- Экземпляры: конкретный пример понятий и его атрибутов (понятие – подозреваемый, отдельный экземпляр – Иванов Вахид Израилевич, паспорт 29 03 393066, выдан Левобережным РУВД г. Иркутска, дата выдачи 31.10.2002, код подразделения 493-003, зарегистрирован по адресу: СПб,194100, Лесной пр. 63, корп. 5, кв. 88).

Формально онтология может быть представлена тройкой:

$O = <T,R,F>$,

где T – понятия и атрибуты предметной области, описываемые онтологией O;

R – отношения между понятиями и атрибутами предметной области;

F – функции интерпретации (аксиомы), заданные на понятиях и отношениях онтологии.

С одной стороны, онтологии – это тезаурусы терминов, которые совместно используются в конкретной области, например, в том же уголовном праве. Безусловно,

они отличаются от канонических тезаурусов, потому что знания, охватываемые терминами, представляются в машиночитаемом формате и задаются на языке представления знаний. Этот язык дает возможность машинным устройствам применять логику и анализировать смысл обрабатываемых терминов. Воспринимаемая семантика должна отражать общее понимание используемых терминов – понятий – как машинами, так и людьми.

С другой стороны, и что важно, онтологии в значительной степени можно сопоставлять с семантическими сетями [33] как инструментом моделирования и структуризации знаний. Многие понятия и принципы реализации, а также графическая форма представления на начальном этапе структуризации являются в онтологиях сходными с семантическими сетями [34], [35]. Многое в онтологиях сильно пересекается с уже давно принятым в информатике и лингвистике понятием тезауруса. Отметим также, что в контексте разработки онтологий именно сетевая платформа целе-ориентированного и агентно-ориентированного моделирования способствует детализации сферы интересов вовлеченных участников [36].

Задачами в рамках подготовки сетевой метаонтологии системы правоохранительной деятельности и, в частности, прикладной онтологии предварительного следствия как платформы создания СППР предварительного следствия (ПС) являются:

1. Корректное описание взаимосвязанных явлений и процессов в данной предметной области с необходимой визуализацией.
2. Создание переносимых элементов системы.
3. Эффективные решения, учитывающие широкий спектр предполагаемых факторов, определяемых системой непротиворечивых сетевых задач.
4. Единое понимание сетевой парадигмы, практик, моделей и подходов всеми участниками обработки информации в ПС.
5. Эффективные классификации, модели, сценарии, оценки рисков в ПС.
6. Надежное выявление специфических структурных образований в региональном, национальном и международном масштабах.

Для реализации в рассматриваемой СППР возможности по анализу различных источников как структурированных, так и неструктурированных данных, а также интеграции уже имеющихся приложений и баз данных была разработана онтология предметной области «Предварительное следствие» (рис. 2).

Стратегии интеграции, основанные на онтологиях, используются в технологиях «Enterprise Application Integration» (EAI) (интеграция приложений предприятия). EAI нацелена на интеграцию отдельных приложений в единое целое, позволяя бизнес-процессам и данным «общаться» друг с другом в разных приложениях [37]. Онтологии играют ключевую роль в EAI, захватывая концептуализацию, лежащую в основе различных приложений, которые должны быть интегрированы.

Предлагаемая концепция СППР (рис. 3) призвана не только разгрузить следователя в его повседневных задачах и автоматизировать, если не полностью, то хотя бы в большей части, механизм проверки материалов уголовного дела, но и дать следователю новые возможности по анализу сведений как в контексте расследуемого уголовного дела, так и относительно других уголовных дел.

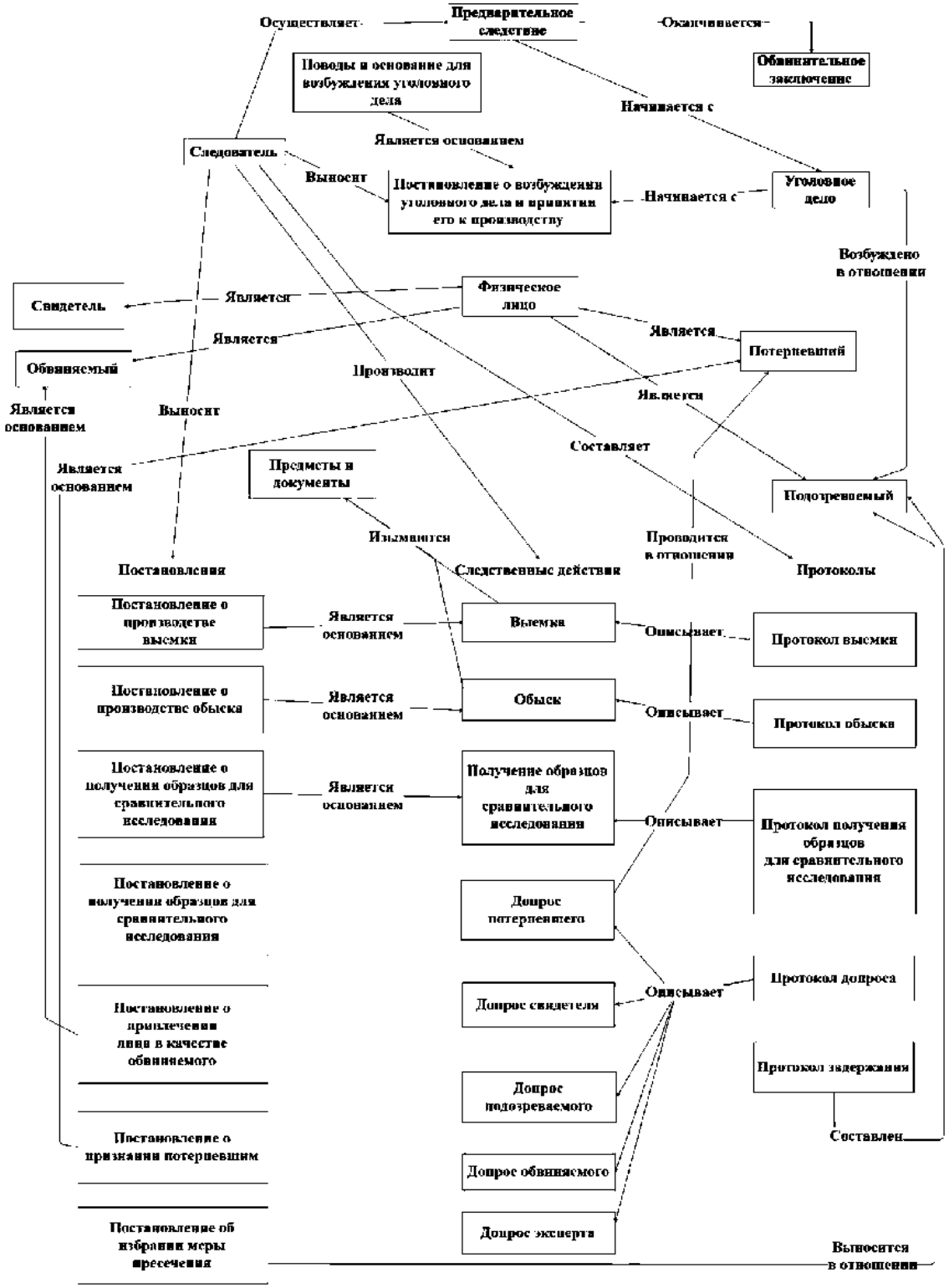

Рис. 2. Часть онтологии предметной области «Предварительное следствие»
(Fig. 2. Part of the ontology of the subject area "Preliminary investigation»)

Рис. 3. Концептуальная модель СППР
(Fig. 3. Conceptual model of information and analytical decision support system)

Использование СППР, оснащенной необходимым функционалом по сбору, хранению и анализу информации, позволит следователю самостоятельно, без привлечения специалиста, проводить базовый анализ связей интересующих лиц или организаций как в контексте расследуемого уголовного дела, так и с учетом накопленной ранее информации.

На текущий момент СППР включает следующие подсистемы:

- систему накопления сведений;
- аналитический блок;
- информационную систему следователя.

Система накопления сведений обеспечивает сбор, обработку и хранение информации. В качестве источников данных выступают:

- данные, полученные в ходе осмотров мобильных телефонов;
- государственные базы данных;
- сведения из баз данных организаций, полученные в ходе осмотров информационных носителей организаций;
- материалы уголовных дел в цифровом виде, в частности протоколы следственных действий;
- сведения, полученные от операторов связи;
- сведения из социальных сетей и облачных хранилищ.

Для осмотров мобильных устройств экспертами ЭКО следственного управления Следственного комитета РФ по Иркутской области применяются: универсальное устройство извлечения судебной информации (UFED) [38], компании «Cellebrite», и специализированное программное обеспечение «Мобильный Криминалист» [39], компании «Оксиджен Софтвер».

Сформированные при помощи программного обеспечения «UFED» и «Мобильный Криминалист» отчеты загружаются СППР для их последующей обработки. В текущий

момент использовались данные из следующих источников: записная книжка и журнал звонков.

При загрузке в СППР материалов уголовных дел проводится первоначальная обработка текста методами компьютерной лингвистики, в частности, токенизация (выделение отдельных слов и символов) и удаление «стоп-слов» (неинформативные слова).

Аналитический блок включает следующие функции:

- построение и анализ графа связей, включающего: эго-сеть интересующего лица, определение групп, выявление «мостов» – индивидов, чьи связи обеспечивают единственное соединение между двумя индивидами или группами, определение «значительности» или «влияния» отдельных индивидов в сети;
- установление связи между юридическими лицами, а также между юридическим и физическим лицом;
- анализ естественного языка, включающий: извлечение информации, в частности, нахождение именованных сущностей (ФИО, местоположение, наименование организации, события и т.д.);
- сохранение выявленной информации, поиск.

Информационная система следователя предназначена для обеспечения следователя различными методиками и инструментами по облегчению рутинных задач, а также выявлению и устранению различных технических ошибок.

Основные функции системы:

- учет изъятых предметов и документов и последующий контроль их местонахождения;
- методическая поддержка при проведении отдельных следственных действий;
- формирование запросов и поручений;
- проверка материалов уголовного дела;
- формирование обвинительного заключения.

Заключение

Таким образом, данная СППР способна облегчить такие следственные задачи, как:

- анализ переписки пользователей;
- выявление круга общения индивидов и устойчивых групп;
- выявление мелких технических и процессуальных ошибок путем анализа материалов уголовного дела;
- формирование обвинительного заключения;
- обеспечение автоматического извлечения именованных сущностей из материалов уголовных дел;
- преобразование цифровых доказательств из нескольких источников и систем в единый источник информации.

Ожидается, что внедрение предлагаемой СППР не только будет способствовать разгрузке следователя от рутинных задач, но и обеспечит мощный аналитический инструмент, который не ограничивается сведениями расследуемого уголовного дела. Объединение цифровых данных в одном месте и возможность следователем использовать инструмент по их анализу помогут вести следствие в правильном направлении, экономя время и ресурсы, а возможно и способствуя более быстрому расследованию преступления.

В дальнейшем планируется провести исследования по оценке как качества разработанной онтологии, так и в целом успеха СППР в работе следователей. Это

позволит получить представление о фактическом использовании и влиянии, которое СППР оказывает как на отдельных следователей, так и на всю организацию предварительного следствия.

СПИСОК ЛИТЕРАТУРЫ:

1. Вехов В. «Использование компьютерных технологий в криминалистической деятельности и уголовном процессе» Вестник академии следственного комитета Российской Федерации. 2014, №1. С. 70–73.
2. Гармаев Ю.П. Настольная книга помощника судьи: Вып. 1: Организация работы и уголовное судопроизводство, Улан-Удэ: САПЭУ, 2009. С. 60–73.
3. Гармаев Ю.П. «Алгоритм проверки материалов уголовного дела» 2009, № 2. С. 16–21.
4. Edwards J.S., «Expert Systems in Management and Administration - Are they really different from Decision Support Systems?» European Journal of Operational Research, 1992, № 61. P. 114–121.
5. Little J.D.C. «Models and managers: The concept of a decision calculus» Management science, 1970. Vol. 16, № 8, P. 466–485.
6. Sprague Jr R.H. «A framework for the development of decision support systems» MIS quarterly. 1980. P. 1–26,
7. Thierauf R.J., «Decision support systems for effective planning and control: A case study approach» Prentice Hall PTR, 1982.
8. Сараев А.Д. и Щербина О.А. «Системный анализ и современные информационные технологии» Труды Крымской Академии наук 2006. С. 47–59.
9. Almeida da Costa Júnior и Gilton Jose Ferreira da Silva «A Decision Support System for Police Patrolling» 2018.
10. «Technology Chicago Police Department» [В Интернете]. URL: https://home.chicagopolice.org/office-of-reform-management/technology (дата обращения: 15 04 2019).
11. Kadar C., Maculan R. и Feuerriegel S. «Public decision support for low population density areas: An imbalance-aware hyper-ensemble for spatio-temporal crime prediction» Decision Support Systems. 2019, № 119. P. 107–117
12. Рзаев Р.Р. и др. «Информационная система поддержки принятия процессуальных решений» Системы и средства информатики. 2016. Т. 26, № 1. С. 182–198.
13. «Edmonton Police Service | IBM» [В Интернете]. URL: view-source:https://www.ibm.com/case-studies/edmonton-police-service-hybrid-cloud-integration-crime (дата обращения: 15 04 2019).
14. Casey, D., Burrell, P. & Sumner, N. «Decision Support Systems in Policing» 2018.
15. Головнин О.К. и Романова Е.А. «Прецедентная система поддержки принятия решений по делам об административных правонарушениях» Программные продукты и системы. 2018. № 1.
16. «Разработка программного обеспечения и баз данных. Создание веб-сайтов. - АРМ следователя (дознавателя)» [В Интернете]. URL: https://ts-group.ru/awp.php (дата обращения: 15 04 2019).
17. «АРМ следователя. АРМ руководителя следственного подразделения» [В Интернете]. URL: http://www.oviont.ru/services/develop/ais/arm/ (дата обращения: 15 04 2019).
18. «Проект "АРМ Следствие"» [В Интернете]. URL: https://vk.com/armsledstvie (дата обращения: 15 04 2019).
19. Benmimoune L. et al. «Ontology-based Medical Decision Support System to Enhance Chronic Patients' Lifestyle within E-care Telemonitoring Platform» ICIMTH. 2015. P. 279–282.
20. Lagos-Ortiz K. et al. «An ontology-based decision support system for the diagnosis of plant diseases» Journal of Information Technology Research (JITR), 2017. Vol. 10, № 4. P. 42–55.
21. Rospocher M. и Serafini L. «An ontological framework for decision support» Joint International Semantic Technology Conference. – Springer, Berlin, Heidelberg. 2012. P. 239–254.
22. Saremi A. et al. «O2dss: A framework for ontology-based decision support systems in pervasive computing environment» 2008 Second Asia International Conference on Modelling & Simulation (AMS). – IEEE. 2008. P. 41–45.
23. Breuker J. «The construction and use of ontologies of criminal law in the ecourt european project» Proceedings of Means of electronic communication in court administration. 2003. P. 15–40.
24. Dzemydiene D. и Kazemikaitiene E. «Ontology-based decision support system for crime investigation processes» Information Systems Development. – Springer, Boston, MA, 2005. P. 427–438.
25. Fawei B. et al. «A Methodology for a Criminal Law and Procedure Ontology for Legal Question Answering» Joint International Semantic Technology Conference. – Springer, Cham. 2018. P. 198–214.
26. Newman M. «Network reconstruction and error estimation with noisy network data» arXiv preprint arXiv:1803.02427, 2018.
27. «Interdisciplinary Training in Complex Networks and Systems: Indiana University Bloomington» [В Интернете]. URL: https://cns-nrt.indiana.edu/ (дата обращения: 02 07 2019).

28. Евин И.А. «Введение в теорию сложных сетей» Компьютерные исследования и моделирование. 2010. Т. 2, № 2. С. 121–141.
29. Borgatti S.P. «Centrality and network flow» Social networks. 2005. Vol. 27, № 1. P. 55–71.
30. «Gephi - The Open Graph Viz Platform» [В Интернете]. URL: https://gephi.org/ (дата обращения: 02 07 2019).
31. Батура Т.В., Мурзин Ф.А. и Проскуряков А.В. «Программный комплекс для анализа данных из социальных сетей» Программные продукты и системы. 2015, № 4 (112).
32. Розенберг И.Н. «Онтологический подход в геоинформатике» Образовательные ресурсы и технологии, 2016, №. 5(17). С. 86–95.
33. «OWL Web Ontology Language Use Cases and Requirements» [В Интернете]. URL: http://www.w3.org/2006/04/OWL_UseCases-ru.html (дата обращения: 01 05 2019).
34. Antipov A.L. et al. «Dynamic ontology of air traffic management systems: Networking and modeling» Kyiv, 2014.
35. Тихомиров А.А. и др. «Сетевое описание и детализация угроз в проблемах обеспечения безопасности мегаполиса» Научные и образовательные проблемы гражданской защиты, № 2, 2014.
36. Salamon J.S. et al. «Using Goal Modeling and OntoUML for Reengineering the Good Relations Ontology» ONTOBRAS. 2017. P. 91–102.
37. Banerjee N., Chordia A. и Rajib P. «SEAMLESS ENTERPRISE COMPUTING USING ENTERPRISE APPLICATION INTEGRATION (EAI)» Journal of Services Research, 2005. Vol. 5, № 1,
38. «Home - Cellebrite» [В Интернете]. URL: https://www.cellebrite.com/en/home/ (дата обращения: 21 05 2019).
39. «Oxygen Forensics – Mobile forensic solutions: software and hardware» [В Интернете]. URL: https://www.oxygen-forensic.com/en/ (дата обращения: 21 05 2019).

REFERENCES:

[1] Vehov V. «Ispol'zovanie komp'juternyh tehnologij v kriminalisticheskoj dejatel'nosti i ugolovnom processe» VESTNIK AKADEMII SLEDSTVENNOGO KOMITETA ROSSIJSKOJ FEDERACII No 1/2014. S. 70–73 (in Russian).
[2] Garmaev Ju.P. Nastol'naja kniga pomoshhnika sud'i: Vyp. 1: Organizacija raboty i ugolovnoe sudoproizvodstvo, Ulan-Udje: SAPJeU, 2009. S. 60–73 (in Russian).
[3] Garmaev Ju.P. «Algoritm proverki materialov ugolovnogo dela». 2009, № 2. S. 16–21 (in Russian).
[4] Edwards J.S. «Expert Systems in Management and Administration - Are they really different from Decision Support Systems?» European Journal of Operational Research. 1992, № 61. P. 114–121.
[5] Little J.D.C., «Models and managers: The concept of a decision calculus» Management science. 1970. Vol. 16, № 8. P. 466–485.
[6] Sprague Jr R.H. «A framework for the development of decision support systems» MIS quarterly. 1980. P. 1–26.
[7] Thierauf R.J., «Decision support systems for effective planning and control: A case study approach» Prentice Hall PTR, 1982.
[8] Saraev A.D. i Shherbina O.A. «Sistemnyj analiz i sovremennye informacionnye tehnologii» Trudy Krymskoj Akademii nauk. 2006. S. 47-59 (in Russian).
[9] Almeida da Costa Júnior и Gilton Jose Ferreira da Silva, «A Decision Support System for Police Patrolling» 2018.
[10] «Technology Chicago Police Department» [On the Internet]. URL: https://home.chicagopolice.org/office-of-reform-management/technology (accessed: 15 04 2019).
[11] Kadar C., Maculan R. и Feuerriegel S., «Public decision support for low population density areas: An imbalance-aware hyper-ensemble for spatio-temporal crime prediction» Decision Support Systems. 2019, № 119. P. 107–117.
[12] Rzaev R.R. i dr. «Informacionnaja sistema podderzhki prinjatija processual'nyh reshenij» Sistemy i sredstva informatiki. 2016. T. 26, № 1. S. 182–198 (in Russian).
[13] «Edmonton Police Service IBM» [On the Internet]. URL: view-source:https://www.ibm.com/case-studies/edmonton-police-service-hybrid-cloud-integration-crime (accessed: 15 04 2019).
[14] Casey, D., Burrell, P. & Sumner, N. «Decision Support Systems in Policing» 2018.
[15] Golovnin O.K. i Romanova E.A. «Precedentnaja sistema podderzhki prinjatija reshenij po delam ob administrativnyh pravonarushenijah» Programmnye produkty i sistemy. 2018, № 1 (in Russian).
[16] «Razrabotka programmnogo obespechenija i baz dannyh. Sozdanie veb-sajtov. - ARM sledovatelja (doznavatelja)» [On the Internet]. URL: https://ts-group.ru/awp.php (accessed: 21 04 2019).
[17] «ARM sledovatelja. ARM rukovoditelja sledstvennogo podrazdelenija» [On the Internet]. URL: http://www.oviont.ru/services/develop/ais/arm/ (accessed: 21 04 2019).
[18] «Proekt "ARM Sledstvie".» [On the Internet]. URL: https://vk.com/armsledstvie (accessed: 21 04 2019).
[19] Benmimoune L. et al. «Ontology-based Medical Decision Support System to Enhance Chronic Patients' Lifestyle within E-care Telemonitoring Platform» ICIMTH. 2015. P. 279–282.

[20] Lagos-Ortiz K. et al. «An ontology-based decision support system for the diagnosis of plant diseases» Journal of Information Technology Research (JITR). 2017. Vol. 10, № 4. P. 42–55.
[21] Rospocher M. и Serafini L. «An ontological framework for decision support» Joint International Semantic Technology Conference. – Springer, Berlin, Heidelberg. 2012. P. 239–254.
[22] Saremi A. et al. «O2dss: A framework for ontology-based decision support systems in pervasive computing environment» 2008 Second Asia International Conference on Modelling & Simulation (AMS). – IEEE. 2008. P. 41–45.
[23] Breuker J. «The construction and use of ontologies of criminal law in the ecourt european project» Proceedings of Means of electronic communication in court administration. 2003. P. 15–40.
[24] Dzemydiene D. и Kazemikaitiene E. «Ontology-based decision support system for crime investigation processes» Information Systems Development. – Springer, Boston, MA, 2005. P. 427–438.
[25] Fawei B. et al. «A Methodology for a Criminal Law and Procedure Ontology for Legal Question Answering» Joint International Semantic Technology Conference. – Springer, Cham. P. 198–214, 2018.
[26] Newman M. «Network reconstruction and error estimation with noisy network data» arXiv preprint arXiv:1803.02427, 2018.
[27] «Interdisciplinary Training in Complex Networks and Systems: Indiana University Bloomington» [On the Internet]. URL: https://cns-nrt.indiana.edu/ (accessed: 02 07 2019).
[28] Evin I.A. «Vvedenie v teoriju slozhnyh setej» Komp'juternye issledovanija i modelirovanie. 2010. T. 2, № 2. S. 121–141 (in Russian).
[29] Borgatti S.P. «Centrality and network flow» Social networks. 2005. Vol. 27, № 1. P. 55–71.
[30] «Gephi - The Open Graph Viz Platform» [On the Internet]. URL: https://gephi.org/ (accessed: 02 07 2019).
[31] Batura T.V., Murzin F.A. i Proskurjakov A.V. «Programmnyj kompleks dlja analiza dannyh iz social'nyh setej» Programmnye produkty i sistemy. 2015, № 4 (112) (in Russia).
[32] Rozenberg I.N. «Ontologicheskij podhod v geoinformatike» Obrazovatel'nye resursy i tehnologii. 2016, №. 5(17). S. 86–95 (in Russian).
[33] «OWL Web Ontology Language Use Cases and Requirements» [On the Internet]. URL: http://www.w3.org/2006/04/OWL_UseCases-ru.html (accessed: 01 05 2019).
[34] Antipov A.L. et al. «Dynamic ontology of air traffic management systems: Networking and modeling» Kyiv, 2014.
[35] Tihomirov A.A. i dr. «Setevoe opisanie i detalizacija ugroz v problemah obespechenija bezopasnosti megapolis» Nauchnye i obrazovatel'nye problemy grazhdanskoj zashhity. 2014, № 2 (in Russian).
[36] Salamon J.S. et al., «Using Goal Modeling and OntoUML for Reengineering the Good Relations Ontology» ONTOBRAS. 2017. P. 91–102.
[37] Banerjee N., Chordia A. и Rajib P., «SEAMLESS ENTERPRISE COMPUTING USING ENTERPRISE APPLICATION INTEGRATION (EAI)» Journal of Services Research, 2005. Vol. 5, № 1.
[38] «Home - Cellebrite» [On the Internet]. USB: https://www.cellebrite.com/en/home/ (accessed: 21 05 2019).
[39] «Oxygen Forensics - Mobile forensic solutions: software and hardware» [On the Internet]. USB: https://www.oxygen-forensic.com/en/ (accessed: 21 05 2019).

Поступила в редакцию – 05 июля 2019 г. Окончательный вариант – 20 августа 2019 г.
Received – July 05, 2019. The final version – August 20, 2019.

Александр И. Чумаков
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-2663

ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ ЛАЗЕРНЫХ МЕТОДОВ ПРИ ОЦЕНКЕ ПАРАМЕТРОВ ЧУВСТВИТЕЛЬНОСТИ БИС К ЭФФЕКТАМ ВОЗДЕЙСТВИЯ ТЯЖЕЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ

DOI: http://dx.doi.org/10.26583/bit.2019.3.05

Аннотация. В работе проводится анализ применимости методов оценки параметров чувствительности БИС по одиночным радиационным эффектам (ОРЭ) с использованием сфокусированного лазерного излучения пикосекундной длительности с целью расширения их применения для субмикронных БИС. Проведено сравнение структуры трека тяжелой заряженной частицы и области ионизации полупроводниковой структуры при облучении сфокусированным лазерным излучением. Показано, что сравнение геометрических размеров необходимо проводить за времена формирования ионизационной реакции, когда область ионизации трека расширяется за счет амбиполярной диффузии. Определены ограничения, обусловленные влиянием оптических неоднородностей, расположенных на поверхности кристалла БИС, а также при облучении с донной стороны кристалла. Показано, что лазерные методы могут быть применимы для оценки зависимостей сечений одиночных радиационных эффектов в функции линейных потерь энергии (ЛПЭ) для полупроводниковых структур с размерами, существенно меньшими, чем диаметр сфокусированного лазерного излучения. Представлены дополнительные возможности лазерных методов, позволяющие определять области возникновения ОРЭ, исследовать влияние режима и эффективность методов парирования ОРЭ. Представленные результаты позволяют использовать методы оценки параметров чувствительности по ОРЭ на основе сфокусированного ЛИ для БИС с глубоко субмиронными размерами.

Ключевые слова: одиночные радиационные эффекты, сфокусированное лазерное излучение, параметры чувствительности.

Для цитирования: ЧУМАКОВ, Александр И. ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ ЛАЗЕРНЫХ МЕТОДОВ ПРИ ОЦЕНКЕ ПАРАМЕТРОВ ЧУВСТВИТЕЛЬНОСТИ БИС К ЭФФЕКТАМ ВОЗДЕЙСТВИЯ ТЯЖЕЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 58-67. 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1217>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.05.

Alexander I. Chumakov
National Research Nuclear University MEPhI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-26637

Possibilities and limitations of focused laser technique application for SEE sensitivity parameters estimation

DOI: http://dx.doi.org/10.26583/bit.2019.3.05

Abstract. The paper analyzes the applicability of methods for estimating the parameters of the VLSI sensitivity by single radiation effects (SEE) using focused laser radiation of picosecond duration in order to expand their application for submicron VLSI. A comparison of ionization track structure from a heavy charged particle and the ionization region of a semiconductor structure under focused laser radiation is made. It is shown that the comparison of geometric dimensions should be carried out during the ionization reaction, when the ionization region of the track expands due to ambipolar diffusion. Limitations due to the influence of optical inhomogeneities located on the surface of the VLSI chip, as well as under irradiation from the bottom side of the chip are determined. It is shown that laser methods can be applied to estimate the dependences of cross sections of single radiation effects as a function of

linear energy transfer (LET) for semiconductor structures with sizes significantly smaller than the diameter of the focused laser radiation. Additional features of laser methods are presented to determine the SEE location on chip surface and to study the influence of the electrical mode and the effectiveness of SEE parry methods. The presented results allow the use of laser technique to estimate SEE sensitivity parameters estimation for deep submicron VLSI.
Keywords: single event effects, focused picosecond laser beam, SEE sensitivity parameters.
For citation: Chumakov, Alexander I. Possibilities and limitations of focused laser technique application for SEE sensitivity parameters estimation. IT Security (Russia), [S.l.], v. 26, n. 3, p. 58-67. 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1217>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.05.

Введение

Современные изделия микроэлектроники имеют высокую чувствительность к эффектам воздействия тяжелых заряженных частиц (ТЗЧ), что во многих случаях приводит к потере информации и функциональным сбоям электронной аппаратуры [1-3]. Подобное поведение больших интегральных микросхем (БИС) создает определенные трудности при построении радиоэлектронной аппаратуры космического пространства из-за возникновения в них одиночных радиационных эффектов (ОРЭ) типа отказов или сбоев. Поэтому с целью парирования нежелательных ОРЭ, приводящих к потере информации, проводят оценку чувствительности БИС к воздействию ТЗЧ на ускорителях ионов. Однако экспериментальная оценка параметров чувствительности БИС по ОРЭ, к которым относятся сечение, насыщение и пороговые значения линейных потерь энергии (ЛПЭ), подобным методом имеет ряд существенных недостатков, связанных как с экономическими факторами, так и собственно с научно-техническими проблемами. В данном случае, например, невозможно точное определение местоположения чувствительной области на кристалле ИС, фактически крайне затруднительно проведение испытаний при отрицательных температурах, очень неэффективными оказываются исследования по влиянию различных режимов и условий эксплуатации на бессбойное функционирование электронной аппаратуры и т.п.

Альтернативой является метод экспериментальных исследований, основанный на применении сфокусированного лазерного излучения (ЛИ) пикосекундной длительности [4-7]. Метод основан на том, что с помощью ЛИ пытаются в полупроводниковой структуре смоделировать пространственно-временное распределение избыточных носителей заряда, такое же, как и при прохождении ТЗЧ. Однако совершенно очевидно, что сделать полную эквивалентность на этом физическом уровне не представляется возможным в силу принципиальных различий в физике взаимодействия оптического излучения и ТЗЧ с материалами полупроводниковой структурой. При этом во многих случаях удается достичь эквивалентности на электрическом уровне, проявляющейся в тождественности возникающих электрических сигналов как внутри БИС, так и на ее выводах. В принципе этого достаточно для корректного моделирования эффектов воздействия ТЗЧ с помощью сфокусированного лазерного излучения.

Следует также сразу отметить, что лазерное излучение не позволяет моделировать все типы возникающих ОРЭ, в частности, эффекты, связанные с ионизацией диэлектрических структур или с образованием радиационных дефектов кристаллической решетки полупроводника типа «спайков» [2].

1. Формирование «трека ТЗЧ» оптическим излучением

В основе моделирования сфокусированным лазерным излучением эффектов воздействия ТЗЧ лежит возможность генерации локального заряда внутри отдельной

полупроводниковой чувствительной области по аналогии с ионизацией внутри трека при прохождении ТЗЧ. Однако в силу физических ограничений минимальный размер оптического пятна ограничен длиной волны и характеристиками фокусирующей системы. Предельно достижимый минимальный диаметр сфокусированного лазерного излучения d_e определяется из соотношения [4]:

$$d_e=4\lambda f/\pi d_l; \quad (1)$$

где λ - длина волны; f - фокусное расстояние объектива, d_l - диаметр фокусирующей линзы.

Таким образом, для получения минимального радиуса фокусирующего пятна на поверхности кристалла БИС необходимо увеличивать диаметр линзы и уменьшать фокусное расстояние. Однако при этом возрастает угол расходимости оптического излучения, что приводит к заметному увеличению диаметра пятна по мере отдаления от точки фокусировки. С учетом того что в современных БИС имеется большая неопределенность в толщинах пассивирующего окисла, необходимо обеспечить, как минимум, относительно слабую расходимость оптического излучения на длине не менее L_p~10 мкм. В этом случае получим, что минимальный диаметр сфокусированного лазерного излучения ограничивается следующим образом:

$$d_e\geq(4\lambda L_p/\pi K_l)^{1/2}; \quad (2)$$

где K_l – допустимый коэффициент увеличения диаметра лазерного пятна на расстоянии L_p от места глубокой фокусировки.

Несложно заметить, что для длины волны в районе $\lambda\approx$1.0 мкм оптимальный диаметр оптического пятна лежит в районе 2…3 мкм.

Наилучшие характеристики лазерного излучения для фокусировки имеют место при гауссовой форме распределения интенсивности изучения в зависимости от радиуса

$$I(r) = I_o \cdot \exp\left[-\left(r/r_{lo}\right)^2\right] \quad (3)$$

где I_o – интенсивность лазерного излучения в центре гауссова пучка; r_{lo} – характерный радиус лазерного пучка. Это исходное распределение и будет определять размеры начального «трека ТЗЧ».

Существуют также ограничения на минимальный размер длины фокусного расстояния. На него накладывается с одной стороны конечная толщина самой линзы (чем больше диаметр линзы, тем она толще), а с другой – необходимость фокусировки ЛИ на поверхность кристалла БИС, находящихся в корпусах. Исходя их этих ограничений, значение f не может быть менее 10 мм.

При воздействии ТЗЧ геометрические размеры области ионизации несколько иные. В первом приближении, радиальное распределение дозы вокруг трека ТЗЧ описывается следующей приближенной зависимостью [8]:

$$D(r) \approx D_o\cdot(r_o/r)^2, \quad (4)$$

где D_o и r_o – коэффициенты аппроксимаций. Величина D_o определяется в первую очередь значениями ЛПЭ, а радиус r_o с типовым значением около долей нм зависит от приведенной на нуклон энергии ТЗЧ.

Исходя из этих соображений, на первый взгляд, кажется невозможным моделирование сфокусированным лазерным излучением треков ТЗЧ, радиус которых в значительной степени определяется пробегами вторичных электронов и существенно меньше характерных размеров сфокусированного оптического пятна ЛИ. Однако, как будет показано ниже, данное обстоятельство во многих случаях не оказывает заметного влияния на конечный результат, а именно оценку параметров чувствительности по одиночным эффектам сбоев и отказов при воздействии ТЗЧ.

2. Влияние геометрических факторов

Из представленных соотношений (3) и (4) для форм распределения генерированных излучением избыточных носителей заряда следует, что напрямую их сравнить сложно. Хотя надо отметить, что в ряде программ физико-топологического моделирования типа TCAD для описания распределения вторичных электронов вдоль оси трека также используется гауссово распределение, правда с совершенно другой величиной характерного радиуса трека. Ясно только одно, что исходный радиус при прохождении ТЗЧ лежит в районе нескольких нм, тогда как оптический радиус около 1 мкм.

На самом деле подобное сравнение не является корректным. Дело в том, что в конечном итоге нас интересует электрический отклик полупроводниковой структуры на локальную ионизацию. Очевидно, что в этом случае можно не анализировать времена, меньшие характерного времени ионизационной реакции полупроводниковой структуры τ_e. Это время меняется в широких пределах и зависит как от технологии изготовления БИС, так и от самого ОРЭ. Например, по эффектам одиночных сбоев

$$\tau_e \approx R_o \cdot C_{in}\,, \tag{5}$$

где R_o – сопротивление открытого транзистора, C_{in} - эквивалентная емкость ячейки памяти по входу.

Для технологий 65…90 нм значения R_o могут составлять несколько кОм, а C_{in} лежать около 10 фФ [9]. Таким образом, для приведенных технологий значение τ_e лежит в пределах десятков пс, а за это время (t) трек, созданный ТЗЧ, за счет процессов амбиполярной диффузии расползается, и распределение концентрации избыточных электронно-дырочных пар приближенно описывается следующим соотношением:

$$n(r,t) \approx \frac{L_z \cdot \rho}{4\pi \cdot \varepsilon_i \cdot D_a \cdot t} exp\left(-\frac{r^2}{4D_a \cdot t}\right); \tag{6}$$

где L_z – линейные потери энергии ТЗЧ; ρ - плотность кремния; ε_i - энергия образования одной электронно-дырочной пары; D_a - коэффициент амбиполярной диффузии.

Нетрудно заметить, что за времена порядка сотен пс трек достаточно сильно изменяется по сравнению со своей первоначальной формой (4) и его характерный размер становится порядка $r_\tau \sim 2\sqrt{D_a \cdot t}$ и составляет уже величину порядка 1 мкм. По сути дела, в диапазоне этих времен уже нельзя говорить об узком исходном треке, проходящем через чувствительную область, а более корректно определять область локальной ионизации, покрывающей отдельную чувствительную область. Следует также отметить, что полученные размеры уже коррелируют с диаметром сфокусированного лазерного излучения (1).

Анализ временных процессов развития одиночных тиристорных эффектов [2, 8] показывает, что для них характерные времена лежат в районе десятков нс. Соответственно, в этом случае величина r_τ лежит уже около 10 мкм, что заведомо больше диаметра сфокусированного лазерного излучения.

Отметим, что в этих временных интервалах на распределение концентрации избыточных носителей заметного влияния процессы рекомбинации электронно-дырочных пар не оказывают. Действительно, характерное время рекомбинации Шокли-Рида составляет величины около 1 мкс, а характерное время процессов Оже рекомбинации даже при концентрациях около 10^{19} см$^{-3}$ не меньше единиц нс.

Надо также подчеркнуть, что полученные ограничения на минимальные размеры эффективного трека могут оказаться еще менее жесткими. Действительно, при высоких концентрациях электронно-дырочных пар происходит полное заливание p-n переходов, которые фактически исчезают. В этот период времени дрейфовые процессы переноса

носителей заряда типа эффекта «воронки» несущественны из-за малых размеров чувствительной области. По сути дела, в этом случае имеют место эффекты, похожие на обычные объемные ионизационные эффекты с очень высокими уровнями ионизации. Другими словами, происходит «насыщение» полупроводниковой структуры, и до тех пор, пока она из него не выйдет, отдельных элементов БИС фактически не существует. По этому критерию также можно оценить максимальный эффективный радиус трека r_{max}, исходя из равенства концентраций носителей заряда в базовой области p-n перехода N_b и в треке:

$$r_{max} = \sqrt{\frac{L_z \cdot \rho}{\pi \cdot e \cdot \varepsilon_i \cdot N_b}}; \quad (7)$$

Даже при ЛПЭ на уровне 1 МэВ·см^2/мг и типовых концентрациях в подложке N_b~10^{16} см$^{-3}$ получаем значение $r_{max} \approx 1$ мкм. Если же значение ЛПЭ увеличивается практически на два порядка (до значений 80 МэВ·см^2/мг), то значение «максимального» радиуса трека уже будет составлять почти 10 мкм. Совершенно очевидно, что в этом случае эквивалентность сфокусированного лазерного излучения и ТЗЧ даже на физическом уровне имеет место.

Таким образом, из представленных результатов следует, что при относительно высоких значениях ЛПЭ (более 5 МэВ·см^2/мг) влияние различий в геометрических размерах трека иона и области ионизации сфокусированным лазерным излучением на электрическую реакцию элементов БИС фактически отсутствует при моделировании одиночных радиационных дефектов, вызванных объемной ионизацией.

3. Влияние оптических потерь

Более сильное влияние могут оказать потери ЛИ на различных оптических неоднородностях, находящихся на поверхности кристалла БИС. Действительно, все вышеизложенное относилось к случаю анализа практически «чистой» и прозрачной поверхности кристалла БИС. В реальной ситуации над чувствительными полупроводниковыми элементами находятся слои металлизации поликремния, оксидов и т.п. Совершенно очевидно, что в этом случае формирование сфокусированного оптического пятна будет происходить другим образом. На эти процессы будут влиять эффекты отражений, в том числе и многократных, интерференции, дифракции и т.п. На рис. 1 в качестве примера представлена упрощенная картинка энерговыделения сфокусированного лазерного излучения внутри чувствительного микрообъема (SV) элемента БИС. Как несложно заметить, классическое приближение (соотношения (1) и (3)) в этом случае практически не работает. К наиболее существенным потерям лазерного излучения следует отнести отражение от слоев металлизации (5), поглощения в слоях поликремния (2) и вышележащих слоях высоколегированных полупроводниковых областей (3). Тем не менее часть оптического излучения даже при наличии практически сплошной металлизации может достичь чувствительной области. В основном это будет вторичное излучение за счет внутреннего отражения от верхней поверхности кристалла ИС (6), многократного отражения от многоуровневой металлизации (7); рассеянного ЛИ (8) и отражения его от донной поверхности кристалла (9). Очевидно, что говорить в этом случае о какой-то конкретной величине диаметра сфокусированного ЛИ и о расчетных оценках величины энергии ЛИ внутри чувствительной области не представляется возможным. Возможным выходом из создавшейся ситуации является экспериментальная оценка либо самих этих величин, либо их влияния на конечный результат.

Экспериментальная оценка величины потерь энергии ЛИ, выделенной в чувствительном объеме, возможна по ионизационной реакции БИС в цепи питания в

предположении, что она формируется по всей облучаемой локальной площади кристалла БИС. Именно такой подход лежит в основе локальной лазерной методики для оценки эффективных значений ЛПЭ при воздействии лазерным излучением [10-12].

Однако при использовании данной методики существует ряд ограничений. Одно из них связано с тем, чтобы оптические потери не превышали двух… трех порядков, так как в противном случае возникновение радиационного эффекта возможно за счет переотраженного оптического излучения, которое тяжело сопоставить с исходным сфокусированным лазерным излучением.

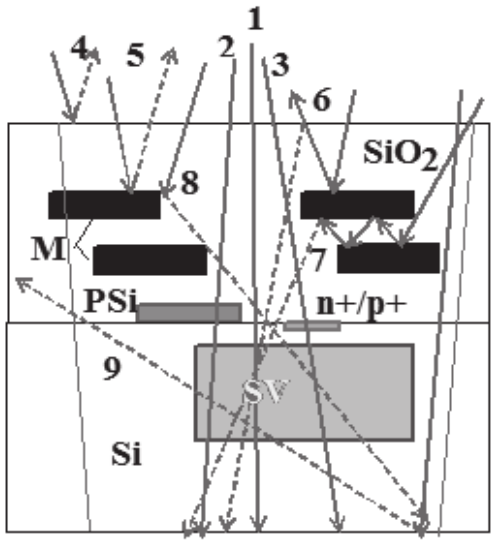

Рис. 1. Энерговыделение ЛИ в чувствительном объеме (SV) элемента БИС при облучении со стороны приборного слоя: 1 – прохождение ЛИ через диоксид кремния с потерями энергии в вышележащих слоях кремния; 2 – дополнительные потери в поликремнии (PSi); 3 – дополнительные потери энергии ЛИ в вышележащих n+/p+ слоях; 4 – отражение ЛИ от поверхности кристалла БИС; 5 – потери энергии ЛИ на слоях металлизации (М); 6 – вторичное ЛИ после внутреннего отражения от поверхности кристалла БИС; 7 – вторичное ЛИ после многократного отражения от многоуровневой металлизации; 8 – рассеяние ЛИ; 9 – отражение ЛИ от донной части кристалла БИС
(Fig. 1. Laser radiation energy losses in the sensitive volume (SV) of VLSI element irradiated by from front chip side: 1 – passing of laser beam through silicon dioxide with energy losses in the upper layers of silicon; 2 – additional losses in polysilicon (PSi); 3 – additional energy losses of laser beam in the upper lying n + / p + layers; 4 – optical reflection from the chip surface; 5 – optical energy losses on the metallization layers (M); 6 – secondary laser radiation after internal reflection from chip surface; 7 – secondary laser radiation after multiple reflection from multi-level metallization; 8 – optical scattering; 9 – laser reflection from the backside of chip)

Другое ограничение обусловлено тем обстоятельством, что в некоторых структурах БИС (например, в некоторых аналоговых и смешанных БИС, в изделиях по КНИ технологии) ионизационный ток может зависеть от местоположения облучаемой локальной области при отсутствии оптических неоднородностей на поверхности кристалла. В этом случае может потребоваться дополнительное сканирование поверхности кристалла БИС локальным рентгеновским воздействием, хотя для КНИ изделий можно обойтись поправочным коэффициентом, учитывающим долю кремневой поверхности.

В случае больших оптических потерь представляется более оправданным переход на облучение сфокусированным (локальным) ЛИ с тыльной стороны кристалла БИС (рис. 2). Очевидно, что в этом случае возрастают потери энергии лазерного излучения в подложке,

особенно, если она является высоколегированной (более $10^{17}…10^{18}$ см$^{-3}$), однако это обстоятельство не является существенным, если за счет этих потерь энергии не происходит существенного разогрева кристалла. Достоинством облучения с тыла являются также более равномерные оптические потери ЛИ по всей поверхности БИС, что позволяет во многих случаях использовать одну и ту же величину коэффициента потерь вне зависимости от места расположения области сфокусированного лазерного воздействия.

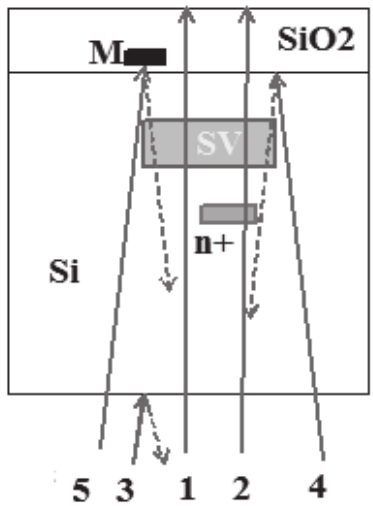

Рис. 2. Энерговыделение ЛИ в чувствительном объеме (SV) элемента БИС при облучении с донной стороны кристалла: 1 – прохождение ЛИ через кремневую подложку с потерями энергии; 2 – дополнительные потери в скрытых n+(p+) слоях; 3 – отражение ЛИ от поверхности кристалла БИС; 4 – вторичное ЛИ после внутреннего отражения от поверхности кристалла БИС; 5 – вторичное ЛИ после внутреннего отражения от металлизации БИС
(Fig. 2. Laser radiation energy losses in the sensitive volume (SV) of VLSI element by backside irradiation: 1 – passing of laser beam through silicon substrate with energy losses; 2 – additional losses in hidden n + / p + layers; 3 – optical reflection from the chip surface; 4 – secondary laser radiation after internal reflection from chip surface; 5 – secondary laser radiation after internal reflection from metallization)

4. Возможности лазерных методов

Лазерным излучением можно смоделировать практически любые ЛПЭ для существующих ядерных частиц. Действительно, в первом приближении можно записать следующую взаимосвязь между энергией лазерного излучения $J_{ли}$ и эффективным значением ЛПЭ L_z [2]:

$$L_z = 1{,}8 \cdot 10^4 \cdot \alpha_o \cdot J_{ли} \cdot \lambda \cdot (1-R_\lambda)/(K_l \cdot \rho), \quad [\text{МэВ}\cdot\text{см}^2/\text{мг}], \qquad (8)$$

где α_o – коэффициент межзонного поглощения лазерного излучения в 1/см; λ – длина волны лазерного излучения в мкм; $J_{ли}$ – энергия лазерного излучения в нДж; R_λ – коэффициент отражения от поверхности ИС; ρ – плотность полупроводника в мг/см^3; K_l – коэффициент потерь ЛИ на оптических неоднородностях.

Таким образом, за счет изменения энергии ЛИ можно получить любое эквивалентное значение ЛПЭ, а за счет плавной регулировки энергии ЛИ удается более точно оценить пороговые эквивалентные значения ЛПЭ для возникновения ОРЭ.

Очевидно, что основная проблема заключается в оценке коэффициента K_l. Рекомендуется проводить его оценку с помощью калибровочных испытаний по результатам облучений ионами не менее чем при двух значащихся значениях сечений

одиночных эффектов [13]. Вместе с тем существует возможность его оценки и другими методами с использованием методики локального лазерного облучения, а также за счет применения импульсных и/или стационарных воздействий [14-15].

Оценка сечения насыщения σ_s проводится из результатов сканирования всей площади кристалла БИС (A_{IC}) при относительно высокой энергии (на порядок больше, чем пороговая энергия возникновения ОРЭ) и определения общего количества возникающих ОРЭ N_{SEE}:

$$\sigma_s \approx A_{IC} \cdot N_{SEE}/N_l; \quad (9)$$

где N_l – общее количество импульсов ЛИ при сканировании общей поверхности кристалла БИС.

Следует отметить, что соотношение (8) может давать заметную погрешность при относительно малых значениях ЛПЭ (менее 5 МэВ·см^2/мг) за счет возможности возникновения одновременно нескольких ОРЭ из-за влияния конечного размера сфокусированного ЛИ. Однако при больших ЛПЭ эти различия исчезают.

Кроме этого, лазерные методы позволяют решить следующие задачи:

- возможность целенаправленного воздействия на интересующие области кристалла БИС;
- исследование влияние электрического и функционального режимов БИС на параметры чувствительности;
- возможность исследования влияния условий эксплуатации (температура, сопутствующая поглощенная доза ионизирующего излучения) на параметры чувствительности;
- отработка мер парирования одиночных радиационных эффектов в составе аппаратуры и т.п.

Действительно, можно воздействовать сфокусированным ЛИ с точностью до долей мкм на определенные участки кристалла БИС для определения наиболее чувствительных элементов и узлов к различным типам ОРЭ. При этом существуют неограниченные возможности по исследованию возникающих эффектов от режима работы, температуры, суммарной дозы и т.п. Например, для тиристорного эффекта можно экспериментально снять зависимость тока в состоянии тиристорного эффекта от координат воздействия ЛИ или карту расположения ОРЭ при разных значения энергии ЛИ (ЛПЭ). Следует отметить, что только с помощью лазерных методов существуют уникальные возможности по привязке частоты синхронизации БИС к моменту воздействия ЛИ.

5. Заключение

Результаты проведенного анализа позволяют сделать следующие краткие выводы:

- методы оценки параметров чувствительности по ОРЭ на основе сфокусированного ЛИ могут использоваться даже для БИС с глубоко субмикронными размерами;
- основное ограничение применения лазерных методов обусловлено влиянием оптических неоднородностей, расположенных на поверхности кристалла БИС. Данное ограничение может быть устранено при облучении БИС с тыльной стороны;
- эквивалентные значения ЛПЭ могут быть определены как с помощью калибровочных испытаний на ускорителе ионов, так и с применением методики локального лазерного воздействия по ионизационной реакции в цепи питания;
- значения сечений ОРЭ определяются путем сканирования всей площади кристалла и определения общего количества возникающих ОРЭ;

- лазерные методы дают уникальные возможности по определению наиболее уязвимых элементов БИС и исследованиям влияния режимов работы и эксплуатации на чувствительность БИС к воздействию ТЗЧ.

СПИСОК ЛИТЕРАТУРЫ:

1. Ионизирующее излучение космического пространства и их воздействие на бортовую аппаратуру космических аппаратов / Под ред. Г.Г. Райкунова. М.: Физматлит, 2013. – 256 с.
2. Чумаков А.И. Действие космической радиации на ИС. М.: Радио и связь. 2004. – 320 с. URL: < https://elibrary.ru/item.asp?id=19635287 > (дата обращения: 11.07.2019).
3. Чумаков А.И., Ужегов В.М., Ахметов А.О., Бойченко Д.В., Яненко А.В., Рясной Н.В. Оценка показателей стойкости интегральных схем при воздействии тяжелых заряженных частиц с использованием различных моделей. Безопасность информационных технологий, [S.l.], v. 24, n. 1. P. 73–84, apr. 2017. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/58> (дата обращения: 11.07.2019). DOI: http://dx.doi.org/10.26583/bit.2017.1.09.
4. Маврицкий О.Б., Чумаков А.И., Егоров А.Н., Печенкин А.А., Никифоров А.Ю. Технические средства проведения лазерных испытаний полупроводниковых элементов на стойкость к воздействию тяжелых заряженных частиц (Обзор). Приборы и техника эксперимента, № 5, 2016. С. 5–29. URL: https://elibrary.ru/item.asp?id=26665034 (дата обращения: 11.07.2019).
5. Чумаков А.И., Печенкин А.А., Егоров А.Н., Маврицкий О.Б., Баранов С.В., Васильев А.Л., Яненко А.В. Методика оценки параметров чувствительности ИС к тиристорному эффекту при воздействии отдельных ядерных частиц. Микроэлектроника, том 37, № 1, 2008. С. 45–51. URL: https://elibrary.ru/item.asp?id=9594374 (дата обращения: 11.07.2019).
6. Егоров А.Н., Маврицкий О.Б., Чумаков А.И., Никифоров А.Ю., Телец В.А., Печенкин А.А., Яненко А.В., Кольцов Д.О., Савченков Д.В. Лазерные имитаторы «ПИКО» для испытаний электронной компонентной базы на стойкость к воздействию отдельных ядерных частиц. Спецтехника и связь, № 4-5, 2011. С. 8–13. URL: https://elibrary.ru/item.asp?id=17307023 (дата обращения: 11.07.2019).
7. Новиков А.А., Печенкин А.А., Чумаков А.И., Ахметов А.О., Маврицкий О.Б. Испытания ИС на стойкость к воздействию ТЗЧ в диапазоне эксплуатационных температур с использованием лазерных методов. Безопасность информационных технологий, [S.l.], v. 23, n. 3. P. 55–60, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/18 (дата обращения: 11.07.2019).
8. Waligorski M.R.P., Hamm R.N., Katz R. The radial distribution of dose around the path of a heavy ion in liquid water //Nucl. Tracks and Radiat. Meas. v. 11, 1986. P. 306−319.
9. Pavlov A. CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies. Spinger, 2008. – 193 p.
10. Чумаков А.И., Маврицкий О.Б., Егоров А.Н., Печенкин А.А., Савченков Д.В., Новиков А.А., Васильев А.Л., Яненко А.В. Способ расчетно-экспериментальной оценки радиационной стойкости интегральных схем к воздействию отдельных заряженных частиц, основанный на локальном лазерном облучении. Патент на изобретение RU 2661556 04.07.2017. URL: <https://elibrary.ru/item.asp?id=37377405.> (дата обращения: 11.07.2019).
11. Chumakov A.I., Pechenkin A.A., Savchenkov D.V., Tararaksin A.S., Vasil'ev A.L., Yanenko A.V. Local Laser Irradiation Technique for SEE Testing of ICs. Proceedings of 2011 12th European Conference on Radiation and Its Effects on Components and Systems. (RADECS 2011). P. 449–453. URL: < https://elibrary.ru/item.asp?id=18056923> (дата обращения: 11.07.2019).
12. Savchenkov D.V., Chumakov A.I., Petrov A.G., Pechenkin A.A., Egorov A.N., Mavritskiy O.B., Yanenko A.V. Study of SEL and SEU in SRAM using different laser techniques. Proceedings of the European Conference on Radiation and its Effects on Components and Systems, RADECS, art. no. 6937411, (2013). URL: < https://elibrary.ru/item.asp?id=23980829> (дата обращения: 11.07.2019).
13. Яненко А.В., Чумаков А.И., Печенкин А.А., Савченков Д.В., Тараракси А.С., Васильев А.Л. Сравнительный анализ испытаний ЭРИ на стойкость к воздействию отдельных ядерных частиц на лазерных имитаторах и ускорителях ионов Спецтехника и связь, №№4-5, 2011. С. 4–7. URL: < https://elibrary.ru/item.asp?id=17307022> (дата обращения: 11.07.2019).
14. Чумаков. А.И., Васильев А.Л., Печенкин А.А., Савченков Д.В., Тараракси А.С., Яненко А. В. Совместное использование лазерной и импульсной гамма_установок при оценке параметров чувствительности БИС к эффектам воздействия отдельных ядерных частиц. Микроэлектроника, т. 41, №4, 2012. С. 243–247. URL: <https://elibrary.ru/item.asp?id=17745871> (дата обращения: 11.07.2019).

15. Чумаков А.И. Лазерная методика оценки параметров чувствительности БИС к эффектам воздействия отдельных заряженных частиц. Микроэлектроника. т. 47, № 3, 2018. С. 198–204. URL: https://elibrary.ru/item.asp?id=34925085 (дата обращения: 11.07.2019).

REFERENCES:

[1] Ioniziruyushcheye izlucheniye kosmicheskogo prostranstva i ikh vozdeystviye na bortovuyu apparaturu kosmicheskikh apparatov /Pod red. G.G. Raykunova. M.: Fizmatlit, 2013. – 256 s. (in Russian).
[2] Chumakov A.I., Deistvie kosmicheskoi radiatsii na IS (Effects of Cosmic Radiation on IC), Moscow: Radio i Svyaz', 2004. – 320 s. URL: https://elibrary.ru/item.asp?id=19635287 (accessed: 11.07.2019) (in Russian).
[3] Chumakov A.I., Uzhegov V.M., Akhmetov O.A., Boychenko D.V., Yanenko A.V., Ryasnoy N.V. Single Event Effects Rate Calculation with Different Models. IT Security (Russia), [S.l.], v. 24, n. 1. P. 73–84, apr. 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/58 (accessed: 11.07.2019). DOI: http://dx.doi.org/10.26583/bit.2017.1.09 (in Russian).
[4] Mavritskii O.B., Egorov A.N., Nikiforov A.Y., Chumakov A.I., Pechenkin A.A. Laser Equipment For Hardness Evaluation Of Semiconductor Elements Exposed To Heavy Charged Particles (Review) Instruments and Experimental Techniques. V. 59, № 5, 2016. P. 627–649. URL: https://elibrary.ru/item.asp?id=26665034 (accessed: 11.07.2019).
[5] Chumakov A.I., Pechenkin A.A., Egorov A.N., Mavritsky O.B., Baranov S.V. Vasil'ev A.L., Yanenko A.V. Estimating IC susceptibility to single-event latchup. Russian Microelectronics, v.37 (1), 2008. P. 41–46. URL: https://elibrary.ru/item.asp?id=9594374 (accessed: 11.07.2019).
[6] Egorov A.N., Mavritskii O.B., Chumakov A.I., Nikiforov A.Y., Телец В.А., Pechenkin A.A., Yanenko A.V., Kol`cov D.O., Savchenkov D.V. Lazernyye imitatory «PICO» dlya ispytaniy elektronnoy komponentnoy bazy na stoykost' k vozdeystviyu otdel'nykh yadernykh chastits. Spetstekhnika i svyaz', № 4-5, 2011. S. 8–13. URL: https://elibrary.ru/item.asp?id=17307023 (accessed: 11.07.2019). (in Russian).
[7] Novikov A.A., Pechenkin A.A., Chumakov A.I., Akhmetov O.A., Mavritskii See laser testing at different temperatures. IT Security (Russia), [S.l.], v. 23, n. 3. P. 55–60, oct. 2016. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/18> (accessed: 11.07.2019) (in Russian).
[8] Waligorski M.R.P., Hamm R.N., Katz R. The radial distribution of dose around the path of a heavy ion in liquid water. Nucl. Tracks and Radiat. Meas. 1986, v. 11. P. 306−319.
[9] Pavlov A. CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies. Spinger. 2008. – 193 p.
[10] Chumakov A.I., Mavritskii O.B., Egorov A.N., Pechenkin A.A., Savchenkov D.V., Novikov A.A., Vasil'ev A.L., Yanenko A.V. Sposob raschetno-eksperimental'noy otsenki radiatsionnoy stoykosti integral'nykh skhem k vozdeystviyu otdel'nykh zaryazhennykh chastits, osnovannyy na lokal'nom lazernom. obluchenii. Patent na izobreteniye RU 2661556 04.07.2017. URL: https://elibrary.ru/item.asp?id=23980829 (accessed: 11.07.2019) (in Russian).
[11] Chumakov A.I., Pechenkin A.A., Savchenkov D.V., Tararaksin A.S., Vasil'ev A.L., Yanenko A.V. Local Laser Irradiation Technique for SEE Testing of ICs. Proceedings of 2011 12th European Conference on Radiation and Its Effects on Components and Systems. (RADECS 2011). P. 449–453. URL: https://elibrary.ru/item.asp?id=18056923 (accessed: 11.07.2019).
[12] Savchenkov D.V., Chumakov A.I., Petrov A.G., Pechenkin A.A., Egorov A.N., Mavritskiy O.B., Yanenko A.V. Study of SEL and SEU in SRAM using different laser techniques. Proceedings of the European Conference on Radiation and its Effects on Components and Systems, RADECS, art. no. 6937411, (2013). URL: https://elibrary.ru/item.asp?id=23980829 (accessed: 11.07.2019).
[13] Yanenko A.V., Chumakov A.I., A.A. Pechenkin A.A., Savchenkov D.V., Tararaksin A.S., A Vasil'ev A.L. Sravnitel'nyy analiz ispytaniy ERI na stoykost' k vozdeystviyu otdel'nykh yadernykh chastits na lazernykh imitatorakh i uskoritelyakh ionov Spetstekhnika i svyaz', № 4-5, 2011. S. 4–7. URL: https://elibrary.ru/item.asp?id=17307022 (accessed: 11.07.2019) (in Russian).
[14] Chumakov A.I., Vasil'ev A.L., Pechenkin A.A., Savchenkov D.V., Tararaksin A.S., Yanenko A.V. Single-event-effect sensitivity characterization of LSI circuits with a laser-based and a pulsed gamma-ray testing facilities used in combination. Russian Microelectronics, v. 41, № 4, 2012. P. 221–225. URL: https://elibrary.ru/item.asp?id=20472612 (accessed: 11.07.2019).
[15] Chumakov A.I. Laser method of evaluating parameters of LSI sensitivity to the impact of single ions Russian Microelectronics, v. 47, № 3, 2018. P. 175–180. URL: https://elibrary.ru/item.asp?id=35483601 (accessed: 11.07.2019)

Поступила в редакцию – 05 июля 2019 г. Окончательный вариант – 18 сентября 2019 г.
Received – July 05, 2019. The final version – September 18, 2019.

Александр В. Барабанов[1], Алексей С. Марков[2], Валентин Л. Цирлов[3]
[1, 2]Московский государственный технический университет имени Н.Э. Баумана,
ул. 2-я Бауманская, 5, г. Москва, 105005, Россия
[3]Научно-производственное объединение «Эшелон»,
ул. Электрозаводская, 24, г. Москва, 107023, Россия
[1]e-mail: mail@cnpo.ru, https://orcid.org/0000-0003-4061-6611
[2]e-mail: a.markov@npo-echelon.ru, https://orcid.org/0000-0003-0111-7377
[3]e-mail: v.tsirlov@bmstu.ru, https://orcid.org/0000-0003-2657-4179

О СИСТЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦЕПЕЙ ПОСТАВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2019.3.06

Аннотация. В работе представлены результаты систематизации мер защиты информационных ресурсов от компьютерных атак на цепи поставок программного обеспечения и программно-аппаратных комплексов. Отмечены феномены, актуальность и востребованность тематики защиты цепей поставки ИТ-продукции. Приведена статистика по заимствованным компонентам программной продукции и программных комплексов. Приведены примеры компьютерных атак на ресурсы и процессы цепи поставок программного обеспечения. Проведен анализ существующей терминологической базы в области безопасности цепей поставок программного обеспечения. Сформулированы основные свойства, характерные для терминов «цепь поставок» и «атака на цепь поставок». Проведен анализ существующих моделей угроз информационной безопасности, связанных с компьютерными атаками на цепи поставок программной продукции. Выявлены ограничения моделей угроз информационной безопасности цепи поставок программного обеспечения. Выполнен обзор и систематизация мер защиты информации от угроз информационной сферы, связанных с компьютерными атаками на цепи поставок программного обеспечения. Рассмотрены известные нормативные и методическое документы в области цепи поставок ИТ-продукции. Сделан вывод о необходимости развития российской законодательной и нормативно-правовой базы информационной безопасности по тематике цепей поставок программного обеспечения. Предложен вариант систематики мер защиты информации в жизненном цикле поставки программного обеспечения информационных систем. Предложены признаки классификации, как-то: используемые механизмы безопасности, методы защиты информации, фазы процесса разработки программного обеспечения. Сформулированы возможные направления совершенствования мер защиты информации от компьютерных атак на цепи поставок программного обеспечения в национальной и международной сфере информационной безопасности.

Ключевые слова: логистическая цепочка, цепочка поставки, атаки на цепь поставки, информационная безопасность, поставка программ, менеджмент безопасной цепи поставки, таксономия угроз информационной безопасности, систематика мер защиты информации.
Для цитирования: БАРАБАНОВ, Александр В.; МАРКОВ, Алексей С.; ЦИРЛОВ, Валентин Л. О СИСТЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦЕПЕЙ ПОСТАВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 68-79, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1218>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.06.

Alexander V. Barabanov[1], Alexey S. Markov[2], Valentin L. Tsirlov[3]
[1, 2]Bauman Moscow State Technical University,
2-nd Baumanskaya, 5, Moscow, 105005, Russia
[2]NPO Echelon, Elektrozavodskaya, 24, Moscow, 107023, Russia
[1]e-mail: mail@cnpo.ru, https://orcid.org/0000-0003-4061-6611
[2]e-mail: a.markov@npo-echelon.ru, https://orcid.org/0000-0003-0111-7377
[3]e-mail: v.tsirlov@bmstu.ru, https://orcid.org/0000-0003-2657-4179

Information security systematics of software supply chains

DOI: http://dx.doi.org/10.26583/bit.2019.3.06

Abstract. The results of the systematization of measures to protect information resources from attacks on the supply chain of software and computer systems are presented. The phenomena, relevance and popular topics of protecting the supply chains of IT products are noted. Statistics on borrowed components of software products and software systems are presented. Examples of computer attacks on resources and processes of the software supply chain are given. The analysis of the existing terminological base in the field of security of supply chains of software is carried out. The features of the terms for supply chain and supply chain attack are formulated. The analysis of existing models of information security threats associated with computer attacks on the supply chain of software products is done. Limitations of models of threats to information security of the software supply chain are revealed. A review and systematization of measures to protect information from threats in the information sphere related to computer attacks on the software supply chain has been carried out. Known regulatory and methodological documents in the field of the supply chain of IT products are considered. It is concluded that it is necessary to develop the Russian legislative and regulatory framework for information security on the subject of software supply chains. A version of the systematics of information security measures in the life cycle of software delivery of information systems is proposed. Classification signs such as the used controls, information security methods, phases of the software development process are proposed. Possible directions of improving measures to protect information from computer attacks on the supply chain of software in the national and international information security are formulated.

Keywords: logistics chain, supply chain, supply chain attacks, information security, software delivery, secure supply chain management, threat taxonomy, controls systematics.

For citation: BARABANOV, Alexander V.; MARKOV, Alexey S.; TSIRLOV, Valentin L. Information security systematics of software supply chains. IT Security (Russia), [S.l.], v. 26, n. 3, p. 68-79, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1218>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.06.

Введение

Актуальность тематики информационной безопасности цепей поставки (supply chain) программ определена двумя феноменами: объективным ростом количества заимствованных компонентов (модулей, библиотек) и развитием сетей дистрибуции и логистики ИТ-продуктов. Так, современная статистика показывает, что:

- более половины организаций-разработчиков программного обеспечения привлекают сторонних разработчиков[1];
- более 70% разработчиков используют компоненты свободного программного обеспечения[2];
- встроенное (микропрограммное) обеспечение программно-аппаратных комплексов, как известно, имеет мульти происхождение из многих зарубежных стран (зачастую даже достоверно неустановленным странам).

Что касается современных систем дистрибуции и логистик, то за последнее десятилетие, к сожалению, стало практикой, когда современные интеграторы, завязанные на ряд иерархически выстроенных сторонних организаций (поставщиков и соисполнителей), не могут контролировать промежуточные цепочки подсистем безопасности и их узкие места [1-3].

С учетом настоящих требований по информационной и кибербезопасности конечного потребителя указанные моменты определяют появление проблемной ситуации, в свою очередь касающейся новых, мало изученных пока типов рисков ИБ,

[1] https://codingsans.com/state-of-software-development-2018
[2] https://www.sonatype.com/2019ssc

связанных:

- с появлением взаимного разного рода мультидоступа к информационным ресурсам головного заказчика, интеграторов, множественных соисполнителей и поставщиков;
- с поставкой конечным пользователям программного обеспечения (ПО) с уязвимостями и не декларированными возможностями заимствованных компонент;
- с поставкой конечным пользователям ИТ-продуктов и систем с вредоносными закладками, преднамеренно внесенными на недостаточно контролируемых множественных этапах внедрения и поставки.

Следует отметить, что в настоящее время наблюдается уверенный рост атак на цепи поставок, особенно на нижние уровни иерархии, касающиеся фрилансеров, а также атаки на интернет вещей [4-6]. Востребованность тематики отмечается даже на самом высоком межгосударственном уровне – в резолюции Генеральной ассамблеи ООН A/RES/73/27[3].

В табл. 1 показаны примеры популярных атак на цепи поставок. Примечательно, что ShadowHammer-атака известна еще и тем, что в расшифрованном фрагменте кода было идентифицировано около 200 MAC-адресов устройств, находящихся на территории России. Можно напомнить, что и известная Stuxnet-атака [7] также относится к атакам на логистическую цепочку[4].

Таблица 1. Известные атаки на цепи поставок программ

Наименование атаки	Краткая характеристика	Годы
Triada	Внедрение вредоносного ПО на этапе установки ПО в смартфоны	2016–2019
The Big Hack	Внедрение аппаратной закладки в материнские платы	2018
ShadowHammer	Распространение вредоносного ПО через утилиту ASUS Live Update. Внедрение вредоносного кода было выполнено на этапе компиляции ПО	2018, 2019

Следует указать, что в ряде передовых стран весьма озабочены данной проблемной ситуацией, что выражается в публикации ряда тематических нормативных документов и обзоров (например, [8-10]). В то же время в нашей стране пока отсутствует общий нормативно-методический документ, посвященный именно безопасности информации программного обеспечения в цепи поставок.

Исследованию указанных вопросов и посвящена данная статья.

1. Постановка задачи

Объектом исследования в работе являются цепи поставок ПО в контексте ИБ. Предметом исследования стали элементы систематики угроз ИБ (связанных с возможностью проведения компьютерных атак на цепи поставок ПО) и организационных и технических мер защиты информации от этих угроз. Цель исследования состоит в систематизации существующих мер защиты информации от угроз, связанных с атаками на цепи поставок, и формировании предложений по их совершенствованию. Для достижения поставленной цели в рамках исследования решаются следующие задачи:

- анализ понятийной базы;

[3] https://undocs.org/A/RES/73/27
[4] https://www.kaspersky.com/content/en-global/images/repository/pr/161)Stuxnet_infogr_en_05_640px.png

- обзор существующих моделей угроз, связанных с атаками на цепи поставок;
- обзор и систематизация мер защиты информации от атак на цепи поставок;
- разработки рекомендаций по совершенствованию соответствующих мер защиты информации.

2. Определение терминологической базы цепи поставок

На основании определения MITRE, NIST SP 800-161, ISO 27036-1 и ISO 28000 (ГОСТ Р 53663), под *цепью поставок ПО*, в целом понимают систему ее участников с взаимосвязанным набором ресурсов и процессов, которые вовлечены в жизненный цикл перемещения ПО от исполнителя к конечному клиенту, а именно: проектирование, разработку, производство, поставку, внедрение, сопровождение программ и выполнение сопутствующих услуг. Следует выделить следующие ключевые характеристики цепи поставок (рис.1):

- цель создания цепи поставок – доставка конечным пользователям программного продукта или услуги (например, по схеме «Platform-as-a-Service» или «Software-as-a-Service»);
- наличие связей (оформленных договорными отношениями) между различными организациями (разработчики, логистические центры, центры дистрибуции и сборки), которые выступают в роли поставщика и (или) потребителя;
- наличие двух потоков передачи материалов/услуг: потоки, связанные с созданием продукта из компонентов сторонних поставщиков («Upstream»), и потоки, связанные с поставкой продукта конечным пользователям через сеть дистрибуции («Downstream»);
- в случае многозвеньевой цепи поставки – самый распространенный вариант – одна и та же организация может выступать одновременно в роли потребителя (по отношению к организации, находящейся в цепи ниже) и поставщика (по отношению к организации, находящейся в цепи выше);
- слабая возможность мониторинга потребителем контроля качества поставляемых продуктов и услуг всей цепи поставки в случае многозвеньевых цепей.

В общем случае связь «поставщик – потребитель» направлена на получение потребителем:

- компонентов ПО, которые будут использоваться потребителем для формирования продукта (услуги или системы), передаваемого конечному пользователю или далее по цепи поставки;
- услуги, которая будет использоваться потребителем для формирования продукта (услуги или системы), передаваемого конечному пользователю или далее по цепи поставки.

Компрометирующие злонамеренные действия на процессы и ресурсы цепи поставок в компьютерной среде принято называть компьютерной *атакой на цепь поставок* (supply chain attack). В общем случае основными целями атакующего являются:

- добавление (вставка) недекларированных возможностей, вредоносного ПО, вредоносного аппаратного обеспечения (закладок, имплантов [11, 12]) или ложной (неверной) информации в объекты цепей поставок;
- замена доверенных элементов (компоненты ПО, документация, конфигурационные файлы) на недоверенные;
- несанкционированная модификация поставляемых объектов.

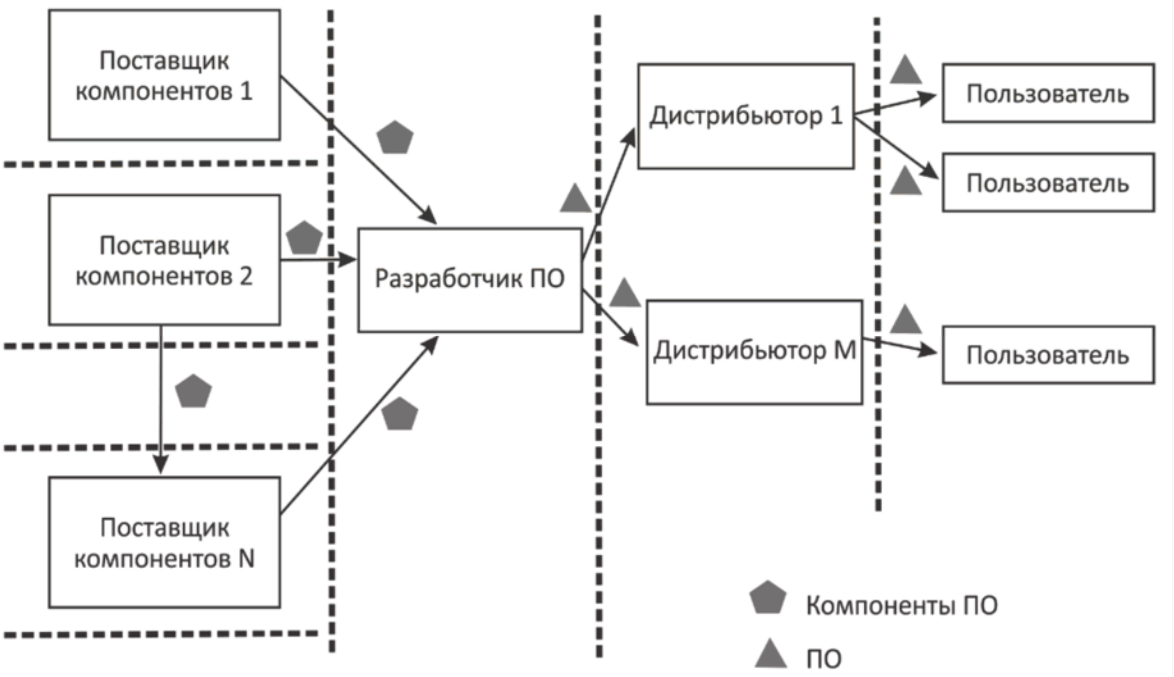

Рис. 1. Типовая структура цепи поставок программ
(Fig. 1. Typical program supply chain structure)

3. Обзор существующих моделей угроз, связанных с атаками на цепи поставок

Решению задачи перечисления угроз, связанных с атаками на цепи поставок, посвящен ряд работ международных научных институтов.

В работе [10] представлены результаты моделирования угрозы для цепей поставок ПО в интересах объектов Минобороны США. Формирование перечня типовых угроз выполнялось с использованием методов анализа и систематизации информации, связанной с реальными инцидентами информационной безопасности, возникшими из-за атак на цепи поставок. Кроме систематизированного перечня (включает в себя 41 наименование), в работе представлены: способ описания угроз и перечень рекомендуемых к внедрению контрмер для нейтрализации идентифицированных угроз. Идентифицированные в работе угрозы связаны с атаками на цепи поставок ПО или преднамеренными действиями нарушителей в среде разработки ПО, - угрозы, связанные с непреднамеренными действиями сотрудников организации – разработчика ПО, не рассматриваются. Следует отметить, что категория «Supply Chain» «Перечня шаблонов атак и их классификации» (Common Attack Pattern Enumeration and Classification, CAPEC[5]) [13] содержит номенклатуру атак на цепи поставок, разработанную на основе публикации [10].

Национальный институт стандартов и технологий NIST разрабатывает перечни угрозы в интересах операторов государственных информационных систем США. В работе [14] представлена номенклатура угроз, актуальных в целом для информационных систем. Отдельная группа из пяти угроз связана с внедрением в информационную систему ПО, содержащего уязвимости или недекларированные возможности, из-за атак на цепи поставок (табл. 2). Следует отметить, что представленная в документе

[5] https://capec.mitre.org

классификация угроз не учитывает особенностей информационных систем, являющихся средами разработки ПО.

Таблица 2. Векторы атак на цепи поставок ПО (по публикации NIST SP 800-30)

Вектор атаки	Краткая характеристика
Создание и задействование ложных организаций с целью внедрения вредоносных компонентов в цепь поставок	Злоумышленник создает ложные организации, имитирующие легитимных поставщиков, которые задействуются в жизненный цикл поставки с целью компрометации компонентов информационной системы в цепи поставки
Внедрение контрафактного или подделанного технического оборудования в цепочку поставок	Злоумышленник перехватывает технические средства у законных поставщиков с целью нелегитимной замены или модификации
Внедрение поддельных критических компонентов в систему организации	Злоумышленник, используя инсайдера и/или цепь поставок, вносит нелегитимные изменения в критические компоненты информационных систем
Проведение атак на цепь поставок, направленных на использование критически важного оборудования, программного обеспечения или встроенного ПО	Злоумышленник проводит атаки на работающие информационные системы путем внедрения вредоносных программ, встроенного программного обеспечения и аппаратного обеспечения, которое выполняет критические функции для организаций
Координация кибератаки с учетом внешних и внутренних (инсайдерских) возможностей и компрометации цепи поставки	Злоумышленник проводит непрерывные (итерационные) скоординированные атаки, используя все три потенциальных вектора атаки (внешние атаки, внутренние атаки, атаки на поставщиков)

Отдельным направлением работы NIST является перечисление угроз, связанных с использованием в информационных системах мобильных устройств [8]. В работе NISTIR 8144 представлены общие сведения о классах таких угроз, приведена методика формирования перечня угроз, используемая специалистами NIST, предложена схема описания угроз по различным характеристикам. Сам каталог угроз доступен в информационной системе NIST[6] в сети интернет. Одной из категорий угроз являются угрозы, связанные с цепями поставки ПО для мобильных устройств и самих мобильных устройств в информационную систему (категория «Supply Chain»). Перечень угроз, представленных в данной категории, по сути, является адаптацией номенклатуры угроз из работы [10] для области мобильных устройств и содержит описание 22 угроз. Угрозы, связанные с непреднамеренными действиями разработчиков или поставщиков приложений для мобильных устройств (например, из-за ошибок или неверного применение практик по разработке безопасного ПО), в работе не рассматриваются.

Описание некоторых угроз, связанных со средой разработки ПО, можно найти в заданиях по безопасности на среду разработки[7] – документах, используемых международной системой сертификации «Common Criteria» при оценке производства объектов сертификации [15]. Перечень угроз, представленный в таких документах, как правило, не является структурированным, а угрозы, связанные с непреднамеренными действиями разработчиков или поставщиков ПО, не рассматриваются.

Следует отметить российские изыскания по линии ТК-362. Информационный ресурс «Банк данных угроз»[8] ведется ФСТЭК России и содержит периодически

[6] https://pages.nist.gov/mobile-threat-catalogue/
[7] https://www.ssi.gouv.fr/uploads/2017/10/anssi-cible-site-2017_07en.pdf
[8] https://bdu.fstec.ru/

обновляемый (в том числе, с учётом анализа реальных инцидентов) классифицированный перечень угроз, предназначенный для операторов и разработчиков информационных систем и используемый ими в процессе моделирования угроз безопасности информации. Угрозы, связанные с атаками на цепи поставок ПО, в явном виде в банке данных не представлены. Национальный стандарт ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения» содержит номенклатуру и описание угроз безопасности информации, которые могут возникать при разработке ПО, в том числе связанных с атаками на инфраструктуру разработчика ПО. Отличительными особенностями данной номенклатуры являются следующие моменты:

- в явном виде указаны угрозы, связанные со средой разработки ПО, реализация которых может привести к внедрению уязвимостей в программу или раскрытию чувствительной информации;
- учитываются непреднамеренные действия разработчиков ПО.

В качестве ограничений всех рассмотренных моделей угроз можно отметить следующие [16]:

- поскольку для угроз при разработке ПО не характерны источники, которые представляют собой физические явления, то рассматриваются только антропогенные угрозы, а угрозы, связанные со стихийными бедствиями, природными явлениями и утечкой информации по техническим каналам, не учитываются;
- представленные перечни угроз, как правило, не являются исчерпывающими и должны быть уточнены в процессе идентификации угроз для конкретной среды разработки ПО или информационной системы.

4. Обзор мер защиты от угроз, связанных с атаками на цепи поставок

В настоящее время наиболее доступны изыскания по тематике безопасности цепей поставки ряда национальных и международных комитетов по стандартизации, среди которых можно выделить US NIST, UK NCSC и ISO.

Так, в публикации NIST - SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations приведен подход к решению задач идентификации, оценки, выбора и внедрения процесса управления рисками, связанными с угрозами информационной безопасности в цепях поставок ПО [17]. Основным содержанием документа являются:

- руководящие указания по внедрению в организацию процесса (гармонизированного с NIST SP 800-39 и NIST SP 800-30) управления рисками, связанными с угрозами безопасности информации в цепях поставок ПО;
- меры защиты информации (в нотации NIST SP 800-53), связанные с защитой от выявленных угроз.

Риск-ориентированный подход, предлагаемый в документе NIST SP 800-161 для оценки рисков, связанных с реализацией угроз из-за атак на цепи поставок, определяется совокупностью фаз [18]:

- определение структуры: сбор требований, определение границ области действия мер по защите цепей поставок;
- оценка: идентификация угроз, оценка рисков информационной безопасности;
- разработка контрмер, связанных с нейтрализацией критичных угроз;
- мониторинг с целью определения эффективности реализованных контрмер.

Технические комитеты Великобритании разрабатывают нормативные и методические документы в области защиты цепей поставок, ориентированные как на

коммерческие, так и на государственные организации. В публикации Supply chain security guidance[9] представлены 12 принципов обеспечения защиты цепей поставок NCSC (UK National Cyber Security Center), среди которых: повышение осведомлённости в области защиты цепей поставок, встраивание мер защиты информации на уровне договорных обязательств, разработка мер, связанных с реагированием на инциденты в цепях поставок. В документе Минобороны Великобритании Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide[10] представлены указания для потребителей и поставщиков по защите цепей поставок от угроз раскрытия информации, связанной с обороноспособностью Великобритании, на основе риск-ориентированного подхода.

Международные стандарты линейки ISO/IEC 27036 содержат нормативно-методические требования и рекомендации, связанные с защитой информации при взаимодействии класса «поставщик-потребитель». Так, стандарт ISO/IEC 27036-2 предъявляет высокоуровневые требования безопасности информации в случае привлечения к работе субподрядных организаций. Стандарт предлагает использование риск-ориентированного подхода к формированию перечня мер защиты информации. Стандарт ISO/IEC 27036-3 уточняет требования при использовании субподрядных организаций с целью получения услуг (сервисов) или компонентов ПО. В стандарте представлены меры защиты цепей поставок, стандарт гармонизирован с ISO/IEC 27001, ISO/IEC 15288 и ISO/IEC 12207 – меры определены с учетом процессов разработки ПО и систем по ISO/IEC 15288 и ISO/IEC 12207. Следует отметить, что наряду с классическими мерами защиты в последнее время разрабатываются подходы к защите цепей поставки ПО на основе технологии блокчейн [19-21].

Кратко отметим состояние отечественной законодательной и нормативной базы с точки зрения раскрытия вопросов обеспечения безопасности цепей поставок. Например, в доктринных документах нашей страны указаны технологические угрозы со стороны зарубежных стран, но (в отличие, скажем, от Национальной стратегии кибербезопасности США) вопрос безопасности логистических цепочек не фигурирует. В текущих версиях нормативных правовых актов по тематике ГИС, АСУ ТП, КИИ и пр. наблюдается аналогичная ситуация. Национальный стандарт ГОСТ Р 56939 содержит требования к безопасной разработке, а новое положение по сертификации средств защиты информации ужесточает требования к сертификации зарубежной продукции, однако в явном виде вопросы безопасности цепей поставок представлены в них весьма лаконично.

С учетом выше сказанного, проведенное исследование позволило авторам представить на суд читателям вариант систематизации мер защиты информации от угроз, связанных с атаками на цепи поставок (рис. 2).

[9] https://www.ncsc.gov.uk/collection/supply-chain-security
[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/718566/20180203_Cyber_Industry_Buyer_and_Supplier_Guide_v2_1.pdf

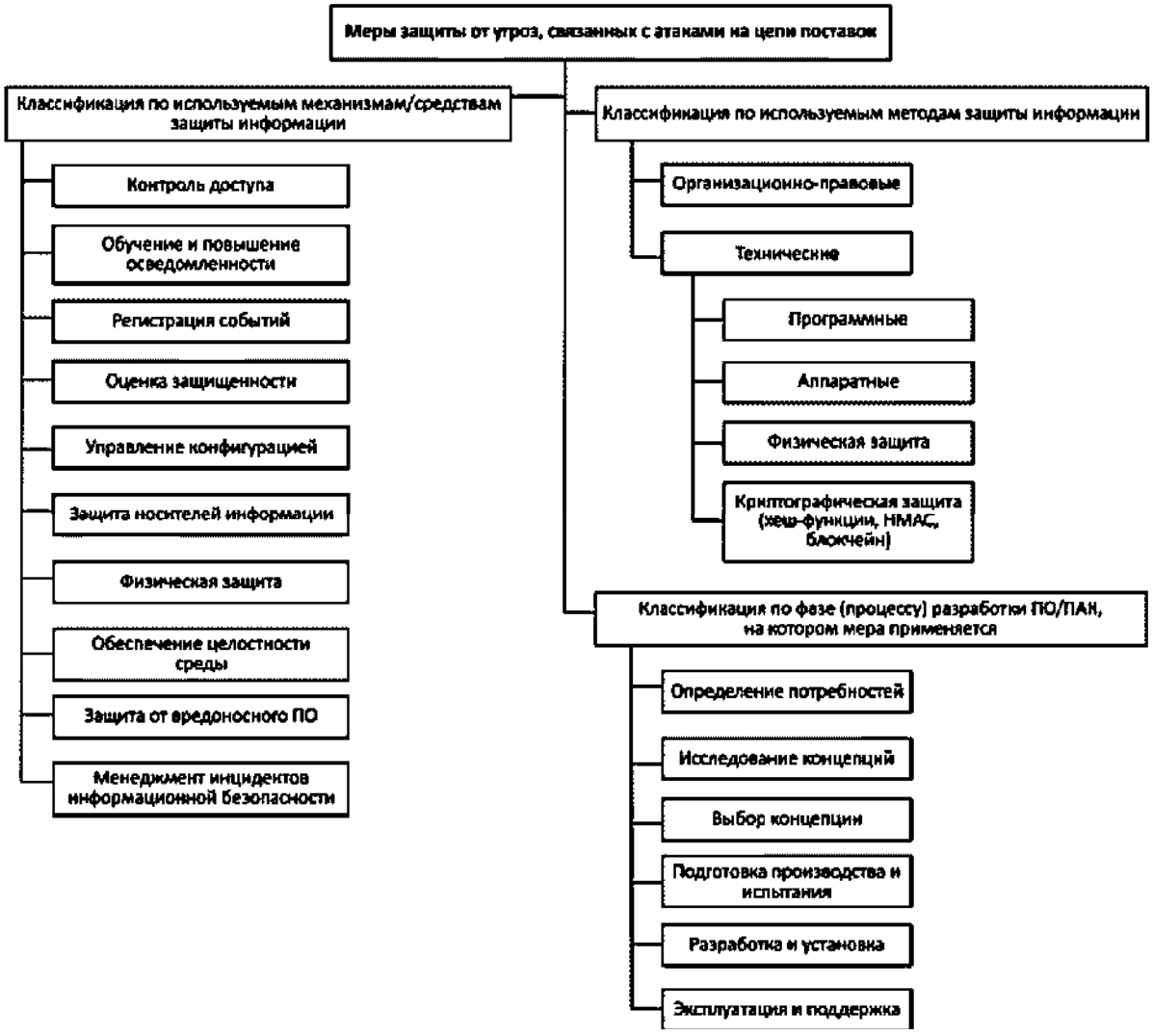

Рис. 2. Результаты систематизации мер защиты информации от угроз, связанных с атаками на цепи поставок
(Fig. 2. Results of systematization of information protection measures against threats related to supply chain attacks)

Заключение

Повсеместное использование цепей поставок ПО и рост инцидентов информационной безопасности, связанных с атаками на них, диктуют необходимость разработки (адаптации существующих) нормативных и методических документов, подходов к защите цепей поставок ПО.

Среди возможных направлений совершенствования в международной сфере можно выделить следующие:

- унификацию законодательства в вопросах борьбы с киберкриминалом, создающим риски, связанные с атаками на цепи поставок;
- формирование этичных норм для использования атак на цепочки поставок в военных целях;
- формирование протоколов обмена информации о подобных угрозах между

странами в рамках военно-политических союзов, таможенных союзов и пр.;

- развитие системы международной сертификации согласно требованиям безопасности: унификации методик проведения сертификационных испытаний, взаимному признанию сертификатов, правилам раскрытия кода и т.п.;
- разработку международного стандарта по управлению рисками информационной безопасности, связанными с атаками на цепочку поставок.

В национальной сфере с учетом высокого уровня зависимости отечественной промышленности от зарубежных информационных технологий можно выделить следующие направления:

- определение на государственном уровне (например, в «Доктрине информационной безопасности») в качестве стратегической цели защиту цепей поставок ПО, предназначенных для функционирования в информационных системах, обрабатывающих сведения, содержащие государственную тайну, критической информационной инфраструктуре, государственных информационных системах;
- формирование рабочей группы с привлечением представителей коммерческих организаций, осуществляющей координацию действий в области обеспечения безопасности цепей поставок;
- формирование и поддержание в актуальном состоянии перечня угроз связанных с атаками на цепи поставок (может быть выполнено в форме национального стандарта по аналогии с угрозами при разработке ПО – ГОСТ Р 58412 или в форме элементов Банка данных угроз ФСТЭК России);
- создание научно обоснованных методов и методик защиты цепей поставок от угроз;
- разработку руководящих указаний по защите цепей поставок ПО для организаций, осуществляющих проектирование информационных систем ГИС, КИИ и пр.;
- разработку руководящих указаний по защите цепей поставок ПО (работа с субподрядчиками) для организаций-разработчиков ПО (может быть выполнено в форме национального стандарта – расширения линейки национальных стандартов в области разработки безопасного ПО) [16, 22];
- формирование протоколов обмена информацией о недобросовестных поставщиках ПО, атаках на цепи поставок и создание национального центра обмена этой информацией и мерах защиты от этих угроз;
- создание и ведение единого хранилища данных о добросовестных поставщиках ПО;
- проведение мероприятий, направленных на повышение осведомлённости организаций в области угроз для цепей поставок (проведение тематических конференций, создание информационных ресурсов).

СПИСОК ЛИТЕРАТУРЫ:

1. Буряк Ю.И., Амирханян В.Г., Калинин В.Л. Обеспечение безопасности цепей поставок промышленной продукции на базе использования современных информационных технологий // Вестник компьютерных и информационных технологий. 2012. № 9 (99). С. 26−33.
2. Погодина В.В., Аристов А.М., Аристов В.М. Проблема обеспечения информационной безопасности логистических процессов на предприятии // Журнал правовых и экономических исследований. 2016. № 3. С. 162−168.
3. Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science. V. 149, 2019. P. 65-70. DOI: 10.1016/j.procs.2019.01.108.
4. Петренко С.А. Управление киберустойчивостью: постановка задачи // Защита информации. Инсайд. 2019. № 3 (87). С. 16−24.
5. Харрис Ш. Кибер войн@. Пятый театр военных действий/Пер. с англ. - М.: Альпина нон-фикшн, 2016. –390 с.

6. Астье Ж.И.; Жуков И.Ю.; Мурашов О.Н. Системы управления «умный дом» и интернет вещей. Безопасность информационных технологий, [S.L.], v. 24, n. 3. P. 18−29, July 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/260 (дата обращения: 01.12.2017). DOI: http://dx.doi.org/10.26583/bit.2017.3.02.
7. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28−36. DOI: 10.21681/2311-3456-2013-1-28-36.
8. Brown C., Dog S., Franklin J.M. and etc. Assessing Threats to Mobile Devices & Infrastructure. The Mobile Threat Catalogue. NISTIR 8144 (draft). NIST, 2016. 50 p. DOI: 10.6028/NIST.IR.8144.
9. Miller, J.F. Supply Chain Attack Framework and Attack Patterns. MTR 14-0228. MITRE, 2013. P. 86. URL: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.
10. Reed M., Miller J.F., Popick P. Supply Chain Attack Patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense, 2014. 88 p. URL: https://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf (дата обращения: 21.07.2019).
11. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. №2 (3). С. 60−65.
12. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. №4 (7). С. 60−68.
13. Yuan X., Nuakoh E.B., Beal J.S., Yu H. Retrieving relevant CAPEC attack patterns for secure software development. In Proceeding of CISR '14 Proceedings of the 9th Annual Cyber and Information Security Research Conference (Oak Ridge, Tennessee, USA, April 08 - 10, 2014). ACM New York, NY, USA, 2014. P. 33−36. DOI: 10.1145/2602087.2602092.
14. Blank R.M. (ed.), Gallagher P.D. (ed.) Guide for Conducting Risk Assessments. NIST SP 800-30, NIST, 2012, Rev.1. 95 p. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата обращения: 21.07.2019).
15. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30−33.
16. Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. P. 356−361. DOI: 10.1109/icaict.2018.8747065.
17. Boyens J., Paulsen C., Moorthy R., Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST SP 800-161. NIST, 2015, 282 p. DOI: 10.6028/NIST.SP.800-161.
18. Sigler K., Shoemaker D., Kohnke A. Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product. Auerbach Publications, 2017. – 278 p.
19. Alzahrani N., Bulusu N. Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 30−35. DOI: 10.1145/3211933.3211939.
20. Hepp T., Wortner P., Schönhals A., Gipp B. Securing Physical Assets on the Blockchain: Linking a novel Object Identification Concept with Distributed Ledgers. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 60−65. DOI: 10.1145/3211933.3211944.
21. Ray S., Chen W., Cammarota R. Protecting the supply chain for automotives and IoTs. In Proceedings of the 55th Annual Design Automation Conference (DAC '18). ACM, New York, NY, USA, 2018. Article 89. P. 1−4. DOI: 10.1145/3195970.3199851.
22. Марков А.С., Цирлов В.Л., Барабанов А.В. Методический аппарат анализа и синтеза комплекса мер разработки безопасного программного обеспечения // Программные продукты и системы. 2015. № 4. С. 166−174. DOI: 10.15827/0236-235X.112.166-174.

REFERENCES:

[1] Buryak YU.I., Amirhanyan V.G., Kalinin V.L. Obespechenie bezopasnosti cepej postavok promyshlennoj produkcii na baze ispol'zovaniya sovremennyh informacionnyh tekhnologij, Vestnik komp'yuternyh i informacionnyh tekhnologij. 2012, n. 9 (99). S. 26−33 (in Russian).
[2] Pogodina V.V., Aristov A.M., Aristov V.M. Problema obespecheniya informacionnoj bezopasnosti logisticheskih processov na predpriyatii, ZHurnal pravovyh i ekonomicheskih issledovanij. 2016, n. 3. S. 162−168 (in Russian).
[3] Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science. V. 149, 2019. P. 65−70. DOI: 10.1016/j.procs.2019.01.108.

[4] Petrenko S.A. Upravlenie kiberustojchivost'yu: postanovka zadachi, Zashchita informacii. Insajd. 2019, n. 3 (87). S. 16−24 (in Russian).
[5] Harris SH. Kiber vojn@. Pyatyj teatr voennyh dejstvij/Per. s angl. -M.: Al'pina non-fikshn, 2016. – 390 s. (in Russia).
[6] Astier J.Y.; Zhukov, I.Y.; Murashov O. N. Smart Building Management Systems and Internet of Things. IT Security, [S.l.], v. 24, n. 3. P. 18−29, july 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/260 (accessed: 01.12.2017). DOI: http://dx.doi.org/10.26583/bit.2017.3.02.
[7] Markov A.S., Fadin A.A. Organizacionno-tekhnicheskie problemy zashchity ot celevyh vredonosnyh programm tipa Stuxnet, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2013, n. 1 (1). P. 28−36. DOI: 10.21681/2311-3456-2013-1-28-36.
[8] Brown C., Dog S., Franklin J.M. and etc. Assessing Threats to Mobile Devices & Infrastructure. The Mobile Threat Catalogue. NISTIR 8144 (draft). NIST, 2016. 50 p. DOI: 10.6028/NIST.IR.8144.
[9] Miller, J.F. Supply Chain Attack Framework and Attack Patterns. MTR 14-0228. MITRE, 2013. P. 86. URL: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.
[10] Reed M., Miller J.F., Popick P. Supply Chain Attack Patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense, 2014. 88 p. URL: https://www.acq.osd.mil/se/docs/Supply-Chain-WP.pdf (accessed: 21.07.2019).
[11] Klyanchin A.I. Katalog zakladok ANB (Spigel). CHast' 1. Infrastruktura, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014, n. 2 (3). S. 60−65 (in Russian).
[12] Klyanchin A.I. Katalog zakladok ANB (Spigel). CHast' 2. Rabochee mesto operatora, Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014, N4 (7). S. 60−68 (in Russian).
[13] Yuan X., Nuakoh E.B., Beal J.S., Yu H. Retrieving relevant CAPEC attack patterns for secure software development. In Proceeding of CISR '14 Proceedings of the 9th Annual Cyber and Information Security Research Conference (Oak Ridge, Tennessee, USA, April 08 - 10, 2014). ACM New York, NY, USA, 2014. P. 33−36. DOI: 10.1145/2602087.2602092.
[14] Blank R.M. (ed.), Gallagher P.D. (ed.) Guide for Conducting Risk Assessments. NIST SP 800-30, NIST, 2012, Rev.1. 95 p. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed: 21.07.2019).
[15] Barabanov A.V., Markov A.S., Cirlov V.L. Mezhdunarodnaya sertifikaciya v oblasti informacionnoj bezopasnosti, Standarty i kachestvo *[Standards and Quality]*. 2016, n. 7. S. 30−33 (in Russian).
[16] Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. P. 356−361. DOI: 10.1109/icaict.2018.8747065.
[17] Boyens J., Paulsen C., Moorthy R., Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST SP 800-161. NIST, 2015, 282 p. DOI: 10.6028/NIST.SP.800-161.
[18] Sigler K., Shoemaker D., Kohnke A. Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product. Auerbach Publications, 2017. – 278 p.
[19] Alzahrani N., Bulusu N. Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 30−35. DOI: 10.1145/3211933.3211939.
[20] Hepp T., Wortner P., Schönhals A., Gipp B. Securing Physical Assets on the Blockchain: Linking a novel Object Identification Concept with Distributed Ledgers. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY, USA, 2018. P. 60−65. DOI: 10.1145/3211933.3211944.
[21] Ray S., Chen W., Cammarota R. Protecting the supply chain for automotives and IoTs. In Proceedings of the 55th Annual Design Automation Conference (DAC '18). ACM, New York, NY, USA, 2018. Article 89. P. 1−4. DOI: 10.1145/3195970.3199851.
[22] Markov A.S., Cirlov V.L., Barabanov A.V. Metodicheskij apparat analiza i sinteza kompleksa mer razrabotki bezopasnogo programmnogo obespecheniya, Programmnye produkty i sistemy *[Software & Systems]*. 2015, n. 4. 166−174. DOI: 10.15827/0236-235X.112.166-174 (in Russian).

Поступила в редакцию – 03 сентября 2019 г. Окончательный вариант – 10 сентября 2019 г.
Received – September 03, 2019. The final version – September 10, 2019.

Оксана И. Бокова[1], Дмитрий И. Коробкин[2], Сергей А. Кухарев[3], Антон Д. Попов[4]
[1, 3, 4]Воронежский институт Министерства внутренних дел Российской Федерации,
просп. Патриотов, 53, г. Воронеж, 394065, Россия
[2]Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина,
ул. Ст. Большевиков, 54а, г. Воронеж, 394016, Россия
[1]e-mail: o.i.bokova@gmail.com, https://orcid.org/0000-0002-4833-2907
[2]e-mail: 516420@mail.ru, https://orcid.org/0000-0002-8236-5534
[3]e-mail: cuharev.serj@yandex.ru, https://orcid.org/0000-0002-9633-8422
[4]e-mail: anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ СРЕДЫ CPN TOOLS

DOI: http://dx.doi.org/10.26583/bit.2019.3.07

Аннотация. В статье с помощью имитационного моделирования представлена математическая модель функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных системах (АС). Данная модель разработана в программной среде CPN Tools с целью дальнейшего ее анализа. Для удобства, наглядности и сохранения логической целостности, модель разбита на подсистемы при помощи встроенного в CPN Tools инструментария. Модель необходима для проведения вычислительного эксперимента, а именно исследования реальных потребительских свойств СЗИ от НСД в АС, а также для разработки программного комплекса анализа и количественной оценки эффективности функционирования этих систем. Результаты имитационного моделирования процесса функционирования СЗИ от НСД в АС могут быть представлены в виде различных характеристик каждого состояния, которые характеризуют работу как системы в целом, так и ее подсистем. Разработанная имитационная модель может быть использована при создании подобных систем, при их эксплуатации, при сертификации систем информационной безопасности, при аттестации объектов информатизации и при периодическом контроле используемых программных средств защиты информации на данных объектах. Используемый CPN Tools язык программирования Meta language позволяет контролировать случайный переход маркера из начального состояния в конечное через промежуточное, устанавливать временные задержки и др. Имитационная модель СЗИ от НСД в АС в дальнейших исследованиях будет использоваться для построения моделей воздействия различных видов угроз к данной системе согласно банку данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации.

Ключевые слова: CPN Tools, сети Петри, система защиты информации, несанкционированный доступ, имитационная модель, автоматизированная система, strongly connected components.
Для цитирования: БОКОВА, Оксана И. et al. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ СРЕДЫ CPN TOOLS. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 80-89, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1220>. Дата доступа: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.07.

Oksana I. Bokova[1], Dmitry I. Korobkin[2], Sergey A. Kukharev[3], Anton D. Popov[4]
[1, 3, 4]Voronezh Institute of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[2]N.E. Zhukovsky and Y.A. Gagarin Air Force Academy,
Str. Bolsheviks, 54 a, Voronezh, 394016, Russia
[1]e-mail: o.i.bokova@gmail.com, https://orcid.org/0000-0002-4833-2907
[2]e-mail: 516420@mail.ru, https://orcid.org/0000-0002-8236-5534
[3]e-mail: cuharev.serj@yandex.ru, https://orcid.org/0000-0002-9633-8422
[4]e-mail: anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X

Development of an imitation model of information protection system from unauthorized access using the cpn tools software

DOI: http://dx.doi.org/10.26583/bit.2019.3.07

Abstract. The paper presents a mathematical model of functioning of the system of information protection (IPS) from unauthorized access (UA) in automated systems (AS). This model was developed in framework of the CPN Tools software environment. For convenience, visibility and preservation of logical integrity, the model is divided into subsystems using the tools built into CPN Tools. The model is necessary for a computational experiment, namely, to study the real consumer properties of IPS from UA in AS, as well as for development a software package for analyzing and quantifying the effectiveness of these systems. The results of the simulation of functioning of the IPS from the UA in the AS can be presented in the form of various characteristics of each state, which characterize the work of the system as a whole and its subsystems. The developed simulation model can be used to create similar systems, during their operation, during certification of information security systems, during certification of informatization facilities, and during periodic monitoring of used information protection software at these facilities. The programming language Meta language used by CPN Tools allows you to monitor random transitions of the marker from the initial state to the final through the intermediate one, to set time delays, etc. The simulation model of IPS from UA to AS will be used in further studies to build the models of impact of various types of threats to this system according to the bank data threats to information security of the Federal Service for Technical and Export Control of Russia.

Keywords: CPN Tools, Petri nets, information protection system, unauthorized access, simulation model, automated system, strongly connected components.

For citation: BOKOVA, Oksana I. et al. Development of an imitation model of information protection system from unauthorized access using the cpn tools software. IT Security (Russia), [S.l.], v. 26, n. 3, p. 80-89, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1220>. Date accessed: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.07.

Введение

Современный этап жизнедеятельности человека характеризуется глубокой информатизацией, которая связана с разработкой, эксплуатацией АС различного назначения. В связи с этим злоумышленниками постоянно совершенствуются способы получения конфиденциальной информации. Для предотвращения попыток НСД в АС внедряются СЗИ от НСД [1, 2]. Зачастую штатные пользователи таких систем пренебрегают своими должностными полномочиями и нарушают правила работы с защищенными системами. Пользовательские ошибки являются самыми распространенными, поэтому в работе допускаем, что была допущена ошибка и вредоносная программа проникла в АС [3]. Будем считать, что нарушитель является внутренним с высоким потенциалом. Рассмотрим именно этот случай для съемного носителя информации CD/DVD/HD/Flesh.

Вредоносная программа может быть реализована в виде отдельного программного продукта (ПП) с функцией автозапуска при подключении к персональному компьютеру (ПК) в случае, когда пользователь сам отключает антивирусное программное обеспечение (ПО), т.к. зачастую АС потребляют большое количество ресурсов, и следовательно, работать становится неудобно, а зачастую невозможно из-за сильной загруженности [3].

Данные аспекты необходимо учитывать при разработке и эксплуатации СЗИ от НСД для определения ее вероятностно-временных характеристик в виде времен выполнения защитных функций, которые в дальнейшем планируется использовать при оценке эффективности ее функционирования [4], для установки взаимосвязей ее подсистем и компонентов, а также построения её логической структуры в целом. Данная задача может быть решена при помощи построения имитационной модели СЗИ от НСД, которая и будет предопределять вышеперечисленные характеристики.

В качестве программной среды построения имитационной модели в данной статье используем программу, разработанную в университете Орхуса (Дания) – CPN Tools [4-8]. Отличительной особенностью CPN Tools является наличие обширного инструментария, позволяющего анализировать различные аспекты функционирования моделей на базе сетей Петри [9-10] (безопасность и ограниченность позиций, уровень активности переходов, наличие тупиковых маркировок и т.д.). CPN Tools используется во множестве реальных проектов в области телекоммуникации, при моделировании сетей и сетевых устройств, при верификации протоколов связи и т.д. В данной среде для построения моделей используются иерархические, временные, раскрашенные сети Петри, которые представляют собой универсальную алгоритмическую систему. Имитационное моделирование в CPN Tools является дискретно-событийным, что предполагает мгновенную смену состояния сети Петри в определенные моменты времени.

Построение модели

Моделирование СЗИ от НСД представляет собой сложный процесс. Первоначальным этапом разработки модели является построение ее подсистем и их компонентов, полностью идентичных реально функционирующей СЗИ от НСД с целью получения ее свойств и характеристик [1, 2, 11-15]. Проведенный анализ показал, что модель может состоять из следующих подсистем:

- подсистема «Включение ПК и идентификация пользователя»;
- подсистема «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов»;
- подсистема «Работа пользователя с файлами и программами»;
- подсистема «Работа пользователя с прикладным программным обеспечением»;
- подсистема «Деструктивное воздействие на СЗИ от НСД».

Введем следующие обозначения для вершин и переходов. Вершины в нашей модели используются двух видов – с индексами r1 и т.д., представляют собой функции, выполняемые СЗИ от НСД, а вершины с индексами r01 и т.д. являются дополнительными, требующимися для ввода вероятностей. И, соответственно, переходы с индексами t1 и т.д. являются основными, а t01 и т.д. являются дополнительными.

Первая модель отображает вход пользователя в СЗИ от НСД посредством его аутентификации (рис. 1). Данная модель даёт визуальное представление о том, что происходит в системе при входе пользователя. Из рисунка 1 видно, что при неправильном вводе пароля (после третьего раза) следует блокировка ПК, что позволяет обеспечить защиту ПК от брутфорса. Переход t01 обеспечивает передачу маркера в подсистему «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов в системе». В таблице 1 приведены состояния рассматриваемой подсистемы.

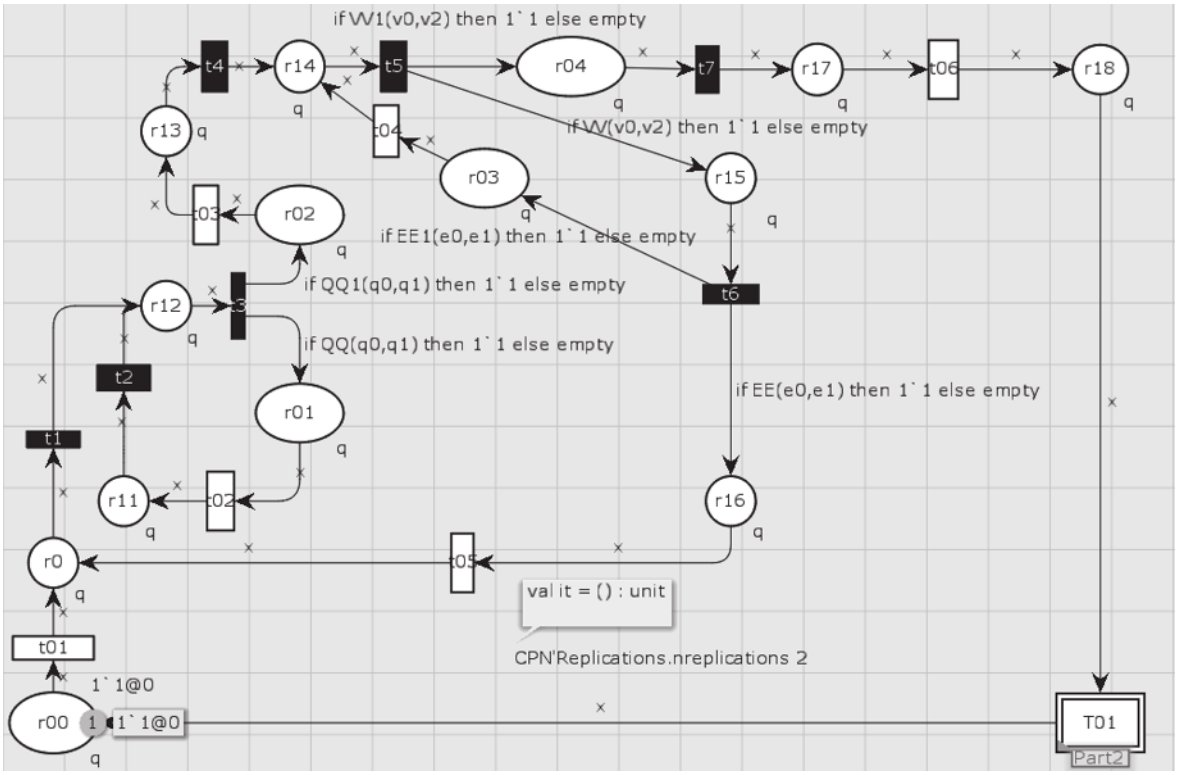

Рис. 1. Включение ПК и идентификация пользователя
(Fig. 1. Turning on the PC and identifying the user)

Таблица 1. Включение ПК и идентификация пользователя

Функции, выполняемые СЗИ от НСД
0. Начало работы СЗИ от НСД (Прекращение выполнения функций СЗИ от НСД)
1.1 Предъявление идентификатора
1.2 Прекращение работы идентификатора
1.3 Допуск к вводу пароля
1.4 Ввод пароля
1.5 Повторный ввод пароля
1.6 Блокировка входа в систему при трехразовом неправильном вводе пароля
1.7 Аутентификация субъекта системы
1.8 Вход в систему

Вторая модель отображает подсистему «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов» (рис. 2). В позиции r241 реализуется вход из подсистемы «Деструктивное воздействие на СЗИ от НСД». После перехода пользователя к работе с носителем вредоносная программа автоматически запускается, и в имитационной модели появляется новый «маркер», который представляет собой деструктивное программное воздействие на СЗИ от НСД, направленное на получение доступа к информации. В таблице 2 приведены состояния рассматриваемой подсистемы.

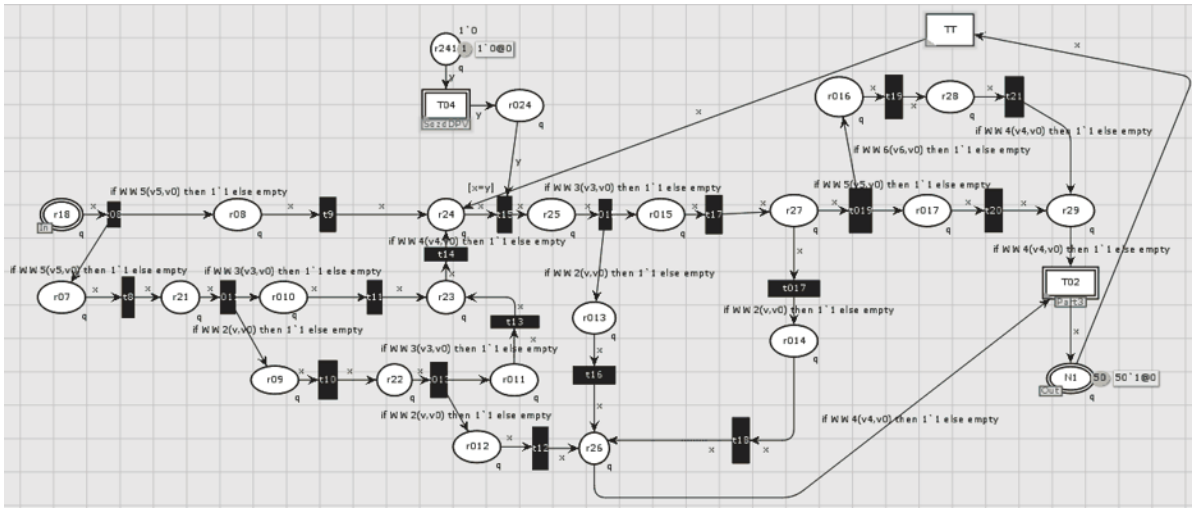

Рис. 2. Инициализация прав пользователя на работу в системе и доступ к каталогу файлов (Fig. 2. Initialization of user rights to work in the system and access to the file directory)

Таблица 2. Инициализация прав пользователя на работу в системе и доступ к каталогу файлов

Функции, выполняемые СЗИ от НСД
1.8 Вход в систему
2.1 Сопоставление идентификационной информации внешнего носителя и пользователя
2.2 Контроль устройств (если устройство не принадлежит пользователю, срабатывает данный механизм)
2.3 Доступ к внешнему носителю
2.4 Обращение к объекту на носителе
2.5 Сопоставление меток конфиденциальности пользователя и ресурса (в СЗИ от НСД реализуется на основе мандатного принципа контроля доступа)
2.6 Блокировка доступа к объекту
2.7 Проверка полномочий доступа пользователя (в СЗИ от НСД реализуется на основе дискреционного принципа контроля доступа)
2.8 Преобразование информации на носителе при помощи шифрования (в СЗИ от НСД применяется метод гаммирования)
2.9 Допуск субъекта к защищаемому объекту

Следующая модель подсистемы СЗИ от НСД описывает работу пользователя с отдельными объектами (рис. 3), она основана на принципе разграничения доступа по аутентификации пользователя и ограничения его прав доступа к отдельным объектам системы. В случае если пользователю запрещено работать с отдельными объектами, то СЗИ от НСД блокирует доступ к объекту и записывает информацию о данном факте в журнале событий. Это помогает выявлять факты НСД пользователя к объектам, к которым он не имеет доступа. Данный функционал заложен во вредоносную программу для того, чтобы провести имитацию реакции СЗИ от НСД на действия злоумышленника. В вершине r29 реализован переход на подсистему «Работа пользователя с прикладными программными продуктами», которая моделирует работу пользователя с отдельными ПП.

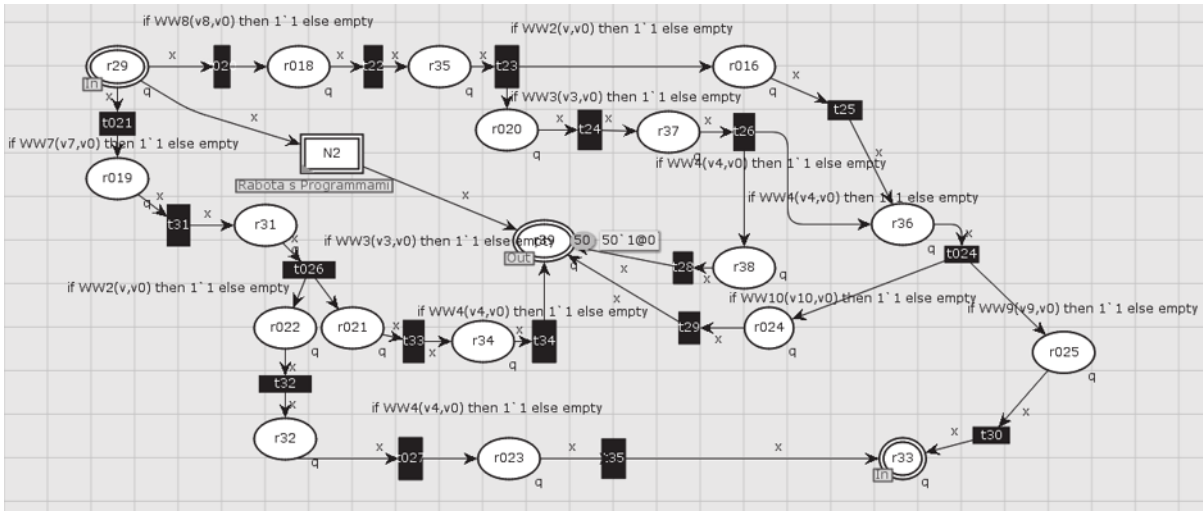

Рис. 3. Работа пользователя с файлами и программами
(Fig. 3. User work with files and programs)

Таблица 3. Работа пользователя с файлами и программами

Функции, выполняемые СЗИ от НСД
2.9 Допуск субъекта к защищаемому объекту
3.1 Запрос на преобразование объекта
3.2 Блокировка преобразования объекта
3.3 Регистрация нарушений работы с СЗИ от НСД
3.4 Пересчет параметров целостности файла
3.5 Запрос на удаление
3.6 Блокировка удаления
3.7 Преобразование объекта перед удалением
3.8 Удаление объекта
3.9 Завершение работы с объектом

Модель подсистемы «Работа пользователя с прикладными программными продуктами» (рис. 4) включает в себя наиболее распространенное ПО. Данная подсистема взаимодействует с подсистемой «Работа пользователя с файлами и программами», соединительной вершиной между ними является r411. Необходимо отметить, что в модели мы рассматриваем работу только с одним ПП, без возможности использовать другие программы параллельно. Данная система отражает работу пользователя с типовым составом ПП, в частности, с такими как Microsoft Office, ABBY Fine Reader, Nero, WinRar, Total Commarder.

Модель «Деструктивное воздействие на СЗИ от НСД» (рис. 5) описывает действия злоумышленника по внедрению вредоносной программы посредством накопленных у него сведений о системе. Предварительный сценарий вредоносного воздействия злоумышленника на защищенный информационный ресурс АС разработан на основе анализа угроз, представленных в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации.

Вывод данной модели осуществлён в вершину r24 «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов», которая отображает работу пользователя с внешним носителем информации.

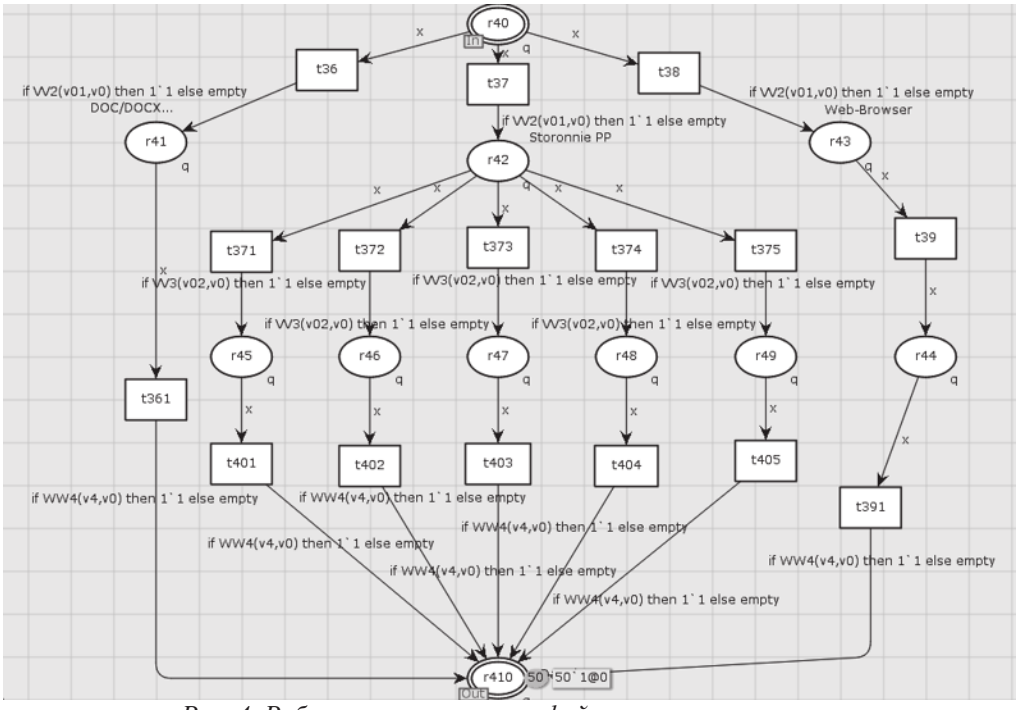

Рис. 4. Работа пользователя с файлами и программами
(Fig. 4. User work with files and programs)

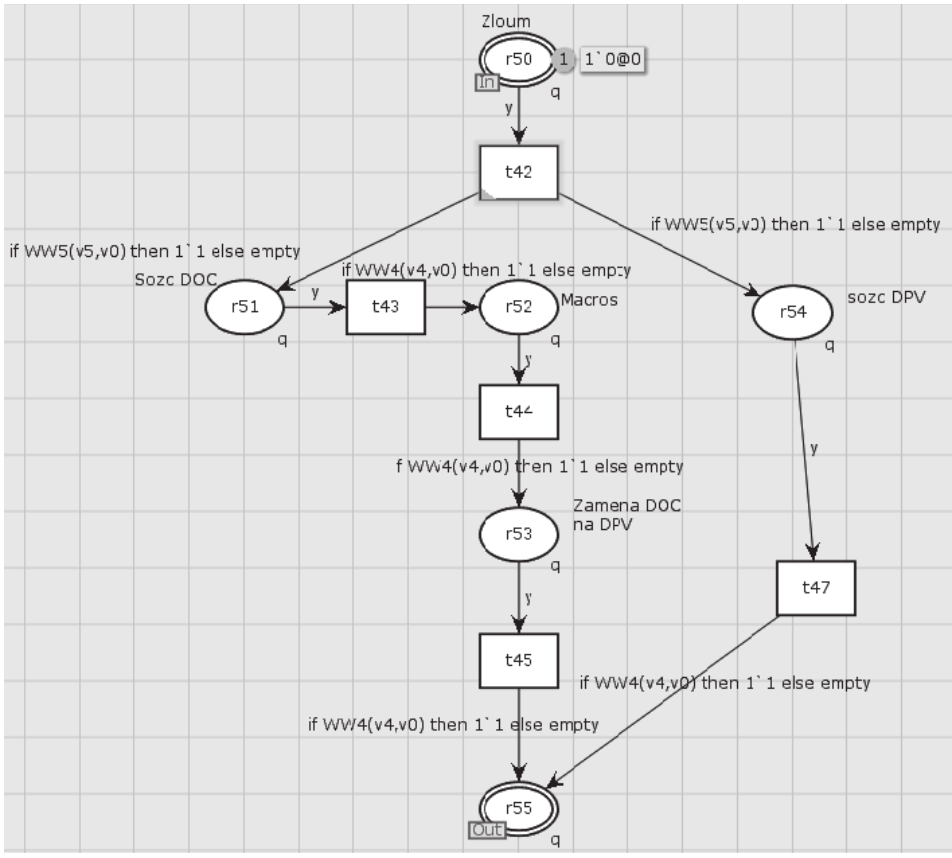

Рис. 5. Деструктивное воздействие на средства защиты информации
от несанкционированного доступа
(Fig. 5. Destructive impact on the means of information protection from unauthorized access)

Таблица 4. Работа пользователя с файлами и программами

Функции, выполняемые СЗИ от НСД
4 Начало работы с программами
4.1 Работа с документами
4.2 Работа с отдельным ПО
4.3 Работа с браузером и в сети (локальной/глобальной)
4.4 Использование различных серверов в Интернете
4.5 Работа с ПП Microsoft Office
4.6 Работа с ПП ABBY Fine Reader
4.7 Работа с ПП Nero
4.8 Работа с ПП WinRar
4.9 Работа с ПП Total Commarder
4.10 Работа с ПП Lock
4.11 Полученные в ходе работы данные или действия с отдельными обьектами (файлами/папками)

Таблица 5. Деструктивное воздействие на СЗИ от НСД

Деструктивное воздействие злоумышленника на информационный ресурс АС (предварительный сценарий)
5 Действия злоумышленника
5.1 Создание документа
5.2 Создание в документе вредоносной программы в виде макроса запускающегося вместе с открытием документа
5.3 Замена на носителе «чистого» документа вредоносным
5.4 Создание вредоносного ПО с функцией автозапуска
5.5 Запись на носитель вредоносного документа или вредоносной программы

После всех проделанных операций получилась рабочая модель СЗИ от НСД. Это позволяет наглядно представить, что происходит при ее работе на системном уровне, а также учесть предполагаемые действия злоумышленника. Имитационная модель будет являться дискретной, динамической, стохастической по причине того, что этими свойствами обладает СЗИ от НСД в автоматизированной системе, поэтому данная модель будет дискретно-событийной, следовательно, отражающей свойства во времени. Вероятность перехода из одного состояния в другое является мгновенной и зависит от времени пребывания в предыдущем состоянии.

Заключение

В данной статье разработана имитационная модель СЗИ от НСД. Выделены ее ключевые подсистемы и функциональные компоненты согласно технической документации [1, 2]. При помощи инструмента «Hierarchy», встроенного в CPN Tools, реализованы взаимосвязи между подсистемами, что позволяет модели соответствовать реально используемой на объектах информатизации СЗИ от НСД. Разработанная имитационная модель функционирования СЗИ от НСД в программной среде CPN Tools в

отличие от существующих формальных моделей [3] позволяет получить вероятностно-временные характеристики (в виде времен выполнения защитных функций). Это дает возможность не проводить вычислительный эксперимент по исследованию вероятностно-временных характеристик этих систем, которые в дальнейшем планируется использовать при количественной оценке эффективности программных средств и систем информационной безопасности в АС на объектах информатизации. Разработанную имитационную модель СЗИ от НСД в программной среде CPN Tools в дальнейших исследованиях планируется использовать как основу для анализа и создания моделей противодействия различным видам угроз НСД к информационному ресурсу защищенных АС.

СПИСОК ЛИТЕРАТУРЫ:

1. СЗИ «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 25.05.2019).
2. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 25.05.2019).
3. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учётом их временных характеристик в автоматизированных системах органов внутренних дел: дис канд. техн. наук. Воронеж / 2018. URL: https://ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (дата обращения: 25.05.2019).
4. Вентцель Е.С. Теория вероятностей. (accessed: 25.05.2019) Наука, 1969. – 576 с.
5. Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag, 2009.
6. Синегубов С.В. Моделирование систем и сетей телекоммуникаций. Воронеж: ВИ МВД РФ, 2016. – 336 с.
7. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.
8. Григорьев В.А., Карпов А.В. Имитационная модель системы защиты информации // Программные продукты и системы. Тверь: МНИИПУ и НИИ «Центрпрограммсистем», 2005. №2. С. 26–30.
9. Питерсон Д.Ж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 264 с.
10. Котов В.Е. Сети Петри. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 160 с.
11. Дровникова И.Г., Змеев А.А., Попов А.Д., Рогозин Е.А. Методика исследования вероятностно-временных характеристик реализации сетевых атак в программной среде имитационного моделирования. Вестник Дагестанского государственного технического университета. Технические науки. 2017. 44 (4). С. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113.
12. Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments // IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.
13. Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.
14. Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P. 104–118.
15. Shang Guan Wei [et. al.] Research of System Modeling and Verification Method Combine with UML Formalization Analysis and Colored Petri Net Third International Symposium on Intelligent Information Technology Application, 2009. P. 488–491.

REFERENCES:

[1] SZI «Strazh NT». Rukovodstvo administratora. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (accessed: 25.05.2019) (in Russian).
[2] Sistema zashchity informacii ot nesankcionirovannogo dostupa «Strazh NT». Opisanie primeneniya. URL: http://www.rubinteh.ru/public/opis30.pdf (accessed: 25.05.2019) (in Russian).
[3] Popov A.D. Modeli i algoritmy ocenki effektivnosti sistem zashchity informacii ot nesankcionirovannogo dostupa s uchyotom ih vremennyh harakteristik v avtomatizirovannyh sistemah organov vnutrennih del: dis kand. tekhn. nauk. Voronezh / 2018. URL: https://vi.mvd.rf/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (accessed: 25.05.2019) (in Russian).

[4] Ventcel' E.S. Teoriya veroyatnostej. – M.: Nauka, 1969. – 576 s. (in Russian).
[5] Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag 2009.
[6] Sinegubov S.V. Modelirovanie sistem i setej telekommunikacij. Voronezh: VI MVD RF, 2016. – 336 s. (in Russian).
[7] Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.
[8] Grigor'ev V.A., Karpov A.V. Imitacionnaya model' sistemy zashchity informacii. Programmnye produkty i sistemy. Tver': MNIIPU i NII «Centrprogrammsistem», 2005. №2. S. 26–30 (in Russian).
[9] Piterson D.ZH. Teoriya setej Petri i modelirovanie sistem: Per. s angl. – M.: Mir, 1984. – 264 s. (in Russia).
[10] Kotov V.E. Seti Petri. Moskva: Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury, 1984. – 160 s. (in Russian).
[11] Drovnikova I.G., Zmeev A.A., Popov A.D., Rogozin E.A. Methodology for investigating the probability-time characteristics of network attacks in the simulation modelling software environment. Herald of dagestan state technical university. Technical sciences. 2017. 44 (4). P. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113 (in Russian).
[12] Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments. IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.
[13] Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.
[14] Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P 104–118.
[15] Shang Guan Wei [et. al.] Research of System Modeling and Verification Method Combine with UML Formalization Analysis and Colored Petri Net Third International Symposium on Intelligent Information Technology Application, 2009. P. 488–491.

Поступила в редакцию – 04 июля 2019 г. Окончательный вариант – 17 сентября 2019 г.
Received – July 04, 2019. The final version – September 17, 2019.

Ирина В. Машкина[1], Елена П. Белова[2]
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
ул. К. Маркса, 12, г. Уфа, 450008, Республика Башкортостан, Россия
[1]e-mail: mashkina.vtzi@gmail.com, https://orcid.org/0000-0002-3096-3102
[2]e-mail: super.yelenar@yandex.ru, https://orcid.org/0000-0001-5488-943X

РАЗРАБОТКА НЕЙРОСЕТЕВОЙ БАЗЫ ДАННЫХ БИОМЕТРИЧЕСКИХ ОБРАЗОВ НА ОСНОВЕ НЕСКОЛЬКИХ ПАРАМЕТРОВ СПЕКТРОВ ГЛАСНЫХ ЗВУКОВ ДЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПО ГОЛОСУ

DOI: http://dx.doi.org/10.26583/bit.2019.3.08

Аннотация. Данное исследование посвящено методам биометрической аутентификации и идентификации администраторов сети по голосу. В работе предложен метод представления уникальных параметров голоса, а также принцип построения искусственной нейронной сети для системы аутентификации пользователя и контроля доступа. Представлена структура системы биометрической аутентификации / авторизации пользователей информационной системы с использованием уникальных параметров голоса: частотного диапазона четвёртой форманты гласного звука, частоты четвёртой форманты и частоты лидирующей форманты спектральной характеристики. Построены две нейросетевые базы данных биометрических образов: первая базируется только на характеристиках четвёртой форманты гласного звука, вторая – кроме них использует и частоту лидирующей форманты. Рассмотрены возможные решения специфических задач построения и обучения искусственной нейронной сети для построения базы биометрических образов пользователей и уменьшения ошибок первого и второго рода.

Ключевые слова: биометрический образ личности, нейросетевая база данных биометрических образов, характеристики четвёртой форманты гласного звука, частота лидирующей форманты спектральной характеристики, аутентификация по голосу, авторизация по голосу.

Для цитирования: МАШКИНА, Ирина В.; БЕЛОВА, Елена П. РАЗРАБОТКА НЕЙРОСЕТЕВОЙ БАЗЫ ДАННЫХ БИОМЕТРИЧЕСКИХ ОБРАЗОВ НА ОСНОВЕ НЕСКОЛЬКИХ ПАРАМЕТРОВ СПЕКТРОВ ГЛАСНЫХ ЗВУКОВ ДЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПО ГОЛОСУ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 90-102, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1221>. Дата доступа: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.08.

Irina V. Mashkina[1], Yelena P. Belova[2]
Ufa State Aviation Technical University,
K. Marx Street, 12, Ufa, 450008, Republic of Bashkortostan, Russia
[1]e-mail: mashkina.vtzi@gmail.com, https://orcid.org/0000-0002-3096-3102
[2]e-mail: super.yelenar@yandex.ru, https://orcid.org/0000-0001-5488-943X

Development of neural network database for biometric images based on several parameters of voice sound spectrum for authentication and authorization by voice

DOI: http://dx.doi.org/10.26583/bit.2019.3.08

Abstract. This study focuses on the methods of biometric authentication and identification of network administrators by voice. The authors propose a method for presenting unique voice parameters, as well as the principle of constructing an artificial neural network for a user authentication system and access control. The structure of the biometric authentication / authorization system of information system users is presented using unique voice parameters: the frequency range of the vowel fourth formant, the fourth formant frequency and the leading formant frequency of spectral characteristic. Two neural network databases of biometric images were built: the first is based only on the characteristics of the vowel fourth formant, the second uses the frequency of the leading formant as well. Possible solutions for specific

tasks of building and teaching ANNs are considered to build a base of user biometric images and reduce first and second types errors.

Keywords: biometric image of a person, neural network database of biometric images, characteristics of the fourth formant of the vowel sound, frequency of the leading spectral characteristic formants, voice authentication, voice authorization.

For citation: MASHKINA, Irina V.; BELOVA, Yelena P. Development of neural network database for biometric images based on several parameters of voice sound spectrum for authentication and authorization by voice. IT Security (Russia), [S.l.], v. 26, n. 3, p. 90-102, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1221>. Date accessed: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.08.

Введение

В настоящее время в индустрии информационных технологий наблюдается развитие биометрических систем аутентификации (БСА) [1], но при этом недостаточно широко освещается проблема использования этих систем с точки зрения достоверности распознавания личности, зависящей от возможных ошибок первого и второго рода. Аутентификация по голосу представляет собой одно из актуальных и развивающихся направлений в области распознавания личности по биометрическим характеристикам. При этом уникальность выбранного биометрического признака обеспечивает высокую достоверность, т.е. приемлемые значения ошибок распознавания личности [2].

Особое значение распознавание личности имеет в сфере компьютерной безопасности. Процедуры аутентификации и авторизации субъектов являются важнейшим механизмом защиты, от качества которого зависит безопасность информационной системы (ИС) [3].

Главным достоинством БСА по голосу, согласно источникам [4, 5], является относительно низкая стоимость, поскольку система может быть построена исключительно с использованием имеющихся на компьютере стандартных средств и разработанных программных модулей. Ещё одно достоинство, выявленное авторами статьи в работе [6], является возможность хранения в БСА биометрического образа пользователя, причём в случае использования искусственной нейронной сети (ИНС) в качестве базы биометрических образов этот эталон невозможно каким-либо способом выявить или скопировать.

К основным недостаткам БСА по голосу относится недостаточная (в случае однофакторной аутентификации) точность распознавания и влияние на результаты психофизиологического состояния личности [7]. Однако точность распознавания можно повысить путём использования различных дополнительных методов обработки голосовых биометрических данных. А зависимость результатов аутентификации по голосу от психофизиологического состояния личности можно использовать при реализации процедуры допуска к работе в информационных системах с высокой ценой ошибки оператора.

Построение искусственной нейронной сети – базы данных биометрических образов пользователей

В работе предлагается система аутентификации / авторизации пользователей, имеющих административные привилегии. В такой системе объекты инфраструктуры разделены на группы и сферы администрирования. Предложен механизм усиленной аутентификации и делегирования полномочий, который позволяет исключить суперпользователя путём создания отдельных ролей: администратора сети,

администратора безопасности, администратора виртуальной инфраструктуры, администратора АСУТП.

На основе построения нейросетевой базы биометрических образов пользователей-администраторов реализуется механизм усиленной аутентификации администраторов, имеющих доступ к управлению конфигурацией.

В данной работе в качестве биометрического образа личности используются сразу несколько спектральных характеристик гласных звуков: характеристики четвёртой форманты и частота лидирующей форманты гласного звука речи, произнесённого пользователем. Такое решение обусловлено тем, что, согласно [8, 9], комбинирование нескольких признаков всегда обеспечивает существенное уменьшение величин ошибок 1-го и 2-го рода.

Под формантой принято понимать концентрацию энергии в ограниченной частотной области [10, 11]. Из данного определения следует, что четвёртая форманта гласного звука – это четвёртый по счёту всплеск энергии в ограниченной частотной области, который фиксируется на спектрограмме гласного звука.

В данной работе используются следующие *характеристики четвёртой форманты*:

- частота $f_{4\max}$, соответствующая максимальному значению амплитуды выброса энергии в четвёртой частотной области на спектрограмме;
- частота f_{4s}, определяющая начало четвёртой ограниченной частотной области на спектрограмме;
- частота f_{4f}, определяющая конец четвёртой ограниченной частотной области на спектрограмме.

В работах [4, 12] отмечается, что «четвёртая форманта характеризует речевой тракт человека». Эффективность её использования доказана авторами данной статьи в [6].

Частота лидирующей форманты f_l – это частота, соответствующая наибольшему значению амплитуды выброса любой из фиксируемых на спектрограмме формант.

Комбинации лидирующих формант гласных звуков различных пользователей имеют существенные отличия, что позволяет повысить точность распознавания личности.

При проведении исследований использовались характеристики четвёртых формант и частоты лидирующих формант, определённые по спектрограммам, полученным при произнесении пользователем трёх гласных звуков: "А", "О" и "Э". Спектрограммы именно этих звуков характеризуются чётко выраженными областями повышенной концентрации энергии в 4-й ограниченной частотной области. Примеры спектрограмм гласных звуков «А», «О» и «Э» представлены на рис. 1-3. На каждой спектрограмме жёлтым цветом отмечены: частота, определяющая начало четвёртой ограниченной частотной области, частота четвёртой форманты и частота, определяющая конец четвёртой ограниченной частотной области. Красным цветом показана частота лидирующей форманты. Спектрограммы звуков «И», «У» и «Ы» не имеют чётко выраженной четвёртой частотной ограниченной области. На рис. 4-5 в качестве примера приведены спектрограммы звуков «И» и «У».

К исследованию привлечено 4 человека: 3 женщины и 1 мужчина. При этом для эксперимента были приглашены женщины именно со схожими голосами, так как схожесть голосов пользователей приводит к близости спектральных характеристик, тем самым создавая одну из главных проблем современных систем аутентификации.

При создании алгоритма нахождения формант авторы статьи опирались на [13], а при написании кода программных модулей – на источники [10, 14]. Выделение характеристик четвёртой форманты гласного звука осуществляется при помощи двух программных модулей [15]. Назначение первого программного модуля – получение спектрограммы гласного звука, произнесённого пользователем для выбранных в эксперименте фонем (рис. 1-5). Второй модуль реализует алгоритм выделения характеристик четвёртой форманты гласного звука.

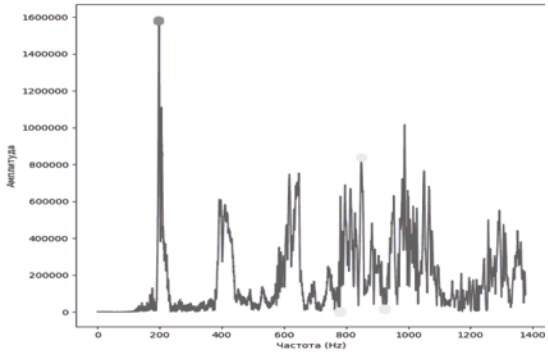

Рис. 1. Спектрограмма звука «А», произнесённого одним из пользователей
(Fig. 1. Spectrogram of sound "A", pronounced by one of the users)

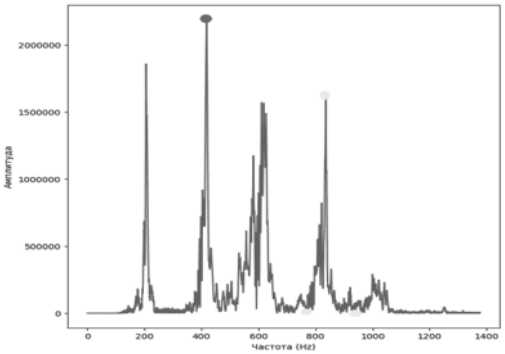

Рис. 2. Спектрограмма звука «О», произнесённого одним из пользователей
(Fig. 2. Spectrogram of sound "O", pronounced by one of the users)

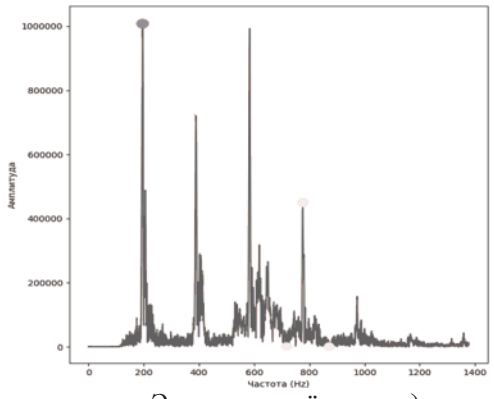

Рис. 3. Спектрограмма звука «Э», произнесённого одним из пользователей
(Fig. 3. Spectrogram of sound "Э", pronounced by one of the users)

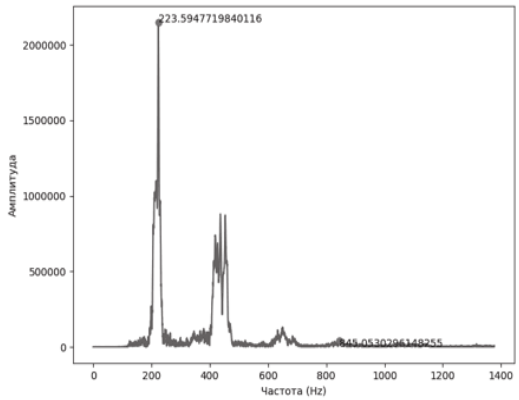

Рис. 4. Спектрограмма звука «И», произнесённого одним из пользователей
(Fig. 4. Spectrogram of sound "И", pronounced by one of the users)

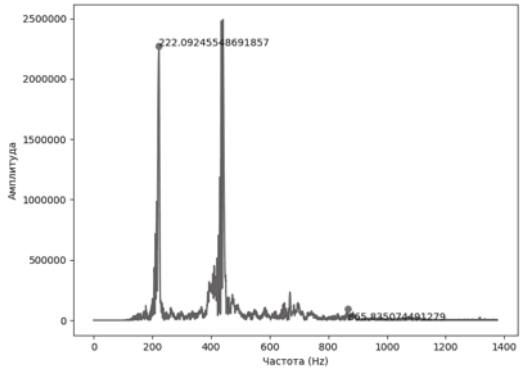

Рис. 5. Спектрограмма звука «У», произнесённого одним из пользователей
(Fig. 5. Spectrogram of sound "У", pronounced by one of the users)

Модуль выделения частоты лидирующей форманты (f_l) в настоящее время не реализован авторами. Поэтому процедура выделения частоты лидирующей форманты осуществлялась при помощи программы bard [16] в полуавтоматическом режиме.

Для реализации механизма аутентификации и авторизации пользователей в работе используется искусственная нейронная сеть (ИНС). В [17, 18] отмечаются следующие достоинства ИНС: быстрота обучения и самообучения, высокий уровень отказоустойчивости и помехоустойчивости, высокая скорость решения задач и широкая область применения.

Применительно к задаче подтверждения личности пользователя по предъявленным им биометрическим данным, процесс построения ИНС включает в себя следующие этапы: постановку задачи, выбор входных и выходных переменных ИНС, выбор архитектуры и структуры ИНС, построение обучающей выборки, получение и обработку результатов обучения и тестирования.

1. Постановка задачи

Задача данного исследования – создать *нейросетевую базу данных* биометрических образов (НБДБО) для усиленной аутентификации и авторизации пользователей ИС с административными полномочиями.

2. Выбор входных и выходных переменных ИНС

В качестве входных переменных используется вектор *X*, включающий в себя следующие показатели: номер пользователя x_1, предъявившего свой идентификатор, 12 входов $(x_2,...,x_{13})$ для предъявленных пользователем биометрических данных, прошедших предварительную обработку по выделению характеристик четвёртых формант и частот лидирующих формант каждого из выбранных гласных звуков. Значения характеристик $x_2,...,x_{13}$ получены после обработки спектрограмм звуков, произнесённых пользователем в соответствии с тремя выбранными гласными фонемами. В качестве выходных переменных ИНС рассматривается вектор *Y*, размерность которого равна четырём (по числу администраторов).

3. Выбор архитектуры и структуры ИНС

Выбрана архитектура сети, позволяющая в полном объёме решить поставленные в работе задачи, а именно: – двухслойный персептрон прямого распространения. Количество нейронов во внутреннем слое выбрано с учётом объёма обучающей выборки, количества входов и выходов [19]:

$$N = \left[\frac{Q * n}{m + n} \right], \quad (1)$$

где: *N* – количество нейронов в скрытом слое,

m – количество входов,

n – количество выходов,

Q – объём обучающей выборки,

[ ] – операция округления до целого числа.

Аргументировать выбор данной архитектуры ИНС можно тем, что она представляет собой универсальный аппроксиматор, позволяющий реализовать нелинейное отображение F:

$$X \longrightarrow Y ,$$

где: $X = (x_1,...x_m)$ – входной вектор размерности *m*;

$Y = (y_1,...y_4)$ – выходной вектор размерности *n*=4.

В рамках данного исследования была создана ИНС, базирующаяся только на характеристиках четвёртой форманты. При этом на входы ИНС *единовременно* подавались результаты обработки спектрограмм произнесённых пользователем гласных звуков всех заявленных фонем (рис. 6).

Входной нейрон 1 – номера идентификаторов пользователей с 1 по 4; входные нейроны 2–4 – значения характеристик четвёртой форманты гласного звука «А»; входные нейроны 5–7 – значения характеристик четвёртой форманты гласного звука «О»; входные нейроны 8–10 – значения характеристик четвёртой форманты гласного звука «Э». Таким образом, $m = 10$. Выходные нейроны П1, П2, П3 и П4 – данные о пользователях с первого по четвёртый. Активный выходной нейрон свидетельствует о том, биометрические данные какого пользователя были поданы на вход нейросети.

Во втором варианте построения ИНС введены дополнительные входы: входной нейрон 11 – значение частоты лидирующей форманты гласного звука «А»; входной нейрон 12 – значение частоты лидирующей форманты гласного звука «О»; входной нейрон 13 – значение частоты лидирующей форманты гласного звука «Э» (рис. 7). То есть $m = 13$.

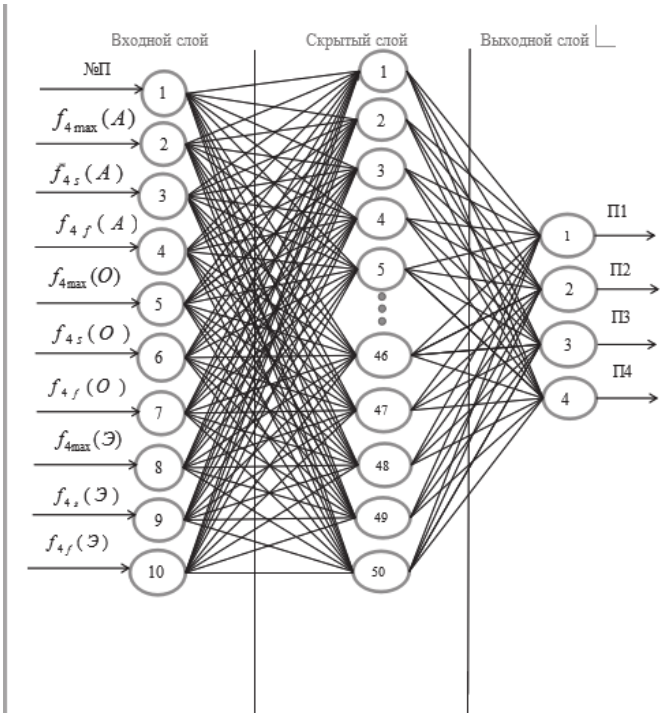

Рис. 6. Архитектура искусственной нейронной сети, базирующейся на характеристиках четвёртой форманты гласных звуков «А», «О» и «Э»
(Fig. 6. The Architecture of an Artificial Neural Network based on the Characteristics of the Fourth Formant of Vowel Sounds "A", "O" and "Э")

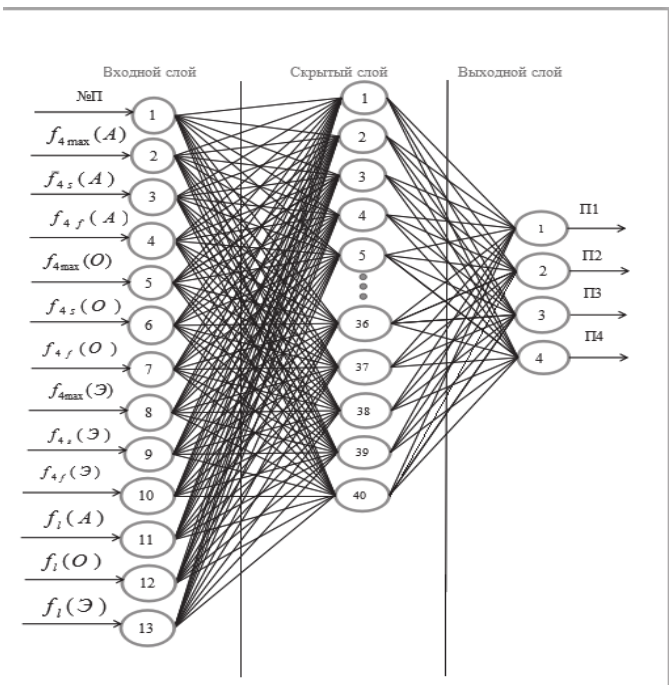

Рис. 7. Архитектура искусственной нейронной сети, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э»
(Fig. 7. The Architecture of an Artificial Neural Network based on the Characteristics of the Fourth Formant and the Frequencies of the Leading Formant of the vowel sounds "A", "O" and "Э")

4. Построение обучающей выборки

Обучающая выборка для второго варианта ИНС приведена в таблицах 1 и 2.

Таблица 1. Входные данные обучающей выборки для ИНС, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э»

№ строки	№ №	Значения характеристик четвёртой форманты гласного звука									Значения частот лидирующей форманты гласного звука		
		$f_{4max}(A)$	$f_{4s}(A)$	$f_{4f}(A)$	$f_{4max}(O)$	$f_{4s}(O)$	$f_{4f}(O)$	$f_{4max}(Э)$	$f_{4s}(Э)$	$f_{4f}(Э)$	$f_l(A)$	$f_l(O)$	$f_l(Э)$
1	1	815	710	908	781	720	961	821	732	900	815	579	647
2	1	849	779	926	808	747	877	822	738	889	199	585	616
...	...	...	...	...	...	...	...	...	...	...	...	...	...
10	1	835	733	920	759	666	802	818	737	879	220	574	610
11	1	774	636	831	902	828	996	762	667	850	196	221	570
12	1	784	710	866	864	784	926	770	675	852	1003	417	574
...	...	...	...	...	...	...	...	...	...	...	...	...	...
19	1	722	639	792	745	675	848	787	668	879	898	198	176
20	1	773	693	832	759	675	828	840	776	945	197	195	650
21	1	531	441	653	539	562	603	529	464	584	531	436	529
...	...	...	...	...	...	...	...	...	...	...	...	...	...
30	1	548	482	603	564	384	668	529	470	569	657	453	529
31	1	898	845	961	912	860	860	880	855	949	898	467	222
...	...	...	...	...	...	...	...	...	...	...	...	...	...
40	1	917	846	873	928	868	962	917	834	1004	917	486	457
41	2	774	636	831	902	828	996	762	667	850	196	221	570
42	2	784	710	866	864	784	926	770	675	852	1003	417	574
...	...	...	...	...	...	...	...	...	...	...	...	...	...
50	2	773	693	832	759	675	828	840	776	945	197	195	650
51	2	815	710	908	781	720	961	821	732	900	815	579	647
...	...	...	...	...	...	...	...	...	...	...	...	...	...
80	2	917	846	873	928	868	962	917	834	1004	917	486	457
81	3	531	441	653	539	562	603	529	464	584	531	436	529
82	3	518	428	563	544	462	604	547	464	611	616	435	547
...	...	...	...	...	...	...	...	...	...	...	...	...	...
90	3	548	482	603	564	384	668	529	470	569	657	453	529
91	3	815	710	908	781	720	961	821	732	900	815	579	647
...	...	...	...	...	...	...	...	...	...	...	...	...	...
120	3	917	846	873	928	868	962	917	834	1004	917	486	457
121	4	898	845	961	912	860	860	880	855	949	898	467	222
122	4	916	843	843	905	832	1027	912	810	1005	916	452	455
...	...	...	...	...	...	...	...	...	...	...	...	...	...
130	4	917	846	873	928	868	962	917	834	1004	917	486	457
131	4	815	710	908	781	720	961	821	732	900	815	579	647
...	...	...	...	...	...	...	...	...	...	...	...	...	...
160	4	548	482	603	564	384	668	529	470	569	657	453	529

Обучающая выборка для сети с использованием частот лидирующих формант (рис. 7) содержит 160 строк (обучающих примеров). Она включает в себя четыре набора строк (по одному набору на одного человека). При этом каждый набор состоит из двух частей: данных для обучения ИНС на распознавание легального пользователя, предоставившего свой идентификатор (примеры 1 — 10, 41 — 50, 81 — 90, 121 — 130), и данных для обучения распознаванию несанкционированных действий администраторов в

случаях их попыток осуществить аутентификацию под идентификатором другого администратора (примеры 11 — 40, 51 — 80, 91 — 120, 131 — 160) с целью получения его привилегий.

Таблица 2. Выходные данные обучающей выборки для ИНС, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э»

№ строки	Номер			
	1	2	3	4
1	1	0	0	0
2	1	0	0	0
...	...	...	...	...
10	1	0	0	0
11	0	1	0	0
12	0	1	0	0
...	...	...	...	...
19	0	1	0	0
20	0	1	0	0
21	0	0	1	0
...	...	...	...	...
30	0	0	1	0
31	0	0	0	1
...	...	...	...	...
40	0	0	0	1
41	0	1	0	0
42	0	1	0	0
...	...	...	...	...
50	0	1	0	0
51	1	0	0	0
...	...	...	...	...
80	0	0	0	1
81	0	0	1	0
82	0	0	1	0
...	...	...	...	...
90	0	0	1	0
91	1	0	0	0
...	...	...	...	...
120	0	0	0	1
121	0	0	0	1
122	0	0	0	1
...	...	...	...	...
130	0	0	0	1
131	1	0	0	0
...	...	...	...	...
160	0	0	1	0

Разработанная ИНС на 160 примерах обучалась, на 160 примерах тестировалась или верифицировалась.

Обучающая выборка для сети с использованием только характеристик четвёртой форманты гласных звуков идентична вышеописанной, в ней лишь отсутствуют столбцы, соответствующие входам, на которые подаются частоты лидирующих формант гласных звуков.

5. Результаты обучения и тестирования

Создание и обучение ИНС осуществлялось при помощи программного комплекса Matlab R2015b.

Настройка сети, базирующейся только на характеристиках четвёртой форманты, произошла за 119 эпох. Величина лучшей среднеквадратичной ошибки сети составила 2,1152e-08.

Сеть, базирующаяся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э», настроилась за 16 эпох. Величина лучшей среднеквадратичной ошибки сети составила 5,7485e-12, что значительно ниже, чем у ИНС, использующей только характеристики четвёртой форманты.

Вычисление ошибок 1-го и 2-го рода проводилось при помощи графического интерфейса nntool программного комплекса Matlab R2015b.

Среднее значение ошибки 1-го рода для сети, базирующейся на характеристиках четвёртой форманты гласных звуков «А», «О» и «Э» составило 10%, так как в 90% случаев легальный пользователь успешно прошёл аутентификацию (табл. 3), среднее значение ошибки 2-го рода – 5% (табл. 4).

Таблица 3. Процентное значение пропуска легального пользователя при использовании ИНС, базирующейся на характеристиках четвёртой форманты гласных звуков «А», «О» и «Э»

№ пользователя	1	2	3	4	Среднее значение:
Итого	90%	70%	100%	100%	90%

Таблица 4. Результаты вычисления ошибки 2-го рода при использовании ИНС, базирующейся на характеристиках четвёртой форманты гласных звуков «А», «О» и «Э»

№ пользователя	1	2	3	4	Среднее значение:
Итого	16,67%	3,33%	0,00%	0,00%	5,00%

Среднее значение ошибки 1-го рода у сети, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э», составило 7,5% (табл. 5).

Таблица 5. Процентное значение пропуска легального пользователя при использовании ИНС, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э»

№ пользователя	1	2	3	4	Среднее значение:
Итого	90%	80%	100%	100%	92,5%

Среднее значение ошибки 2-го рода составило 5% (табл. 6).

Таблица 6. Результаты вычисления ошибки 2-го рода при использовании ИНС, базирующейся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э»

№ пользователя	1	2	3	4	Среднее значение:
Итого	13,33%	6,67%	0%	0%	5%

Благодаря одновременной подаче характеристик четвёртой форманты трех выбранных гласных звуков и использованию частот лидирующих формант этих же звуков удалось снизить ошибки даже при аутентификации пользователей, имеющих похожие голоса.

Согласно результатам проведённых исследований, целесообразно использовать ИНС, базирующуюся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э». Введение дополнительного речевого параметра (частоты лидирующей форманты) во втором варианте построения ИНС позволило уменьшить среднее значение ошибки 2-го рода на 2,5% по сравнению с первым вариантом архитектуры ИНС. Оба варианта построения сетей прошли исследование на данных пользователей, имеющих близкие спектральные характеристики, то есть полученные результаты соответствуют наихудшему случаю. Полученные величины ошибок в обеих сетях являются приемлемыми по сравнению с величинами ошибок распознавания, основанного на использовании других методов и речевых параметров [4, 20].

Заключение

Аутентификация по голосу пользователей с похожими спектральными характеристиками является одной из важных задач распознавания личности. Искусственная нейронная сеть, базирующаяся на характеристиках четвёртой форманты гласных звуков «А», «О» и «Э», и искусственная нейронная сеть, базирующаяся на характеристиках четвёртой форманты и частотах лидирующих формант гласных звуков «А», «О» и «Э», могут стать одними из инструментов её решения. Полученные значения ошибок 1-го и 2-го рода у этих сетей показывают результативность идеи и возможность проведения дальнейших исследований в данном направлении. Планируется проведение исследований с целью распознавания «чужого».

СПИСОК ЛИТЕРАТУРЫ:

1. Мировой рынок биометрических систем 2015-2022 гг. Обзор рынка, январь 2017 г. // URL: http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618, свободный (дата обращения: 14.05.2019).
2. Сорокин В.Н. Верификация диктора по спектрально-временным параметрам речевого сигнала / В.Н. Сорокин, А.И. Цыплихин // Информационные процессы. 2010. Т. 10, №2. С. 87–104.
3. Актуальные аспекты информационной безопасности / под ред. О.Б. Макаревича: Монография. – Таганрог: Издательство ТТИ ЮФУ, 2011. – 448 с.
4. Сорокин В.Н. Распознавание личности по голосу: аналитический обзор [Текст] / В.Н. Сорокин, В.В. Вьюгин, А.А. Тананыкин // Информационные процессы. Том 12, №1. Институт проблем передачи информации, Российская академия наук, Москва. 2012. С. 1–30.
5. Первушин Е.А. Обзор основных методов распознавания дикторов / Е.А. Первушин // Математические структуры и моделирование. 2011. Вып. 24. С. 41–54.
6. Belova Ye.P., Mashkina I.V., Research Results of Artificial Neural Network for User Authentication According to Frequency of Fourth Formant of Vowel Sound Phoneme // Сборник научных трудов «2018 International Russian Automatisation Conference (RusAutoCon)», издательство: институт IEEE. DOI: 10.1109/RUSAUTOCON.2018.8501680, 2018 г. URL: https://ieeexplore.ieee.org/document/8501680 (дата обращения: 14.05.2019).
7. Новиков А.С., Нестеров К.С. Биометрическая система аутентификации с использованием голосовых данных / А.С. Новиков, К.С. Нестеров // Известия ТулГУ. Технические науки. 2016. №2. URL: https://cyberleninka.ru/article/n/biometricheskaya-sistema-autentifikatsii-s-ispolzovaniem-golosovyh-dannyh (дата обращения: 05.05.2019).
8. Матвеев Ю.Н. Исследование информативности признаков речи для систем автоматической идентификации дикторов [Текст] / Ю.Н. Матвеев // Известия вузов. Приборостроение. 2013. Т. 56, №2. С. 47–51.
9. Матвеев Ю.Н., Симончик К.К. Система идентификации дикторов по голосу для конкурса NIST SRE 2010 // Тр. 20-й Междунар. конф. по компьютерной графике и зрению «ГрафиКон 2010». СПб: СПбГУ ИТМО, 2010. С. 315–319.
10. Рабинер Л.Р., Шафер Р.В. Цифровая обработка речевых сигналов. – М.: Радио и связь, 1981. – 496 с.
11. Сидоренко И.А., Кускова П.А. О спектральном анализе фонем с использованием звуковых редакторов [Текст] / Научные ведомости БелГУ, серия История. Политология. Экономика. Информатика. 2013, №22 (165). С. 246–250.

12. Сорокин В.Н. Теория речеобразования. – М.: Радио и связь, 1985. – 312 с.
13. Оганесян А.Г. Эффективный алгоритм выделения формант из спектра речевого сигнала / А.Г. Оганесян // Вычислительная техника и информатика Том LIX, №1. Известия НАН РА и ГИУА, Москва. 2006. С. 177–183.
14. Лукин А. Введение в цифровую обработку сигналов [Электронный ресурс]. URL: http://audio.rightmark.org/lukin/dspcourse/dspcourse.pdf свободный (дата обращения: 26.04.2019).
15. Герасимов В.В., Белова Е.П., Машкина И.В. Выделение характеристик четвёртой форманты гласного звука // Свидетельство о государственной регистрации программы для ЭВМ от 3 апреля 2019 года №2019614367.
16. Bard 0.1.7. URL: http://psi-logic.narod.ru/bard/bard.htm, свободный (дата обращения: 26.04.2019).
17. Рутковский, Л. Методы и технологии искусственного интеллекта / Лешек Рутковский. – Пер. в польского И.Д. Рудинского. – М.: Горячия линия-Телеком, 2010. – 520 с.
18. Осовский С. Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.
19. Кафаров В.В. и др. К вопросу моделирования и управления непрерывными технологическими процессами с помощью нейронных сетей / В.В. Кафаров, Л.С. Гордеев, М.Б. Глебов, Го Цзинбао // ТОХТ. 1995, №2.
20. Кулибаба О.В., Привалов М.В. Выбор признаков для аутентификации по голосу в компьютеризированной системе контроля доступа [Текст] // Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС та КМ-2010)/ Матеріали І всеукраїнської науково-технічної конференції студентів, аспірантів та молодих вчених – 19-21 травня 2010 р., Донецьк, ДонНТУ. 2010. С. 33–37.

REFERENCES:

[1] The global market for biometric systems 2015-2022. Market review, January 2017. URL: http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618, free (accessed: 14.05.2019) (in Russian).
[2] Sorokin V.N. Speaker verification by spectral parameters of a speech signal. V. N. Sorokin, A. I. Tsiplihin. Informatsionnye protsessi. 2010. Vol. 10, №2. S. 87–104 (in Russian).
[3] Topical Aspects of Information Security by ed. O. B. Makarevich: Monograph. – Taganrog: Publishing TTI YuFU, 2011. – 448 p. (in Russian).
[4] Sorokin V.N. Voice Recognition: An Analytical Review. V.N. Sorokin, V.V. Vjugin, A.A. Tananykin. Informatsionnye protsessi. Vol. 12, №1. Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow. 2012. P. 1–30. (in Russian).
[5] Pervushin Ye.A. Overview of the main speaker recognition methods. Ye.A. Pervushin. Matematicheskie structuri i modelirovaniye. 2011. Vol. 24. S. 41–54 (in Russian).
[6] Belova Ye.P., Mashkina I.V. Research Results of Artificial Neural Network for User Authentication According to Frequency of Fourth Formant of Vowel Sound Phoneme. Collection of scientific papers «2018 International Russian Automatisation Conference (RusAutoCon)», Publisher: IEEE Institutею DOI: 10.1109/RUSAUTOCON.2018.8501680, 2018. URL: https://ieeexplore.ieee.org/document/8501680 (accessed: 20.04.2019).
[7] Novikov A.S., Nesterov K.S. «Biometric authentication system using voice data» [Text]. Izvestiya TulGU. Tehnicheskie nauki, 2016. №2. URL: https://cyberleninka.ru/article/n/biometricheskaya-sistema-autentifikatsii-s-ispolzovaniem-golosovyh-dannyh (дата обращения: 05.05.2019) (in Russian).
[8] Matveev Yu.N. Investigation of the informativeness of speech signs for systems of automatic speaker identification [Text]. Yu.N. Matveev. Izvestiya Vuzov. Priborostroenie. 2013. Vol. 56, №2. S. 47–51. (in Russian).
[9] Matveev Yu.N., Simonchik K.K. Voice Recognition Identification System for Competition NIST SRE 2010. Proceedings of the 20th Intern. conf. on computer graphics and vision «GrafiCon 2010». Saint Petersburg:SPbSU ITMO, 2010. P. 315–319 (in Russian).
[10] Rabiner L.R., Shafer R.V. Digital processing of speech signals. – M.: Radio i svyaz, 1981. – 496 s. (in Russian).
[11] Sidorenko I.A., Kuskova P.A. About spectral analysis of phonemes using sound editors [Text]. Nauchnye vedomosti BelGU, series Istoriya. Politologiya. Economica. Informatika. 2013, №22 (165). S. 246–250. (in Russian).
[12] Sorokin V.N. Theory of Speech Formation. – Moscow: Radio i svyaz, 1985. – 312 s. (in Russian).
[13] Oganesyan A.G. Efficient algorithm for formant extraction from speech spectrum. Oganesyan A.G. Vichislitelnaya tehnika i informatika Vol. LIX, No1. Izvestiya NAN RA i GIYA, Moscow. 2006. S. 177–183 (in Russian).

[14] Lukin A. Introduction to digital signal processing [Electronic resource]. URL: http://audio.rightmark.org/lukin/dspcourse/dspcourse.pdf free (accessed: 26.04.2019).
[15] Gerasimov V.V., Belova Ye.P., Mashkina I.V. Isolation of the characteristics of the fourth formant of vowel sound. Certificate of state registration of the computer program of April 3, 2019 No. 201414367.
[16] Bard 0.1.7. URL: http://psi-logic.narod.ru/bard/bard.htm, free (accessed: 26.04.2019).
[17] Rutkovsky, L. Methods and technologies of artificial intelligence. L. Rutkovsky – Trans. from Polish I.D. Rudinsky. – M.: Goryachaya Liniya-Telekom, 2010. – 520 s. (in Russian).
[18] Osovsky S. Neural networks for information processing. Trans. from Polish I.D. Rudinsky. –M.: Finansy i Statistika, 2002. – 344 s. (in Russian).
[19] Kafarov V.V. et al. On the issue of modeling and control of continuous technological processes using neural networks. Kafarov V.V., Gordeev L.S., Glebov M.B., Guo Jingbao. TOXT. 1995. No2 (in Russian).
[20] Kulibaba O.V., Privalov M.V. The Selection of Characteristics for Voice Authentication in a Computerized Access Control System students, students and young people – 19-21 grass 2010, Donetsk, DonNTU. 2010. P. 33–37.

Поступила в редакцию – 19 мая 2019 г. Окончательный вариант – 13 сентября 2019 г.
Received – May 19, 2019. The final version – September 13, 2019.

Кирилл В. Плаксий[1], Андрей А. Никифоров[2], Наталья Г. Милославская[3]
Национальный исследовательский ядерный университет «МИФИ»
Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail: kirillplaksiy@mail.ru, http://orcid.org/0000-0002-8949-6772*
[2]*e-mail: andreinikiforov993@gmail.com, http://orcid.org/0000-0002-2726-0000*
[3]*e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805*

ИССЛЕДОВАНИЕ ГРАФОВЫХ СУБД, ПРИГОДНЫХ ДЛЯ РАБОТЫ С БОЛЬШИМИ ДАННЫМИ ПРИ ОБНАРУЖЕНИИ ДЕЛ ПО ОТМЫВАНИЮ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА*

DOI: http://dx.doi.org/10.26583/bit.2019.3.09

Аннотация. В статье рассматриваются популярные в настоящее время графовые системы управления базами данных (СУБД), способные работать с большими данными, с помощью которых можно реализовать хранение информации, полученной в ходе генерации преступных дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма (ОД/ФТ). Цель работы заключается в выборе защищенной графовой СУБД, подходящей для работы с большими данными финансовых расследований. Для этого решаются следующие задачи: рассматриваются имеющиеся графовые СУБД, проводится их анализ и сравнение друг с другом с особым акцентом на методы защиты, используемые для обеспечения безопасности хранимых данных. Были изучены достоинства и недостатки программных продуктов, а также было проведено сравнение по ряду параметров, характеризующих защиту информации в них. Каждый критерий сравнения имеет развёрнутые комментарии, на основе которых был выбран наиболее удобный, гибкий и современный вариант СУБД для использования при поиске случаев ОД/ФТ. По полученным результатам было установлено, что графовые СУБД подходят для работы с большими данными, а также по ряду параметров была выбрана одна из рассмотренных СУБД, а именно Janus Graph.

Ключевые слова: отмывание доходов, полученных преступным путем, финансирование терроризма, ОД/ФТ, информационная безопасность, типология, большие данные, системы управления базами данных (СУБД).
Для цитирования: ПЛАКСИЙ, Кирилл В.; НИКИФОРОВ, Андрей А.; МИЛОСЛАВСКАЯ, Наталья Г. ИССЛЕДОВАНИЕ ГРАФОВЫХ СУБД, ПРИГОДНЫХ ДЛЯ РАБОТЫ С БОЛЬШИМИ ДАННЫМИ ПРИ ОБНАРУЖЕНИИ ДЕЛ ПО ОТМЫВАНИЮ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 103-116, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1222>. Дата доступа: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.09.

***Благодарности.** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-00088.*

Kirill V. Plaksiy[1], Andrey A. Nikiforov[2], Natalia G. Miloslavskaya[3]
National Research Nuclear University MEPhI,
Kashirskoe shosse, 31 Moscow, 115409, Russia
[1]*e-mail: kirillplaksiy@mail.ru, http://orcid.org/0000-0002-8949-6772*
[2]*e-mail: andreinikiforov993@gmail.com, http://orcid.org/0000-0002-2726-0000*
[3]*e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805*

Investigation of graph databases suitable for work with big data while detecting money laundering and terrorism financing cases*

DOI: http://dx.doi.org/10.26583/bit.2019.3.09

Abstract. This paper discusses the currently popular graph database management systems (DBMSs) working with Big Data and can be used to store information obtained while dealing with money laundering and terrorist financing criminal (ML/FT) cases. The aim of this study is to choose a secure graph DBMS suitable for working with Big Data for such financial investigations. The authors consider the existing graph DBMSs, analyze and compare them with each other with special emphasis on the information security protection methods of stored data. The advantages and disadvantages of software products are studied and a comparison with the help of selected parameters characterizing system's ability to keep information secure is made. The results of the comparison are followed by detailed comments. On its basis the most convenient, flexible and up-to-date DBMS was chosen for usage while searching ML/FT cases. It was found that graph DBMSs are suitable for Big data tasks and as a final result JanusGraph was selected as a foreground DBMS in this project according to selected parameters.
Keywords: money laundering, terrorism financing, ML/FT, information security, typology, Big Data, Database Management System (DBMS).
For citation: PLAKSIY, Kirill V.; NIKIFOROV, Andrey A.; MILOSLAVSKAYA, Natalia G. Investigation of graph databases suitable for work with big data while detecting money laundering and terrorism financing cases. IT Security (Russia), [S.l.], v. 26, n. 3, p. 103-116, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1222>. Date accessed: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.09.

***Acknowledgement.** The research was carried out under the financial support of the RFBR in the framework of scientific project No. 18-07-00088.*

Введение

С каждым годом количество производимых человеком и техникой данных резко возрастает. Сначала таблицы и графы насчитывали в себе сотни или тысячи значений и вершин и для их хранения использовались обычные базы данных (БД). С развитием технологий и возрастанием объёмов получаемых сведений появился термин «Большие данные» (англ. Big Data), что дало толчок развитию новых средств сбора, обработки и хранения информации. Это подвело учёных к необходимости пересмотра существующих хранилищ с целью создания современных систем управления БД, способных отвечать актуальным запросам бизнеса и разносторонних исследований. При этом от простых числовых значений разработчики пришли к увеличению множества типов данных, которые могут храниться в таких БД. Так, из-за нехватки памяти для уменьшения избыточности данных и сохранения их целостности появилась реляционная СУБД [1], основанная на теории нормализации.

Интерес научного сообщества к подобным технологиям огромен. В последнее десятилетие было разработано множество инструментов для обработки больших объемов информации, условно разделяемых на структурированные (длина и формат данных четко определены, обычно хранятся в реляционных СУБД), неструктурированные (данные без определенного формата, сохраняются в том виде, в котором они были собраны) и полуструктурированные данные (данные, которые не ограничиваются определенными полями, но имеют маркеры для разделения информации, например, как в стандарте JSON (JavaScript Object Notation) [2]).

Различные типы данных могут храниться в разных форматах. Использование универсального хранилища со множеством форматов требуется в случаях, когда речь идет о больших объемах крайне изменчивой информации, например, в социальных сетях.

Способность графовых СУБД связывать информацию определяет их применимость для задач информационной безопасности (ИБ), например, для обнаружения мошенничества, управления процессом аутентификации, управления угрозами ИБ и т.д. Специалист с развитым умением понимать структуру и анализировать содержание

подобных БД получает большие возможности для исследования, так как эти СУБД наглядно демонстрируют ошибки в защите и взаимосвязи объектов, которые могут в дальнейшем повлиять на другие смежные системы в организации.

Графовые СУБД активно используются в финансовых организациях как для поддержки и контроля бизнес-процессов, так и для обеспечения их ИБ [3]. Развитая инфраструктура вкупе с созданными под конкретные задачи хранилищами повышает успех обнаружения инцидентов ИБ и уменьшает время успешного реагирования на них. Но злоумышленники могут применить координально новый подход к преступлению или модернизируют его схему. Тогда необходимо заранее иметь комплекс превентивных мер и средств защиты от него.

Финансовые преступления, а точнее, результаты их анализа и каталогизации можно отнести к большим данным, так как они характеризуются их тремя базовыми свойствами: volume – большим объёмом данных, velocity – обработкой информации с большой скоростью, variety – многообразием и неструктурированностью данных. При рассмотрении больших схем преступлений с сотней участников (физлиц, финансовых учреждений, индивидуальных предпринимателей) у всех будут свои идентификационные данные, различные логические связи, множество проведенных денежных операций и т.п. При этом возможны модифицированные и комбинированные схемы преступлений.

Данная статья продолжает работы, посвященные использованию графов в расследованиях финансовых преступлений, а именно генерации вариантов типологий (наиболее распространенных схем) для последующего их использования в поиске схем отмывания денег, полученных преступным путем, и финансирования терроризма (ОД/ФТ) [4]. Ее актуальность обусловлена необходимостью обоснованного выбора защищенных графовых СУБД, подходящих для этих целей и работы с большими данными финансовых расследований. Для этого решаются следующие задачи: рассматриваются имеющиеся графовые СУБД, проводится их анализ и сравнение друг с другом с особым акцентом на методы защиты, используемые для обеспечения безопасности хранимых данных. Для достижения поставленной цели статья структурирована следующим образом: сначала кратко проанализированы работы в данной области, далее выделены распространенные методы защиты данных в СУБД, представлены наиболее известные графовые хранилища, приведено сравнение и выбор подходящей СУБД.

1. Работы в данной области

В ходе исследования были рассмотрены различные графовые хранилища данных, которые могут быть применены к делам ОД/ФТ. Графы как средство визуализации используются для работы с данными [5], что упрощает восприятие человеком информации и уменьшает её объемы за счет различных подходов, учитывающих специфику решаемой задачи. Для выполнения всевозможных операций над данными графы начали применяться и в программировании, что было описано еще в начале XXI века [6].

В сфере противодействия ОД/ФТ (ПОД/ФТ) графы также используются, позволяя избавиться от незначимых в рамках решаемых задач данных и оставляя только необходимую для анализа информацию [7]. Поскольку данные о транзакциях и различных операциях давно превзошли пределы обычных данных, то для ПОД/ФТ стали применяться инструменты больших данных, например, система SAS Anti-Money Laundering (SAS AML), специально созданная для банковских систем, отслеживания операций банка, консолидации информации и выявления подозрительных действий [8].

В графовых СУБД информация хранится в виде узлов или объектов, а отношения между ними позволяют получать дополнительную информацию, имеющую большую ценность. Несмотря на то, что эта технология является относительно новой, наиболее значимые результаты получаются с 2013 года, и уже существуют СУБД, которые работают в реальных системах. Для хранения новых данных и работы с ними используются, например, платформы Neo4j [9], DataStax Enterprise Graph [10], AllegroGraph, ArangoDB и другие.

Про графовые СУБД доступно много публикаций разных авторов. Например, в [11] обосновывается актуальность и необходимость использования графовых БД, а также сравниваются популярные в 2018 году решения. В [12] описаны цели и способы проектирования и реализации графовых баз, а также показаны не совсем стандартные случаи применения. В [13] приводится небольшой раздел по графовым базам и их сравнение между собой. В [14] показаны возможности построения новой платформы для моделирования с целью отображения уязвимостей в сетях. Эти и другие публикации были положены в основу данного исследования.

2. Распространённые методы защиты данных в СУБД

С ростом потребностей в операциях с информацией возрастала необходимость в средствах обеспечения ИБ этой информации в БД. Средства защиты в различных СУБД несколько отличаются, однако общим является многоуровневость защиты – чем больше барьеров-уровней, тем сложнее будет их преодолеть злоумышленнику. На нижних уровнях находятся стандартные способы защиты: пароли, шифрование данных, разграничение прав доступа к объектам БД, контрольные следы выполняемых операций, резервное копирование.

Перечисленные способы являются частью более общей классификации уровней безопасности. Согласно «Критериям определения безопасности компьютерных систем» [15] определяются четыре класса безопасности (Security Classes): D, C, B и A. Класс D обеспечивает минимальную защиту (Minimal Protection), класс C – дискреционную (Discretionary), класс B – мандатную (Mandatory), а класс A – верифицируемую (Verified).

Дискреционное управление доступом осуществляется по усмотрению владельца данных и делится на 2 подкласса – C1 и C2, где подкласс C1 является менее безопасным, чем подкласс C2. Требованием класса C1 является разделение данных и пользователя, помимо взаимного доступа к данным возможно их раздельное использование пользователями. Класс C2 предусматривает дополнительный учет на основе входа в систему, аудита и изоляции ресурсов. Дискреционное управление доступом поддерживается многими СУБД и базируется на идентификации пользователей, объектах БД (таблицах, представлениях, доменах, определенных пользователем наборе символов, хранимых процедурах и т.д.) и привилегиях – наборе действий над тем или иным объектом.

При мандатном управлении доступом объектам данных присваиваются определенные классификационные уровни, образующие строгий иерархический порядок (например, «секретно», «совершенно секретно», «для служебного пользования» и т.д.), а каждый пользователь имеет соответствующий уровень допуска. Защита класса B делится на три подкласса – B1, B2 и B3, где подкласс B1 наименее безопасен, а B3 является наиболее безопасным подклассом. В соответствии с требованиями класса B1 каждый объект данных содержит отметку о его уровне классификации, а также неформальное сообщение о действующей политике безопасности. Согласно требованиям класса B2 дополнительно требуется формальное утверждение о действующей политике

безопасности. Кроме того, необходимо решить вопрос о защищённых каналах передачи информации. Наконец, класс B3 помимо прочего требует поддержки аудита, восстановления данных и назначения администратора режима безопасности.

Верифицируемая защита класса A является наиболее безопасной, но требует математического доказательства соответствия метода обеспечения безопасности заданной политике.

Шифрование данных. Существуют два режима работы с зашифрованными БД. Первый заключается в расшифровании необходимого файла или части файла на внешнем носителе. После выполнения необходимых действий с открытой информацией она вновь зашифровывается на внешнем запоминающем устройстве. Независимое последовательное функционирование средств шифрования и СУБД является несомненным достоинством такого режима. Однако в результате сбоя или отказа часть БД может остаться записанной в незашифрованном виде. Расшифрование также может проводиться в оперативной памяти непосредственно перед выполнением необходимых действий с данными. Процедуры шифрования часто встроены в СУБД. Необходимо отметить, что несмотря на достаточно высокий уровень защиты от несанкционированного доступа, снижается уровень производительности СУБД в связи с ее усложнением.

Защита полей. Поскольку в большинстве случаев изменение информации в СУБД является следствием человеческих действий, целесообразно применять защиту полей и записей в таблицах и формах. Защита данных в полях таблиц подразумевает следующие уровни прав доступа: полный запрет доступа, только чтение и разрешение всех операций (просмотр, ввод, удаление и изменение). Некоторые поля готовых таблиц могут быть скрыты для ряда пользователей. Для экранных форм готовых приложений обычно запрещают вызов конструктора, чтобы конечный пользователь случайно не изменил приложение. В самих экранных формах отдельные элементы также могут быть защищены.

Контрольный след выполняемых операций позволяет регистрировать детальные сведения обо всех операциях пользователей с БД. Такая сохраненная информация играет существенную роль в обнаружении несанкционированного вмешательства в БД, выявлении уязвимостей в системе защиты и устранении каких-либо внесенных искажений данных.

Резервное копирование позволяет восстанавливать данные на случай аппаратных или программных сбоев.

Также существуют средства защиты, присущие какой-то одной конкретной БД, что делает её функционал уникальным, например, как это сделано в тройных атрибутах в семантической графовой БД AllegroGraph [16]. Это позволяет сделать данные прозрачными для пользователей на основе ролей. Они обеспечивают возможность связывания графовых СУБД с защитой доступа к данным. Пока тройка атрибутов задействована в установленной уже связи, их не получится изменить без изменения самой связи.

3. Современные графовые хранилища

В настоящее время существуют десятки графовых СУБД, из которых наиболее известными сейчас являются AllegroGraph (мультитиповая), ArangoDB, FlockDB, Giraph, HyperGraphDB, InfiniteGraph, InfoGrid, Neo4j, OrientDB, SparkSee (ранее DEX), Sqrrl, Titan, Datomic, JanusGraph. По данным [17] на август 2019 года среди именно графовых СУБД лидирующие позиции занимает Neo4j, 6 место – JanusGraph, 8 и 9 делят Dgraph и Giraph, соответственно, на 11 располагается TigerGraph, 13 – AllegroGraph, на 17 – InfiniteGraph, 19 место отдано FlockDB, 21 – InfoGrid, 23 – HyperGraphDB, с 25 по 28 занимают Sparksee,

TinkerGraph, GraphBase, HGraphDB, а общий рейтинг на 30–32 местах замыкают Memgraph, DataChemist и FlureeDB.

Neo4j [18] представляет из себя свободно распространяемую графовую СУБД с открытым исходным кодом. Разработчиком является одноимённая компания, которая начала работу над проектом в 2003 г., а в 2007 году представила первую готовую версию. На сегодняшний день последней версией продукта является 3.5.4 от апреля 2019 года Основными языками реализации являются Java и Scala.

JanusGraph [19] – масштабируемая графовая БД, оптимизированная для их хранения и обработки, причем графы могут содержать сотни миллионов вершин и ребер, распределенных по кластеру из нескольких машин. Реализовано удобное взаимодействие с другими СУБД (Apache Cassandra, Apache HBase, Google Cloud Bigtable, Oracle BerkeleyDB). Масштабируемость зависит от технологий, которые используются вместе с СУБД. Например, используя Apache Cassandra в качестве хранилища, масштабируемость до нескольких центров обработки данных предоставляется «из коробки».

Dgraph [20] – свободная, масштабируемая, распределённая графоориентированная СУБД. Она развивается с учетом обеспечения минимальных задержек выполнения запросов, что позволяет использовать её для обработки информации в режиме реального времени. Архитектура поддерживает создание распределённых конфигураций из нескольких экземпляров Dgraph, давая возможность масштабировать хранилища путём добавления дополнительных узлов при росте нагрузки или увеличении размера данных.

TigerGraph [21] представляет собой одну из графических СУБД нового типа: это первая система, способная выполнять анализ данных в режиме реального времени в масштабе веб-сети. Дизайн Native Parallel Graph (NPG) ориентирован как на хранение, так и на вычисления, поддерживает обновление графиков в реальном времени и предлагает встроенные параллельные вычисления. Язык запросов SQL-подобных графов (GSQL) обеспечивает специальное исследование и интерактивный анализ больших данных. Благодаря возможностям GSQL и скорости NPG пользователь может выполнять аналитику Deep Link: обнаруживать соединения, слишком громоздкие в плане обработки информации.

AllegroGraph [22] – высокопроизводительная графическая (мульти) СУБД с закрытым исходным кодом. AllegroGraph совмещает эффективное использование оперативной памяти с использованием дисковых хранилищ. Поддерживает языки запросов к данным SPARQL, RDFS++ и Prolog и автоматически использует те из них, которые совместимы с приложениями пользователя. В настоящее время используется в проектах с открытым исходным кодом, в коммерческих проектах и проектах Министерства обороны США. Является компонентой хранения данных в проекте TwitLogic, реализующем концепцию Семантической паутины в системе обработки данных социальной сети Twitter.

Все приведенные СУБД имеют большой потенциал для работы с большими данными, обладают нужным функционалом и наполнением. Ниже представлена сравнительная таблица (табл. 1), в которой акцент был сделан на методах защиты, реализованных в выбранных СУБД. Критерии для сравнения были выбраны с учетом того, что СУБД должна иметь механизмы защиты данных, которые не затрудняли бы работу с самой СУБД в условиях проводимого исследования. Чем более гибко реализована возможность настройки защиты, тем лучше.

Таблица 1. Сравнение популярных графовых СУБД

	Neo4j	**JanusGraph**	**Dgraph**	**TigerGraph**	**AllegroGraph**
Распространение	Открытый исходный код	Открытый исходный код	Открытый исходный код	Коммерческая лицензия	Коммерческая лицензия
Языки реализации	Java, Scala	Java	Go	C++	Java, Python, Common Lisp
Серверные операционные системы	Linux, OS X, Solaris, Windows Может использоваться и без сервера в качестве встроенной базы данных Java	Linux, OS X, Unix, Windows	Linux, OS X, Windows	Linux	Linux, OS X, Windows
Контроль доступа	Присутствует	Осуществляется через Rexter Graph Server	Нет (запланировано на будущие версии)	Ролевая система управления доступом	Ролевая система управления доступом
Аутентификация	Подключаемая аутентификация с поддерживаемыми стандартами (LDAP, Active Directory, Kerberos)	Базовая и токен-аутентификация	Нет (запланировано на будущие версии)	Аутентификация GSQL и REST ++, токены	Базовая аутентификация с настройкой дополнительных фильтров
Шифрование	Целенаправленного внутреннего шифрования нет, поддержка стороннего шифрования	Целенаправленного внутреннего шифрования нет, поддержка стороннего шифрования	Шифрование данных в состоянии покоя HDFS	Запатентованная схема шифрования + поддержка стандартных методов шифрования	FIPS 140-2 шифрование для передачи данных
Целостность данных	Использование ограничений	Контроль целостности данных при загрузке	Использование двойных баз	Пока не реализовано	Запись всех процессов в журналы
Резервные копии	Да, как для одной машины, так и для кластеров	Собственные копии, а также поддержка сторонних средств	Копии работающих кластеров	Интегрированный инструмент для резервного копирования и восстановления данных и словаря данных одного узла	Поддержка создания копий онлайн

Помимо представленной таблицы 1 для выбора хранилища информации в исследовании интерес представляют те преимущества и недостатки (табл. 2), которые могут быть важны для хранения сгенерированных графовых данных типологий финансовых преступлений.

Таблица 2. Достоинства и недостатки популярных графовых СУБД

Название	Достоинства	Недостатки
Neo4j	• Простой язык запросов и может предоставлять наглядный результат, что удобно в решении аналитических задач; • гибкая структура данных, что позволяет вносить изменения в случае изменения требований; • можно сразу создавать модели, которые приближены к реальным условиям без низкоуровневых деталей; • высокая производительность при использовании специфических моделей данных и легкость работы с ними	• Места на диске уходит больше по сравнению с реляционными СУБД; • простые запросы до определенного уровня имеют более низкую эффективность выполнения (производительность) нежели в реляционных базах
JanusGraph	• Поддержка очень больших графов, которые масштабируются в зависимости от количества машин в кластере; • поддержка большого числа параллельных транзакций. Транзакционная емкость масштабируется в зависимости от количества машин в кластере и отвечает на сложные запросы обхода на огромных графах за миллисекунды; • поддержка глобальной аналитики графов и пакетной обработки графов через платформу Hadoop; • поддержка полнотекстового поиска для вершин и ребер на очень больших графах; • многочисленные конфигурации на уровне графов для улучшения производительности; • оптимизированное представление диска, что позволяет эффективно использовать хранилище и скорость доступа; • отдельные преимущества при использовании СУБД вместе с конкретными инструментами, например, с Cassandra или с HBase	• Трудно сделать ручное управление транзакциями; • понижение производительности при добавлении вершин при наличии большого количества уже существующих
Dgraph	• Разбиение данных горизонтально на сотни серверов, что предназначено для минимизации количества обращений к диску и сетевых вызовов; • высокая скорость работы. Dgraph построена как поисковая система – запросы разбиваются на подзапросы, которые запускаются одновременно для достижения низкой задержки и высокой пропускной способности; • соответствие требованиям ACID (Atomicity, Consistency, Isolation, Durability) – нет необходимости беспокоиться о целостности данных; • автоматический запуск синхронной репликации, поэтому потеря жесткого диска или сервера не влияет на сервисы; • равномерная сбалансированность данных по серверам путем автоматического размещения и улучшения использования ресурсов для высокой производительности; • пользовательский интерфейс для легкого просмотра и управления данными; • эффективное использование аппаратных средств хранения. Внутреннее хранилище ключей Dgraph, Badger, предназначено для уменьшения использования ОЗУ. Оптимизация на SSD (solid-state drive) повышает производительность.	• Сложность выполнения больших аналитических запросов; • большое значение имеет задание связей между узлами графа, что влияет на эффективность поиска; • кластер состоит из разных компонентов (zero, server и ratel), и каждый компонент предназначен для своей цели, что без должного внимания и определения функций компонентов снижается эффективность работы

Название	Достоинства	Недостатки
TigerGraph	• Быстрая загрузка данных для быстрого построения графов; • ускоренное выполнение алгоритмов параллельных графов; • возможность унифицировать аналитику в реальном времени с крупномасштабной автономной обработкой данных; • возможность масштабирования для распределенных приложений; • возможность прохождения огромного количества вершин/ребер в секунду и загрузки от 50 до 150 ГБ данных в час (на машину)	• При наличии низкоуровневых ошибок возможна каскадная реакция, что затрудняет поиск неправильных фрагментов графа или зависимости; • выбор систем на серверах и используемые языки жёстко ограничены небольшим набором
AllegroGraph	• Можно смешивать геопространственную, временную, социальную сетевую аналитику и анализ, все в одном запросе (SPARQL или Prolog); • трехуровневая безопасность с фильтрами; • резервное копирование в онлайн-хранилище, восстановление на момент времени, репликация	• Занятые тройные атрибуты могут привести к усложнению логики запросов из-за их текущего задействования в работе СУБД

4. Сравнение СУБД и обсуждение результатов

На основе данных из открытых источников, выявленных выше особенностях СУБД и с учётом приоритетов проводимого исследования осуществлялся выбор графовой СУБД. Для удобства сравнения СУБД по обеспечению ИБ ниже по каждой из строк таблицы даны комментарии и выделены приоритетные решения.

Аутентификация и контроль доступа.

Ядро модели безопасности Neo4j сосредоточено вокруг ряда предопределенных ролей доступа к данным на глобальном уровне. Каждая роль включает в себя набор действий, разрешенных для графа данных. Neo4j предоставляет собственного поставщика аутентификации, который локально хранит информацию о пользователях и ролях на диске. Другой способ управления аутентификацией и авторизацией – через внешнее ПО, такое как Active Directory или OpenLDAP, доступ к которому осуществляется через встроенный соединитель LDAP. В СУБД предоставляется опция плагина для создания пользовательских интеграций. В дополнение к LDAP (Lightweight Directory Access Protocol), собственным и пользовательским решениям, для аутентификации и единого входа Neo4j поддерживает Kerberos. Поддержка Kerberos обеспечивается с помощью дополнения Neo4j Kerberos.

JanusGraph поддерживает соединения, которые используют HTTP-запросы или через WebSockets. Все соединения выполняются по HTTPS (HyperText Transfer Protocol Secure) и требуют аутентификации. HTTP-запросы поддерживают базовую и токен-аутентификацию. Для чего-либо, кроме разового вызова, использование WebSockets или аутентификации по токенам приводит к повышению производительности. Обычная аутентификация для СУБД, когда имя пользователя и пароль отправляются вместе с запросом, – это дорогостоящий по ресурсам процесс.

При первой инсталляции TigerGraph аутентификация пользователя отключена. В процессе установки создается суперпользователь gsql, у которого есть профиль с именем и паролем. Пока пароль пользователя tigergraph равен tigergraph, аутентификация gsql остается отключенной. Это разработано для удобства пользователя в однопользовательских конфигурациях или установках типа демонстрационных и обучающих примеров, не требующих защиты.

В AllegroGraph реализована ролевая система управления доступом с поддержкой различных фильтров безопасности, что позволяет установить гибкие ограничения и минимизировать потери производительности.

Рассмотрев аутентификацию и контроль доступа в данных СУБД, а также принимая во внимание приоритетность выполнения запросов перед их скоростью, как оптимальное решение выбираем JanusGraph.

Шифрование.

Хотя в настоящее время Neo4j не занимается явным шифрованием данных, для сценариев, где требуется дополнительная безопасность, распространены два подхода: шифрование файловой системы, в которой находится БД, и шифрование самих данных из приложения. Шифрование файловой системы – это простой, полезный шаг, который приводит к усилению защиты данных на диске. Однако одного такого шифрования недостаточно для полной защиты данных. Это связано с тем, что Neo4j использует архитектуру на основе REST (Representational State Transfer), которая отвечает на операторы Cypher, отправленные в виде вызовов веб-службы, ответы на эти вызовы (то есть данные) передаются по Сети в виде открытого текста. Хотя следующим логическим шагом является использование HTTPS для шифрования сетевого взаимодействия, некоторые приложения требуют дополнительной защиты, такой как ограничение доступа к данным только тем, кто авторизован для работы с ними. С этого начинается шифрование на уровне приложений – процесс, при котором приложение динамически изменяет данные во время выполнения, выполняя шифрование и расшифрование данных до и после записи или чтения данных из БД. Многие широко признанные отраслевые стандарты безопасности, например, такие как HIPPA (Health Insurance Portability and Accountability Act) и FERPA (Family Educational Rights and Privacy Act) для областей здравоохранения и образования, могут быть реализованы с помощью защиты на уровне приложений. В случае приложений на основе Java библиотека Neo4j Object Graph Mapping (OGM) может использоваться для реализации безопасности на уровне приложений. Поскольку Neo4j может сохранять данные в формате, отличном от формата коренной модели (например, сохранение даты в виде Long или String), OGM предлагает концепцию конвертации атрибутов. Создание пользовательской реализации подобных преобразований является хорошей отправной точкой для шифрования на уровне приложений.

Достоинство – простой в применении подход приводит к детальному шифрованию, которое обеспечивает безопасность данных как на диске, так и во время передачи по Сети на сервер Neo4j и от него. Конкретный используемый процесс шифрования данных может быть полностью адаптирован в соответствии с конкретными потребностями.

Недостаток – дополнительная защита не улучшает производительности системы. Сам процесс шифрования данных влечет за собой вычислительные затраты с точки зрения памяти и вычислительной мощности. Тот факт, что данные передаются в своем зашифрованном формате (который обычно намного больше, чем его открытый текст), отрицательно скажется на использовании Сети. По самой природе зашифрованные данные становятся более трудными для работы за пределами приложения, и функции БД, такие как индексы, поиск и случайные запросы Cypher, становятся нежизнеспособными. Наконец, существующие данные необходимо преобразовать в желаемый зашифрованный формат, чтобы они совпадали с требуемым форматом, поэтому следует позаботиться о том, чтобы приложение могло успешно работать как с зашифрованными, так и с незашифрованными значениями.

У JanusGraph шифрование отдано на реализацию тому продукту, с которым осуществляется взаимодействие, а таких достаточно много. Можно найти компромисс между оперативностью выполнения запросов и шифрованием.

В Dgraph предусмотрена функция шифрования данных в состоянии покоя HDFS (Hadoop Distributed File System), которая, если она включена, позволяет хранить данные в зашифрованных каталогах HDFS, называемых зонами шифрования. Все файлы в зоне шифрования прозрачно шифруются и расшифровываются на стороне клиента. Следовательно, расшифрованные данные никогда не хранятся в HDFS.

TigerGraph использует запатентованную схему шифрования, которая сжимает и скрывает данные, если пользователь не знает схему шифрования/расшифрования. Кроме того, система TigerGraph поддерживает интеграцию со стандартными методами шифрования данных при хранении на диске. Шифрование данных в состоянии покоя может применяться по-разному на усмотрение пользователя. Также это осуществимо в режиме ядра. Для запуска в режиме ядра требуется разрешение суперпользователя. Шифрование файловой системы использует передовые алгоритмы шифрования, например AES. Шифрование обычно связано с процессором, а не с вводом/выводом. Если загрузка процессора ниже 100%, тесты TigerGraph не показывают существенного снижения производительности.

Поскольку AllegroGraph широко используется в силовых структурах США, в ней интегрировано шифрование с использованием FIPS 140-2. Этот стандарт не распространен в России, к тому же в последнее время он подвергается критике. Целесообразно будет дождаться окончательной оценки экспертов по этому вопросу.

Проанализировав возможности СУБД по шифрованию и оценив их потенциал, сделали вывод, что приоритетными вариантами по данному параметру в условиях большого проекта являются JanusGraph и Neo4j.

Целостность данных.

Neo4j помогает обеспечить целостность данных с использованием ограничений, применяемых к узлам или отношениям. Могут быть созданы уникальные ограничения свойств узлов, а также ограничения существования свойств узлов и свойств отношений. Также могут быть реализованы ключи узлов, которые гарантируют как существование, так и уникальность. Ограничения уникальных свойств гарантируют, что значения свойств являются уникальными для всех узлов с определенной меткой. Уникальные ограничения не означают, что все узлы должны иметь уникальное значение для свойств – узлы без свойства не подчиняются этому правилу. Ограничения существования свойства гарантируют, что свойство существует для всех узлов с определенной меткой или для всех отношений с определенным типом. Все запросы, которые пытаются создать новые узлы или отношения без свойства, или запросы, которые пытаются удалить обязательное свойство, теперь не будут выполнены. Ключи узла гарантируют, что для данной метки и набора свойств все свойства существуют на всех узлах с этой меткой и сочетание значений свойств является уникальным.

Как и в предыдущем случае, в JanusGraph целостность данных контролируется дополнительными продуктами. В самой же СУБД осуществляется контроль целостности данных при загрузке.

В Dgraph хранилища данных графа представляются как слой графа над какой-либо другой БД SQL/NoSQL для управления данными. Эта другая БД отвечает за резервное копирование, моментальные снимки, сбои сервера и целостность данных.

AllegroGraph поддерживает целостность данных с помощью журналирования на момент их появления в общем реестре, а также в ходе их изменения. Целостность во

время выполнения процессов обеспечивается сторонними модулями, что позволяет иметь разные журналы и различные точки зрения в случае возникновения инцидентов.

По параметру обеспечения целостности в рамках проекта интересными считаются JanusGraph и AllegroGraph ввиду гибкости настройки контроля целостности и взаимодействия с другими программными продуктами.

Резервное копирование.

Почти все СУБД имеют похожие по принципу действия инструменты для создания резервных копий. Возможны копии как одной машины, так и кластера. У некоторых осуществимо копирование в режиме онлайн. Отдельного упоминания стоит инструмент, разработанный целенаправленно для одной из рассмотренных баз.

GBAR (Graph Backup and Restore) – это интегрированный инструмент для резервного копирования и восстановления данных и словаря данных (схемы, загрузки заданий и запросов) одного узла TigerGraph. В режиме резервного копирования он упаковывает данные TigerGraph и информацию о конфигурации в один файл на диск или в удаленную корзину AWS S3. Несколько файлов резервных копий могут быть заархивированы. Позже можно использовать режим восстановления для отката системы на любую точку резервного копирования. Этот инструмент также можно легко интегрировать с Linux Cron для выполнения периодических заданий резервного копирования.

По параметру резервного копирования нельзя однозначно выделить лидера, так как данная функция является одной из жизненно важных для СУБД. Поэтому в данном разделе выбор любой из СУБД будет хорошим вариантом.

В результате проведенного исследования для выполнения поставленной задачи хранения данных финансовых преступлений (сгенерированных на основе типологий объектов и логических связей между ними) была выбрана JanusGraph из-за её преимуществ перед другими СУБД. Среди ее достоинств были выделены масштабируемая обработка графовых данных и выполнение аналитических запросов в реальном времени, которая пригодится при сравнении реальных операций со сгенерированными, обработка графов через платформу Hadoop (данная платформа является самой популярной для работы с большими данными), полнотекстовый поиск для вершин и ребер на очень больших графах, взаимодействие с различными популярными инструментами больших данных и работа под основными операционными системами и с самыми популярными языками программирования.

Заключение

В работе проведено исследование некоторых наиболее популярных графовых СУБД с целью выбора реализации, наиболее подходящей для решения задач ПОД/ФТ. По полученным результатам было установлено, что графовые СУБД подходят для задач работы с большими данными, а также была выбрана одна из рассмотренных СУБД, а именно Janus Graph по выше перечисленным параметрам.

В будущем планируется заполнение выбранной СУБД сгенерированными данными финансовых преступлений, их проверка на реалистичность, анализ прошедших отбор для повышения эффективности поиска финансовых нарушений, а также выявление новых преступных схем ОД/ФТ.

СПИСОК ЛИТЕРАТУРЫ:

1. National Research Council et al. Funding a revolution: Government support for computing research. National Academies Press, 1999.
2. Understanding JSON Schema. URL: https://json-schema.org/understanding-json-schema/reference/type.html (дата обращения: 12.08.2019).
3. Eifrem E. Why Graph Database Could Be Key to Addressing Financial Services Challenges. URL: https://financialit.net/blog/financial-services/why-graph-database-could-be-key-addressing-financial-services-challenges (дата обращения: 15.08.2019).
4. Plaksiy K., Nikiforov A., Miloslavskaya N. Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism. Proceedings of 2018 6th International Conference on Future Internet of Things and Cloud (FiCloud2018). Barcelona (Spain), 6-8 August 2018. P. 70–77. DOI 10.1109/W-FiCloud.2018.00017.
5. Харари Ф. Теория графов. – М.: Мир, 1973. – 296 с.
6. Касьянов В.Н. Визуализация информации на основе графовых моделей. Научная визуализация. В.Н. Касьянов, Е.В. Касьянова. – М.: Наука, 2014, Т.6. № 1. С. 31–50.
7. Drezewski R., Sepielak J., Filipkowski W. The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection. In Digital Investigation June 2012 9(1). P. 8–21. Elsevier Ltd.
8. SAS Anti-Money Laundering (SAS AML). URL:http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:SAS_Anti-Money_Laundering_(SAS_AML) (дата обращения: 14.08.2019).
9. Neo4j – Platform for connected data. URL: https://neo4j.com/ (дата обращения: 02.08.2019).
10. DataStax Enterprise Graph Super-powering your data relationships. URL: https://www.datastax.com/products/datastax-enterprise-graph/ (дата обращения: 03.08.2019).
11. Fernandes D., Bernardino J. Graph Databases Comparison: AllegroGraph, ArangoDB, InfiniteGraph, Neo4J, and OrientDB. DATA. 2018. P. 373–380.
12. Robinson I., Webber J., Eifrem E. Graph databases. O'Reilly Media. 2013.
13. Tabacchi M. E. et al. Designing Cognitive Cities. Designing Cognitive Cities. Springer, Cham, 2019. P. 3–27.
14. Noel S. et al. Big-data architecture for cyber attack graphs representing security relationships in nosql graph databases. 2015.
15. Qiu L. et al. Trusted computer system evaluation criteria. National Computer Security Center. 1985.
16. AllegroGraph 6.6.0 Triple Attributes. URL: https://franz.com/agraph/support/documentation/current/triple-attributes.html (дата обращения: 02.08.2019).
17. DB-Engines Ranking of Graph DBMS. URL: https://db-engines.com/en/ranking/graph+dbms (дата обращения: 22.08.2019).
18. Габриелян Г.А. Графовая база данных NEO4J для проектирования высоконагруженных систем. Студенческий электрон. научн. журн. 2018. № 11(31). URL: https://sibac.info/journal/student/31/111409. (дата обращения: 12.08.2019).
19. JanusGraph. URL: https://janusgraph.org/ (дата обращения: 18.08.2019).
20. Dgraph. URL: https://dgraph.io/ (дата обращения: 22.08.2019).
21. TigerGraph. URL: https://www.tigergraph.com/ (дата обращения: 27.08.2019).
22. AllegroGraph. URL: https://franz.com/agraph/allegrograph/ (дата обращения: 27.08.2019).

REFERENCES:

[1] National Research Council et al. Funding a revolution: Government support for computing research. National Academies Press, 1999.
[2] Understanding JSON Schema. URL: https://json-schema.org/understanding-json-schema/reference/type.html (accessed: 12.08.2019).
[3] Eifrem E. Why Graph Database Could Be Key to Addressing Financial Services Challenges URL: https://financialit.net/blog/financial-services/why-graph-database-could-be-key-addressing-financial-services-challenges (accessed: 15.08.2019).
[4] Plaksiy K., Nikiforov A., Miloslavskaya N. Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism. Proceedings of 2018 6th International Conference on Future Internet of Things and Cloud (FiCloud2018). Barcelona (Spain), 6-8 August 2018. P. 70–77. DOI 10.1109/W-FiCloud.2018.00017
[5] Harari F. Graph Theory. – M.: Mir, 1973. – 296 s. (in Russian).
[6] Kasyanov, V.N., Information visualization based on graph models. Scientific visualization. V.N. Kasyanov, E.V. Kasyanova. M.: Nauka, 2014. V. 6. n. 1. P. 31–50 (in Russian).

[7] Drezewski R.; Sepielak J.; Filipkowski W. The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection. In Digital Investigation June 2012 9(1). P. 8–21. Elsevier Ltd.
[8] SAS Anti-Money Laundering (SAS AML). URL:http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:SAS_Anti-Money_Laundering_ (SAS_AML) (accessed: 14.08.2019).
[9] Neo4j – Platform for connected data. URL: https://neo4j.com (accessed: 02.08.2019).
[10] DataStax Enterprise Graph Super-powering your data relationships. URL: https://www.datastax.com/products/datastax-enterprise-graph/ (accessed: 03.08.2019).
[11] Fernandes D., Bernardino J. Graph Databases Comparison: AllegroGraph, ArangoDB, InfiniteGraph, Neo4J, and OrientDB. DATA. 2018. P. 373–380.
[12] Robinson I., Webber J., Eifrem E. Graph databases. O'Reilly Media. 2013.
[13] Tabacchi M. E. et al. Designing Cognitive Cities. Designing Cognitive Cities. Springer, Cham, 2019. P. 3–27.
[14] Noel S. et al. Big-data architecture for cyber attack graphs representing security relationships in nosql graph databases. 2015.
[15] Qiu L. et al. Trusted computer system evaluation criteria. National Computer Security Center. 1985.
[16] AllegroGraph 6.6.0 Triple Attributes. URL: https://franz.com/agraph/support/documentation/current/triple-attributes.html. Access date: 02.08.2019.
[17] DB-Engines Ranking of Graph DBMS URL: https://db-engines.com/en/ranking/graph+dbms (accessed: 22.08.2019).
[18] Gabrielyan G.A. GRAPHIC DATABASE NEO4J FOR DESIGN OF HIGH-LOADED SYSTEMS. Student electronic scientific journal. 2018. № 11 (31). URL: https://sibac.info/journal/student/31/111409 (accessed: 08.12.2019) (in Russian).
[19] JanusGraph. URL: https://janusgraph.org/ (accessed: 18.08.2019).
[20] Dgraph. URL: https://dgraph.io/ (accessed: 22.08.2019).
[21] TigerGraph. URL: https://www.tigergraph.com/ (accessed: 27.08.2019).
[22] AllegroGraph. URL: https://franz.com/agraph/allegrograph/ (accessed: 27.08.2019).

Поступила в редакцию – 28 августа 2019 г. Окончательный вариант – 16 сентября 2019 г.
Received – September 28, 2019. The final version – September 16, 2019.

Отзыв статьи (ретракция) «Влияние человеческого фактора на защищенность программных средств учебного назначения»

Статья: **ГУРОВ, Валерий Валентинович. ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ЗАЩИЩЕННОСТЬ ПРОГРАММНЫХ СРЕДСТВ УЧЕБНОГО НАЗНАЧЕНИЯ. Безопасность информационных технологий, [S.l.], v. 23, n. 2, p. 21-32, june 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/75>. Дата доступа: 14 sep. 2019. (доступ свободный)** отозвана (ретрагирована) редакцией журнала в соответствии с правилами отзыва (ретракции) журнала "Безопасность информационных технологий" по заявлению автора.

Автор заявляет: Прошу Вас отозвать из публикации в журнале «Безопасность информационных технологий» мою статью «Влияние человеческого фактора на защищенность программных средств учебного назначения» (The influence of human factor on security of software intended for educational purposes), опубликованную в № 2, 2016 г., страницы 21-32, (https://bit.mephi.ru/index.php/bit/article/view/75) т.к. в статье произошло дублирование материалов из моей диссертации на тему «Разработка методов и средств анализа и обеспечения качества программных систем учебного назначения» (диссертация кандидата технических наук: 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей / Гуров Валерий Валентинович; [Место защиты: Московский государственный инженерно-физический институт]. – Москва, 2008. – 213 с. : ил.). Ссылок на диссертацию в статье по моей оплошности не приведено.

The paper «The influence of human factor on security of software intended for educational purposes» is retracted

The article: **GUROV, Valeriy Valentinovich. The influence of human factor on security of software intended for educational purposes. IT Security (Russia), [S.l.], v. 23, n. 2, p. 21-32, june 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/75>. Date accessed: 14 sep. 2019.** is retracted by the Editorial board in accordance with the rules of retraction of the "IT Security (Russia)" journal (Bezopasnost` Informatsionnykh Tekhnologiy ISSN: 2074-7128 (Print); ISSN: 2074-7136 (On-Line)

Редакция приносит извинения читателям за доставленные неудобства

Отзыв статьи (ретракция) «Статистическое тестирование псевдослучайных последовательностей»

Статья: **КОРЕНЕВА, Алиса Михайловна; ФОМИЧЁВ, Владимир Михайлович. СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. Безопасность информационных технологий, [S.l.], v. 23, n. 2, p. 36-42, june 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/77>. Дата доступа: 14 сентября 2019. (доступ свободный)** отозвана (ретрагирована) редакцией журнала в соответствии с правилами отзыва (ретракции) журнала «Безопасность информационных технологий».

В ходе проверки статьи по материалам экспертизы http://wiki.dissernet.org/wsave/BIT_2016_2_2publ.html выяснилось, что значительную часть статьи составляют некорректные заимствования в значительном объеме из следующего источника: Алиса Дорохова, аналитик компании «Код Безопасности», «Случайности не случайны?» http://savepearlharbor.com/?p=270810 (Опубликовано 21.12.2015).

The paper «Statistical testing of pseudorandom sequences» is retracted

The article: **KORENEVA, Alisa Mikhailovna; FOMICHEV, Vladimir Mikhailovich. Statistical testing of pseudorandom sequences. IT Security (Russia), [S.l.], v. 23, n. 2, p. 36-42, june 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/77>. Date accessed: 14 sep. 2019.** is retracted by the Editorial board in accordance with the rules of retraction of the "IT Security (Russia)" journal (Bezopasnost` Informatsionnykh Tekhnologiy ISSN: 2074-7128 (Print); ISSN: 2074-7136 (On-Line).

Редакция приносит извинения читателям на доставленные неудобства

Отзыв статьи (ретракция) «Обеспечение безопасности функционирования программных систем при проектировании»

Статья: **ТЕРСКОВ, Виталий Анатольевич; ТИМОХОВИЧ, Александр Степанович; ШЕЕНОК, Дмитрий Александрович. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНЫХ СИСТЕМ ПРИ ПРОЕКТИРОВАНИИ. Безопасность информационных технологий, [S.l.], v. 23, n. 2, p. 78-84, june 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/84>. Дата доступа: 14 сентября 2019. (доступ свободный)** отозвана (ретрагирована) редакцией журнала в соответствии с правилами отзыва (ретракции) журнала "Безопасность информационных технологий".

В ходе проверки статьи по материалам экспертизы http://wiki.dissernet.org/wsave/BIT_2016_2_1publ.html выяснилось, что значительную часть статьи составляют некорректные заимствования в значительном объеме из следующего источника: ОПТИМИЗАЦИЯ ПРОГРАММНОЙ АРХИТЕКТУРЫ НА ОСНОВЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА С АЛЛЕЛЯМИ В ШКАЛЕ ПОРЯДКА Шеенок Д.А., Терсков В.А. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2013. № 2. С. 179-188.

The paper «Secutity operation of the software systems on design stage» is retracted

The article: **TERSKOV, Vitaly Anotolevich; TIMOHOVICH, Alexandr Stepanovich; SHEENOK, Dmitry Alexandrovich. Secutity operation of the software systems on design stage. IT Security (Russia), [S.l.], v. 23, n. 2, p. 78-84, june 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/84>. Date accessed: 14 sep. 2019.** is retracted by the Editorial board in accordance with the rules of retraction of the "IT Security (Russia)" journal (Bezopasnost` Informatsionnykh Tekhnologiy ISSN: 2074-7128 (Print); ISSN: 2074-7136 (On-Line).

Редакция приносит извинения читателям за доставленные неудобства

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;

– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы с почтовым адресом, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, ПРОПИСНЫМИ буквами), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив); аннотация (200 – 250 слов, по ширине, строчными буквами – см. **правила формления аннотации**);

– далее повторяются все сведения о статье **на английском языке.**

– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;

– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы, оформленный в соответствии с действующими стандартами (как правило, не менее 15 наименований в научной статье и 50 – в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные автора(авторов) и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации (т.е. латинскими буквами).

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).

Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи**:**

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.

Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения,

важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научых 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.

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 9087.
Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 9087.
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода – 4 раза в год / Periodicity - 4 times a year

Подписка на журнал
производится в почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Технический редактор П.А. Золотухина
Корректор Авдюшкина М.Г.

Подписано в печать 20. 09. 2019 г. Формат 60 x 84 1/8.
Печ. л. 17,5. Уч. - изд. л. 17,5. Тираж 500 экз. Изд. № 002 - 3.

Национальный исследовательский ядерный университет «МИФИ».
Каширское ш., 31, Москва, 115409, Россия.
National Research Nuclear University MEPHI.
Kashirskoe shosse, 31, Moscow, 115409, Russia

Типография ООО «ТИПОГРАФИЯ»
115477, г. Москва, ул. Кантемировская, 60