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.*

АЛЕКСАНДР ВЛАДИМИРОВИЧ СТАРОВОЙТОВ
(к 80-летию со дня рождения)

18 октября исполнилось 80 лет Старовойтову Александру Владимировичу – одному из основателей и бессменному на протяжении более трех десятков лет руководителю редакционных органов нашего журнала.

Александр Владимирович окончил в 1962 г. Пензенский политехнический институт и прошел путь от инженера до генерального директора Пензенского научно-производственного объединения «Кристалл». С 1986 г. проходил военную службу в КГБ СССР, почетный сотрудник госбезопасности. В сложный период возрождения российской государственности создал и организовал плодотворную работу в качестве Генерального директора Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ). Командовал войсками правительственной связи и частями радиоэлектронной разведки, генерал армии.

С февраля 2006 г. возглавляет «Центр информационных технологий и систем органов исполнительной власти» (ФГАНУ ЦИТиС). В 2015 г. Решением ВПК назначен заместителем председателя Совета коллегии ВПК по проблемам обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Старовойтов А.В. в течение продолжительного времени руководил реализацией системных работ по созданию перспективных, отвечающих требованиям информационной безопасности, телекоммуникационных и информационно-телекоммуникационных систем для АСУ военного назначения, систем управления органов государственной власти Российской Федерации, в том числе в качестве Генерального конструктора различных информационно-телекоммуникационных систем спецназначения. В последние годы под руководством Старовойтова А.В. выполнен крупный комплекс работ по автоматизации информационно-аналитической и управленческой деятельности в сфере науки и образования.

Александр Владимирович – автор 170 научных работ, в том числе 5 монографий и 48 изобретений. Старовойтов А.В. награжден орденами и медалями, «Заслуженный деятель науки и техники Российской Федерации», лауреат Государственной премии.

В дни празднования юбилея многоуважаемого Александра Владимировича редакционная коллегия журнала «Безопасность информационных технологий» от имени многочисленной армии авторов, подписчиков и читателей журнала желает ему крепкого здоровья и дальнейших творческих успехов, в том числе в деле воспитания молодого поколения.

СОДЕРЖАНИЕ

CONTENT

Алексей Ю. Нестеренко[1], Александр М. Семенов[2]
Национальный исследовательский университет «Высшая школа экономики»,
Московский институт электроники и математики им. А.Н. Тихонова (МИЭМ НИУ ВШЭ),
ул. Таллинская, 34, Москва, 123458, Россия
[1]e-mail: anesterenko@hse.ru, https://orcid.org/0000-0002-9105-8798
[2]e-mail: amsemenov@hse.ru, https://orcid.org/0000-0003-3251-0534

КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ КОНТРОЛЬНЫХ И ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ*

DOI: http://dx.doi.org/10.26583/bit.2020.4.01

Аннотация. В работе описываются ключевые особенности криптографического протокола, обеспечивающего защищенное взаимодействие контрольных и измерительных устройств. Описывается иерархическая структура, лежащая в основе данного протокола, и связи между транспортным и сеансовым уровнями модели ISO, к которой привязаны различные этапы обработки сообщений. Безопасность данного протокола, основана на применении стандартизированных отечественных криптографических алгоритмов и механизмов, которые позволяют обеспечить аутентификацию и целостность передаваемых данных. Протокол поддерживает различные варианты установления соединения, в зависимости от используемого метода аутентификации и технических возможностей устройств. Протокол разработан в соответствии с рекомендациями национальной системы стандартизации Российской Федерации по принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, оформлен в виде рекомендаций по стандартизации в 2020 г. В работе сформулирован ряд определенных свойств безопасности, идентичных задачам, которые ставит перед собой нарушитель при попытке компрометации работы протокола и необходимых для обоснования криптографической стойкости рассматриваемых механизмов. Показана выполнимость рассмотренных свойств безопасности, основанная на различных механизмах, заложенных в структурные элементы и логику работы протокола, и на сложности компрометации стандартизированных отечественных криптографических решений.

Ключевые слова: криптографические протоколы, защищенное взаимодействие, свойства безопасности.

Для цитирования: НЕСТЕРЕНКО, Алексей Ю.; СЕМЕНОВ, Александр М. КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ КОНТРОЛЬНЫХ И ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 7–16, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1301>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.01.

***Благодарности.** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 19-37-90155.*

Alexey Yu. Nesterenko[1], Alexander M. Semenov[2]
National Research University «Higher school of economics»,
Tikhonov Moscow Institute of Electronics and Mathematics (MIEMNRU HSE),
Tallinskaya str., 34, 123458, Moscow, Russia
[1]e-mail: anesterenko@hse.ru, https://orcid.org/0000-0002-9105-8798
[2]e-mail: amsemenov@hse.ru, https://orcid.org/0000-0003-3251-0534

Cryptographic mechanisms for secure interaction of control and measuring devices*

DOI: http://dx.doi.org/10.26583/bit.2020.4.01

Abstract. The paper describes the key features of the cryptographic protocol providing secure interaction between control and measuring devices. The hierarchical structure underlying this protocol and the

relationship between the transport and session levels of the ISO model, to which different stages of message processing are linked are described. The security of the protocol is based on the use of the standardized domestic cryptographic algorithms and mechanisms that ensure the authentication and integrity of transferred data. The protocol supports different options for establishing a connection, depending on used authentication method and technical capabilities of the devices. The protocol was developed in accordance with the recommendations of the national system of standardization of the Russian Federation on the principles of development and modernization of encryption (cryptographic) means of information protection, and is designed as recommendations on standardization in 2020. In this paper a number of the certain properties of safety identical to tasks which are put by the infringer at attempt of compromise of work of the protocol and necessary for substantiation of cryptographic stability of considered mechanisms are formulated. Feasibility of the considered properties of safety, based on various mechanisms embedded in structural elements and logic of the protocol, and on complexity of compromise of the standardized domestic cryptographic solutions is shown.

Keywords: cryptographic protocols, secure communication, security features.

For citation: YURIEVICH, Alexey N.; MIKHAILOVICH, Aleksandr S. Cryptographic mechanisms for secure interaction of control and measuring devices. IT Security (Russia), [S.l.], v. 27, n. 4, p. 7–16, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1301>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.01.

***Acknowledgement.** The reported study was funded by RFBR, project number 19-37-90155.*

Введение

Современные контрольные и измерительные устройства представляют собой большой класс технических устройств, построенных на основе микроконтроллеров с различной архитектурой. При объединении таких устройств в большие гетерогенные сети, существующие различия в технических характеристиках приводят к необходимости использовать для связи каналы, различающиеся как по своим свойствам, так и по среде распространения информации. Криптографические механизмы, используемые для обеспечения защищенного взаимодействия контрольных и измерительных устройств, не должны зависеть от физического уровня передачи информации и, в частности, от наличия или отсутствия свойства гарантированной доставки сообщений.

Другой важной особенностью взаимодействия контрольных и измерительных устройств является необходимость поддержки максимально возможного числа криптографических механизмов аутентификации участников взаимодействия, основанных как на использовании предварительно распределенной ключевой информации, так и на применении инфраструктуры сертификатов открытых ключей.

Первый механизм аутентификации применим в классе устройств, срок жизни которых невелик, а уникальная ключевая информация может быть помещена в устройство на этапе его производства. Второй механизм предпочтителен для большего класса устройств, чей срок эксплуатации превышает время действия ключевой информации, или устройств, целью которых является предоставление услуги доступа к защищенному взаимодействию различным физическим лицам (например, кассовые аппараты, терминалы удаленного доступа). При этом наличие единого криптографического механизма взаимодействия позволит объединять в сети устройства независимо от используемого ими механизма аутентификации [1].

В работе рассматривается разработанный авторами механизм взаимодействия, обеспечивающий оба механизма аутентификации. Данный механизм утвержден в качестве рекомендаций по стандартизации Р 1323565.1.028-2019.

1. Криптографические механизмы взаимодействия

Авторами был рассмотрен ряд существующих международных и отечественных решений с целью их адаптации под перечисленные выше задачи, в частности, рекомендации по протоколуTLS 1.2(Р 1323565.1.020-2018), и протоколу CRISP(МР 26.4.001-2019). При проектировании рассматриваемого протокола был принят во внимание опыт отечественных и зарубежных исследователей по анализу криптографических протоколов [2–6], схожих по функциональному назначению. В результате была выбрана двухуровневая модель организации защищенного взаимодействия:

- на нижнем уровне реализуется транспортный протокол – протокол отправки/получения сообщений, содержащих как открытую, так и зашифрованную части, а также имитовставку, позволяющую обеспечивать целостность передаваемых данных. При этом открытая информация используется как для формирования используемой при шифровании синхропосылки, так и для возможности реализации механизмов упорядочивания и защиты от повторов при приеме сообщений. Примером такого протокола может служить протокол ESP. Однако его прямое копирование, в данном случае, невозможно как в силу жесткой привязки к IP протоколу, так и в силу необходимости поддержки используемого в IPSec механизма security association. Протокол транспортного уровня использует криптографические механизмы, но не контролирует вопросы выработки ключевой информации;
- уровнем выше располагается сеансовый протокол, основная задача которого заключается в реализации механизмов аутентификации участников протокола, механизмов выработки и согласования смены ключевой информации. Сеансовый протокол рассматривает нижележащий транспортный протокол как криптографический туннель, через который передается информация, поступающая с прикладного уровня.

Приведенная модель позволяет отделить криптографические вопросы – вопросы аутентификации участников протокола и выработки ключевой информации, от механизмов передачи зашифрованной информации по каналам связи. Один и тот же механизм выработки ключевой информации может быть реализован как для каналов с гарантированной доставкой сообщений, так и без нее. При этом обоснование криптографической стойкости криптографических механизмов сеансового уровня не зависит от используемого транспортного протокола. Выбор криптографических алгоритмов, используемых для обеспечения защищенного взаимодействия, основывался на принципах максимального использования отечественных стандартизированных криптографических решений, в частности:

- для шифрования информации допускается использование только алгоритмов блочного шифрования, регламентируемых ГОСТ Р 34.12-2015;
- режим шифрования информации и алгоритм выработки имитовставки регламентируется ГОСТ Р 34.13-2015 и рекомендациями Р 1323565.1.026–2019;
- для аутентификации участников защищенного взаимодействия рекомендуется криптографический механизм, позволяющий связывать вместе уникальные идентификаторы и ключи аутентификации устройств;
- для аутентификации участников защищенного взаимодействия также рекомендуется применение инфраструктуры сертификатов открытых ключей; при этом обеспечивается поддержка инфраструктуры, регламентируемой Федеральным законом от 06.04.2011 № 63–ФЗ «Об электронной подписи»; алгоритмы выработки и проверки электронной подписи регламентируются ГОСТ Р 34.10-2012;

- в основу протокола выработки ключей положена схема «Эхинацея» [7], регламентируемая рекомендациями по стандартизации Р 1323565.1.004-2017;
- в качестве алгоритма выработки производной ключевой информации выбрана функция, описываемая рекомендациями по стандартизации Р 1323565.1.022-2018;
- в качестве алгоритмов выработки производных ключей шифрования и имитовставки выбраны алгоритмы, регламентируемые рекомендациями по стандартизации Р 1323565.1.017-2018;

Использование существующих и обоснованных решений позволило провести исследование криптографических механизмов защищенного взаимодействия контрольных и измерительных устройств с учетом полученных ранее результатов анализа.

2. Схемы работы протокола

Процесс защищенного взаимодействия начинается с установления соединения и выполнения протокола выработки ключей. Данный протокол предназначен для генерации общей для клиента и сервера ключевой информации, которая будет использована для выработки сеансовых ключей связи. Протокол выработки ключей реализуется в группе точек эллиптической кривой [8, 9].

Спецификация протокола, см. рекомендации по стандартизации Р 1323565.1.028-2019, описывает общую универсальную конструкцию установления соединения. На практике допускается использование одной из трех указанных в Р 1323565.1.028-2019 схем взаимодействия, являющиеся частными случаями общей конструкции.

Схема A1 описывает процедуру взаимной аутентификацией на основе предварительно распределенного ключа PSK и предназначена для контрольных и измерительных устройств, для которых уникальная ключевая информация может быть выработана на этапе их производства (рис. 1).

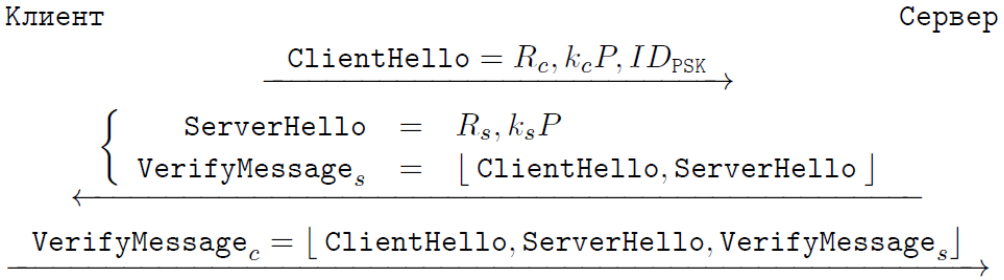

Рис. 1. Схема аутентификации на основе предварительно распределенного ключа. Сеансовый уровень
(Fig. 1. Authentication scheme based on pre-shared key. Session layer)

На сеансовом уровне сообщения рассматриваются как сериализованные представления вводимых спецификацией структур данных. Данные сообщения передаются в ходе выполнения протокола в незашифрованном виде и без имитовставок, подтверждающих целостность передаваемых сообщений. При анализе протокола мы считаем, что сеансовый уровень реализуется в «идеальном» канале связи – канале, не допускающем изменение и навязывание передаваемой информации. Транспортный уровень реализуется в «реальном» канале связи, в котором нарушитель моделируется в рамках модели Долева-Яо [10]. Такой канал требует реализации мер защиты от нарушения конфиденциальности и целостности передаваемой информации. Шифрование

передаваемых сообщений и вычисление для них имитовставки производится на транспортном уровне защищенного взаимодействия (рис. 2).

Рис. 2. Схема аутентификации на основе предварительно распределенного ключа. Транспортный уровень
(Fig. 2. Authentication scheme based on pre-shared key. Transport layer)

Другой схемой, определенной спецификацией протокола, является схема A2, регламентирующая процедуру с аутентификацией на основе ключа проверки электронной подписи (рис. 3). Для аутентификации используются ключи электронной подписи и ключи проверки электронной подписи, сертификаты которых не известны абонентам до начала выполнения протокола.

Рассматриваемая схема A2 применима для класса устройств, целью которых является предоставление услуги доступа к защищенному взаимодействию различным физическим лицам – обладателям пары асимметричных ключей аутентификации. При этом в качестве ключей аутентификации выступают ключ электронной подписи и ключ проверки электронной подписи.

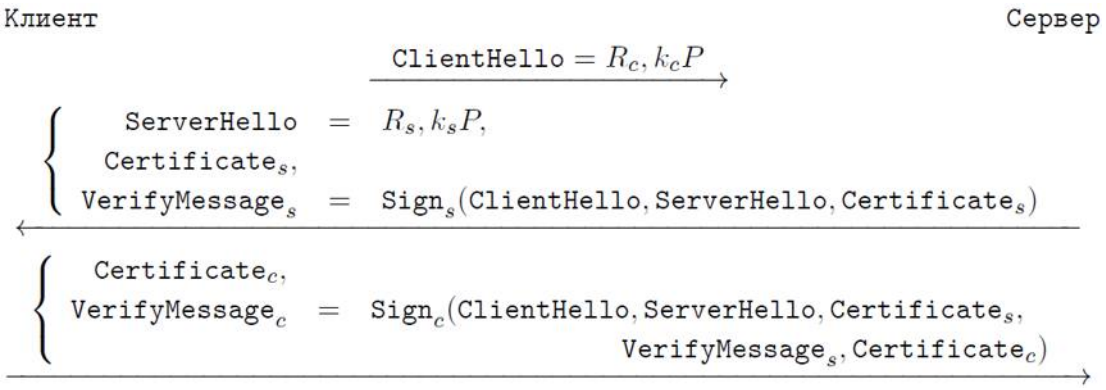

Рис. 3. Схема аутентификации на основе ключа проверки электронной подписи. Сеансовый уровень
(Fig. 3. Authentication scheme based on digital signature. Session level)

При этом, шифрование и вычисление имитовставки производится на транспортном уровне защищенного взаимодействия (рис. 4).

Спецификация предусматривает еще один вариант схемы, регламентирующий процедуру аутентификации на основе ключа проверки электронной подписи. В схеме A3 для аутентификации используются ключи электронной подписи и ключи проверки электронной подписи, сертификаты которых известны абонентам до начала выполнения

протокола. При использовании данной схемы взаимодействия стороны обмениваются не сертификатами, а информацией об используемом сертификатами ключа проверки электронной подписи, которые предварительно распределены между сторонами. В остальном взаимодействие происходит аналогично схеме A2.

Рис. 4. Схема аутентификации на основе ключа проверки электронной подписи. Транспортный уровень
(Fig. 4. Authentication scheme based on digital signature. Transport layer)

3. Цели нарушителя и свойства безопасности

Под целью нарушителя будем подразумевать понятие компрометации защищенного взаимодействия, заключающееся в:

- нарушении конфиденциальности;
- подделке и/или навязывании передаваемой информации;
- нарушении аутентификации участвующих во взаимодействии сторон.

При анализе защищенного взаимодействия невозможность компрометации обеспечивается выполнением ряда «свойств безопасности», комплексное выполнение которых позволяет обеспечить защиту от достижения нарушителем указанных целей.

В настоящей работе рассматривается набор свойств безопасности, разработанный международным сообществом IETF [11, 12], дополненных рядом свойств, возникших в ходе проведенного исследования. Аналогичный подход к рассмотрению свойств безопасности использован в работах [13–17]. Кратко рассмотрим указанный набор свойств.

Формирование уникальных ключей. Уникальные сеансовые ключи формируются для каждого сеанса связи. Это достигается за счет использования варианта схемы Диффи-Хеллмана [18], в ходе которой вырабатывается общая случайная точка эллиптической кривой $Q = k_c k_s P$ с использованием программного или физического датчика для генерации случайных чисел k_c и k_s.

Стойкость при компрометации сеансовых ключей. Для нарушения рассматриваемого свойства с помощью теоретико-вероятностных и/или статистических методов анализа должна использоваться зависимость между ключами из различных сеансов связи. Поскольку для выработки сеансовых ключей из общей точки эллиптической кривой Qиспользуется криптографическая функция HMAC [19], описанная в рекомендациях по стандартизации Р 50.1.113-2016, то можно сделать вывод, что сложность восстановления сеансовых ключей из одного сеанса по известным ключам из другого сеанса не меньше, чем сложность обращения функции HMAC.

Защита от чтения вперед/назад. Выполнение данного свойства подразумевает, что сеансовый ключ, генерируемый с использованием долговременных ключей, не будет

скомпрометирован, в случае компрометации одного или нескольких долговременных ключей.

В качестве долговременного ключа в схеме A1 используется предварительно распределенный ключ аутентификации PSK. Данный ключ используется в ключевой развертке при формировании ключевой информации, используемой для получения производных ключей шифрования и имитозащиты. Также при формировании ключевой информации используется общая точка эллиптической кривой Q. Таким образом, знание ключа PSK недостаточно для определения производных ключей, а сложность компрометации ключей не менее, чем сложность решения задачи дискретного логарифмирования в группе точек эллиптических кривых.

Для остальных схем под долговременными ключами понимаются секретные ключи цифровой подписи, которые напрямую не участвуют в генерации сеансовых ключей шифрования.

Подтверждение ключа. Подтверждение ключей шифрования и имитозащиты происходит за счет использования сообщения VerifyMessage, которое отправляется в зашифрованном виде. Последовательные расшифрование и проверка имитовставки позволяют другому абоненту подтвердить факта наличия обоих ключей у другого абонента. Более того, косвенно подтверждаются корректность использованной ключевой информации и целостность сеанса связи, так как при формировании сеансовых ключей используются хэш-коды всей переданной при установлении соединения информации.

Аутентификация абонентов. Способ аутентификации абонентов зависит от выбранной схемы работы протокола. Аутентификация осуществляется на основе сертификатов открытого ключа или предварительно распределенного ключа PSK путем отправки случайных данных и проверки имитовставки или электронной подписи от отправленных данных.

Аутентификация сообщения. Аутентификация источника данных для схемы A1 основана на выполнении свойства аутентификации пользователя и свойства подтверждения ключа для ключа PSK. Выполнение данных свойств позволяет идентифицировать автора сообщения по факту обладания секретным ключом PSK, а также закрепить авторство передаваемых сообщений за счет использования имитовставок и выполнения свойства подтверждения и аутентификации для ключей шифрования.
Аутентификация источника данных для остальных схем основана на выполнении свойств аутентификации пользователя и использовании электронных подписей, которые позволяют явно определить автора сообщения.

Свойство защищенной возможности договориться о параметрах безопасности. Выполнение данного свойства обеспечивается тем, что передаваемые сообщения между абонентами сообщения VerifyMessage содержат криптографические контрольные суммы, содержащие информацию о переданных параметрах. Кроме того, выполнение свойства подтверждения ключей для всех рассмотренных схем косвенно позволяет убедиться в целостности передаваемых сообщений и параметров безопасности.

Свойство аутентификации ключа. В ходе выполнения протокола осуществляется привязка ключей к текущему сеансу связи и сформированным в рамках соединения сообщениям. Тогда выполнение свойства аутентификации ключа следует из выполнения совокупности свойств аутентификации и подтверждения ключа.

Если одновременно выполнено свойство аутентификации и свойство подтверждения ключа, то один абонент получает подтверждение того, что другой абонент явно идентифицирован и обладает корректно сформированными ключами. Выполнение свойства защиты от чтения вперед/назад и свойства защищенной возможности

договориться о параметрах безопасности, в совокупности с выполнением свойств аутентификации и подтверждения ключа, гарантирует, что в текущем сеансе ни один другой абонент, выбранный заранее, не может получить доступ ни к одному формируемому сеансовому ключу.

Защита от навязывания ключевых значений. Выполнение данного свойства следует из выполнения свойства аутентификации ключа и свойства защищенной возможности договориться о параметрах безопасности.

Анонимность идентификаторов. Пассивный нарушитель, прослушивающий канал связи, не имеет возможности определить идентификаторы пользователей, поскольку идентификаторы либо передаются в зашифрованном виде, либо используются неявно. В последнем случае они считаются известными участникам до начала процесса установления соединения.

В случае активного нарушителя данное свойство выполняется только для идентификатора клиента. Действительно, злоумышленник может инициировать сессию протокола, выдавая себя за клиента, и, получив ответ от сервера, определить идентификатор сервера, содержащийся в его сертификате ключа проверки электронной подписи. Дальнейшее выполнение протокола выработки ключей зависит от действий сервера. В случае проведения взаимной аутентификации установление соединения не может быть завершено, так как злоумышленник не сможет подделать электронную подпись, содержащуюся в сообщении VerifyMessageи выдать себя за клиента. В случае односторонней аутентификации соединение будет успешно установлено.

Конфиденциальность. Конфиденциальность обеспечивается за счет использования алгоритмов шифрования как на этапе установления соединения, так и в ходе выполнения протокола передачи прикладных данных. Выполнение свойства конфиденциальности передаваемых сообщений следует из выполнения совокупности свойств безопасности: защищенной возможности договориться о параметрах безопасности, подтверждения ключа и аутентификации ключа.

Заключение

Проведенное исследование позволяет сделать вывод о том, что компрометация криптографических механизмов, регламентируемых Р 1323565.1.028-2019, сводится к компрометации стандартизированных отечественных криптографических решений, а сами криптографические механизмы удовлетворяют всем предъявленным свойствам безопасности.

СПИСОКЛИТЕРАТУРЫ:

1. Ноздрунов В., Семенов А. Подходы к криптографической защите коммуникаций в IoT и M2M. Информационная безопасность, № 5, 2019. С. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (дата обращения: 23.07.2020).
2. Гребнев С.В., Лазарева Е.В., Лебедев П.А., Нестеренко А.Ю., Семенов А.М. Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1. 3. ПДМ. Приложение, 2018, №11. С. 62–65. DOI:http://dx.doi.org/10.17223/2226308X/11/19.
3. Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E. et al. On post-handshake authentication and external PSKs in TLS 1.3. JComputVirol Hack Tech (2020). DOI: http://dx.doi.org/10.1007/s11416-020-00352-0.
4. Krawczyk H. (2003) SIGMA: The «SIGn-and-MAc»Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols. In: Boneh D. (eds) Advances in Cryptology – CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-540-45146-4_24.
5. Krawczyk H., Paterson K.G., Wee H. (2013) On the Security of the TLS Protocol: A Systematic Analysis. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in

Computer Science, vol. 8042. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-642-40041-4_24.
6. Canetti R., Krawczyk H. (2001) Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Pfitzmann B. (eds) Advances in Cryptology – EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/3-540-44987-6_28.
7. Semenov A.M.,Analysis of Russian key-agreement protocols using automated verification tools, Матем. вопр. криптогр.,2017.Т. 8, вып. 2. P. 131–142. DOI: http://dx.doi.org/10.4213/mvk229.
8. E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev, On the security properties of Russian standardized elliptic curves, Матем. вопр. криптогр., 2018. Т. 9, вып. 3. P. 5–32.DOI: http://dx.doi.org/10.4213/mvk260.
9. A.Yu. Nesterenko, Construction of strong elliptic curves suitable for cryptographic applications, Матем. вопр. криптогр., 2019. Т. 10, вып. 2. P. 135–144. DOI:http://dx.doi.org/10.4213/mvk291.
10. D. Dolev and A. Yao, "On the security of public key protocols," in IEEE Transactions on Information Theory, vol. 29, no. 2. P. 198–208, March 1983. DOI: http://dx.doi.org/10.1109/TIT.1983.1056650.
11. Черемушкин А.В., «Криптографические протоколы: основные свойства и уязвимости», ПДМ, 2009, приложение № 2. С. 115–150.
12. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997.
13. А.Ю. Нестеренко, Об одном подходе к построению защищенных соединений, Матем. вопр. криптогр., 2013. Т. 4, вып. 2. С. 101–111.DOI: http://dx.doi.org/10.4213/mvk86.
14. Горбатов Виктор С., Жуков Игорь Ю., Мурашов Олег Н. Криптографический протокол аутентификации и выработки общего ключа контрольных устройств автотранспорта. Безопасность информационных технологий, [S.1.]. Т. 24. № 4. С. 27–34, 2017. DOI: http://dx.doi.org/10.26583/bit.2017.4.03.
15. Нестеренко А.Ю. Новый протокол выработки общего ключа. Системы высокой доступности. № 2. 2012. С. 81–90.
16. Tristan Ninet. Formal verification of the Internet Key Exchange (IKEv2) security protocol. Cryptography and Security [cs.CR]. Université Rennes 1, 2020. HAL Id: tel-02882167.
17. Avalle, M., Pironti, A. &Sisto, R. Formal verification of security protocol implementations: a survey. Form Asp Comp 26, P. 99–123 (2014). DOI: http://dx.doi.org/10.1007/s00165-012-0269-9.
18. W. Diffie, M. Hellman,“New directions in cryptography,” in IEEE Transactions on Information Theory? vol. 22, no. 6. P. 644–654. November 1976. DOI: http://dx.doi.org/10.1109/TIT.1976.1055638.
19. Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, Матем. вопр. криптогр., 2016. Т. 7, вып.1. С. 5–38. DOI: http://dx.doi.org/10.4213/mvk172.

REFERENCES:

[1] Nozdrunov V., Semenov A. Approaches to cryptographic protection of communications in IoT and M2M. Information security, № 5, 2019. P. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (accessed: 23.07.2020) (in Russian).
[2] Grebnev S.V., Lazareva E.V., Lebedev P.A., NesterenkoA.Yu., Semenov A.M. Integration of russian key-agreement protocols into the TLS 1. 3. PDM. Application, 2018, №11. P. 62–65. DOI: http://dx.doi.org/10.17223/2226308X/11/19.
[3] Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E. et al. On post-handshake authentication and external PSKs in TLS 1.3. J ComputVirol Hack Tech (2020). DOI: http://dx.doi.org/10.1007/s11416-020-00352-0.
[4] Krawczyk H. (2003) SIGMA: The «SIGn-and-MAc» Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols. In: Boneh D. (eds) Advances in Cryptology – CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-540-45146-4_24.
[5] Krawczyk H., Paterson K.G., Wee H. (2013) On the Security of the TLS Protocol: A Systematic Analysis. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol. 8042. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-642-40041-4_24.
[6] Canetti R., Krawczyk H. (2001) Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Pfitzmann B. (eds) Advances in Cryptology – EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/3-540-44987-6_28.

[7] Semenov A.M., Analysis of Russian key-agreement protocols using automated verification tools, Mat. Vopr. Kriptogr., 2017. Vol. 8, Issue 2. P.131–142. DOI: http://dx.doi.org/10.4213/mvk229.
[8] E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev, On the security properties of Russian standardized elliptic curves, Mat. Vopr. Kriptogr., 2018. Vol. 9, Issue 3. P. 5–32. DOI: http://dx.doi.org/10.4213/mvk260.
[9] A.Yu. Nesterenko, Construction of strong elliptic curves suitable for cryptographic applications, Mat. Vopr. Kriptogr., 2019. Vol. 10, Issue 2. P. 135-144. DOI: http://dx.doi.org/10.4213/mvk291.
[10] D. Dolev and A. Yao, "On the security of public key protocols," in IEEE Transactions on Information Theory, vol. 29, no. 2. P. 198–208, March 1983. DOI: http://dx.doi.org/10.1109/TIT.1983.1056650.
[11] Cheremushkin A.V., Cryptographic protocols: basic properties and vulnerabilities, PDM, 2009, application № 2, P. 115–150 (in Russian).
[12] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997.
[13] A.Yu. Nesterenko, On an approach to the construction of secure connections, Mat. Vopr. Kriptogr., 2013. Vol. 4, Issue 2. P. 101–111. DOI: http://dx.doi.org/10.4213/mvk86 (in Russian).
[14] GorbatovViktorS., ZhukovIgorY., MurashovOlegN. Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security, [S.1.]. Vol. 24, no. 4. P. 27–34, 2017. DOI: http://dx.doi.org/10.26583/bit.2017.4.03 (in Russian).
[15] Nesterenko A.YU. The new Protocol develop common key. Sistemy vysokoj dostupnosti. № 2. 2012. P. 81–90 (in Russian).
[16] Tristan Ninet. Formal verification of the Internet Key Exchange (IKEv2) security protocol. Cryptography and Security [cs.CR]. Université Rennes 1, 2020. HAL Id: tel-02882167.
[17] Avalle, M., Pironti, A. &Sisto, R. Formal verification of security protocol implementations: a survey. Form Asp Comp 26. P. 99–123 (2014). DOI: http://dx.doi.org/10.1007/s00165-012-0269-9.
[18] W. Diffie, M. Hellman, “New directions in cryptography,” in IEEE Transactions on Information Theory? Vol. 22, no. 6. P. 644–654. November 1976. DOI: http://dx.doi.org/10.1109/TIT.1976.1055638.
[19] E.K. Alekseev, I.B. Oshkin, V.O. Popov, S.V. Smyshlyaev, On the cryptographic properties of algorithms accompanying the application of standards GOST R 34.11-2012 and GOST R 34.10-2012, Mat. Vopr. Kriptogr., 2016. Vol.7, Issue1. P. 5–38. DOI: http://dx.doi.org/10.4213/mvk172 (in Russian).

Поступила в редакцию - 13 июля 2020 г. Окончательный вариант – 01 ноября 2020 г.
Received –July13, 2020. The final version – November 01, 2020.

Даниил А. Похачевский
Московский физико-технический институт
(национальный исследовательский университет),
Институтский пер., 9, Долгопрудный, Московская область, 141701, Россия
e-mail: daniek9898@gmail.com, https://orcid.org/0000-0001-7403-0307

АНАЛИЗ УЯЗВИМОСТЕЙ, ВОЗНИКАЮЩИХ ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ACTIVE DIRECTORY

DOI: http://dx.doi.org/10.26583/bit.2020.4.02

Аннотация. В статье представлены результаты анализа и синтеза научно-технической литературы, нормативных актов, стандартов в области обеспечения информационной безопасности информационных систем (ИС), использующих сторонние сервисы аутентификации пользователей. Вводится контекст рассматриваемой ИС. Описываются уязвимости, возникающие при аутентификации пользователей с использованием службы каталогов Active Directory. На основе функциональных особенностей клиентского приложения, входящего в ИС, проводится построение концептуальной модели угроз информационной безопасности ИС, которая применяется для выявления и исследования возможных атак на процесс аутентификации пользователей. В результате выявления критических мест безопасности системы, формируются основные требования, соблюдение которых позволит повысить состояние защищенности систем, а именно: необходимость обеспечения подлинности и целостности ЭВМ, принимающих участие в процессе аутентификации пользователей в приложении, необходимость обеспечения конфиденциальности передаваемых и хранимых аутентифицирующих данных пользователей. Результаты данной работы позволяют обезопасить процесс аутентификации с использованием технологии Active Directory, а также проводить дальнейшие исследования в области аутентификации пользователей в распределенных системах. Проведенный анализ позволяет сделать вывод о безопасности применения предложенного способа аутентификации при соблюдении выявленных требований.
Ключевые слова: служба каталогов, Active Directory, аутентификация, модель угроз, объектно-ориентированный подход, требования безопасности.
Для цитирования: ПОХАЧЕВСКИЙ, Даниил А. АНАЛИЗ УЯЗВИМОСТЕЙ, ВОЗНИКАЮЩИХ ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ACTIVE DIRECTORY. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 17–24, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1302>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.02.

Daniil A. Pokhachevskiy
Moscow Institute of Physics and Technology (National Research University),
Institutskiy per., 9, Dolgoprudny, Moscow region, 141701, Russia
e-mail: daniek9898@gmail.com, https://orcid.org/0000-0001-7403-0307

Analysis vulnerabilities of user authentication process using Active Directory

DOI: http://dx.doi.org/10.26583/bit.2020.4.02

Abstract. The paper presents the results of the analysis and synthesis of scientific and technical literature, regulations, standards in the field of information security of information systems (IS), using third-party user authentication services. The context of the considered IS is introduced. Vulnerabilities in user authentication using the Active Directory service are described. Based on the functional features of the client application included in the IS, a conceptual model of threats to the information security of the IS is built. This model is used to identify and investigate possible attacks on the user authentication process. As a result of identifying critical points of system security, the main requirements are formed, the observance of which will improve the state of security of systems, namely: the need to ensure the authenticity and integrity of computers participating in the process of authenticating users in the application, the need to

ensure the confidentiality of transmitted and stored user authenticating data. The results of this work make it possible to secure the authentication process using Active Directory technology, as well as to carry out further research in the field of user authentication in distributed systems. The analysis performed allows us to conclude that the proposed authentication method is safe if the identified requirements are met.
Keywords: directory service, Active Directory, user authentication, threat model, object-oriented approach, safety requirements.
For citation: POKHACHEVSKIY, Daniil A. Analysis vulnerabilities of user authentication process using Active Directory. IT Security (Russia), [S.l.], v. 27, n. 4, p. 17–24, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1302>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.02.

Введение

Процесс аутентификации заключается в проверке принадлежности предъявленного идентификатора субъекту [1 с. 241].

В данный момент популярным явлением является аутентификация пользователей информационных систем выполняется с помощью сторонних сервисов, поэтому введение в научный оборот анализа уязвимостей, возникающих при аутентификации пользователей с использованием Active Directory, будет полезным.

Объектом анализа является процесс аутентификации пользователей с использованием службы каталогов технологии Active Directory.

Объект защиты рассматривается как часть следующей информационной системы (рис. 1). Клиентское приложение, в котором есть подсистема аутентификации, исполняется на некоторой ЭВМ, находящейся в одном сегменте вычислительной сети с контроллером домена. Рассматриваемая подсистема аутентификации входит в состав клиентского приложения. Возможности пользователей использовать определенную функциональность приложения зависят от результатов авторизации пользователей. Active Directory развернута на контроллере домена. Служба каталогов предоставляет интерфейс прикладного уровня сетевой модели OSI для взаимодействия с хранилищем Active Directory по протоколу LDAP. Клиентское приложение использует этот интерфейс для обращения к базе данных пользователей, хранящейся в LDAP-хранилище.

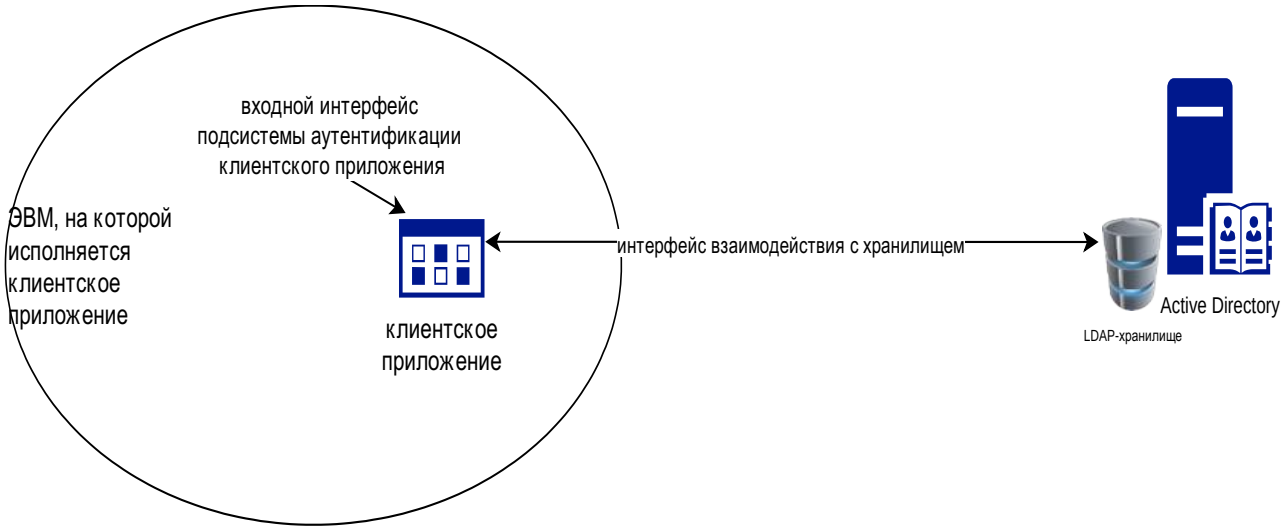

Рис. 1. Информационная система, в которой будет проводиться анализ уязвимостей
(Fig. 1. Informatization system, in which the analysis of vulnerabilities will be carried out)

1. Уязвимости, возникающие при аутентификации пользователей с использованием Active Directory

Общие угрозы процедуры аутентификации известны и приведены в [2]. Для рассматриваемой системы характерны следующие угрозы:

1. Так как ЭВМ, на которой исполняется клиентское приложение в общем случае не является доверенной, возникает угроза несанкционированного доступа к переменному окружению среды исполнения клиентского приложения. В результате процесс аутентификации в клиентском приложении может быть обойден злоумышленником.
2. Клиентское приложение обращается к LDAP-хранилищу AD с использованием интерфейса взаимодействия. Поскольку предполагается, что клиентское приложение работает в ЭВМ, не являющейся контроллером домена Active Directory, возникает угроза обеспечения конфиденциальности передаваемых данных между клиентским приложением и контроллером домена AD. (Подробно об угрозе нарушения конфиденциальности данных приведено в [2 с. 64–65]).
3. Угроза нарушения целостности данных LDAP-хранилища AD является актуальной, поскольку целостность базы данных является фактором, влияющим на процесс аутентификации клиентского приложения в целом. (Подробнее об угрозе нарушения целостности данных LDAP-хранилища в [3 с. 163]).
4. Угроза нарушения свойства доступности данных LDAP-хранилища AD также является актуальной, поскольку доступность базы данных является фактором, влияющим на процесс аутентификации клиентского приложения в целом. (Подробнее об угрозе нарушения доступности LDAP-хранилища в [4 с. 152]).
5. Стоит также упомянуть об угрозе нарушения подлинности контроллера домена Active Directory, на котором расположено LDAP-хранилище учетных данных пользователей. (Подробнее об угрозе нарушения подлинности контроллера домена в [5 с. 4478]).

2. Разработка модели угроз информационной безопасности ИС

Для построения модели угроз информационной безопасности ИС используются методики и каталог угроз из методических документов ФСТЭК [6], стандартов Банка России [7].

Согласно [6, 8 с. 1052] модель угроз должна включать в себя:

- Описание информационной системы и особенностей ее функционирования.
- Модель нарушителя.
- Актуальные угрозы информационной безопасности.

Хорошо построенная модель угроз позволит сформулировать требования, выполнение которых приведет к обеспечению защищенности системы от рассматриваемых угроз.

В рамках данной работы воспользуемся объектно-ориентированным подходом, описанным в [9] для построения проекта модели угроз.

Для корректного построения модели необходимо принимать во внимание все особенности ИС, ее свойства. Однако, в данной работе не было цели рассмотреть все возможные угрозы для ИС данного вида (см. рис. 1). Входными данными модели будут являться функциональные особенности клиентского приложения: выполнение аутентификации пользователей с использованием Active Directory, зависимость доступности пользователю определенного функционала приложения от авторизации пользователя, исполнение приложения в недоверенной среде. Для рассматриваемого объекта анализа имеет смысл выбрать стандартные источники угроз [7]: внутренний

пользователь системы, внешний пользователь (злоумышленник, не имеющий санкционированного доступа к системе). Угрозы, отражаемые в модели, состоят из угроз, характерных для рассматриваемого объекта анализа [10 с. 61], а также базовых угроз приложений ИС [7]. Благодаря рассмотрению ИС под углом ее функциональных особенностей можно считать данный список угроз исчерпывающим.

На рис. 2 показана концептуальная модель угроз.

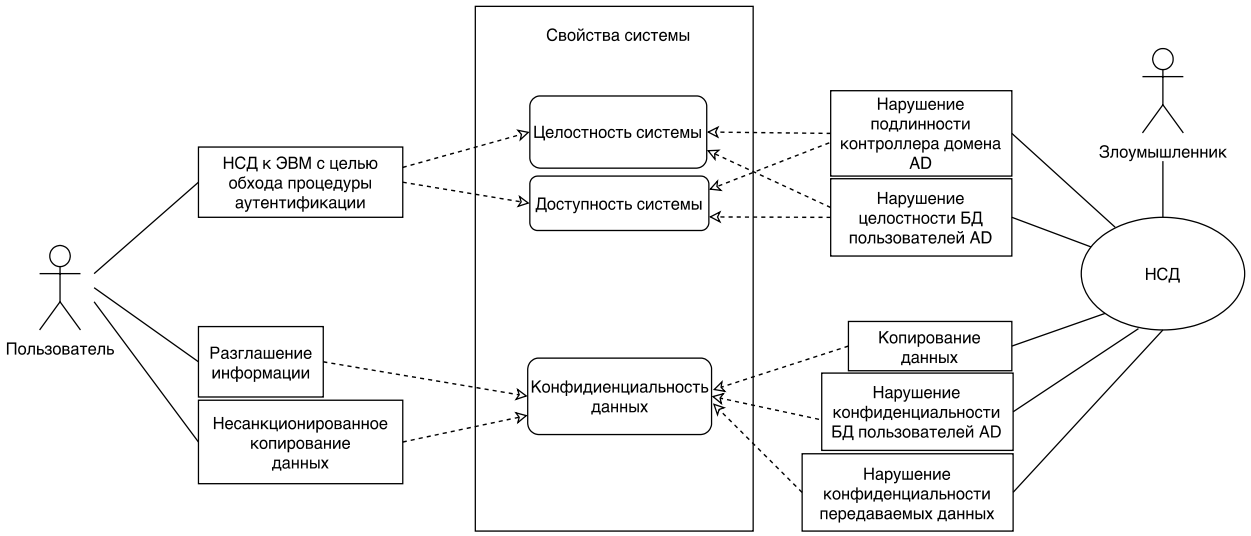

Рис. 2. Концептуальная модель угроз
(Fig. 2. Conceptual Threat Model)

В данном представлении *системой* является клиентское приложение. Под целостностью системы понимается целостность базы данных пользователей из активного каталога, а также подлинность ЭВМ, на котором данная база данных хранится. Под доступностью системы понимается доступность соответствующего (данному пользователю) функционала и данных клиентского приложения конкретному авторизованному пользователю.

Критически важными свойствами системы являются ее целостность, конфиденциальность и доступность данных. Схема позволяет визуализировать способы реализации рассматриваемых угроз для каждого из свойств системы. Пунктиром показана связь между рассматриваемыми угрозами их влиянием на свойства системы. Сплошной линией показаны возможные действия для источников угроз.

Переход от данного представления к детальному описанию атак для рассматриваемого процесса не вызывает трудностей, поскольку становятся явно видны связи между источниками угроз, угрозами и активами системы.

Результаты анализа атак для процесса аутентификации пользователей приведены в табл. 1.

Построенная таблица позволяет выявить критические места безопасности системы и сформировать требования, необходимые для повышения уровня безопасности систем, использующих AD для аутентификации.

Таблица 1. Перечень атак для рассматриваемого процесса аутентификации пользователей

Номер атаки	Описание атаки	Уязвимости	Последствия
1	НСД к ЭВМ-исполнителю клиентского приложения с целью обхода процедуры аутентификации	Отсутствие возможности контроля целостности ПО ЭВМ-исполнителя клиентского приложения	Обход процедуры аутентификации в клиентском приложении
2	Пассивный НСД к передаваемым данным между клиентским приложением и контроллером домена AD с целью дальнейшего НСД к клиентскому приложению	Отсутствие шифрования передаваемых данных	Утечка АИП пользователей с последующим НСД к клиентскому приложению
3	Активный НСД к передаваемым данным между клиентским приложением и контроллером домена AD с целью обхода процедуры аутентификации; нарушения доступности функционала клиентского приложения	Отсутствие взаимной аутентификации контроллера домена AD и клиентского приложения	Обход процедуры аутентификации клиентского приложения. Запрет доступа для легальных пользователей.
4	Активный НСД к LDAP-хранилищу КД с целью обхода процедуры аутентификации; нарушения доступности функционала клиентского приложения	Отсутствие контроля целостности содержимого LDAP-хранилища на контроллере домена AD.	Обход процедуры аутентификации с помощью модификации состояния БД пользователей. Запрет доступа для легальных пользователей.
5	Пассивный НСД к LDAP-хранилищу КД с целью обхода процедуры аутентификации	Отсутствие шифрования содержимого LDAP-хранилища КД AD.	Обход процедуры аутентификации с последующим использованием АИП легального пользователя

В результате детального рассмотрения атаки 1, можно сформировать следующее требование безопасности: нарушитель, имеющий возможность контролировать среду исполнения клиентского приложения, не должен иметь возможности обойти процедуру аутентификации клиентского приложения. Данное требование может быть реализовано разными способами, например на уровне архитектуры процессора ЭВМ, на которой исполняется приложения [2 с. 106, 11 с. 6076].

В результате детального рассмотрения атаки 3, можно сформулировать следующее требование безопасности: необходимо выполнять проверку подлинности контроллера домена Active Directory при каждой процедуре аутентификации. Данное требование может

быть реализовано с помощью инфраструктуры открытых ключей в объединении с концепцией РКБ [12].

В результате детального рассмотрения атаки 2, можно сформулировать следующее требование безопасности: необходимо обеспечить конфиденциальность передаваемых данных по каналу связи клиентского приложения с контроллером домена AD. Данное требование может быть реализовано с помощью криптографических средств [13 с. 196] защиты информации; либо за счет установки доверенного сеанса связи между данными объектами [14 с. 46949, 15].

В результате детального рассмотрения атаки 4, можно сформулировать следующее требование безопасности: необходимо обеспечить целостность LDAP-хранилища AD. Данное требование может быть реализовано с использованием СДЗ, имеющего функциональность контроля целостности системы.

В результате детального рассмотрения атаки 5, можно сформулировать следующее требование безопасности: необходимо обеспечить конфиденциальность хранимых данных в LDAP-хранилище. Данное требование может быть реализовано с помощью криптографических методов защиты информации.

Итого, с учетом проведенного выше анализа и лучших практик в области информационной безопасности процессов аутентификации сформулируем следующие требования безопасности:

1. Нарушитель с соответствующими привилегиями контроля среды клиентского приложения не должен иметь возможности обойти процедуру аутентификации клиентского приложения.
2. Должна быть обеспечена конфиденциальность данных, передаваемых между клиентским приложением и контроллером домена AD.
3. Должна быть обеспечена конфиденциальность данных, находящихся в LDAP-хранилище.
4. Должна быть обеспечена целостность LDAP-хранилища AD.
5. Должна быть обеспечена подлинность контроллера домена AD.

Заключение

Построенная концептуальная модель угроз позволяет понять связь между источниками угроз, свойствами системы и угрозами. Слабым местом рассматриваемой системы являются уязвимости, связанные с отсутствием явного шифрования передаваемых и хранимых учетных данных пользователей; уязвимости, связанные с отсутствием контроля целостности и подлинности ЭВМ, принимающих участие в процедуре аутентификации пользователей в приложении. В результате анализа были сформулированы необходимые требования безопасности, направленные на обеспечение подлинности контроллера домена, а также обеспечение конфиденциальности передаваемых и хранимых данных. Основные требования могут быть удовлетворены с помощью использования криптографических методов защиты информации, а также использования РКБ на ЭВМ, участвующих в процессе аутентификации. Результаты данной работы позволяют проводить дальнейшие исследования в области аутентификации пользователей в распределенных системах.

Таким образом, проведен анализ уязвимостей и атак для рассматриваемого процесса аутентификации пользователей. Из анализа можно сделать вывод о целесообразности применимости (с точки зрения информационной безопасности) данного способа аутентификации при соблюдении требований безопасности, обозначенных выше.

СПИСОК ЛИТЕРАТУРЫ:

1. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты., М.: Книжный мир, 2009. – 352 с. URL: https://computer-museum.ru/books/computer_safety.pdf (дата обращения: 15.08.2020).
2. Конявский В.А., Конявская С.В. Доверенные информационные технологии: от архитектуры к системам и средствам. Москва: URSS, 2019. – 264 с.
3. Deepa G., Thilagam P. S. Securing web applications from injection and logic vulnerabilities: Approaches and challenges //Information and Software Technology. 2016. Vol. 74. P. 160–180. DOI: http://dx.doi.org/10.1016/j.infsof.2016.02.005.
4. Obimbo C. et al. Vulnerabilities of LDAP As An Authentication Service. J. Information Security. 2011. Vol. 2. No. 4. P. 151–157. DOI: http://dx.doi.org/10.4236/jis.2011.24015.
5. Binduf A. et al. Active Directory and Related Aspects of Security. 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. P. 4474–4479. DOI: http://dx.doi.org/10.1109/NCG.2018.8593188.
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 15 февраля 2008 г. URL: https://fstec.ru/component/attachments/download/289 (дата обращения: 27.05.2020).
7. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014. Принят и введен в действие распоряжением Банка России от 17.05.2014 No Р-399. URL: http://cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения: 27.05.2020).
8. Hoque M. A., Hasan R. Towards a Threat Model for Vehicular Fog Computing. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2019. С. 1051–1057. DOI: http://dx.doi.org/10.1109/UEMCON47517.2019.8993064.
9. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования. Вопросы безопасности. 2017. № 2. С. 25–34. DOI: http://dx.doi.org/10.7256/2409-7543.2017.2.22065. URL: https://nbpublish.com/library_read_article.php?id=22065.
10. Matsuda W., Fujimoto M., Mitsunaga T. Detecting apt attacks against active directory using machine leaning. 2018. IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2018. С. 60–65. DOI: http://dx.doi.org/10.1109/AINS.2018.8631486.
11. Alhaidary M. et al. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018. Vol. 6. P. 6071–6081. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2789301.
12. Конявский, В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). М.: Беллитфонд, 2004. – 282 с. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf.
13. Buchanan W.J., Li S., Asif R. Lightweight cryptography methods. Journal of Cyber Security Technology. 2017. Vol. 1. №. 3–4. С. 187–201. DOI: http://dx.doi.org/10.1080/23742917.2017.1384917.
14. Qian J. et al. A Trusted-ID Referenced Key Scheme for Securing SCADA Communication in Iron and Steel Plants. IEEE Access. 2019. Vol. 7. P. 46947–46958. DOI: http://dx.doi.org/10.1109/ACCESS.2019.2909011.
15. Конявский В. А. Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем – на старт, внимание, МАРШ! //Комплексная защита информации. Материалы XV международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М.: 2010. С. 166–169; URL: http://www.accord.ru/konyavskiy_2010_1.htm1.

REFERENCES:

[1] Shherbakov, A.Ju. Modern computer security. Theoretical bases. Practical aspect., M.: Knizhnyi mir, 2009. – 352 p. URL: https://computer-museum.ru/books/computer_safety.pdf (accessed: 15.08.2020) (in Russian).
[2] Konjavskij V.A., Konjavskaja S.V. Trusted information technologies: from architecture to systems and tools. Moskva: URSS, 2019. – 264 p. (in Russian).
[3] Deepa G., Thilagam P. S. Securing web applications from injection and logic vulnerabilities: Approaches and challenges //Information and Software Technology. 2016. Vol. 74. P. 160–180. DOI: http://dx.doi.org/10.1016/j.infsof.2016.02.005.
[4] Obimbo C. et al. Vulnerabilities of LDAP As An Authentication Service. J. Information Security. 2011. Vol. 2. No. 4. P. 151–157. DOI: http://dx.doi.org/10.4236/jis.2011.24015.
[5] Binduf A. et al. Active Directory and Related Aspects of Security //2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. P. 4474–4479. DOI: http://dx.doi.org/10.1109/NCG.2018.8593188.

[6] The basic model of threats to the security of personal data during their processing in personal data information systems. February 15, 2008. URL: https://fstec.ru/component/attachments/download/289 (accessed: 27.05.2020) (in Russian).
[7] Standard of the Bank of Russia " ensuring information security of organizations of the banking system of the Russian Federation. Generalities» STO BR IBBS-1.0-2014. Adopted and put into effect by the order of the Bank of Russia from May 17, 2014 No R-399. URL: http://cbr.ru/credit/Gubzi_docs/st-10-14.pdf (accessed: 27.05.2020) (in Russian).
[8] Hoque M. A., Hasan R. Towards a Threat Model for Vehicular Fog Computing. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2019. P. 1051–1057. DOI: http://dx.doi.org/10.1109/UEMCON47517.2019.8993064.
[9] Gribanova-Podkina M.Ju. Building a model of threats to information security of an information system using the methodology of object-oriented design. Voprosy bezopasnosti. M.: 2017. No 2. P. 25–34. DOI: http://dx.doi.org/10.7256/2409-7543.2017.2.22065 (in Russian).
[10] Matsuda W., Fujimoto M., Mitsunaga T. Detecting apt attacks against active directory using machine leaning. 2018 IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2018. P. 60–65. DOI: http://dx.doi.org/10.1109/AINS.2018.8631486.
[11] Alhaidary M. et al. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018. Vol. 6. P. 6071–6081. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2789301.
[12] Konjavskij, V. A., Gadasin V. A. Fundamentals of understanding the phenomenon of electronic information exchange (Library of the magazine "UZI"; Book 2). M.: Bellitfond, 2004. – 282 p. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf (in Russian).
[13] Buchanan W. J., Li S., Asif R. Lightweight cryptography methods //Journal of Cyber Security Technology. – 2017. Vol. 1. №. 3–4. P. 187–201. DOI: http://dx.doi.org/10.1080/23742917.2017.1384917.
[14] Qian J. et al. A Trusted-ID Referenced Key Scheme for Securing SCADA Communication in Iron and Steel Plants. IEEE Access. 2019. Vol. 7. P. 46947–46958. DOI: http://dx.doi.org/10.1109/ACCESS.2019.2909011.
[15] Konjavskij V.A. A trusted communication session. Development of the paradigm of trusted computing systems - at the start, attention, MARSh! Comprehensive information protection. Materials of the XV International scientific and practical conference (Irkutsk (Russia), 1–4 June 2010). M.: 2010. P. 166–169; URL: http://www.accord.ru/konyavskiy_2010_1.htm1 (in Russian).

Поступила в редакцию – 15 августа 2020 г. Окончательный вариант – 01 ноября 2020 г.
Received – August 15, 2020. The final version – November 01, 2020.

Сергей В. Скрыль[1], Елена В. Смирнова[2], Александр В. Заряев[3],
Ле Ву Хыонг Занг[4], Анжелика С. Хмелина[5]
[1,2,5]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)
ул. 2-я Бауманская, 5, Москва, 105005, Россия
[3]Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю,
ул. 9 Января, 280а, Воронеж, 3940209, Россия
[4]Center of Quality Assurance Ho Chi Minh City University of Economics and Finance (UEF), Viet Nam, 141-145, Dien Bien Phu St., W.15, Binh Thanh Dist., HCMC
[1]e-mail: karel105@mail.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: bmstu.smirnova@gmail.com, https://orcid.org/0000-0003-2275-3276
[3]e-mail: zaryaev@yandex.ru, https://orcid.org/0000-0003-1316-8032
[4]e-mail: gianglvh@uef.edu.vn, https://orcid.org/0000-0003-4990-0731
[5]e-mail: anjel.hmelina2010@yandex.ru, https://orcid.org/0000-0002-3517-1235

СИСТЕМАТИЗАЦИЯ ХАРАКТЕРИСТИК ЗАЩИЩЕННОСТИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2020.4.03

Аннотация. В статье обосновывается возможность распространения закономерностей, характерных для информационного процесса, на образовательный процесс. Рассматриваются особенности проявления свойства защищенности информации в условиях образовательной деятельности, связанной с подготовкой специалистов в области информационной безопасности. Анализируются недостатки оценки данного свойства количественными методами. Обосновывается возможность оценки защищенности образовательной деятельности качественными методами. Определяются классификационные основания для систематизации характеристик защищенности. Приводится структура характеристик защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности. Формулируются методические положения для реализации процедуры синтеза данной структуры. Приводятся варианты характеристических таблиц и пример таблицы решений для оценки значений характеристик защищенности образовательной деятельности в терминах лингвистической шкалы. Полученные результаты позволят практически оценить целесообразность проведения мероприятий по обеспечению безопасности информации в процессе образовательной деятельности. Разработанная методика может рассматриваться как методическое обеспечение решения задачи оценки защищенности образовательной деятельности.

Ключевые слова: подготовка специалистов, информационная безопасность, защищенность образовательной деятельности, количественные методы оценки, качественные методы оценки, структура характеристик защищенности образовательной деятельности.

Для цитирования: СКРЫЛЬ, Сергей В. и др. СИСТЕМАТИЗАЦИЯ ХАРАКТЕРИСТИК ЗАЩИЩЕННОСТИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 25–36, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1303>. Дата доступа: 19 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.03.

Sergey V. Skryl'[1], Elena V. Smirnova [2], Alexandr V. Zaryaev[3],
Le Vu Huong Giang[4], Anzhelika S. Khmelina[5]
[1,2,5]Federal State Educational Institution of Higher Education «Bauman Moscow State Technical University»,
2nd Bauman str., 5, Moscow, 105005, Russia
[3]State research and testing Institute of problems of technical protection of information of the FSTEC of Russia,

9 on January str., 280a, Voronezh, 394020, Russia
[4]Center of Quality Assurance Ho Chi Minh City University of Economics and Finance (UEF), Viet Nam, 141-145, Dien Bien Phu St., W.15, Binh Thanh Dist., HCMC
[1]e-mail: karel105@mail.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: bmstu.smirnova@gmail.com, https://orcid.org/0000-0003-2275-3276
[3]e-mail: zaryaev@yandex.ru, https://orcid.org/0000-0003-1316-8032
[4]e-mail: gianglvh@uef.edu.vn, https://orcid.org/0000-0003-4990-0731
[5]e-mail: anjel.hmelina2010@yandex.ru, https://orcid.org/https://orcid.org/0000-0002-3517-1235

Systematization of security characteristics of educational activities for training specialists in the field of information security

DOI: http://dx.doi.org/10.26583/bit.2020.4.03

Abstract. The possibility of extending the patterns characteristic of the information process to the educational process is substantiated in this paper. The features of the manifestation of information security properties in the context of educational activities related to the training of specialists in the field of information security are considered. The disadvantages of evaluating this property by quantitative methods are analyzed. It substantiates the possibility of assessing the security of educational activity by qualitative methods. Classification grounds for systematization of security characteristics are determined. The structure of the characteristics of the security of educational activities for the training of specialists in the field of information security is given. Methodological provisions for the implementation of the synthesis procedure of this structure are formulated. Variants of characteristic tables and an example of a decision table for assessing the values of the security characteristics of educational activities in terms of a linguistic scale are given. The results obtained will allow us to assess the feasibility of carrying out measures practically to ensure the information security of educational activities. The developed method can be considered as a methodological support for solving the practical problem of assessing the security of educational activities.

Keywords: specialists training, information security, security of educational activities, quantitative assessment methods, qualitative assessment methods, structure of characteristics of educational activity security.

For citation: SKRYL', Sergey V. et al. Systematization of security characteristics of educational activities for training specialists in the field of information security. IT Security (Russia), [S.l.], v. 27, n. 4, p. 25–36, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1303>. Date accessed: 19 nov. 2020. doi: http://dx.doi.org/10.26583/bit.2020.4.03.

Введение

Методологический уровень теоретических основ информатики, как результата практики развития информационных технологий позволяет сформировать понятийный базис для понимания одной из фундаментальных категорий информатики – категории «информационный процесс» [1]. Широта восприятия всех аспектов данного понятия позволяет распространить закономерности реализации процедур накопления, обработки и передачи информации на такой специфичный вид деятельности как образовательная. Анализ этой деятельности, информационной по своей сути, позволяет выявить в процедурах накопления знаний, их усвоения и передачи целый ряд свойств, характерных для образовательного процесса, как процесса информационного. Речь идет о полноте, адекватности, целостности и своевременности реализации процедур образовательной деятельности [2]. Это, в свою очередь, позволило разработать целый ряд математических моделей для количественной оценки перечисленных характеристик [3] и предложить вариант интегральной количественной оценки качества подготовки специалистов [4, 5].

Вместе с тем при оценке качества такой специфичной, но весьма важной сферы деятельности, как подготовка специалистов в области информационной безопасности, следует учитывать и тот факт, что на качество образовательного процесса оказывает

существенное влияние информационная характеристика «защищенность», а значит, необходимо исследовать возможности оценки количественными методами качества защиты информации в образовательном процессе [6]. Вместе с тем, несмотря на существующую практику количественной оценки отдельных характеристик образовательного процесса [3, 7], применение количественных методов для оценки защищенности образовательного процесса сопряжено с рядом трудностей, перечисленных в [8]. Главной причиной этих трудностей является довольно большое число слабо формализуемых факторов проявления угроз безопасности информации в рамках образовательной деятельности, и отсутствие возможности определения их влияния на ее обеспечение в рамках количественной шкалы оценки.

Указанные трудности использования количественных методов для оценки защищенности образовательного процесса обусловили необходимость поиска таких подходов к оценке данной характеристики, которые учитывали бы особенности влияния угроз безопасности информации на виды обеспечения образовательной деятельности [9]. В этих условиях одним из возможных путей оценки защищенности образовательной деятельности является синтез комплексного показателя, характеризующего возможности образовательных учреждений, осуществляющих подготовку специалистов в области информационной безопасности, по реализации мер защиты информации от угроз ее безопасности.

В работе [10] предложен принципиально новый подход к решению проблемы оценки защищенности образовательной деятельности в процессе подготовки специалистов в области информационной безопасности, суть которого состоит в систематизации разнородных проявлений эффекта реагирования на воздействие угроз безопасности информации и синтеза структуры характеристик защищенности такого рода информационной деятельности. Принципиальным здесь является то обстоятельство, что проявление эффекта от принимаемых мер защиты информации можно оценить лишь в качественных терминах [11, 12].

1. Принципы формирования структуры характеристик защищенности образовательной деятельности в процессе подготовки специалистов в области информационной безопасности

В общем виде процедура синтеза структуры характеристик защищенности образовательной деятельности сводится к упорядочению множества проявлений эффекта реагирования на воздействие угроз безопасности информации в процессе такого рода деятельности [13]. При этом упорядочение осуществляется в соответствии с определенными классификационными основаниями, а сама структура является композиционной структурой, уровни которой соответствуют этим основаниям.

Классификационными основаниями для упорядочения множества проявлений эффекта реагирования на воздействие угроз безопасности информации в процессе образовательной деятельности являются возможности по оценке:

1) состояний защищенности информации в процессе реализации образовательной деятельности;

2) защищенности информации о видах обеспечения образовательного и воспитательного процесса;

3) безопасности информации в процессе реализации основных компонент образовательных технологий;

4) целевого назначения принимаемых мер защиты информации от воздействия угроз ее безопасности в процессе образовательной деятельности [14–16].

На рис. 1 представлена структура характеристик защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности.

Рис. 1. Структура характеристик защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности
(Fig. 1. Structure of security characteristics of educational activities for training specialists in the field of information security)

Характеристикой, классифицируемой как целевая, является степень обеспечения защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности.

Процедура синтеза структуры характеристик защищенности образовательной деятельности в процессе подготовки специалистов в области информационной безопасности реализуется с учетом следующих методических положений.

1. Характеристика целевого назначения принимаемых мер защиты информации от воздействия угроз безопасности информации в процессе образовательной деятельности является системной характеристикой ее защищенности и должна представляться единым системным показателем.

2. Единый системный показатель формируется на основе характеристик, классифицируемых в соответствии с приведенными выше основаниями в порядке их убывания.

3. Структура формируемой системы характеристик является многоуровневой. Ее уровни соответствуют рассмотренным выше классификационным основаниям.

4. Композиционная процедура формирования структуры характеристик защищенности образовательной деятельности в процессе подготовки специалистов в

области информационной безопасности реализуется в следующей последовательности:

1) формирование характеристик защищенности информации видов обеспечения образовательного и воспитательного процесса путем установления композиционных отношений между характеристиками обеспечения состояний защищенности информации в процессе реализации образовательной деятельности;

2) формирование характеристик безопасности информации в процессе реализации основных компонент образовательных технологий путем установления композиционных отношений между характеристиками защищенности информации видов обеспечения образовательного и воспитательного процесса;

3) формирование показателя защищенности образовательной деятельности в процессе подготовки специалистов в области информационной безопасности путем установления композиционных отношений между характеристиками безопасности информации в процессе реализации основных компонент образовательных технологий.

Таким образом, очевидно, что исходными при синтезе структуры характеристик защищенности образовательной деятельности в процессе подготовки специалистов в области информационной безопасности являются характеристики обеспечения состояний защищенности. Определим эти характеристики как первичные. Остальные характеристики будут считаться производными от первичных и определяются как вторичные.

Композиционные отношения «многие ко многим» в синтезируемой структуре являются отношениями между разнотипными характеристиками, а композиционные отношения «многие к одному» являются отношениями, образуемыми в результате приведения разнотипных характеристик к однотипным. Логика этих отношений представляется в лингвистических терминах. Оценка этих характеристик осуществляется в рамках однотипной качественной шкалы в терминах лингвистических переменных.

Оценка первичных характеристик осуществляется экспертными методами при помощи характеристических таблиц, а оценка остальных характеристик и системного показателя осуществляется формальными методами с помощью таблиц решений.

2. Методический аппарат лингвистической оценки качества подготовки специалистов в области информационной безопасности

При формировании характеристических таблиц для оценки характеристик обеспечения состояний защищенности информации в процессе реализации образовательной деятельности [11] будем полагать, что первичная характеристика обладает:

– свойством конфиденциальности информации учебно-методического и учебно-лабораторного обеспечения образовательного процесса, а также информационного обеспечения воспитательного процесса, если всесторонне обеспечиваются функции противодействия техническим каналам утечки конфиденциальной информации, которую получают студенты в процессе накопления знаний, формирования навыков и практической отработки умений по работе со средствами защиты информации;

– свойством целостности информации учебно-методического обеспечения образовательного процесса и информационного обеспечения воспитательного процесса, если обеспечивается требуемый уровень достоверности информации в процессе накопления знаний, формирования навыков и практической отработки умений по работе со средствами рассматриваемого типа;

– свойством доступности информации учебно-лабораторного обеспечения образовательного процесса, если невозможно затруднение ее использования в процессе формирования навыков и практической отработки умений работы со средствами

защиты информации;

– свойством защищенности информационного обеспечения воспитательного процесса от информационно-психологического воздействия, если всесторонне реализуются функции контроля нарушений, вызванных с навязыванием чуждых идеологических и социальных установок, формирования ложных стереотипов поведения, трансформации настроений, чувств и воли студентов при выработке у них стиля мышления, обладателя правосознания и менталитета, духовных идеалов и ценностных установок, типичных для носителя требуемых норм мировоззрения;

– свойством защищенности информационного обеспечения воспитательного процесса от дезинформации, если всесторонне реализуются функции защиты от навязывания ложной информации.

Характерные признаки первичных свойств выявляются в результате анализа возможностей принимаемых мер защиты информации [15] по обеспечению состояний ее защищенности в процессе реализации образовательной деятельности и оцениваются следующими лингвистическими переменными:

ОВ (очень высокая) – все принимаемые меры защиты информации с данным признаком (свойством) являются эффективными;

В (высокая) – подавляющее большинство принимаемых мер защиты информации с данным признаком (свойством) являются эффективными;

ВС (выше среднего) – практически все принимаемые меры защиты информации с данным признаком (свойством) являются эффективными;

С (средняя) – некоторые принимаемые меры защиты информации с данным признаком (свойством) являются эффективными;

НС (ниже среднего) – отдельные принимаемые меры защиты информации с данным признаком (свойством) являются эффективными;

Н (низкая) – меры защиты информации принимаются;

ОН (очень низкая) – меры защиты информации не принимаются.

В табл. 1–5 приводятся варианты характеристических оценок защищенности информации в процессе подготовки специалистов в области информационной безопасности.

Таблица 1. Характеристические оценки конфиденциальности информации учебно-методического и учебно-лабораторного обеспечения образовательного процесса, а также - информационного обеспечения воспитательного процесса

Характеризуемое свойство и состояния его обеспеченности	**Оценка**
Представление документированных требований к реализации мер обеспечения конфиденциальности информации	
Требования представлены наставлениями руководителей учебных подразделений	ОВ
Требования представлены руководством учебного заведения, ответственного за соблюдение режимных требований	В
Требования представлены типовыми инструкциями	ВС
Требования представлены отраслевыми методическими рекомендациями	С
Требования представлены отраслевыми нормативными документами	НС
Требования представлены ГОСТами	Н
Требования отсутствуют	ОН
Реализуемость процедур разграничения полномочий доступа к информации при работе с программными средствами специального назначения	
Все процедуры реализуются в полном объеме	ОВ
Реализуются все процедуры, за исключением процедур идентификации фактов нарушения полномочий доступа	В

Таблица 1 (окончание)

Характеризуемое свойство и состояния его обеспеченности	**Оценка**
Реализуются лишь процедуры разграничения полномочий по функциям доступа к информации, включая процедуры идентификации фактов нарушения полномочий доступа	ВС
Реализуются лишь процедуры разграничения полномочий по доступу к части данных, включая процедуры идентификации фактов нарушения полномочий доступа	С
Реализуются лишь процедуры разграничения полномочий по функциям доступа к информации, исключая процедуры идентификации фактов нарушения полномочий доступа	НС
Реализуются лишь процедуры разграничения полномочий по доступу к части данных, включая процедуры идентификации фактов нарушения полномочий доступа	Н
Процедуры не реализуются	ОН
Реализуемость функций защиты информации от утечки по техническим каналам	
Функции реализуются в отношении всех возможных каналов утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) в пределах всей контролируемой зоны, включающей учебные помещения и помещения со средствами вычислительной техники (СВТ), работающими с программными средствами специального назначения	ОВ
Функции реализуются в отношении всех каналов утечки информации через ПЭМИН, исключая программно управляемое ПЭМИН, в пределах всей контролируемой зоны, включающей учебные помещения и помещения с СВТ, работающими с программными средствами специального назначения	В
Функции реализуются в отношении побочных электромагнитных излучений (ПЭМИ) в пределах контролируемой зоны, включающей помещения с СВТ, работающими с программными средствами специального назначения	ВС
Функции реализуются в отношении наводок электромагнитных излучений (ЭМИ) в пределах контролируемой зоны, включающей помещения с СВТ, работающими с программными средствами специального назначения	С
Функции реализуются в части защиты информации от утечки по каналам ПЭМИН по отношению к отдельным СВТ, работающими с программными средствами специального назначения	НС
Функции реализуются в части защиты информации от утечки по каналам ПЭМИ по отношению к отдельным СВТ, работающими с программными средствами специального назначения	Н
Функции отсутствуют	ОН

Таблица 2. Характеристические оценки целостности информации учебно-методического обеспечения образовательного процесса и информационного обеспечения воспитательного процесса

Характеризуемое свойство и состояние его обеспеченности	**Оценка**
Выполнение функций контроля достоверности и целостности информации при реализации образовательного и воспитательного процесса	
Функции выполняются постоянно	ОВ
Функции контроля достоверности информации выполняются постоянно, а функции контроля целостности информации – по команде	В
Функции контроля достоверности информации выполняются по команде, а функции контроля целостности информации – постоянно	ВС
Функции контроля достоверности и целостности информации выполняются по команде	С

Таблица 2 (окончание)

Характеризуемое свойство и состояние его обеспеченности	**Оценка**
Функции контроля достоверности информации выполняются по команде, контроль целостности информации отсутствует	НС
Функции контроля целостности информации выполняются по команде, контроль достоверности информации отсутствует	Н
Функции контроля достоверности и целостности информации отсутствуют	ОН
Выполнение функций восстановления целостности информации при реализации образовательного и воспитательного процесса	
Имеются в наличии полные копии учебно-методического обеспечения образовательного процесса и информационного обеспечения воспитательного процесса	В
Имеется в наличии полная копия учебно-методического обеспечения образовательного процесса и неполная копия информационного обеспечения воспитательного процесса	С
Имеется в наличии полная копия информационного обеспечения воспитательного процесса и неполная копия учебно-методического обеспечения образовательного процесса	Н
Имеются в наличии неполные копии учебно-методического обеспечения образовательного процесса и информационного обеспечения воспитательного процесса	ОН

Таблица 3. Характеристические оценки доступности информации учебно-лабораторного обеспечения образовательного процесса

Характеризуемое свойство и состояние его обеспеченности	**Оценка**
Реализуемость функций контроля блокирования доступа к устройствам СВТ, работающих с программными средствами специального назначения	
Реализованы функции контроля блокирования доступа к устройствам, портам и сетевому оборудованию СВТ	ОВ
Реализованы функции контроля блокирования доступа к сетевому оборудованию СВТ	В
Реализованы функции контроля блокирования доступа к процессорному устройству СВТ	ВС
Реализованы функции контроля блокирования доступа к памяти СВТ	С
Реализованы функции контроля блокирования доступа к портам СВТ	НС
Реализованы функции контроля блокирования доступа к устройствам ввода/вывода информации СВТ	Н
Отсутствуют функции контроля блокирования доступа к устройствам СВТ, работающих с программными средствами специального назначения	ОН
Своевременность реагирования на блокирование доступа к устройствам СВТ, работающих с программными средствами специального назначения	
Время реагирования не превышает 5 минут	В
Время реагирования не превышает 15 минут	С
Время реагирования не превышает часа	Н
Время реагирования превышает час	ОН

На основе полученных при помощи характеристических таблиц 1–5 значений характеристик обеспечения состояний защищенности информации в процессе реализации образовательной деятельности определяются характеристики защищенности информации видов обеспечения образовательного и воспитательного процесса. Для этого используются соответствующие таблицы решений.

Таблица 4. Характеристические оценки защищенности информационного обеспечения воспитательного процесса от информационно-психологического воздействия

Характеризуемое свойство и состояние его обеспеченности	**Оценка**
Реализуемость функций контроля нарушений процесса выработки у студентов требуемых норм мировоззрения	
Реализованы функции постоянного контроля со стороны руководства учебных подразделений	ОВ
Реализованы функции контроля по планам подразделений, осуществляющих воспитательную работу	В
Установлен периодический контроль над влиянием всех средств информационно-психологического воздействия на сознание студента как носителя требуемых норм мировоззрения	ВС
Установлен периодический контроль над влиянием агитационной деятельности общественных организаций, политических партий, кандидатов в политические лидеры на сознание студента как носителя требуемых норм мировоззрения	С
Установлен периодический контроль над влиянием средств массовой информации на сознание студента как носителя требуемых норм мировоззрения	НС
Установлен периодический контроль над влиянием виртуально-психологических средств на сознание студента как носителя требуемых норм мировоззрения	Н
Функции контроля нарушений процесса выработки у студента требуемых норм мировоззрения реализуются лишь по последствиям информационно-психологического воздействия	ОН
Реализуемость функций контроля признаков дезинформации в информационном обеспечении воспитательного процесса	
Реализуются подразделением, осуществляющим воспитательную работу	ОВ
Реализуются учебным управлением образовательного учреждения	В
Реализуются должностными лицами	ВС
Реализуются руководством учебных подразделений	С
Реализуются режимным подразделением	НС
Реализуются профильной кафедрой	Н
Не реализуются	ОН

Таблица 5. Характеристические оценки защищенность информационного обеспечения воспитательного процесса от дезинформации

Состояние обеспеченности характеризуемого свойства	**Оценка**
Мероприятия по выявлению и блокированию источников угроз дезинформации реализуются	В
Мероприятия по выявлению и блокированию источников угроз дезинформации не реализуются	Н

Примером таблицы решений для оценки защищенности информации учебно-методического обеспечения образовательного процесса является таблица 6.

Аналогичным образом строятся таблицы решений для оценки всех остальных вторичных характеристик защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности, включая показатель защищенности.

Из изложенного следует, что результативность предложенного методического подхода к оценке защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности является предпосылкой его практического использования.

Таблица 6. Оценка защищенности информации учебно-методического обеспечения образовательного процесса

Наименование характеристик обеспечения состояний защищенности информации	**Оценка**	**Оценка защищенности информации учебно-методического обеспечения**
Представление документированных требований к реализации мер обеспечения конфиденциальности информации	ВС	ВС
Реализуемость процедур разграничения полномочий доступа к информации при работе с программными средствами специального назначения	С	
Реализуемость функций защиты информации от утечки по техническим каналам	ВС	
Выполнение функций контроля достоверности и целостности информации	В	
Выполнение функций восстановления целостности информации	В	

Заключение

В статье обоснован и практически реализован методический подход к оценке защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности на основе систематизации характеристик возможностей по обеспечению безопасности информации в процессе такого рода деятельности.

Разработана методика систематизации характеристик возможностей по обеспечению безопасности информации в процессе образовательной деятельности по подготовке специалистов в области информационной безопасности. В соответствии с данной методикой предложено:

– совокупность характеристик возможностей по обеспечению безопасности информации в процессе образовательной деятельности по подготовке специалистов в области информационной безопасности представлять в виде иерархической структуры с последовательным обобщением этих возможностей

– уровни данной структуры представлять в виде подмножеств характеристик, соответствующих определенным классификационным основаниям;

– в качестве аппарата для формализации логики оценок целесообразно использовать характеристические таблицы и таблицы решений.

Полученные результаты позволяют практически оценить целесообразность проведения мероприятий по обеспечению безопасности информации в процессе образовательной деятельности по подготовке специалистов в области информационной безопасности.

Разработанная методика может рассматриваться как методическое обеспечение решения практической задачи оценки защищенности образовательной деятельности по подготовке специалистов в области информационной безопасности.

Предложенный в статье методический подход позволяет исследовать деятельность по обеспечению безопасности информации в широком диапазоне параметров.

СПИСОК ЛИТЕРАТУРЫ:

1. Булдакова Т.И., Карпенко А.П., Рудаков И.В. Особенности подготовки кадров по информатике и вычислительной технике / В сборнике: Перспективные направления развития отечественных информационных технологий. Материалы IV межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. 2018. С. 339–341.
2. Скрыль С.В., Ле Ву Хыонг Занг, Нгуэн Тхань Ньян. Показатели эффективности процесса подготовки специалистов // Вестник Воронежского института МВД России. – Воронеж: Воронежский институт МВД России, 2015. №. 3. С. 64–71. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-protsessa-podgotovki-spetsialistov/viewer (дата обращения: 07.10.2020).
3. Скрыль С.В., Пономарев В.А., Хыонг Занг Ле Ву. Математические модели комплексной оценки качества деятельности по подготовке специалистов технического профиля в высших учебных заведениях. // Промышленные АСУ и контроллеры. – М: Научтехлитиздат, 2016. №10. С. 8–16. URL: https://elibrary.ru/item.asp?id=27180767 (дата обращения: 07.10.2020)
4. Зеленцова Е.В., Ле Ву Хыонг Занг и др. Методические положения по реализации процедур систематизации характеристик качества подготовки специалистов // Научный взгляд: труды международной научно-практической конференции. – М.: Московский государственный областной университет, 2015. С. 225–230.
5. Скрыль С.В., Ле Ву Хыонг Занг и др. Структура системы характеристик качества деятельности по подготовке специалистов в высших учебных заведениях // Промышленные АСУ и контроллеры. – М: «Научтехлитиздат», 2016. №9. С. 11–15. URL: https://elibrary.ru/item.asp?id=26702710 (дата обращения: 07.10.2020).
6. Dortman, Svetlana, Информационная безопасность ребенка, как субъекта образовательного процесса /Защита детства: проблемы, поиски, решения // Сборник материалов Всероссийской научно-практической конференции, приуроченной к Десятилетию детства в России. 2018. С. 315–319. URL: https://ssrn.com/abstract=3469614 (дата обращения: 07.10.2020). DOI: http://dx.doi.org/10.25791/asu.1.2020.1118.
7. Скрыль С.В. и др. Математическая модель для оценки эффективности подготовки специалистов по информационной безопасности на основе временных характеристик образовательного процесса // Промышленные АСУ и контроллеры. – М: «Научтехлитиздат», 2020. №1. С. 28–35. DOI: http://dx.doi.org/10.25791/asu.1.2020.1118.
8. Надеждин Е.Н., Шептуховский В.А. Методика оценивания рисков информационной безопасности в вычислительных сетях образовательных учреждений // Педагогическая информатика. 2012. № 4. С. 84–92.
9. Надеждин Е.Н., Шептуховский В.А. Алгоритмический подход к оценке рисков информационной безопасности образовательных учреждение // Научный поиск. 2013. №2.5. С. 23–27.
10. Щербаков Н. П. Совершенствование системы оценки качества высшего образования /Н.П. Щербаков // Гарантии качества профессионального образования: тезисы докладов международной научно-практической конференции / [редкол.: Я.Л. Овчинников и др.]. Барнаул: Изд-во АлтГТУ, 2015. С. 9–11.
11. Гузаиров М.Б., Машкина И.В., Степанова Е.С. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. №2. С. 37–49.
12. Rabai L.B., Rjaibi N., Aissa A.B. (2012) Quantifying security threats for E-learning systems. DOI: http://dx.doi.org/10.1109/ICEELI.2012.6360592.
13. Skryl’ S. et al. (2019) Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A., Groumpos P., Shcherbakov M., Kultsova M. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol 1084. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-29750-3_20.
14. Долженко А.И., Потапов Л.И. Анализ информационной безопасности образовательного процесса университета на базе нечетких моделей / SOFT MEASUREMENTS AND COMPUTING. Vol. 30, No. 5, 2020. P. 32–40. URL: https://elibrary.ru/item.asp?id=43929605 (дата обращения: 20.10.2020).
15. Горбатов, Виктор Сергеевич и др. Постановка задачи по реализации доверенного сеанса связи при дистанционном обучении. Безопасность информационных технологий, [S.l.]. Т. 20, № 3. С. 104–105, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/328 (дата обращения: 07.10.2020).
16. Тулиганова Л.Р., Павлова И. А., Машкина И.В. Разработка моделей объекта защиты и угроз нарушения безопасности в информационной системе, базирующейся на технологии виртуализации // Известия ЮФУ. Технические науки № 8 (157). – Таганрог: Изд-во ТТИ ЮФУ, 2014. С. 32–41.

REFERENCES:

[1] Buldakova T.I., Karpenko A.P., Rudakov I.V. Features of training in computer science and engineering. In the collection: Perspective directions of development of domestic information technologies. materials of the IV interregional scientific and practical conference. Sevastopol state University; scientific ed. by B. V. Sokolov. 2018. P. 339–341 (in Russian).

[2] Skryl' S.V., Le Vu Huong Zang, Nguyen Thanh Nyan Productive characteristics of the specialists' preparation. The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia. 2015. Vol. 3. P. 64–71. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-protsessa-podgotovki-spetsialistov/viewer (accessed: 07.10.2020) (in Russian).

[3] Skryl' S.V., Ponomarev V.A., Hyong Zang Le Vu, Ivanova O.G. Mathematical models of comprehensive evaluation of the quality of the preparation of technical specialists in higher educational institutions. Industrial Automatic Control Systems and Controllers. Scientific & Technical Literature Publishing House «NAUCHTECHLITIZDAT». 2016. Vol. 10. P 8–16. URL: https://elibrary.ru/item.asp?id=27180767 (accessed: 07.10.2020) (in Russian).

[4] Zelentsova E.V., Le Vu Hyong Zang et. al. Methodical recommendations on systematic procedure of the specialists' preparation quality features // Scientific view: The International scientific-practical conference proceedings. – M.: Moscow State Regional University, 2015. P. 225–230 (in Russian).

[5] Skryl' S.V., S.A. Barkalov, Le Vu Hyong Zang, V.A. et al. System Structure Characteristics of Quality Activities in Specialists' Preparation in Higher Education Institutions. Industrial Automatic Control Systems and Controllers. Scientific & Technical Literature Publishing House «NAUCHTECHLITIZDAT». 2016. Vol. 9. P. 11–15. URL: https://elibrary.ru/item.asp?id=26702710 (accessed: 07.10.2020) (in Russian).

[6] Dortman, Svetlana Information Security of the Child as a Subject of the Educational Process // Protection of childhood: problems, searches, solutions collection of materials of the all-Russian scientific and practical conference dedicated to the Decade of childhood in Russia. 2018. P. 315–319. URL: https://ssrn.com/abstract=3469614 (accessed: 07.10.2020) (in Russian).

[7] Skryl' S.V. et al. Mathematical model to assess the effectiveness of training specialists in information security based on time characteristics of the educational process. Industrial Automatic Control Systems and Controllers. Scientific & Technical Literature Publishing House «NAUCHTECHLITIZDAT». 2020. Vol. 1. P. 28–35. DOI: http://dx.doi.org/10.25791/asu.1.2020.1118 (in Russian).

[8] Nadezhdin E.N., Sheptuhovsky V.A. Methodical method for information security risks assessing in computer networks of educational institutions. Educational Informatics. 2012. № 4. P. 84–92. DOI: http://dx.doi.org/10.25791/asu.1.2020.1118 (in Russian).

[9] Nadezhdin E.N., Sheptuhovsky V.A. Algorithmic approach to assessing information security risks in educational institutions // Scientific research. 2013. №2.5. P. 2–27 (in Russian).

[10] Tscherbakov N.P. Improving the quality assessment system of higher education. N.P. Tscherbakov. Quality assurance of professional education: abstracts of reports of the international scientific and practical conference [ed.: Ya. L. Ovchinnikov et al.]. Barnaul: AltSTU Publishing house,2015. P. 9–11 (in Russian).

[11] Guzairov M.B., Mashkina I.V., Stepanova E.S. Building a threat model using fuzzy cognitive maps based on network security policy. ITSecurity. 2011. № 2. P. 37–49 (in Russian).

[12] Rabai L.B., Rjaibi N., Aissa A.B. (2012) Quantifying security threats for E-learning systems. DOI: https://doi.org/10.1109/ICEELI.2012.6360592.

[13] Skryl' S.V. et al. (2019) Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A.G. et. al. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol 1084. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-29750-3_20.

[14] Dolzenko A.I., Potapov L.I. Analysis of information security of the University educational process based on fuzzy models / SOFT MEASUREMENTS AND COMPUTING. Vol. 30, No. 5, 2020. P. 32–40. URL: https://elibrary.ru/item.asp?id=43929605 (accessed: 07.10.2020).

[15] Gorbatov, Victor Sergeevich et al. Statement of the Problem on Implementing a Trusted Communications Session in E-learning Systems. IT Security (Russia), [S.l.]. Vol. 20. No. 3. P. 104–105, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/328 (accessed: 07.10.2020) (in Russian).

[16] Tuliganova L.R., Pavlova I.A., Mashkina I.V. Development of models of the protection objects and security threats in an information system based on virtualization technology. News of the southern Federal University. Technical Studies № 8 (157). Taganrog, 2014. P. 32–41 (in Russian).

Поступила в редакцию – 07 октября 2020 г. Окончательный вариант – 01 ноября 2020 г.
Received – October 07, 2020. The final version – November 01, 2020.

Сергей Е. Парьев[1], Дмитрий И. Правиков[2], Владимир Г. Карантаев[3]
[1]Независимый эксперт
[2]Российский государственный университет
(национальный исследовательский университет) имени И.М. Губкина
Ленинский пр-кт, 65, корп. 1, Москва, 119991, Россия
[3]Центр НТИ МЭИ
ул. Красноказарменная, 17, Москва, 111250, Россия
[1]e-mail: sergey.pariev@mail.ru, https://orcid.org/0000-0001-5698-7471
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: vladimir.karantaev@gmail.com, https://orcid.org/0000-0003-1628-7635

ОСОБЕННОСТИ ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

DOI: http://dx.doi.org/10.26583/bit.2020.4.04

Аннотация. В статье анализируется взаимосвязь понятия «безопасность» с производными понятиями. Выделена объективная научно-практическая потребность в научном и регуляторном закреплении термина «кибербезопасность», дано его определение. В результате анализа перспективных подходов к обеспечению безопасности отмечена сохраняющаяся актуальность риск-ориентированного подхода. При этом в качестве методов оценки рисков кибербезопасности в ближайшей перспективе будут рассматриваться экспертные методы на основе возможного ущерба. Сделан вывод о необходимости развития инструментов автоматизации оценки рисков кибербезопасности при применении инженерных методик расчета cyberPHA, Security PHA Review и других. В академическом плане наиболее приоритетным направлением исследований остается проблема разработки моделей вычисления вероятности наступления рисков кибербезопасности в киберфизических системах.

Ключевые слова: кибербезопасность, комплексная безопасность, оценка рисков, риск-ориентированный подход, киберфизические системы, АСУ ТП.
Для цитирования: ПАРЬЕВ, Сергей Е.; ПРАВИКОВ, Дмитрий И. Правиков; КАРАНТАЕВ, Владимир Г. ОСОБЕННОСТИ ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 37–52, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1304>. Дата доступа: 20 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.04.

Sergey E. Pariev[1], Dmitry I. Pravikov[2], Vladimir G. Karataev[3]
[1]Independent expert, Russia
[2]National University of Oil and Gas «Gubkin University»,
Leninsky av. 65, bd. 1, Moscow, 119991, Russia
[3]Center for Scientific and technical information of the Moscow power engineering Institute (MEI)
17 Krasnokazarmennaya str., Moscow, 111250, Russia
[1]e-mail: sergey.pariev@mail.ru, https://orcid.org/0000-0001-5698-7471
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: vladimir.karantaev@gmail.com, https://orcid.org/0000-0003-1628-7635

Features of the risk-based approach to ensure cyber security of industrial facilities

DOI: http://dx.doi.org/10.26583/bit.2020.4.04

Abstract. We analyze a relationship between the concept of "security" and derived concepts. The objective scientific and practical need for scientific and regulatory consolidation of the term "cybersecurity" is highlighted, and its definition is given. As a result of the analysis of promising approaches to security, the

risk-based approach remains relevant. At the same time, expert methods based on possible damage will be considered as methods for assessing cybersecurity risks in the near future. It is concluded that it is necessary to develop tools for automating cybersecurity risk assessment when using engineering calculation methods cyberPHA, Security PHA Review, and others. In academic terms, the most priority area of research remains the problem of modeling and developing models for calculating the probability of occurrence of cybersecurity risks in cyberphysical systems.
Keywords: cybersecurity, risk assessment, risk-oriented approach, IACS, ICS, cyber physical systems, integrated safety and security.
For citation: PAREVE, Sergey E.; PRAVIKOV, Dmitry I.; KARATAEV, Vladimir G. Features of the risk-based approach to ensure cyber security of industrial facilities IT Security (Russia), [S.l.], v. 27, n. 4, p. 37–52, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1304>. Date accessed: 20 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.04.

Введение

В общем случае безопасность можно трактовать достаточно широко и для того, чтобы очертить предмет дальнейшего рассмотрения, сформулируем ряд исходных постулатов.

Объектом исследования выбрана безопасность промышленного объекта, оснащенного средствами автоматизации технологических (например, АСУ ТП) и вспомогательных процессов. Далее такой объект мы будем называть защищаемым объектом. В соответствии с ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования» *безопасность защищаемого объекта* – состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру(ам), ландшафтной архитектуре; окружающей природной среде.

Традиционно по отношению к указанным выше составляющим защищаемого объекта, рассматриваемого как социотехническая система, – физическим лицам, имуществу, оборудованию, окружающей среде рассматривались угрозы различного вида (технические сбои; пожары; информационные, химические, бактериологические, радиационные виды воздействий и т.д.), противодействие которым обеспечивал соответствующий «вид безопасности». Вместе с тем, усложнение структуры самих защищаемых объектов, процессов, работу которых они обеспечивают, а также широкое внедрение средств автоматизации и информатизации в различные подсистемы, в том числе в подсистемы обеспечения безопасности, привело к тому, что различные виды безопасности начали тесно переплетаться.

Помимо «видов безопасности», связанных с соответствующим видом угроз (например, пожарная безопасность) используются и «виды безопасности», в которых во главу угла ставится тип защищаемого объекта или вида деятельности. Например, охрана труда (как вид безопасности) нацелена в первую очередь на защиту жизни и здоровья сотрудников предприятия от любых негативных воздействий, а охрана окружающей среды – соответственно на защиту окружающей среды также от любого негативного воздействия. Наличие таких двух групп «видов безопасности», которые по сфере своего применения имеют множественные пересечения, еще больше запутывает картину их взаимосвязей.

В российской научной литературе предлагался подход, определяемый как комплексная безопасность, и описанный, в частности, в [1]. Суть данного подхода можно описать следующим образом. Безопасность современного предприятия, например, предприятия ТЭК рассматривается как комплекс безопасностей: функциональной, производственной, физической, пожарной, химической, информационной и т.д. При этом,

по каждому направлению безопасности на современном предприятии развертывается система, обеспечивающая мониторинг состояния объекта, своевременное выявление предпосылок к нарушению безопасности, обработку событий безопасности (фильтрацию, нормирование, обогащение, реагирование и др.), расследование и ликвидацию последствий, а также своевременное информирование персонала. По отдельным направлениям система безопасности может автоматически включать средства нейтрализации угроз, например, средства пожаротушения. Перечисленные системы, как правило, создаются с использованием программно-аппаратных средств, которые в свою очередь подвержены угрозам информационной безопасности.

Необходимо отметить, что комплексный характер безопасности на более высоком, междисциплинарном уровне рассматривался раньше в других работах, например, [2]. При этом на уровне технической реализации под комплексными системами безопасности, как правило, понимались интегрированные системы пожарной и охранной сигнализации, управления доступом, системы видеонаблюдения и т.п. [3].

Изучение зарубежного опыта, в частности применительно к предприятиям в нефтегазовой отрасли, показывает, что в настоящее время понятие безопасности также начинает носить комплексный характер так, как это было отмечено в [1]. Так, например, на рис. 1 показано, на какие документы опираются методические рекомендации, подготовленные Cisco, Schneider Electric и Aveva, для защиты (в части кибербезопасности) нефте- и газопроводов[1].

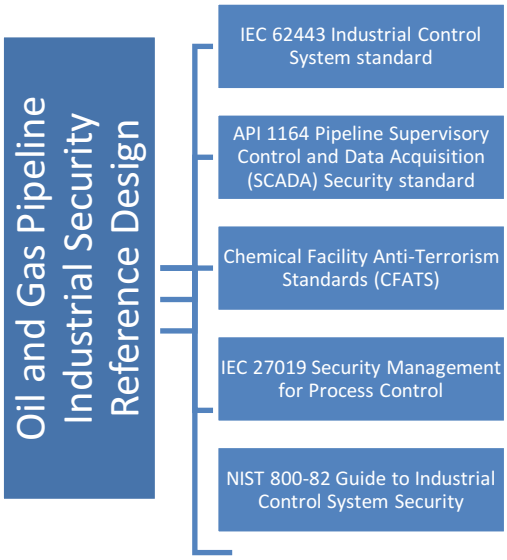

Рис. 1. Методическая основа рекомендаций по безопасности нефте- и газопроводов
(Fig. 1. Methodological basis of recommendation for security of the oil and gas pipe lines)

Осознание факта связанности «отдельных видов безопасности» привело к тому, что стали больше говорить о безопасности «в целом» (или «комплексной безопасности»). По нашему мнению, это понимание получило свое отражение и в последних российских нормативных документах. В частности, можно отметить Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в названии которого использован именно термин «безопасность», а не «информационная безопасность». В ст. 1 ФЗ-187 при определении целей закона акцент сделан на

[1]URL:https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/Security-IRD.pdf (accessed: 08.10.2020).

«устойчивости функционирования» объектов критической инфраструктуры как цели обеспечения безопасности, а не на традиционном для информационной безопасности сохранении конфиденциальности, целостности и доступности информации. Это говорит о комплексности охватываемой этим документом проблематики и о возможном желании авторов документа привести рассматриваемые угрозы (т.е. компьютерные атаки) к общему знаменателю с другими видами угроз.

Данный подход разделяется и другими исследователями, которые отмечают, что под критической информационной инфраструктурой понимаются системы, нарушение работы которых приведет к неблагоприятным последствиям, а именно нарушение или остановка деятельности и/или нарушение безопасности информации [4], т.е. негативное воздействие не обязательно связано с воздействием на информацию.

Уточним, что в нашем понимании «устойчивость функционирования» защищаемого объекта – это способность объекта сохранять свои основные функции с заданным качеством (в заданных пределах) под воздействием деструктивных факторов (в частности, под воздействием компьютерных атак). При этом не должно оказываться негативного влияния, выходящего за заранее заданные пределы, на жизнь и здоровье персонала, населения, на окружающую среду и т.д.

В данной статье ограничимся рассмотрением только такого вида негативного воздействия на защищаемый объект как компьютерные атаки, т.е. актов целенаправленного предумышленного или непредумышленного воздействия на информатизированные и (или) автоматизированные подсистемы защищаемого объекта посредством программных и (или) программно-аппаратных средств.

Может показаться, что критериями обеспечения безопасности защищаемого объекта являются такие параметры как количество атак на объект, количество отраженных атак, количество пропущенных атак. Однако они вторичны и, более того, могут давать ложное ощущение защищенности. Основным критерием может быть только нахождение/не нахождение объекта в определенном состоянии (наборе состояний), в котором он способен продолжать функционировать в допустимых пределах (это могут быть, в том числе, и какие-то деградированные состояния), т.е. исполнять свои основные функции с заданным качеством и при этом продолжать обладать способностью отражать, ограничивать и бороться с последствиями воздействия деструктивных факторов.

Исходя из изложенного, дадим определение кибербезопасности защищаемого (промышленного) объекта. Кибербезопасность защищаемого (промышленного) объекта – все аспекты, связанные с определением, достижением и поддержанием состояния безопасности защищаемого объекта, при котором обеспечивается его устойчивое функционирование в условиях проведения в отношении него компьютерных атак.

Необходимо отметить, что приведенное определение весьма сходно с другим определением кибербезопасности, приведенным в [5]: «кибербезопасность – безопасность защищаемого объекта, системы которого функционируют в условиях деструктивных информационных воздействий».

Аналогичный подход к определению кибербезопасности рассматривался в [6]: «Цифровая трансформация промышленного уклада привела к эволюции понятия «информационная безопасность», превратив его в понятие «кибербезопасность», в основе которого лежит не столько обеспечение конфиденциальности, целостности и доступности информации, сколько защита автоматизированных и киберфизических систем от компьютерных атак. Для таких систем сохранение способности к корректному функционированию в условиях киберугроз является приоритетной задачей».

Отличием предлагаемого авторами определения от сформулированных ранее определений кибербезопасности является выделение не только свойства устойчивого функционирования защищаемого объекта, но и состояние его безопасности, а также негативных воздействий на его окружение.

В качестве итогов рассмотрения понятий безопасности их взаимосвязь представлена на рис. 2.

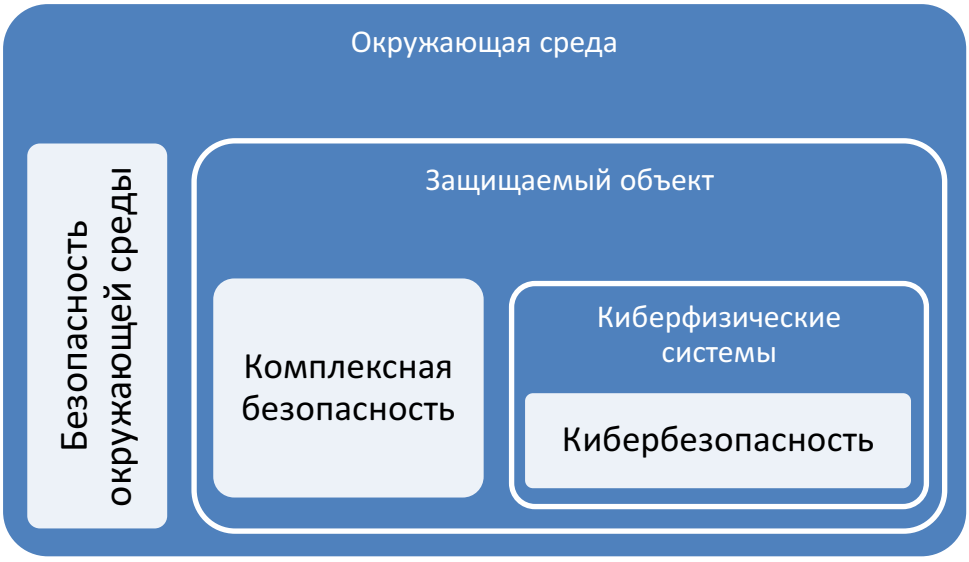

Рис. 2. Взаимосвязь понятий безопасности
(Fig. 2. Interrelation of the notions of security)

1. Риск-ориентированный подход в обеспечении информационной безопасности

Наличие свойства безопасности у защищаемых объектов обуславливает поиск путей достижения (обеспечения) указанного свойства. В качестве наиболее перспективного как за рубежом, так и в Российской Федерации, рассматривается риск-ориентированный подход, давно применяемый для обеспечения различных видов безопасности, в том числе для обеспечения безопасности критической информационной инфраструктуры [7]. Тем не менее, его применение к обеспечению кибербезопасности имеет свои особенности.

Краеугольным камнем риск-ориентированного подхода является оценка рисков, поэтому в последнее время в Российской Федерации начали подниматься вопросы развития методических подходов по оценке рисков кибербезопасности промышленных объектов [8].

Системное обсуждение назрело по целому ряду причин:

- отсутствие официальных методик оценки риска, оценки угроз безопасности информации, а тем более угроз кибербезопасности. Одним из значимых шагов в этом направлении стало Постановление Правительства РФ от 08.02.2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры …», в котором были введены критерии значимости (фактически это виды негативных последствий, которые относятся как к самому предприятию, так и населению, окружающей среде и государству) и был задан в общем виде процесс выявления и оценки этих критериев, что в целом представляет собой процесс оценки рисков. Однако говорить о готовой методике оценки рисков, конечно, не представляется возможным. В последнее

время начали появляться отдельные отраслевые методики категорирования, но пока они также носят довольно общий характер;

- всё большая зависимость рисков HSE (Health, Safety & Environmental) – зарубежный аналог, покрывающий промышленную безопасность, охрану труда и безопасность окружающей среды, связанную с жизнедеятельностью промышленного объекта) от рисков кибербезопасности, практически никак не отраженная в нормативной и методической базе;
- слабость или полное отсутствие отраслевых методических подходов, которые бы создавали «систему координат» для всех участников процесса: компаний реального сектора экономики, поставщиков решений и услуг, разработчиков средств защиты информации и средств автоматизации промышленных объектов;
- нормативно технические требования, относящиеся к разным видам безопасности не гармонизированы между собой.

Рассматривая методические подходы по оценке рисков кибербезопасности промышленных объектов невозможно обойти стороной обсуждение ряда международных документов:

- IEC 62443-2-1 (2010);
- ISO/IEC 27001 (2013);
- ISA TR84.00.09 (2017).

Необходимо отметить, что семейство стандартов 62443 в русскоязычных научных статьях в основном упоминалось, но детально не анализировалось. Из известных работ можно отметить [9], в которой рассматривались вопросы построения защищенной архитектуры АСУ ТП. За рубежом, очевидно в силу более активного использования, можно отметить руководство по стандарту 62443 [2].

Стандарт ISO/IEC 27001 в русскоязычных научных работах по сравнению с семейством стандартов 62443 рассмотрен более глубоко. В качестве примера можно привести [9]. Из зарубежных источников можно отметить соответствующее руководство по анализу угроз[3].

Стандарт ISA TR84.00.09 в русскоязычных научных источниках практически не упоминается, поэтому его рассмотрение велось на основании материалов, находящихся в открытом доступе[4].

Рассмотрим более детально принципы, заложенные в серию стандартов ISA/IEC 62443. На рис. 3 представлен текущий статус разработки серии стандартов ISA/IEC 62443.

Второй документ серии ISA/IEC 62443 гармонизирован в Российской Федерации в виде национального стандарта ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики», который посвящен методическим вопросам построения системы управления кибербезопасностью промышленного объекта (если более точно, то рассматривается не весь промышленный объект, а только его система автоматизации и технологического управления) и базируется на применявшихся ранее

[2]Quick Start Guide: An Overview of the ISA/IEC 62443 Standards. URL: https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards (accessed: 31.03.2020).
[3]Cyber-related process hazard analysis. URL: https://www.isa.org/templates/news-detail.aspx?id=160155 (accessed: 31.03.2020).
[4]Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: https://youtu.be/8oZGYcRDjzc (accessed: 31.03.2020).

стандартах построения систем менеджмента в ИТ системах: ИСО/МЭК 17799 и ИСО/МЭК 27001.

			Название	Дата
Обзор	1-1	TS	Терминология, концепции и модели	2007
	1-2	TR	Основной список терминов и сокращений	
	1-3		Показатели эффективности систем кибербезопасности	
	1-4		Жизненный цикл безопасности и сценарии использования систем промышленной автоматики и контроля (IACS)	
Политика и процедуры	2-1	IS	Создание программы обеспечения безопасности систем промышленной автоматики и контроля (IACS)	2009
	2-2		Основные параметры программ безопасности систем промышленной автоматики и контроля (IACS)	2022
	2-3	TR	Управления обновлениями программного обеспечения (ПО) в среде систем промышленной автоматики и контроля (IACS)	2015
	2-4	IS	Требования к программам безопасности для поставщиков услуг систем промышленной автоматики и контроля (IACS)	2018
	2-5	TR	Руководство по внедрению для владельцев активов систем промышленной автоматики и контроля (IACS)	
Системы	3-1	TR	Технологии безопасности для систем промышленной автоматики и контроля (IACS)	
	3-2	IS	Оценка рисков безопасности, системное разделение и уровни безопасности	2020
	3-3	IS	Требования к безопасности системы и уровни безопасности	2013
Компонент	4-1	IS	Требования к жизненному циклу разработки безопасности продукта	2018
	4-2	IS	Технические требования безопасности для компонентов систем промышленной автоматики и контроля (IACS)	2019

Рис. 3. Статус разработки серии стандартов ISA/IEC 62443
(Fig. 3. Status of development of the standard series IEC 62443)

Стандарт, фактически, фиксирует происходящие перемены, связанные с технологиями, которые находят все более массовое использование во вновь создаваемых и модернизируемых промышленных объектах. Речь идет о, так называемых, готовых коммерческих технологиях (COTS Software – Commercial Off-The-Shelf Software), использование которых сильно повышает риски кибербезопасности.

Согласно стандарту система управления кибербезопасностью (Cyber Security Management System – CSMS) промышленного объекта состоит из элементов, относящихся к трем основным категориям:

- анализ рисков;
- устранение риска при помощи CSMS;
- контроль и усовершенствование CSMS.

В свою очередь категория «анализ рисков» включает:

- экономическое обоснование;
- выявление, классификация и оценка рисков.

В категории «выявление, классификация и оценка рисков» стандарт представляет 14 обобщенных требований к работам, связанным с оценкой рисков. Отмечается, что могут применяться количественные и качественные методы оценки, при этом делается вывод о том, что в виду отсутствия накопленной статистики инцидентов на текущем этапе целесообразно применять качественные (экспертные) методы.

Требования к процессу оценки рисков детализируется в проекте международного стандарта IEC 62443-3-2 ED1 «Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design», принятого в виде окончательного документа в 2020 г.

Место стандартов МЭК 62443-2-1 и МЭК 62443-3-2 в общей иерархии серии IEC 62443 представлено на рис. 4.

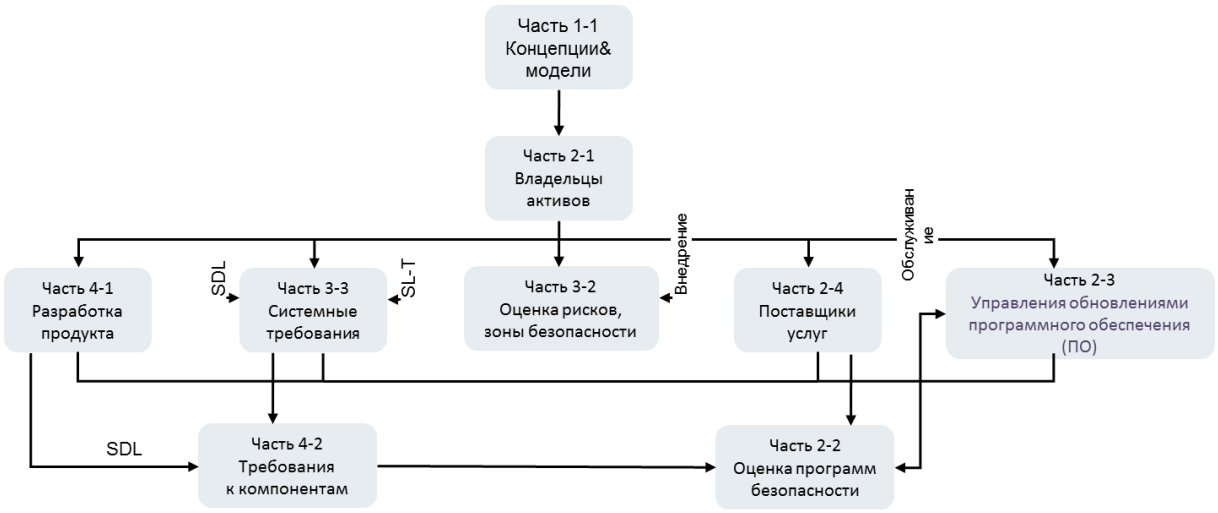

Рис. 4. Общая структура серии стандартов ISA/IEC 62443
(Fig. 4. A structure of the standard series ISA/IEC 62443)

Описание процесса оценки рисков кибербезопасности промышленного объекта приведено на рис. 5.

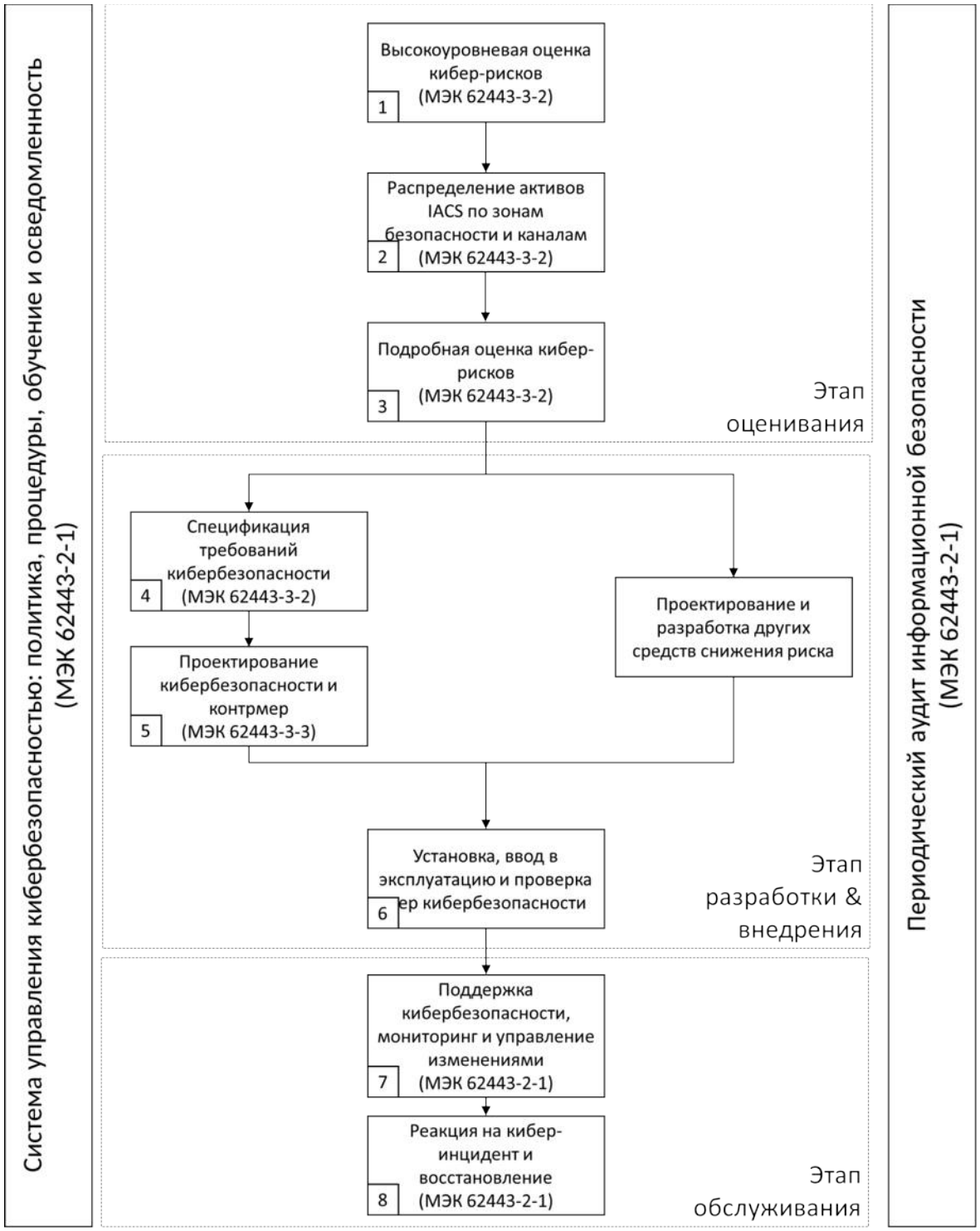

Рис. 5. Процесс оценки рисков кибербезопасности системы автоматизации и технологического управления промышленного объекта ISA/IEC 62443-3-2
(Fig. 5. Process of cybersecurity risk assessment of Industrial Automation and Control System of Industrial object ISA/IEC 62443-3-2)

Подтверждением выше сформулированного тезиса о том, что сообщество специалистов задумалось о «комплексной безопасности» является вектор развития другого международного стандарта IEC 61511.

Вторая редакция IEC 61511-1 (2016) «Functional safety. Safety instrumented systems for the process industry sector. Part 1. Terms, definitions and technical requirements» требует проводить оценку рисков с целью выявления уязвимостей систем противоаварийной защиты (ПАЗ, SIS – Safety Instrumented System). Вместе с тем стандарт не содержит подробных требований по оценке рисков, но п. 8.2.4. содержит ссылки на документы, применение которых позволит реализовать это требование.

Наибольший интерес из них вызывает новая редакция технического отчета ISA TR84.00.09 (2017), который на данный момент является одним из самых полных документов, описывающих реализацию требований по обеспечению кибербезопасности ПАЗ на всех стадиях жизненного цикла систем. Документ ISA TR84.00.09 (2017) содержит положения IEC 62443 и NIST «Cybersecurity Framework». В российском нормативном поле подобных документов, к сожалению, не разработано.

Таким образом, приведенный краткий обзор международных нормативно технических документов позволяет утверждать, что методическая база для оценки HSE-рисков с учетом оценки рисков кибербезопасности сформировалась. Методическая база объединяет как количественные, так и качественные методы анализа. Динамика работы и сформированные планы по развитию международных документов всех типов в ISA и IEC позволяет сделать вывод, что данный методический подход будет развиваться и далее.

2. Пример метода оценки рисков HSE, учитывающего риски кибербезопасности

Можно утверждать, что в международной практике сформировался подход Cyber Process Hazard Analysis (Cyber PHA), основанный на классическом подходе к выявлению, оценке и управлению опасностями технологического процесса – PHA (Process Hazard Analysis), но включающем в себя и аспекты, связанные с рисками кибербезопасности.

Так, например, в рамках одной из ведущих конференций S4[5], проходившей в США в 2017 г. компания aeSolutions представляла этот подход, а в 2018 г. в рамках конференции «Промышленная кибербезопасность: цифровая трансформация – вызовы и возможности»[6] американская компания Kenexis представила еще одну практическую модификацию классического подхода под названием Security PHA Review.

Особый интерес вызывает востребованность данных подходов и соответствующих услуг в реальном секторе экономики, в частности в США. В 2019 г. на форуме ARC Industry Forum, компания Shell представила доклад[7], в котором был представлен практический опыт компании, по совместному применению методик оценки HSSE-рисков (Health, Safety, Security and Environment) традиционными методиками оценки, используемыми в рамках PHA: HAZOP и LOPA и методики оценки рисков кибербезопасности (Security Risk Assessment).

Практическая деятельность компании Shell, основана на реализации положений технического отчета ISA-TR84.00.09. Компания Shell также называет свой подход Cyber PHA, который основан на оценке факторов эскалации, приводящих к нарушению целостности функций безопасности, реализуемых защитными барьерами, в частности ПАЗ

[5]Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: https://youtu.be/ (accessed: 31.03.2020).
[6]Security PHA review for analyzing process plant vulnerability to cyberattack. URL: https://youtu.be/QnfBRlgBaHg, URL: https://ics.kaspersky.ru/media/ics-conference-2018/Edward-Marszal-Security-PHA-review-for-analyzing-process-plant-vulnerability-to-cyberattack-En.pdf (accessed: 31.03.2020).
[7]Cyber-related process hazard analysis. URL: https://www.isa.org/templates/news-detail.aspx?id=160155 (accessed: 31.03.2020).

(SIS), вследствие возможного наличия актуальных угроз кибербезопасности (сценариев эксплуатации уязвимостей), которые есть или могут быть в программно-аппаратных комплексах применяемых средств автоматизации. В рамках представленного подхода оцениваться не только HSSE риски, но и риски коммерческих потерь (в данной части риски, не связанные с реализаций угроз safety), репутационных потерь, рисков снижения эффективности функционирования защитных барьеров. Данный подход сочетает применение количественных и качественных методов анализа. Для визуализации процесса применяется модель «галстук-бабочка». Пример такой модели представлен на рис. 6.

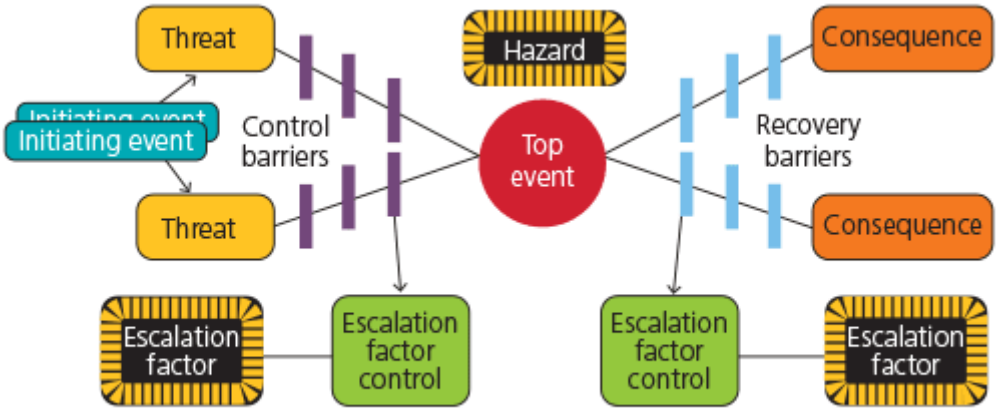

Рис. 6. Модель процесса анализа рисков «галстук-бабочка»
(Fig. 6. Model of the "bow tie" risk analysis process)

3. Проблематика риск-ориентированного подхода

Помимо преимуществ, описанных выше, и, несмотря на достаточную распространенность, накопленный практический опыт позволил выявить также ряд ограничений и недостатков текущих методик применения риск-ориентированного подхода. Ограничения связаны с тем, что в настоящее время информатизация затрагивает практически все основные процессы современного предприятия. В результате возникают сложные цепочки типа: «пожарная безопасность влияет на состояние вычислительной среды, безопасность вычислительной среды влияет на промышленную и, как следствие, экологическую безопасность» и просчитать риски в отдельных ситуациях становится затруднительно. Более того, режим реального времени работы многих функциональных систем и систем их защиты практически отсекает человека от принятия тактических решений, а значит и непосредственного управления рисками.

Одной из проблем применения риск-ориентированного подхода является проблема определения вероятности наступления риска. Вероятность хорошо оценивается для физических детерминированных процессов с более-менее устойчивым распределением вероятности различных событий (например, для физических отказов оборудования). Но определение вероятности для разных типов атак (или использования разного рода технических приемов нарушителем) представляется практически невозможным. Более того, сама постановка такой задачи является некорректной из-за самой природы рисков кибербезопасности. Попытки определения вероятности наступления рисков рассматривались, в частности, в [11].

В настоящее время подходы к определению вероятности наступления определенного события сводятся либо к анализу статистики предыдущих периодов, либо к применению экспертного метода.

Одной из трудностей получения достоверных статистических данных по компьютерным инцидентам является тот факт, что реальные инциденты в промышленных системах в настоящее время сравнительно редки (а большая часть, скорее всего, не замечается, либо приписывается физическим отказам, а то и замалчивается) и собрать даже для однотипных промышленных объектов какую-либо релевантную статистику по реальным инцидентам практически невозможно.

Следует отметить, что после принятия Федерального закона № 116-ФЗ «О промышленной безопасности опасных производственных объектов» в качестве актуальной научной задачи рассматривалась разработка и внедрение в отечественную практику научно обоснованных методов анализа и оценки техногенного риска, позволяющих всесторонне оценить возникновение чрезвычайных ситуаций на опасном производственном объекте. В работе [12] отмечено, что «основная проблема количественного анализа риска опасного производственного объекта на основе методов теории вероятности, математической статистики и др. связана с нахождением частотной оценкой возникновения чрезвычайной ситуации вследствие неопределённости исходных данных».

Даже оставляя за скобками отсутствие в данный момент накопленной и статистически релевантной информации по инцидентам, вероятностный подход имеет и куда более серьезные недостатки. Использование статистики предыдущих периодов подразумевает определенную устойчивость распределения вероятности, причем устойчивость не только во времени, но и по месту (объекту, типу объекта). Предположим, известно, что в мире есть единственная преступная группа, которая на протяжении 10 лет раз в год атакует один из 1000 однотипных защищаемых объектов с использованием эксплойтов в определенном сетевом сервисе. Какова вероятность, что в следующем году выбранный защищаемый объект будет атакован? Ответ не может быть дан на основании данной статистики. Неизвестно на основании чего преступная группа выбирает тот или иной объект (может быть атаки проводятся равновероятно по всему списку, тогда вероятность атаки для выбранного объекта будет 0,001, а может конкуренты каждый год платят за атаку на выбранный объект, тогда вероятность будет равна единице) или тот или иной способ атаки, даже обладая какой-то статистикой за предыдущие периоды.

Еще больше неопределенности в определении вероятности сценария (метода, техники, использования конкретных типов уязвимостей) проведения атаки и наступления соответствующих сценарию рисков. По мнению авторов, говорить, например, о вероятности использования злоумышленником конкретной уязвимости абсолютно некорректно. Даже о вероятности атаки на конкретную подсистему промышленного объекта говорить практически бессмысленно, т.к., если злоумышленник принял решение атаковать промышленный объект, то он проверит все доступные (с учетом ресурсных ограничений) ему способы атаки, пока не придет к необходимому ему результату. В терминах риск-ориентированного подхода это означает, что в общем случае необходимо принимать вероятность осуществления атаки по конкретному сценарию как равной единице.

Экспертный метод в свою очередь имеет как очевидные, так и скрытые от неискушенного взора недостатки. Основным недостатком является субъективизм таких оценок – два разных эксперта в одной и той же ситуации могут дать совершенно разные оценки и привести их к какому-то общему знаменателю не так просто. Кроме того, сейчас не существует объективных способов оценки квалификации самих экспертов, которых в экспертные группы обычно приглашают соответствующие руководители, ориентирующиеся на собственные представления об уровне экспертизы. Менее очевидной проблемой является проблема усреднения экспертных оценок нескольких экспертов из-за

чего крайние (т.е. минимальные и максимальные) значения в такой усредненной оценке будут встречаться существенно реже, чем должны были быть. Также необходимо учитывать психологическую склонность любого человека оценивать вероятность событий, с которыми в реальности он никогда не встречался, меньше, чем тех, с которыми приходилось иметь дело на практике.

Выходом из сложившейся ситуации, на наш взгляд, может быть переход к оценке риска на основе возможного ущерба в результате наступления негативных последствий (что в какой-то степени коррелирует с подходом, приведенном в Постановлении Правительства РФ №127 и новой методике моделирования угроз безопасности информации ФСТЭК России, проект которой в настоящее время стал доступен для публичного обсуждения) без учета вероятности наступления этого события (т.е. в предположении, что вероятность наступления этого события равна единице). Дополнительным фактором ранжирования рисков может служить сложность (например, выраженная в количестве затрачиваемых ресурсов) проведения соответствующей атаки.

Подводя итог можно отметить, что риск-ориентированный подход к управлению кибербезопасностью, несмотря на все его недостатки, в ближайшей перспективе будет применяться за отсутствием других продуктивных подходов.

Как было отмечено выше, обеспечение кибербезопасности является необходимым, но не достаточным условием для обеспечения безопасности защищаемого объекта. Риск-ориентированный подход хорошо себя зарекомендовал для управления разнородными рисками из разных предметных областей. Если посмотреть на историю развития методов обеспечения информационной безопасности, то можно отметить, что используемые концепции принципиально не отбрасывались, а становились частью подходов, приходящих им на смену. Так и сейчас, риск-ориентированный подход еще не исчерпал себя и как существенный элемент общей системы защиты может использоваться в дальнейшем.

Можно также предположить дальнейшее развитие риск-ориентированных подходов. Так, в работе [13] разрабатывается модель угроз для цифровых подстанций для оценки рисков, возникающих в результате кибератак. Более того, есть ряд случаев, например, при управлении высокоавтоматизированным транспортным средством [14], когда риск, выраженный в стоимостном выражении, определяется ситуативно, упрощенного говоря, с транспортным средством какой стоимости произошла авария. В общем случае, для систем промышленной автоматизации как развитие риск-ориентированных подходов в качестве перспективных следует рассматривать подходы, связанные с пониманием и управлением комплексной безопасностью [15].

Заключение

Основной проблемой применения риск-ориентированного подхода является оценка вероятности компьютерных атак. Применение традиционных, основанных на исторических данных, количественных методик оценки рисков кибербезопасности на настоящий момент себя не оправдали в силу самой природы рисков кибербезопасности помноженной на всё увеличивающуюся сложность киберфизических систем. Единственной областью, где достигнуты сколько-нибудь значимые количественные результаты, можно считать только методы сравнительной оценки уязвимостей (например, CVSS 3.1). Как следствие, исходя из принципов риск-ориентированного подхода, вероятность наступления соответствующих событий (т.е. реализации риска) приходится принимать равной единице, а риск – равным ущербу от наступления этого события (точнее его негативных последствий). При этом оценка ущерба проводится на основе экспертных и полуэкспертных методов.

На основе анализа, проведенного в статье, авторы предлагают две группы выводов: первая группа – относится к вопросам практической реализации риск-ориентированного подхода и обеспечения кибербезопасности, вторая – лежит в плоскости развития академических исследований:

- с точки зрения практического применения риск-ориентированного подхода продолжат развиваться и адаптироваться гибридные методы анализа угроз кибербезопасности. То есть подходы, объединяющие методы функциональной (промышленной) и информационной безопасности. Продолжатся попытки перехода к оценке рисков в денежном эквиваленте или других параметрах, оценивающих эффективность и непрерывность ведения бизнеса;
- при условии гармонизации требований серии стандартов МЭК 62443 компании реального сектора экономики с высоким уровнем зрелости процессов управления информационной безопасностью и имеющие опыт практического применения серии стандартов МЭК 27000 начнут использовать предлагаемые методические подходы по оценке и управлению рисками;
- в ближайшей перспективе будут превалировать качественные оценки на основе экспертных мнений;
- потенциалом применения обладают методы теории системного анализа, которые могут позволить добавить объективности экспертным методам оценки;
- возрастает потребность в разработке прикладных информационных систем, позволяющих разрабатывать гибридные модели угроз и (отчасти) автоматизировать процесс оценки рисков.

С академической точки зрения процесс формирования теоретической и методологической базы кибербезопасности социотехнических и киберфизических объектов (и промышленных объектов, имеющих в своем составе системы АСУ ТП, как типичных представителей таких объектов) нельзя признать законченным и исследования должны быть продолжены. До сих пор нет сколько-нибудь значимых онтологий базовых понятий, описывающих все аспекты кибербезопасности промышленного объекта, более того нет онтологий современного состояния как комплексной безопасности, так и, казалось бы, более академически развитой информационной безопасности (за исключением отдельных узких областей).

Учитывая, тот факт, что в ближайшей перспективе экспертные методы оценки будут превалировать, потенциалом обладают исследования в области систем искусственного интеллекта – систем, основанных на знаниях, применение которых позволит масштабировать накапливаемые экспертные знания.

СПИСОК ЛИТЕРАТУРЫ:

1. Гриняев С.Н., Правиков Д.И., Медведев Д.А. Комплексная безопасность ТЭК как объект научного анализа. // Естественные и технические науки № 3/2. 2019. С. 24–30. URL: https://www.elibrary.ru/item.asp?id=38506340 (дата обращения: 08.10.2020).
2. Губайдуллина И.Н., Ковтунова С.Ю. К вопросу обеспечения комплексной безопасности. // Инновационная экономика: перспективы развития и совершенствования № 2 (7). 2015. С. 92–95. URL: https://cyberleninka.ru/article/n/k-voprosu-obespecheniya-kompleksnoy-bezopasnosti (дата обращения: 08.10.2020).
3. Ильин А.П., Мальцев А.В., Мальцев А.С. Анализ современных комплексных систем безопасности // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций № 1(7). Т. 2. 2016. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-kompleksnyh-sistem-bezopasnosti. (дата обращения: 08.10.2020).
4. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // student № 9. 2020. С. 1438–1448. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 08.10.2020).

5. Правиков Д.И., Петухов А.В. Кибербезопасность как новое фундаментальное направление в области информационной безопасности // Вестник современны цифровых технологий № 1. 2019. С. 19–25. URL: https://www.elibrary.ru/item.asp?id=41496052 (дата обращения: 08.10.2020).
6. Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции. Диссертация на соискание ученой степени доктора технических наук. – СПбПУ. 2019. URL: https://www.dissercat.com/content/metodologiya-predotvrashcheniya-kompyuternykh-atak-na-promyshlennye-sistemy-na-osnove-adapti (дата обращения: 08.10.2020).
7. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности № 3 (4). 2014. С. 35–40. URL: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami-obektov-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 08.10.2020).
8. Колосок И.Н., Гурина Л.А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении № 2 (14). 2019. С. 40–51. URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy (дата обращения: 08.10.2020).
9. Сухих, Ян А.; Правиков, Дмитрий И.; Кузичкин, Алексей А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 97–117, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1274 (дата обращения: 08.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.08.
10. Пащенко И.Н., Васильев В.И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия Южного федерального университета. Технические науки № 12 (149). 2013. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-k-sisteme-zaschity-informatsii-v-intellektualnoy-seti-smart-grid-na-osnove-standartov-iso-iec-27001-i-27005 (дата обращения: 08.10.2020).
11. Крундышев В.М. Построение безопасных крупномасштабных динамических сетей. // Материалы 29-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2020. СПб: Изд-во Политехнического университета. С. 5–6. URL: https://www.elibrary.ru/item.asp?id=44017238 (дата обращения: 08.10.2020).
12. Протасов А.В., Вильвер П.Ю. Особенности использования метода индексирования при анализе техногенного риска в России // Вестник Иркутского государственного технического университета. 2011. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-metoda-indeksirovaniya-pri-analize-tehnogennogo-riska-v-rossii (дата обращения: 08.10.2020).
13. Карантаев В.Г., Карпенко В.И.. Возможные методы анализа последствий влияния кибератак на системы релейной защиты и автоматики цифровых и высокоавтоматизированных подстанций. // РУМ №3 (593). 2020. С. 4–12.
14. Правиков Д.И., Пономарева Е.А., Куприяновский В.П. Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств. International Journal of Open Information Technologies. Т. 8. № 6. 2020. С. 98–103. URL: http://www.injoit.org/index.php/j1/article/view/949 (дата обращения: 08.10.2020).
15. Правиков Д.И., Щербаков А.Ю., Корнеев Н.В., Тихоненко О.О. Комплексная безопасность систем промышленного оборудования // Вестник современных цифровых технологий № 2.2020. С. 30–35. URL: https://www.elibrary.ru/item.asp?id=42533459 (дата обращения: 08.10.2020).

REFERENCES:

[1] Grinyaev S.N., Pravikov D.I., Mededev D.A. Kompleksnaya bezopasnost` toplivno energeticheskogo kompleksa kak ob`ekt nauchnogo analyza. Estestvennye i technicheskie nauki № 3/2. 2019. S. 24–30. URL: https://www.elibrary.ru/item.asp?id=38506340 (accessed: 08.10.2020) (in Russian).
[2] Gubaidullina I.N., Kovtunova S.U. K voprosu obespecheniya kompleksnoy bezopasnostyю Innovacionnaya economica: perspecrivy razvitiya i sovershenstvovania. № 2 (7). 2015. S. 92–95. URL: https://cyberleninka.ru/article/n/k-voprosu-obespecheniya-kompleksnoy-bezopasnosti (accessed: 08.10.2020) (in Russian).
[3] Il`in A.P., Maltsev A.V., Maltsev A.S. Analyz sovremennykh kompleksnyh system bezopasnosty. Sovremennye tehnologii obespecheniay grazdanskoy oborony I likvidacii posledstvii chrezvychainikh situaciy № 1(7). Vol 2. 2016. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-kompleksnyh-sistem-bezopasnosti (accessed: 08.10.2020) (in Russian).

[4] Gorelik V.U., Bezus M.U. O bezopasnosti kriticheskoy informacionnoy infrastructury Rossiskoi Federacii. Student № 9. 2020. S. 1438–1448. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (accessed: 08.10.2020) (in Russian).

[5] Pravikov D.I., Petukhov A.V., Kiberbezopasnost` kak novoe fundamental`noye napravleniey v oblasty informacionnoy bezopasnosty. Vestnik sovremennyh cifrovykh tehnologii № 1. 2019. S. 19–25. URL: https://www.elibrary.ru/item.asp?id=41496052 (accessed: 08.10.2020) (in Russian).

[6] Lavrova D.S. Mtodologiya predotvrasheniya komputernykh atak na promyshlennye systemy na osnove analyza adptivnogo prognozirovaniya I samoregulacii. Dissertacia na soiskanie uchenoy stepeni doctora technicheskyh nauk. SPbTU. 2019. URL: https://www.dissercat.com/content/metodologiya-predotvrashcheniya-kompyuternykh-atak-na-promyshlennye-sistemy-na-osnove-adapti (accessed: 08.10.2020) (in Russian).

[7] Kalashnikov A.O. Upravlenie informatsionnimi riskami obektov kriticheskoy informacionnoy infrastructury Rossiskoi Federacii. Voprosy kiberbezopasnosty № 3 (4). 2014. S. 35–40. URL: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami-obektov-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (accessed: 08.10.2020) (in Russian).

[8] Kolosok I.N., Gurina L.A. Ocenka riskov kiberezopasnosty informacionno-kommunikacionnoy infrastructury intellectualnoy energeticheskoy systemy. Informacionnye I matematicheskie technologii v nauke I upravlenii. № 2 (14). 2019. S. 40–51. URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy (accessed: 08.10.2020) (in Russian).

[9] Sukhikh, Yan A.; Pravikov, Dmitry I.; Kuzichkin, Alexey A. Development of secure architectures for process control systems. IT Security (Russia), [S.l.]. Vol. 27, no. 2. P. 97–117, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1274. (accessed: 08.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.08 (in Russian).

[10] Pashnko I.N., Vasilyev V.I. Razrabotka trebovaniy k systeme zashity informacii v intellectualnoy sety Smart Grid na osnove standartov ISO/IEC 27001 i 27005. Izvestiay Uznogo federal1nogo universiteta. Technicheskie nauki № 12 (149). 2013. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-k-sisteme-zaschity-informatsii-v-intellektualnoy-seti-smart-grid-na-osnove-standartov-iso-iec-27001-i-27005 (accessed: 08.10.2020) (in Russian).

[11] Krundyhev V.M. Postoyenie bezopasnykrh krupnomashtabnykrh dinamicheslyh setey // Materialy 29 nauchno-technicheskoy konferencii “Metody I tehnicheskie sredstva obespecheniay bezopasnosty informacii”. – 2020. – SPb: Izdatel`svo Polytehnicheskogo universiteta. S. 5– 6. URL: https://www.elibrary.ru/item.asp?id=44017238 (accessed: 08.10.2020) (in Russian).

[12] Protasov A.V., Vil`ver P.U. Osobennosty ispol`zovania metoda indeksirovania pri analyze technogennogo riska v Rossii. Vestnik Irkutskogo gosudarstvennogo tecknicheskogo univeriteta. 2011. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-metoda-indeksirovaniya-pri-analize-tehnogennogo-riska-v-rossii (accessed: 08.10.2020) (in Russian).

[13] Karantayev V.G., Karpenko V.I. Vozmoznye metody analyza posledstviy vliyania kiberatak na systemy releynoy zashity i avtomatiky cifrovykh I visokoavtomatizirovannykh podstanciy. RUM №3 (593). 2020. S. 4–12 (accessed: 08.10.2020) (in Russian).

[14] Dmitry Pravikov, Evgeniya Ponomareva, Vasily Kupriyanovsky. Problems of ensuring information security of highly automated vehicles. International Journal of Open Information Technologies. Vol. 8. № 6. 2020. P. 98–103. URL: http://www.injoit.org/index.php/j1/article/view/949 (accessed: 08.10.2020) (in Russian).

[15] Pravikov D.I., Sherbakov A.U., Korneev N.V., Tikhonenko O.O. Kompleksnaya bezopasnost` system promyshlennogo oborudovania. Vestnik sovremennyh cifrovykh tehnologii № 2. 2020. S. 30–35. URL: https://www.elibrary.ru/item.asp?id=42533459 (accessed: 08.10.2020) (in Russian).

Поступила в редакцию – 07 сентября 2020 г. Окончательный вариант – 20 ноября 2020 г.
Received – September 07, 2020. The final version – November 20, 2020

Кирилл В. Плаксий[1], Лидия Л. Кулагина[2], Андрей А. Никифоров[3],
Наталья Г. Милославская[4]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: KVPlaksii@mephi.ru, http://orcid.org/0000-0002-8949-6772
[2]e-mail: lidusy_0104@mail.ru, https://orcid.org/0000-0003-1261-1119
[3]e-mail: andreinikiforov993@gmail.com, http://orcid.org/0000-0002-2726-0000
[4]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

ИССЛЕДОВАНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 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.2020.4.05

Аннотация. Исследуются вопросы обеспечения информационной безопасности (ИБ) в популярных в настоящее время графовых системах управления базами данных (СУБД), способных работать с большими данными и хранить информацию, созданную в ходе генерации преступных дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма (ОД/ФТ). Продолжая предыдущее исследования авторов, в данной работе ставится цель анализа угроз ИБ и уязвимостей графовых СУБД. Эти СУБД отличаются от реляционных видом хранимых данных и принципом их хранения, поэтому актуальной является проблема составления перечня угроз ИБ в связи с отсутствием такового в мировом масштабе. На основе анализа угроз ИБ для обычных СУБД и с учётом особенностей графовых СУБД, их структуры и уязвимостей конкретных графовых СУБД предлагаются собственный перечень угроз ИБ и методы по защите от них, а также некоторые рекомендации по устранению уязвимостей, используемых угрозами ИБ.

Ключевые слова: отмывание доходов, полученных преступным путем, финансирование терроризма, ОД/ФТ, информационная безопасность, большие данные, системы управления базами данных (СУБД), угрозы ИБ, уязвимости СУБД.

Для цитирования: ПЛАКСИЙ, Кирилл В. и др. ИССЛЕДОВАНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 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. 27, p. 53–64, n. 4, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1306>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.05.

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

Kirill V. Plaksiy[1], Lidiia L. Kulagina[2], Andrey A. Nikiforov[3], Natalia G. Miloslavskaya[4]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31 Moscow, 115409, Russia
[1]e-mail: kirillplaksiy@mail.ru, http://orcid.org/0000-0002-8949-6772
[2]e-mail: lidusy_0104@mail.ru, https://orcid.org/0000-0003-1261-1119
[3]e-mail: andreinikiforov993@gmail.com, http://orcid.org/0000-0002-2726-0000
[4]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Investigation of information security issues for graph databases suitable for big data processing while detecting money laundering and terrorism financing cases*

DOI: http://dx.doi.org/10.26583/bit.2020.4.05

Abstract. The information security (IS) issues in the currently popular graph database management systems (DBMS), suitable for big data processing and storing information created during the generation of criminal cases on money laundering and financing of terrorism (ML/FT), are examined. This paper continues the previous authors' research and aims to analyze IS threats and vulnerabilities of graph DBMS. These DBMS differ from the relational ones in the type of stored data and the principle of their storage; therefore the compiling of a list of IS threats is urgent due to its absence on a global scale. The original IS threat list and methods for protecting against them, as well as some recommendations for eliminating vulnerabilities used by IS threats are proposed. The obtained results are based on the analysis of IS threats for conventional DBMS and taking into account the peculiarities of graph DBMS, their structure as well as vulnerabilities of specific graph DBMS.

Keywords: money laundering, terrorism financing, ML/FT, information security, typology, Big Data, Database Management System (DBMS), information security threats, vulnerabilities.

For citation: PLAKSIY, Kirill V. et al. Investigation of information security issues for graph databases suitable for big data processing while detecting money laundering and terrorism financing cases. IT Security (Russia), [S.l.], v. 27, n. 4, p. 53–64, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1306>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.05.

***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 утечек информации неуклонно растет. Поскольку основным хранилищем данных выступает система управления базами данных (СУБД), то атаки на СУБД являются одними из самых опасных для организаций. Согласно отчету об утечках данных компании Verizon [1], СУБД – один из наиболее уязвимых активов различных организаций. Графовые СУБД – не исключение. Это приводит к необходимости обеспечения информационной безопасности (ИБ) всей инфраструктуры, связанной с использованием графовых СУБД. Обеспечение ИБ СУБД должно начинаться с устранения существующих уязвимостей. Сократить их количество возможно лишь при комплексном подходе к защите данных в графовых СУБД. Создание эффективной системы обеспечения ИБ СУБД требует оценки актуальных угроз ИБ с учетом ценность защищаемой информации и методов несанкционированного воздействия на нее. Среди основных угроз ИБ обычно выделяют угрозы несанкционированного использования информации в СУБД системными администраторами, пользователями, злоумышленниками, вирусных атак с различными последствиями, SQL-инъекций, технических проблем, снижения производительности, отказа в доступе, исключающего возможность использования информации, физического ущерба, нанесенного оборудованию или каналам связи, наличия ошибок и недоработок, несанкционированных возможностей программного обеспечения (ПО), управляющего СУБД и операционных систем (ОС) и т.п.

Во многом нереляционные СУБД более безопасны из-за отсутствия SQL-запросов и невозможности провести SQL-инъекцию [2]. Но отсутствие SQL-кода в запросе еще не означает, что система полностью защищена. Так, СУБД NoSQL состоит из приложения, интерфейса прикладного программирования (API) NoSQL и NoSQL-СУБД, каждый из которых имеет свои уязвимости. Например, сама СУБД, как и любое другое приложение, подвержена атакам переполнения буфера и имеет уязвимости в системе аутентификации. Для злоумышленника этот уровень сложно атаковать, так как его уязвимостями отслеживают разработчики и сообщество пользователей. На уровне API в большинство нереляционных СУБД находятся библиотеки, используемые для организации доступа к данным. Они часто имеют открытый исходный код, что помогает обнаружить их уязвимости злоумышленникам. Чаще всего атакуется верхний уровень, содержащий

уязвимости в проверке входных данных. При этом используется тот же подход, что и при SQL-инъекциях, но основанный на других языках запросов, характерных для нереляционных СУБД.

Данное исследование продолжает работу, начатую авторами в [3, 4], и ставит своей целью проанализировать типичные уязвимости и угрозы ИБ для графовых СУБД и выработать некоторые рекомендации по устранению уязвимостей, используемых этими угрозами ИБ.

1. Угрозы информационной безопасности графовых СУБД

В ходе исследования были рассмотрены различные графовые хранилища данных, которые могут быть применены при обнаружении преступных дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма (ОД/ФТ). Для работы с данными в качестве средства визуализации хорошо подходят графы [5], что упрощает восприятие человеком информации и уменьшает её объемы за счет различных подходов, учитывающих специфику решаемой задачи.

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 г. и уже существуют СУБД, которые работают в реальных системах. Для хранения новых данных и работы с ними используются такие платформы как Neo4j [6], AllegroGraph [7], JanusGraph [8]. Для исследования были выбраны Neo4j, JanusGraph и Dgraph из-за их популярности (рис. 1) [9], а также открытого кода, языков реализации, мультиплатформенности и разнообразия средств обеспечения ИБ (табл. 1).

Rank			DBMS	Database Model	Score		
Jun 2020	May 2020	Jun 2019			Jun 2020	May 2020	Jun 2019
1.	1.	1.	Neo4j	Graph	48.27	-1.49	-1.28
2.	2.	2.	Microsoft Azure Cosmos DB	Multi-model	30.80	+0.13	+2.56
3.	3.	↑ 4.	ArangoDB	Multi-model	5.38	+0.70	+0.81
4.	4.	↓ 3.	OrientDB	Multi-model	4.82	+0.68	-0.77
5.	5.	5.	Virtuoso	Multi-model	2.28	-0.07	-0.83
6.	6.	↑ 7.	Amazon Neptune	Multi-model	2.17	+0.41	+0.93
7.	7.	↓ 6.	JanusGraph	Graph	2.01	+0.36	+0.46
8.	↑ 9.	↑ 11.	Dgraph	Graph	1.40	+0.31	+0.51
9.	↓ 8.	↓ 8.	GraphDB	Multi-model	1.25	+0.06	+0.16
10.	↑ 12.	↑ 18.	FaunaDB	Multi-model	1.19	+0.25	+0.84
11.	↓ 10.	↑ 13.	Stardog	Multi-model	1.15	+0.08	+0.44
12.	↓ 11.	↓ 9.	Giraph	Graph	0.97	+0.02	-0.11
13.	13.	↓ 12.	TigerGraph	Graph	0.90	+0.05	+0.18

Рис. 1. Популярные СУБД
(Fig. 1. Popular databases)

В ходе исследования было установлено, что специального перечня уязвимостей и угроз ИБ для графовых СУБД не создано при том, что их различия с реляционными СУБД существенны [3, 4]. Поэтому было решено провести анализ существующих перечней угроз ИБ для реляционных СУБД и, учитывая специфику графовых СУБД, сформулировать актуальные для последних.

Таблица 1. Графовые СУБД

	Neo4j	**JanusGraph**	**Dgraph**
Языки реализации	Java, Scala	Java	Go
Серверные ОС	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
Контроль доступа	Присутствует	Осуществляется через Rexter Graph Server	Нет (запланировано на будущие версии)
Аутенти-фикация	Подключаемая аутентификация с поддерживаемыми стандартами (LDAP, Active Directory, Kerberos)	Базовая и токен-аутентификация	Нет (запланировано на будущие версии)
Шифрование	Целенаправленного внутреннего шифрования нет, поддержка стороннего шифрования	Целенаправленного внутреннего шифрования нет, поддержка стороннего шифрования	Шифрование данных в состоянии покоя HDFS
Целостность данных	Использование ограничений	Контроль целостности данных при загрузке	Использование двойных баз
Резервные копии	Да, как для одного компьютера, так и для кластеров	Собственные копии, а также поддержка сторонних средств	Копии работающих кластеров

Сначала были рассмотрены типовые угрозы безопасности персональных данных (ПДн), которые обычно хранятся в различных базах данных (БД) и обрабатываются в информационных системах ПДн (ИСПДн) [10]. В целях формирования систематизированного перечня угроз в базовой модели ФСТЭК России они классифицируются в соответствии со следующими признаками:

- вид защищаемой информации, содержащей ПДн;
- вид возможных источников угроз;
- тип ИСПДн, на которые направлена реализация угроз;
- способ реализации угроз;
- вид нарушаемого свойства информации (вид несанкционированных действий, осуществляемых с ПДн);
- используемая уязвимость;
- объект воздействия.

Далее на основе базы угроз ФСТЭК России были определены наиболее типичные угрозы для БД и сформулированы угрозы ИБ для графовых СУБД, включая следующие:

- угроза использования механизмов авторизации для повышения привилегий (УБИ.031);
- угроза повышения привилегий (УБИ.122);
- угроза несанкционированного создания учётной записи пользователя (УБИ.090);
- угроза межсайтового скриптинга (УБИ.041);
- угроза межсайтовой подделки запроса (УБИ.042);
- угроза искажения XML-схемы (УБИ.026);
- угроза неконтролируемого копирования данных внутри хранилища больших данных (УБИ.057);
- угроза несанкционированного удаления защищаемой информации (УБИ.091);
- угроза несанкционированной модификации защищаемой информации (УБИ.179);
- угроза несанкционированного удаления защищаемой информации (УБИ.091);

- угроза неконтролируемого уничтожения информации хранилищем больших данных (УБИ.060);
- угроза, сбоя автоматического управления системой разграничения доступа хранилища больших данных (УБИ.148);
- угроза несогласованности правил доступа к большим данным (УБИ.097);
- угроза обхода некорректно настроенных механизмов аутентификации (УБИ.100);
- угроза приведения системы в состояние «отказ в обслуживании» (УБИ.140)

2. Уязвимости графовых СУБД

В ходе работы были выделены типичные уязвимости, характерные для СУБД и для графовых СУБД в частности:

1. Уязвимость в системе аутентификации. Многие графовые СУБД по умолчанию устанавливаются без пароля. Разработчики предполагают, что установка СУБД происходит в доверенном окружении.

2. Уязвимость в системе авторизации. Изначально в некоторых графовых СУБД любой новый пользователь имеет по умолчанию доступ к чтению всей БД. Также существует уязвимость в системе авторизации администратора – пользователь Admin имеет доступ к БД и права на чтение и запись. Если по умолчанию отсутствует пароль, то предоставляется полный доступ.

3. Уязвимость драйверов БД, приводящая к переполнению буфера и позволяющая нарушителю вызвать атаку «отказ в обслуживании».

4. Незашифрованный текст. Данные передаются в БД в открытом виде и могут быть перехвачены при любой атаке типа «человек по середине».

5. Уязвимость, опускающая инъекции в регулярных выражениях. Многие нереляционные СУБД позволяют осуществлять поиск с помощью регулярных выражений. Их неправильное использование может нанести вред. Аутентификация пользователя может осуществляться посредством запроса, указывающего в качестве пароля регулярное выражение. Переменная password не фильтруется, что позволяет злоумышленнику получить несанкционированный доступ (НСД) к БД.

6. Уязвимость, допускающая инъекции кода. Графовые СУБД не поддерживают SQL, но ни одна СУБД не может обойтись без использования языка запросов. Для каждой графовой СУБД существует свой язык запросов, с помощью которого можно осуществить разного рода атаки-инъекции, если отсутствует входная фильтрация данных.

7. Возможность манипуляции REST-интерфейсом. В ходе развития сервис-ориентированной архитектуры большую популярность получили REST-решения (REpresentational State Transfer, рис. 2). В некоторые графовые СУБД входит простой REST-интерфейс, позволяющий получать доступ к БД в режиме чтения.

Для каждой СУБД уязвимости уникальны [11-13]. Входящие в базу CVE (Common Vulnerabilities and Exposures) уязвимости графовых СУБД были сведены в табл. 2.

3. Распространённые методы защиты данных, применимые к графовым СУБД

При росте потребностей в операциях с информацией возрастала необходимость в средствах обеспечения ИБ данных в СУБД. Средства защиты в различных СУБД несколько отличаются, однако общим является многоуровневость защиты – чем больше барьеров-уровней, тем сложнее их преодолеть злоумышленнику. Подход к обеспечению защиты данных в графовых СУБД, как и в других системах, складывается из обеспечения конфиденциальности, целостности и доступности [14]. На нижних уровнях находятся стандартные способы защиты: пароли, шифрование данных, разграничение прав доступа к объектам БД, контрольные след выполняемых операций, резервное копирование.

Таблица 2. Уязвимости графовых СУБД

№	Neo4j	JanusGraph	Dgraph
1	CVE-2018-18389. Настройка LDAP-аутентификации с помощью STARTTLS и системной учетной записи авторизации позволяет злоумышленнику войти на сервер, отправив любое допустимое имя пользователя с произвольным паролем из-за неправильного контроля доступа Neo4j Enterprise Database Server 3.4.x до 3.4.9.	CVE-2018-1000632. Версия dom4j до версии 2.1.1 содержит уязвимость, которая может привести к изменению злоумышленником XML-документов с помощью XML-инъекции в класс «элементы» методами: addElement, addAttribute. Атака реализуется при указании атрибутов или элементов в XML-документе.	CVE-2019-5736. Уязвимость модуля Runc Go до версии 1.0-rcb, использованного в Docker до версии 18.09.2 и других продуктах, позволяет злоумышленнику перезаписать двоичный файл runc хоста (и получить root-доступ к хосту), используя возможность выполнять команду как root. Причина: неправильная обработка файлового дескриптора, связанного с /proc/self/exe.
2	CVE-2018-1000820. СУБД Neo4j-contrib neo4j-apoc-procedures версии содержит внешние XML-сущности (XXE) с уязвимостью XML-парсера, что может привести к раскрытию конфиденциальной информации, отказу в обслуживании, сканированию портов.	CVE-2015-5211. В некоторых ситуациях Spring Framework 4.2.0–4.2.1, 4.0.0–4.1.7, 3.2.0–3.2.14 и более ранние версии уязвимы для атаки Reflected File Download (RFD). Злоумышленник создает URL-адрес с расширением пакетного сценария, в результате чего ответ загружается (а не отображается) и включает некоторые входные данные, отраженные в ответе.	CVE-2020-10661. Инструменты безопасного хранения конфиденциальной информации в динамических облачных средах HashiCorp Vault и Vault Enterprise версий 0.11.0–1.3.3 Go модуля, чей API использует Dgraph, могут при определенных обстоятельствах иметь существующие политики вложенного пути к файлу, предоставляющие доступ к пространствам имен, созданным позднее.
3	CVE-2013-7259. Множественные уязвимости подделки межсайтовых запросов (CSRF) в Neo4J 1.9.2 позволяют удаленным злоумышленникам перехватывать аутентификацию администраторов для запросов, выполняющих произвольный код.	CVE-2013-1801. Httparty gem 0.9.0 и более ранние версии для Ruby не ограничивают должным образом приведение строковых значений, что может позволить удаленным злоумышленникам внедрять объекты и выполнять произвольный код или вызывать «отказ в обслуживании» с помощью действия «Поддержка пакетов для преобразования типа YAML».	CVE-2020-10660. Инструменты безопасного хранения конфиденциальной информации в динамических облачных средах HashiCorp Vault и Vault Enterprise версий 0.9.0–1.3.3 Go модуля, чей API использует Dgraph, могут при определенных обстоятельствах непреднамеренно включать в себя группы, к которым, в сущности, не имеют прав доступа.
4	CVE-2013-7220. js/ui/screenShield.js в GNOME Shell (gnome-shell) до версии 3.8. Допускалось, что злоумышленники, находящиеся недалеко физически, могли выполнять случайные команды путем использования рабочей станции, оставленной без присмотра, и поиском активности на клавиатуре.	CVE-2013-0156. active_support/ core_ext/hash/conversions.rb в Ruby до версий до 2.3.15, 3.0.x до 3.0.19, 3.1.x–3.1.10 и 3.2.x–3.2.11 неправильно ограничивает приведение строк values, что позволяет удаленным злоумышленникам внедрять объекты и выполнять произвольный код или вызывать «отказ в обслуживании» с использованием вложенных ссылок на объекты XML, используя поддержку Action Pack.	CVE-2020-7220. Инструменты безопасного хранения конфиденциальной информации в динамических облачных средах HashiCorp Vault и Vault Enterprise версий с 0.11.0 по 1.3.1 Go модуля, чей API использует Dgraph, при определенных обстоятельствах аннулируют динамические секреты для монтирования в удаленном пространстве имен.

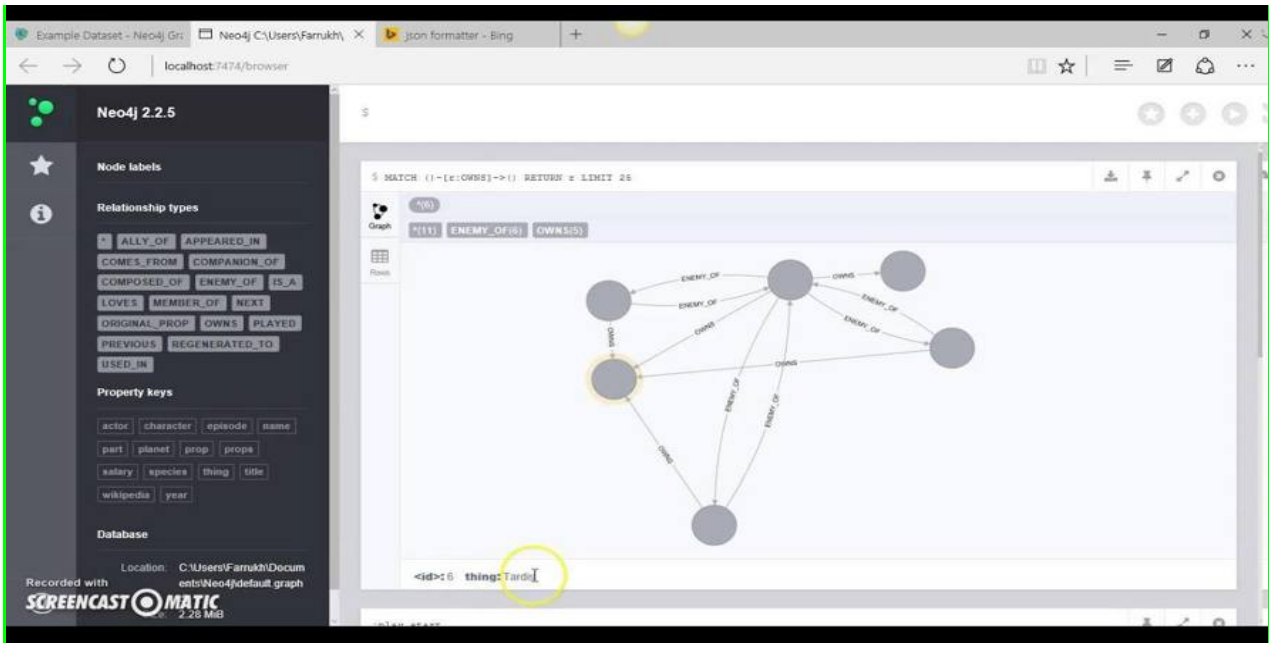

Рис. 2. REST-API Neo4j
(Fig. 2. REST-API Neo4j)

Перечислим наиболее распространенные методы защиты СУБД.

1. *Разграничение прав доступа и аутентификация*. Это гибкая система многопользовательской СУБД, при которой администратор предоставляет пользователям права доступа исходя из минимальных полномочий, необходимых для выполнения должностных обязанностей. Большинство СУБД имеют встроенный набор средств по разграничению прав доступа, с помощью которого пользователи и/или группы наделяются правами. В СУБД имеется возможность управления правами и действиями над определенными объектами, такими как чтение, добавление, изменение и удаление записей.

Одним из примеров применения разграничения доступа является ядро модели безопасности Neo4j с предопределенными ролями доступа пользователей, которые включают в себя набор разрешенных действий. Графовая СУБД Neo4j осуществляет аутентификацию пользователей с помощью собственного сервиса, который хранит данные о пользователях и ролях локально, на диске [15]. Другим вариантом авторизации пользователей в Neo4j является использование внешнего ПО, такого как Active Directory или OpenLDAP. Также реализовать аутентификацию и единый вход Neo4j можно с помощью дополнения Neo4j Kerberos.

В СУБД JanusGraph используются соединения, основанные на HTTP-запросах или WebSockets. Соединения выполняются по HTTPS (HyperText Transfer Protocol Secure), запрашивающему аутентификацию пользователей. HTTP-запросы реализуют базовую аутентификацию и аутентификацию с помощью токенов. В отличие от обычной аутентификации для СУБД (отправки имени пользователя и пароля вместе с запросом) однократная регистрация, WebSockets и аутентификация с помощью токенов повышают производительность.

2. *Шифрование данных*. Отсутствие шифрования позволяет получить доступ к СУБД с помощью коммуникационного канала, а использование средств криптографической защиты позволяет предотвратить данную угрозу. Шифрование должно использоваться при хранении и передаче конфиденциальных данных в зашифрованном

виде, а также при преобразовании исходных данных специальным алгоритмом для сокрытия их содержания. Новое представление зашифрованных данных с секретным ключом шифрования хранится в БД и передается по коммуникационному каналу [14]. Существует два режима работы зашифрованных БД:

а) расшифрование файла с конфиденциальной информацией на внешнем носителе и работа с ним, после чего файл вновь зашифровывается. Независимое взаимодействие СУБД и средств шифрования является очевидным достоинством данного режима, но при сбое или отказе часть СУБД может остаться незашифрованной;

б) расшифрование файла происходит в оперативной памяти перед выполнением действий с конфиденциальной информацией. Такие процедуры в большинстве случаев встроены в СУБД, что позволяет поддерживать высокий уровень защиты от НСД, но снижает производительность из-за усложнения процесса обработки данных.

В настоящее время графовая СУБД Neo4j [15] не шифрует данных. Дополнительная защита данных осуществляется с помощью шифрования файловой системы или самих данных из приложения. Шифрование файловой системы является простым способом усиления защиты данных на диске, но недостаточным для осуществления полной защиты данных. Neo4j использует архитектуру, основанную на REST и операторах Cypher в виде вызова веб-службы. Ответы на вызовы передаются по сети открытым текстом. Некоторые приложения кроме использования протокола HTTPS требуют введения дополнительных средств защиты. Одним из дополнительных способов является ограничение доступа к данным – только авторизованным для данной работы пользователям. В ходе процесса шифрования данных на уровне приложений они динамически изменяются, выполняется зашифрование и расшифрование до/после чтения или записи данных в БД. С помощью защиты на уровне приложения могут быть реализованы многие стандарты безопасности для областей здравоохранения и образования, такие как HIPPA (Health Insurance Portability and Accountability Act) и FERPA (Family Educational Rights and Privacy Act). Также для реализации защиты приложений на основе Java используется библиотека Neo4j Object Graph Mapping (OGM), которая позволяет конвертировать атрибуты, поскольку Neo4j может сохранять данные в формате, отличном от начального (например, дату в виде формата Long или String). Такие преобразования являются начальной точкой для шифрования на уровне приложений. Данный подход обеспечивает защиту данных как на диске, как и во время передачи от/на сервер Neo4j. Но для шифрования данных задействуются память и вычислительные мощности, что негативно сказывается на использовании ресурсов сети. Зашифрованные данные трудны для использования вне приложения и не пригодны для таких действий над данными в БД, как поиски, индексация и случайные запросы Cypher.

Графовая СУБД JanusGraph способна взаимодействовать со множеством продуктов, осуществляющих шифрование.

Графовая СУБД Dgraph [16] может шифровать данные в состоянии покоя HDFS (Hadoop Distributed File System), что позволяет хранить их в зашифрованных каталогах HDFS (зонах шифрования). Расшифрованные данные никогда не хранятся в каталогах HDFS, так как зашифрование и расшифрование данных происходит на стороне клиента.

3. *Защита полей, целостность данных*. Изменение данных в СУБД чаще всего происходит в результате действий пользователей, поэтому целесообразным является использовать защиту полей и записей в таблицах СУБД. Для защиты полей используются следующие уровни прав доступа: полный запрет доступа, только чтение и полный доступ для просмотра, ввода, изменения и удаления. Также применяется сокрытие от избранных

пользователей полей таблиц и запрет на вызов конструктора, чтобы пользователь не смог изменить приложение.

В графовой СУБД Neo4j защита полей осуществляется с использованием ограничений узлов и отношений, что позволяет обеспечить целостность данных. Создаются уникальные ограничения свойств, а также ограничения существования свойств узлов и отношений. Реализованы ключи узлов, гарантирующие уникальность значения свойств для всех узлов с данной меткой. Ограничение существования свойств узлов и отношений определяет их существование только с данной меткой/типом. При таком методе защиты запросы на создание новых узлов и отношений без свойств выполнены не будут. Ключи узлов позволяют гарантировать, что на всех узлах с данной меткой существуют определенные свойства, и их значения свойств уникальны.

В графовой СУБД JanusGraph целостность данных гарантируется сторонними продуктами, контроль целостности осуществляется при загрузке данных.

Графовая СУБД Dgraph представляет хранилище данных как верхний слой над другой БД SQL/NoSQL, и именно она отвечает за целостность данных.

4. *Контрольный след выполняемых операций* отображает детальные сведения в СУБД о действиях пользователя. Данная информация позволяет обнаруживать несанкционированные вмешательства, выявлять уязвимости в защите и предотвращать некорректные изменения данных в СУБД. При работе с важными данными или при выполнении критических операций всегда возникает необходимость регистрации контрольного следа выполняемых операций. Если, например, противоречивость данных приводит к подозрению, что совершено несанкционированное вмешательство в БД, то контрольный след используется для прояснения ситуации и подтверждения того, что все процессы находятся под контролем. Если это не так, то контрольный след поможет, по крайней мере, обнаружить нарушителя. Для сохранения контрольного следа обычно используется особый файл, в котором система автоматически записывает все выполненные пользователями операции при работе с БД.

5. *Резервное копирование* или «бэкап» (backup copy). Это создание копии файлов и папок на дополнительном носителе информации (внешнем жестком диске, CD/DVD-диске, флэш-памяти, в облачном хранилище и т.д.). Резервное копирование необходимо для восстановления данных, если они повредились или разрушились в основном месте их хранения (на внутреннем жестком диске компьютера или флэш-памяти мобильного устройства). Осуществляет восстановление данных на случай аппаратных или программных сбоев. Многие СУБД имеют инструменты, похожие по принципу создания резервных копий как одного компьютера, так и кластера. Существует режим копирования онлайн.

Графовая СУБД Neo4j имеет открытый исходный код и обеспечивает ACID-совместимый транзакционный сервер. Данные в Neo4j хранятся точно так же, как и на диске, а БД использует указатели для навигации и перемещения по графу. Для производственных сценариев Neo4j обеспечивает поддержку кластера и отказоустойчивость во время выполнения. При необходимости автоматизировать процесс резервного копирования и восстановления БД можно использовать возможности управления конфигурацией Ansible, который является открытым исходным кодом, и способен повышать масштабируемость, согласованность и надежность любой ИТ-среды. Ansible также можно использовать для автоматизации таких задач, как подготовка серверов, необходимых в инфраструктуре, и для управления конфигурацией или развертывания приложений.

Описанные методы обеспечения ИБ определяют основные средств защиты информации, которые необходимы для информационных систем в целом и в графовых СУБД в частности.

4. Средства, используемые для устранения уязвимостей графовых СУБД

В табл. 3 приведены уязвимости графовых СУБД и средства их устранения.

Таблица 3. Средства устранения уязвимостей графовых СУБД

Уязвимости	Средства устранения уязвимостей
Уязвимость в системе аутентификации Уязвимость в системе авторизации	Использование средств разграничения доступа: • Active Directory, OpenLDAP на основе сетевых протоколов аутентификации LDAP (Lightweight Directory Access Protocol) и Kerberos; • аутентификация с помощью токенов; • использование компонентов экосистемы Apache Hadoop.
Уязвимость, вызывающая переполнение буфера и отказ в обслуживании	Использование Apache Hadoop для хранения данных: • распределенная между узлами вычислительного кластера файловая система HDFS (Hadoop Distributed File System); • MapReduce для распределенных операций предварительной обработки.
Нешифрованный текст	Использование средств шифрования: • алгоритмы шифрования AES (Advanced Encryption Standard); • использование HTTPS для шифрования сетевого взаимодействия; • использование компонента экосистемы Apache Hadoop. Cloudera, обеспечивающего шифрование данных HDFS-файлов (Hadoop Distributed File System).
Уязвимость, допускающая инъекции в регулярных выражениях Уязвимость, допускающая инъекции кода Возможность манипуляции с REST-интерфейсом	Проверка входных данных: • использование компонента экосистемы Apache Hadoop Native Auditing, журналы аудита периметра на шлюзе Knox, мониторинг запросов доступа, операций обработки и изменения данных; • ограничение использования регулярных выражений и REST-интерфейса.

Заключение

В настоящее время безопасность СУБД является одним из значительных аспектов обеспечения ИБ организации. Количество данных продолжает увеличиваться экспоненциально, что непосредственно влияет на способы хранения данных и устаревание. Получение доступа к данным СУБД подразумевает полный контроль над ними и перехват управления внутренними сервисами ресурса злоумышленником. Здесь важно осознание и устранение способствующих этому уязвимостей СУБД. Обеспечение ИБ современных информационных систем, включая СУБД, требует комплексного подхода, что невозможно без широкого применения набора защитных средств, объединенных в единую инфраструктуру. Многие из таких средств получили распространение не только в мировом масштабе, но и в России. В данных условиях обеспечение ИБ должно быть динамичным и непрерывным, включая согласованную деятельность всех заинтересованных сторон – как пользователей, так и администраторов.

Графовые СУБД можно представить, как совокупность данных, совместно хранящихся и обрабатывающихся в соответствии с определенными правилами. Они широко используются организациями по всему миру. Их производители постоянно усовершенствуют и обновляют свои продукты, в связи с чем растет количество

потребителей. С появлением нового формата хранения данных в нереляционных графовых СУБД обычные атаки претерпевают изменения. Поэтому обеспечение полноценной и работоспособной системы обеспечения ИБ для графовых СУБД требует немало сил и финансовых вложений. Также необходимо своевременно и корректно устранять имеющиеся в них уязвимости.

В ходе данного исследования были рассмотрены популярные графовые СУБД по данным DB-Engine за июнь 2020 г. – Neo4j, JanusGraph и Dgraph, проведено сравнение их функциональных возможностей для определения преимуществ и недостатков. Описанные методы обеспечения ИБ определяют основные средств защиты информации, которые необходимы для информационных систем в целом и графовых СУБД в частности. Кроме это показано, какими средствами можно устранить типичные уязвимости графовых СУБД. Также было установлено, что не все из них могут быть устранены рассмотренными методами. Поэтому в последующей работе будет описано ПО, которое поможет закрыть оставшиеся уязвимости, связанные с инъекциями кода в графовых СУБД.

СПИСОК ЛИТЕРАТУРЫ:

1. Отчет Verizon об утечках данных. URL: https://www.dataarmor.ru/десятка-крупнейших-угроз-безопаснос/ (дата обращения: 15.10.2020).
2. NoSQL – Инъекции на примере нереляционной СУБД. URL: https://cyberleninka.ru/article/n/nosql-inektsii-na-primere-nerelyatsionnoy-subd-mongodb/viewer. (дата обращения: 15.10.2020).
3. 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.]. Т. 26, № 3. С. 103–116, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1222 Дата (дата обращения: 15.10.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.09.
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: http://dx.doi.org/10.1109/W-FiCloud.2018.00017.
5. Харари Ф. Теория графов. М.: Мир. 1973. – 296 с.
6. Neo4j – Платформа для связанных данных. URL: https://neo4j.com/ (дата обращения: 15.10.2020).
7. Fernandes D., Bernardino J. Graph Databases Comparison: AllegroGraph, ArangoDB, InfiniteGraph, Neo4J, and OrientDB. DATA. 2018. P. 373–380. DOI: https://doi.org/10.5220/0006910203730380.
8. JanusGraph. URL: https://janusgraph.org/ (дата обращения: 15.10.2020).
9. DB-Engines Рейтинг графовых БД. URL: https://db-engines.com/en/ranking/graph+dbms. (дата обращения: 15.10.2020).
10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. URL: https://fstec.ru/component/attachments/download/289. (дата обращения: 15.10.2020).
11. Распространенные уязвимости Neo4j. URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=neo4j (дата обращения: 15.10.2020).
12. National Vulnerability Database. URL: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Neo4j&search_type=all (дата обращения: 15.10.2020).
13. Go Module Vulnerabilities. URL: https://github.com/dgraph-io/dgraph/issues/5569 (дата обращения: 15.10.2020).
14. DataArmor. С чего начинается защита базы данных? URL: https://www.dataarmor.ru/%D1%81-%D1%87%D0%B5%D0%B3%D0%BE-%D0%BD%D0%B0%D1%87%D0%B8%D0%BD%D0%B0%D0%B5%D1%82%D1%81%D1%8F-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%B1%D0%B0%D0%B7%D1%8B-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85/ (дата обращения: 15.10.2020).
15. 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: 15.10.2020).
16. Dgraph. URL: https://dgraph.io/ (дата обращения: 15.10.2020).

17. Data & Insight. 6 категорий решений для защиты Big Data в Apache Hadoop URL: https://dis-group.ru/company-news/articles/6-kategorij-reshenij-dlya-zashhity-big-data-v-apache-hadoop/ (дата обращения: 15.10.2020).

REFERENCES:

[1] Verizon data breach report. URL: https://www.dataarmor.ru/десятка-крупнейших-угроз-безопаснос/ (accessed: 15.10.2020) (in Russian).
[2] Fremuchkov A.N. NoSQL — Injection on the example of a non-relational DBMS. URL: https://cyberleninka.ru/article/n/nosql-inektsii-na-primere-nerelyatsionnoy-subd-mongodb/viewer (accessed: 15.10.2020) (in Russian).
[3] 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.]. Vol. 26, no. 3. P. 103–116, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1222 (accessed: 15.10.2020). 2020. DOI: http://dx.doi.org/10.26583/bit.2019.3.09 (in Russian).
[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: http://dx.doi.org/10.1109/W-FiCloud.2018.00017.
[5] Harari F. Graph theory. M.: Mir, 1973. 296 p. (in Russian).
[6] Neo4j – Platform for connected data. URL: https://neo4j.com/ (accessed: 15.10.2020).
[7] Fernandes D., Bernardino J. Graph Databases Comparison: AllegroGraph, ArangoDB, InfiniteGraph, Neo4J, and OrientDB. DATA. 2018. P. 373–380. DOI: https://doi.org/10.5220/0006910203730380.
[8] JanusGraph. URL: https://janusgraph.org/ (accessed: 15.10.2020).
[9] DB-Engines Ranking of Graph DBMS. URL: https://db-engines.com/en/ranking/graph+dbms (accessed: 15.10.2020).
[10] The basic model of threats to the security of personal data during their processing in information systems personal data. URL: https://fstec.ru/component/attachments/download/289 (accessed: 15.10.2020) (in Russian).
[11] Common Vulnerabilities and Exposures Neo4j. URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=neo4j (accessed: 15.10.2020).
[12] National Vulnerability Database. URL: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Neo4j&search_type=all (accessed: 15.10.2020).
[13] Go Module Vulnerabilities. URL: https://github.com/dgraph-io/dgraph/issues/5569 (accessed: 15.10.2020).
[14] DataArmor. Where does database protection begin? URL: https://www.dataarmor.ru/%D1%81-%D1%87%D0%B5%D0%B3%D0%BE-%D0%BD%D0%B0%D1%87%D0%B8%D0%BD%D0%B0%D0%B5% D1%82%D1%81%D1%8F-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%B1%D0%B0% D0%B7%D1%8B-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85/ (accessed: 15.10.2020).
[15] Gabrielan G.A. Graph database NEO4J for the design of high-load systems. Student electron. scientific. journal 2018. № 11(31). URL: https://sibac.info/journal/student/31/111409 (accessed: 15.10.2020) (in Russian).
[16] Dgraph. URL: https://dgraph.io/ (accessed: 15.10.2020).
[17] Data & Insight. 6 categories of security solutions Big Data in Apache Hadoop. URL: https://dis-group.ru/company-news/articles/6-kategorij-reshenij-dlya-zashhity-big-data-v-apache-hadoop/ (accessed: 15.10.2020) (in Russian).

Поступила в редакцию – 15 октября 2020 г. Окончательный вариант – 05 ноября 2020 г.
Received – October 15, 2020. The final version – November 05, 2020.

Аркадий И. Фрид[1], Алексей М. Вульфин[2], Виктория В. Берхольц[3]
Уфимский государственный авиационный технический университет,
ул. Карла Маркса, 12, Уфа, 450000, Россия
[1]e-mail: frid46@mail.ru, http://orcid.org/0000-0002-6129-6875
[2]e-mail: vulfin.alexey@gmail.com, http://orcid.org/0000-0001-5857-2413
[3]e-mail: torina4@yandex.ru, http://orcid.org/0000-0002-8065-7197

СПОСОБ МОНИТОРИНГА ЦЕЛОСТНОСТИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ ДВИГАТЕЛЯ ЛЕТАТЕЛЬНОГО АППАРАТА

DOI: http://dx.doi.org/10.26583/bit.2020.4.06

Аннотация. В статье представлен способ мониторинга целостности телеметрических данных о состоянии мобильного объекта, а именно, двигателя летательного аппарата, на основе сравнения технологических временных рядов. Технологические временные ряды, полученные с мобильного объекта, сравниваются с технологическими временными рядами, генерируемыми моделью мобильного объекта на предприятии-разработчике (изготовителе). Сравнение временных рядов осуществляется в выбранном временном окне за счет вычисления параметров согласованности: коэффициент детерминации, евклидово расстояние и средний процент отклонений. По вычисленным параметрам согласованности определяется тип согласованности в данном временном окне (7 типов), а также определяется тип динамики мобильного объекта: статический или динамический. Решение о целостности данных принимается по сформулированным правилам нечеткой логики, которые опираются на три параметра: тип динамики мобильного объекта, тип согласованности технологических временных рядов и сигнале системы контроля. Тестирование предложенного способа проводилось на данных, генерируемых системой автоматического управления двигателя летательного аппарата. Оценка вероятности правильности принятого решения составила 0,85.

Ключевые слова: двигатель летательного аппарата, телеметрия, целостность данных, инсайдер, временные ряды, близость временных рядов.

Для цитирования: ФРИД, Аркадий И.; ВУЛЬФИН, Алексей М.; БЕРХОЛЬЦ, Виктория СПОСОБ МОНИТОРИНГА ЦЕЛОСТНОСТИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ ДВИГАТЕЛЯ ЛЕТАТЕЬНОГО АППАРАТА. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 65–76, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1307>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.06.

***Благодарности.** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №20-08-00668.*

Arkadıi I. Frıd[1], Aleksеı M. Vulfın[2], Vıktoriya V. Berkholts[3]
Ufa State Aviation Technical University,
12, Karl Marks str., Ufa, 450008, Russia
[1]e-mail: frid46@mail.ru, http://orcid.org/0000-0002-6129-6875
[2]e-mail: vulfin.alexey@gmail.com, http://orcid.org/0000-0001-5857-2413
[3]e-mail: torina4@yandex.ru, http://orcid.org/0000-0002-8065-7197

The method of aviation gas turbine engine state information integrity monitoring*

DOI: http://dx.doi.org/10.26583/bit.2020.4.06

Abstract. The paper presents a method for monitoring the integrity of telemetric data on the state of a mobile object, namely, an aircraft engine, based on a comparison of technological time series. The technological time series obtained from the mobile object are compared with the technological time series generated by the model of the mobile object at the developer (manufacturer). Comparison of time series is carried out in the selected time window by calculating the consistency parameters: the coefficient of determination, Euclidean distance and the average percentage of deviations. According to the calculated

consistency parameters, the type of consistency in a given time window (7 types) is determined, and the type of dynamics of the mobile object is also determined: static or dynamic. The decision on data integrity is made according to the formulated rules of fuzzy logic, which are based on three parameters: the type of dynamics of the mobile object, the type of consistency of technological time series and the signal of the control system. Testing of the proposed method was carried out on the data generated by the automatic control system of the aircraft engine. The estimate of the probability of the correctness of the decision made was 0.85.

Keywords: aircraft engine, telemetry, data integrity, insider, time series, time series proximity.
For citation: FRID, Arkadii I.; VULFIN, Alekseı M.; BERKHOLTS, Vıktoriya V. Protection of the data integrity in telemetry systems about the state of mobile objects. IT Security (Russia), [S.l.], v. 27, n. 4, p. 65–76, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1307>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.06.

***Acknowledgement.** The study was carried out with the financial support of the Russian Foundation for Basic Research within the framework of scientific project No. 20-08-00668.*

Введение

Требования к безопасности мобильных объектов обязывают регистрировать и хранить данные об их состоянии с помощью бортовых контрольных устройств и самописцев. Подобные требования распространяются как на наземный транспорт в соответствии с приказом Минтранса России от 13 февраля 2013 г. № 36 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства», так и на воздушный транспорт в соответствии с приказом Минтранса РФ от 31 июля 2009 г. N 128 «Об утверждении Федеральных авиационных правил «Подготовка и выполнение полетов в гражданской авиации Российской Федерации». Обеспечение гарантоспособности систем передачи данных об объекте – телеметрической информации (ТМИ), является одной из важных задач обеспечения эффективного функционирования мобильного объекта. Возможность передачи ТМИ о мобильном объекте (МО), сгенерированной в процессе эксплуатации, на предприятие-разработчик (изготовитель) (ПР) позволяет более эффективно осуществлять техническое обслуживание МО, проводить своевременный ремонт, а также проводить расследование при возникновении аварийных ситуаций и других инцидентов, происходящих в процессе эксплуатации. В данной статье в качестве исследуемого МО представлен двигатель летательного аппарата (ЛА).

Обязательная передача ТМИ о состоянии отдельных компонентов ЛА в конструкторское бюро является необходимым условием для поддержания полного жизненного цикла сложного технического изделия (СТИ). Так, ГОСТ Р 55255-2012 «Система технического обслуживания и ремонта авиационной техники. Организация работ по диагностике технического состояния авиационной техники говорит о необходимости передачи информации о состоянии ЛА и его отдельных элементов между станциями технического обслуживания и промышленностью (пункт 6.2.2 г.)».

Передача ТМИ для анализа ее инженерами и персоналом по техническому обслуживанию. является одним из направлений совершенствования перспективных бортовых систем [1–4], и позволяет ПР получить конкурентное преимущество. Актуальной является проблема построения защищенных систем сбора, хранения и обработки данных о состоянии мобильного объекта в подобных системах [5].

Рассмотрим существующие методики контроля целостности данных.

1. Традиционные (общепринятые) методики защиты целостности:

ХЭШ-суммы, RAID-массивы, электронно-цифровая подпись (ЭЦП). Перечисленные способы обеспечения целостности не анализируют передаваемый контент. Внутренний злоумышленник, инсайдер, например, находящийся на станции ТО, может подвергнуть данные модификациям, после чего вычислить ХЭШ-функцию и передать ложную информацию вместе с контрольной суммой, или же подписать ложные данные с помощью ЭЦП.

2. Методики контроля целостности, учитывающие специфику сферы применения:

А) Обнаружение нарушений целостности навигационного поля пеленгационным методом контроля [6]. В данной методике предполагается контролировать целостность получаемых координат навигационных объектов при помощи вычисления координат пеленгационным методом и сравнения этих координат. Этот способ учитывает передаваемый контент, а также основан на сравнении получаемых данных и вычисляемых эталонных данных. Недостатком данного способа является узкий диапазон применения.

Б) В работе [7] применяется подход, основанный на анализе функциональных зависимостей в исследуемом объекте и расчете контрольных значений, на сравнении которых выносится решение о целостности данных. Такой подход уместен, если модель объекта описывается рядом простых моделей. Если же МО является многокомпонентным и связь его компонентов описывается математически нетривиальными способами, параметры МО характеризуются многомерностью и нелинейностью, простое сравнение контрольных значений с точностью до погрешности недостаточно.

Таким образом, необходимо построить систему мониторинга целостности, которая бы принимала решение о наличии или отсутствии вмешательства в данные на основе близости технологических временных рядов.

Мониторинг целостности данных, получаемых с мобильного объекта на ПР (изготовитель), ранее рассматривался авторами в [8]. Данный способ основывался на сравнении технологических временных рядов (ТВР), характеризующих поведение параметров мобильного объекта и модели этого же объекта, установленной на предприятии. Сравнение двух ТВР основывалось на вычислении коэффициента корреляции и детерминации и среднего процента отклонения, получении сигнала системы контроля исправности мобильного объекта и определении его режима работы.

Недостатком такого подхода стала низкая вероятность обнаружения вмешательства инсайдера, обусловленная тем, что для определения режима работы объекта использовался алгоритм кластеризации. Автоматическая классификация более, чем на два класса, не позволяет с высокой точностью определить режим работы объекта, что может привести к уменьшению вероятности обнаружения вмешательства злоумышленника. Сложная реализация алгоритма кластеризации режимов работы объекта требует дополнительных вычислительных ресурсов. Дополнительным фактором, снижающим вероятность обнаружения вмешательств злоумышленника, является то, что оба коэффициента корреляции и детерминации, иллюстрируют долю дисперсии, таким образом, согласованность ТВР фактически определяется только по двум параметрам: доле дисперсии и среднему проценту отклонения, что приводит к уменьшению точности оценки согласованности ТВР.

Целью данной статьи является повышение вероятности принятия правильного решения об установлении факта атаки на целостность данных.

Для достижения этой цели необходимо решить следующие задачи:

1. Разработать классификатор режима работы мобильного объекта, отличающий только два режима.

2. Разработать систему правил для блока принятия решения.

1. Система мониторинга целостности данных о состоянии мобильного объекта

Предлагаемая система мониторинга целостности данных, получаемых с эксплуатируемого мобильного объекта, основана на выделении в автоматическом режиме особенностей ТВР [4, 5].

Блок принятия решений о состоянии канала передачи данных с мобильного объекта на ПР обеспечивает обработку ТВР, генерируемых на эксплуатируемом мобильном объекте, и проводит сравнение этих данных с данными, генерируемыми моделью на предприятии [9].

На рис. 1 приведена структурная схема мониторинга целостности данных, получаемых с бортовых систем мобильного объекта.

В систему управления мобильным объектом поступает вектор *F*, характеризующий свойства внешней среды, например, температура и давление за бортом ЛА. Вектором *E* обозначены дополнительные эксплуатационные факторы [9].

Исходящими из объекта управления являются векторы *Y* и *X*. Вектор *Y* включает в себя параметры регулирования мобильным объектом. Вектор *X* включает характеристики мобильного объекта, например, расход топлива, рабочая температура, давление в рабочей зоне и т.п. В систему управления мобильным объектом поступает вектор управляющих воздействий *U*, формируемый системой управления. Система контроля мобильного объекта формирует сигнал о состоянии системы управления (исправна *K*=1/неисправна *K*=0).

Векторы *X, Y, K, F, E* направляются через канал передачи данных на предприятие-изготовитель. Канал подвергаются воздействию внешних факторов и шуму, воздействие которых обозначено вектором *N*.

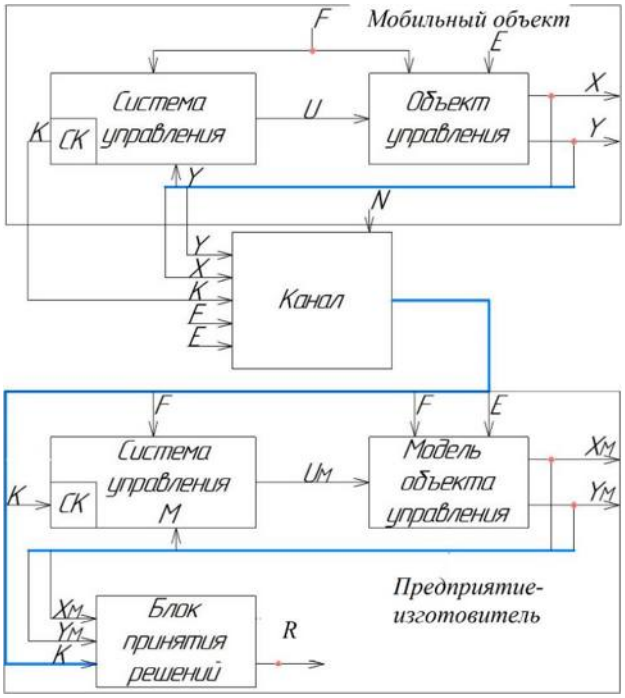

Рис. 1 Структурная схема мониторинга целостности данных, получаемых с бортовых систем мобильного объекта
(Fig. 1. Block diagram for the method of monitoring the integrity of data received from the mobile object systems)

На ПР модель мобильного объекта по параметрам работы (векторы *E* и *F* генерирует сигналы *YM* (аналог вектора *Y*), *XM* (аналог вектора *X*), исходящие из модели

объекта управления, и *UM*-вектор регулирующих воздействий модели мобильного объекта. Векторы *X, Y, YM, XM*, сигнал системы контроля *K* являются входными данными для блока принятия решения (БПР). В блоке проверятся близость временных рядов *X, Y, YM, XM* на основе вычисления метрик близости и анализируется состояние системы контроля *K*.

Выходом БПР является принятое решение *R* о целостности данных: 1 или 0 в зависимости от наличия или отсутствия несанкционированных модификаций злоумышленником, а также произошел ли отказ в оборудовании. Кроме того, можно получить оценку вероятности (степень уверенности) в принятом решении (*P*) [10].

2. Реализация системы мониторинга целостности ТМИ на примере системы управления авиационным газотурбинным двигателем

В качестве мобильного объекта рассмотрен газотурбинный двигатель (ГТД) ЛА его система автоматического управления (САУ), На рис. 2 приведена структурная схема блока принятия решений о состоянии целостности принимаемых данных

Данная система отличается от системы [10] реализацией классификатора режима работы мобильного объекта, а именно системы автоматического управления ГТД. На выходе блока формируется решение о том, в каком режиме находится модель САУ ГТД: установившемся или переходном. [11].

На вход классификатора режима САУ ГТД поступают производная частоты вращения ротора высокого давления и сигнал с выхода селектора минимального значения рассогласований управляемых параметров двигателя, являющегося элементом САУ ГТД [12], вычисляют абсолютные значения этих величин и сравнивают их с пороговыми значениями. Режим считается установившимся, если выполняется следующее условие:

$$\{|\Delta x| \le x_0\} \wedge \{|\dot{n_2}| \le \dot{n_{20}}\}=1, \quad (1)$$

где Δx – выход сектора минимума, $x_0 = 0{,}2\%$ от регулируемого в настоящий момент параметра, $\dot{n_2}$ –это производная частоты вращения ротора высокого давления, $\dot{n_{20}} = (0{,}05 - 0.1\%)$ $n_{2\,max}$/с. Для конкретных САУ ГТД эти значения могут отличаться от указанных.

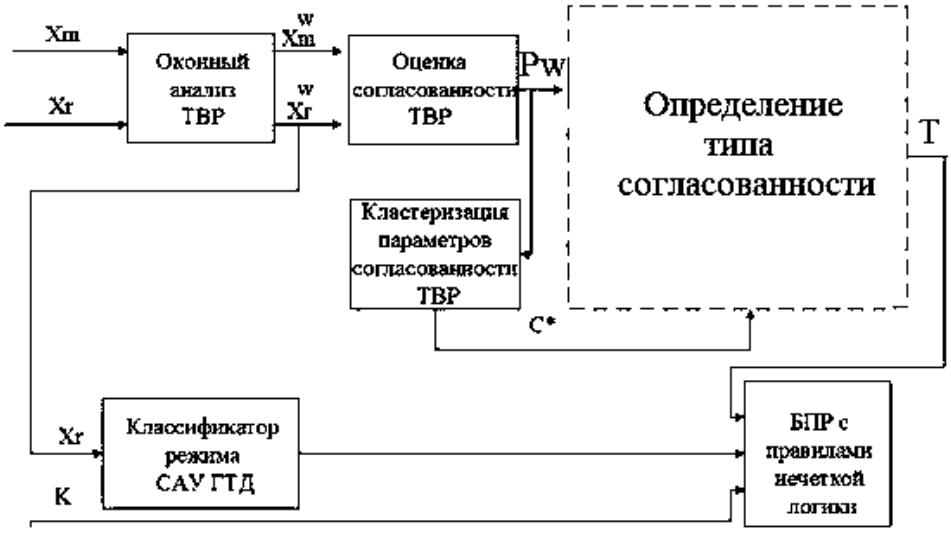

Рис. 2. Структурная схема блока принятия решений о целостности принимаемых данных
(Fig. 2. Block diagram of the block for making decisions on the state of TMI)

Если условие (1) не выполняется, то режим САУ ГТД считается переходным. В случае, если в выбранном временном окне встречаются и переходный, и установившийся режимы, то считают, что в данном временном окне САУ ГТД находится в переходном состоянии.

Оценка близости ТВР осуществляется с помощью набора метрик: коэффициент детерминации, средний процент отклонения (MAPE) [12] и евклидово расстояние [13].

Тестирование представленного способа проводилось на данных, представляющих два типа технологических временных рядов: ТВР, полученных с модели, и ТВР, полученных с ЛА. На ТВР, полученных с ЛА, с учетом реальных помех, возникающих при передаче данных, а также симулировались различные случаи нарушения целостности злоумышленником [14]. В общем случае подобные воздействия в момент времени *t* можно описать следующим выражением:

$$x(t) = \varepsilon(t) * (\varphi(x'(t)), \quad (2)$$

где $x(t)$ – значение принимаемого параметра САУ ГТД, $\varepsilon(t)$ – шум, накладываемый на сигнал, $x'(t)$ – передаваемое значение параметра САУ ГТД, $\varphi(x'(t))$ – воздействие внутреннего злоумышленника на передаваемое значение параметра САУ ГТД.

Нарушитель может осуществлять следующие действия по внесению модификаций в ТМИ и нарушению целостности [15, 16]:

- подмен передающей/принимающей станции – подавление сигнала истинной радиостанции и передача поддельной информации с ложной радиостанции станции;
- передача модифицированных данных по каналу передачи – упаковка модифицированной ТМИ в пакет и отправка на ПИ;
- многократное отправление ранее перехваченных данных по каналу связи.

Для описания правил при принятии решения о целостности данных были введены лингвистические переменные, характеризующие каждый из параметров согласованности, представленные в табл. 1.

Таблица 1. Лингвистические переменные

Термы лингвистических переменных	Коэф. Детерминации	Евклидово расстояние	MAPE
низкий	x<0.6	x>3	x>15
средний	0.6<x<0.8	1<x<3	10<x<15
высокий	x>0.8	x<1	x<10

Для формирования правил нечеткой логики необходимо выделить типы согласования ТВР. При текущем количестве метрик близости ТВР (3 метрики) будем руководствоваться следующими правилами компоновки

1. Объединим в первый тип метрики, если хотя бы 2 из них относятся к категории «высокий», и лишь одна может принимать значение «средний».
2. Объедим во второй тип метрики, если одна из них принимает значение «высокий», а две другие принимают значение «средний».
3. Объединим метрики в третий тип, если все они принимают значение «средний», или их среднее лингвистическое состоянии тоже можно охарактеризовать как средний
4. Объединим в четвертый тип согласованности метрики так, чтобы две из них принимали значение «средний», и только одна принимала значение «низкий»
5. Объединим в пятый тип метрики, если есть комбинация значения метрик «высокий» и «низкий»

6. Объединим в 6-й тип метрики, значение которых «низкий» и «средний». При этом, ни одна метрика не принимает значение «высокий».

Такое распределение метрик близости ТВР покрывает все возможные комбинации (27 комбинаций) при текущем количестве метрик. Однако, существуют режимы работы ГТД, при которых коэффициент детерминации может принимать значение NaN («Not a number», «нечисло») – несуществующее значение при постоянном значении параметра в текущем окне временного ряда. Для такого состояния коэффициента детерминации и при высоких показателях других метрик близости выделим отдельный 7-й тип согласованности, а также внесем такое состояние в другие типы согласованности.

При решении задачи кластеризации на типы согласованности, описанные 7 типов представлены в табл. 2

Таблица 2. Типы согласованности

Коэф. Детерминации	Евклидово расстояние	MAPE	Тип согласования ТВР
высокий	высокий	Высокий	1 тип
высокий/NaN	высокий	Средний	
высокий/NaN	средний	Высокий	
средний/NaN	высокий	Высокий	
высокий/NaN	средний	Средний	2 тип
средний/NaN	высокий	Средний	
средний/NaN	средний	Высокий	
высокий/NaN	низкий	Средний	3 тип
высокий/NaN	средний	Низкий	
низкий/NaN	высокий	Средний	
низкий/NaN	средний	Высокий	
средний/NaN	средний	Средний	
средний/NaN	низкий	Средний	4 тип
средний/NaN	средний	Низкий	
низкий/NaN	средний	Средний	
высокий/NaN	низкий	Низкий	5 тип
низкий/NaN	высокий	Высокий	
низкий/NaN	низкий	Высокий	
высокий/NaN	высокий	Низкий	
низкий/NaN	высокий	Низкий	
высокий/NaN	низкий	Высокий	
средний/NaN	низкий	Низкий	6 тип
низкий/NaN	средний	Низкий	
низкий/NaN	низкий	Низкий	
низкий/NaN	низкий	Средний	
NaN	высокий	Высокий	7 тип

БПР реализует набор правил, на основании которых выносится решение о целостности принятой ТМИ, которые представлены в табл. 3, где РРС – режим работы

САУ двигателя (установившийся и переходный), СК – система контроля. Если сигнал К=1, САУ ГТД исправна, в противном случае К=0. При сигнале системы контроля К=0 данные, полученные с ЛА, будут считаться недействительными. Это выделено в особое событие для БПР «Отказ САУ ГТД».

Таблица 3. Правила для принятия решения о целостности данных

К	РРС	Тип согласования	Результат
0	Любой	Любой	Отказ САУ ГТД
1	установившийся	1	нормальная работа
1	установившийся	2	нормальная работа
1	установившийся	7	нормальная работа
1	установившийся	3	нарушение целостности
1	установившийся	4	нарушение целостности
1	установившийся	5	нарушение целостности
1	установившийся	6	нарушение целостности
1	неустановившийся	1	нормальная работа
1	неустановившийся	2	нормальная работа
1	неустановившийся	3	нормальная работа
1	неустановившийся	4	нарушение целостности
1	неустановившийся	5	нарушение целостности
1	неустановившийся	6	нарушение целостности

Тестирование алгоритма проводилось на 5500 тестовых ТВР. Каждая пара ТВР (ТВР с модели и ТВР, генерируемых САУ ГТД, записанных при реальной передаче данных с учетом реальных шумов, возникающих в каналах передачи данных), представляет временное окно, состоящее из 100 отсчетов ТВР во временном окне. На рис. 3 представлен пример такого окна.

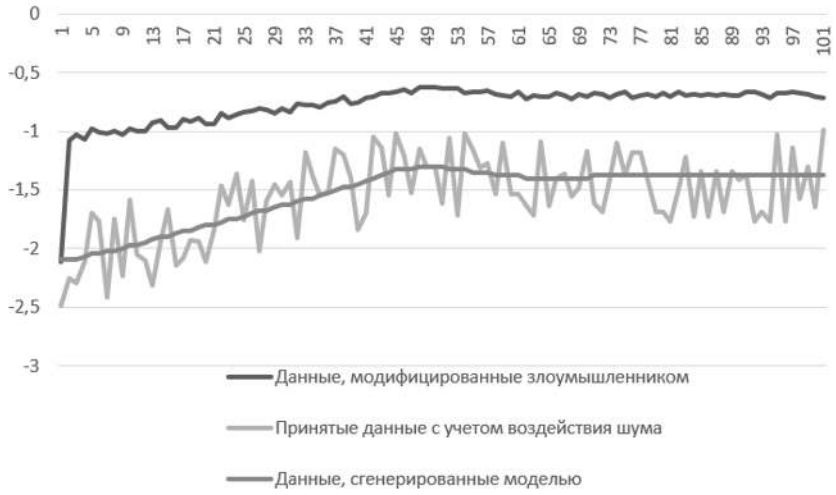

Рис. 3. Пример временного окна
(Fig. 3. Example of time window)

На некоторые данные, полученные с САУ ГТД, были проведены атаки злоумышленника, описанные в [16], для получения разных типов согласования ТВР. Далее, для каждой пары вычислялись параметры согласования ТВР.

Примеры приведены в табл. 4.

Вычисляем метрики близости двух ТВР, переводим их в значения лингвистических термов согласно табл. 1, определяем тип согласованности согласно табл. 2:

Таблица 4. Примеры

№	Значение	Коэф. Детерм.	Евклидово расстояние	MAPE	Тип согласованности	K	PPC
1	Численное значение	0,921	3,211	5,111%	2	1	Устан.
	Термы лингв. переменных	высокий	средний	средний			
2	Численное значение	0,654	5,232	10,2%	4	1	Неустан
	Термы лингв. переменных	средний	низкий	средний			
3	Численное значение	0,410	6,321	14,4	5	1	Устан.
	Термы лингв. переменных	низкий	низкий	средний			

Тогда согласно правилам, приведенным в таб. 3.

1 пара ТВР: Если «Тип согласованности = 1» И «К=1» И «PPC = Установившийся», то результат работы БПР – «нормальная работа».

2 пара ТВР: Если «Тип согласованности = 4» И «К=1» И «PPC=Неустановившийся», то результат работы БПР – «нарушение целостности».

3 пара ТВР: Если «Тип согласованности = 5» И «К=1» И «PPC=Установившийся», то результат работы БПР – «нормальная работа».

Итоговый протокол работы БПР представлен в табл. 5.

Таблица 5. Итоговый протокол работы БПР о целостности данных

Режим работы САУ ГТД	Количество тестовых выборок	Количество случаев успешного распознавания атаки	Оценка вероятности успешного распознавания атаки
Установившийся	3945	3498	0,89
Переходный	3415	2755	0,81
Итого	**5576**	**4670**	**0,85**

Таким образом, как видно из табл. 4, оценка вероятности правильности принятого решения о типе согласованности ТВР, а, следовательно, и о целостности данных, принятых с борта ЛА, составила 0,85.

Для сравнения, в работе [17] оценка целостности проводилась на циклических кодах, и находила 10-15% модифицированных пакетов при случайных угрозах безопасности. Однако, как отмечают сами авторы, данный способ не тестировался на модификациях, при которых злоумышленник знаком с системой обеспечения целостности, и может пересчитать циклический код уже после внедрения модификаций. При равных вероятностях обнаружения нарушения целостности (значение вероятности

обнаружения 0,89 при установившихся режимах работы и 0,85 при всех режимах работы), предложенный вид контроля целостности способен выявлять еще один вид модификаций (внутренним злоумышленником) благодаря анализу контента передаваемых данных.

Заключение

В статье представлена система мониторинга целостности данных о состоянии САУ ГТД, позволяющая выявить несанкционированные воздействия на данные и тем самым повысить уровень защиты информации при ее передаче с борта ЛА на предприятие-разработчик (изготовитель). Система мониторинга целостности данных основывается на оценке параметров согласованности ТВР: коэффициент детерминации, средний процент отклонения и евклидово расстояние; а также на определении режима работы САУ ГТД (установившийся или переходный) и состоянии системы контроля САУ ГТД.

Блок принятия решения о целостности данных реализует итоговое принятие решения о текущем состоянии системы и позволяет определить наличие одного из состояний согласованности данных модели и САУ ГТД: «Отказ системы автоматического управления газотурбинным двигателем», «Нормальная работа», «Нарушение целостности», и оценить вероятности такого состояния.

В дальнейшем авторами предполагается работа для усовершенствования работы БПР, а именно планируется обеспечивать мониторинг целостности для многомерных ТВР, включающих в себя несколько параметров, а также рассматривать не только отдельные временные окна, но и всю принятую информацию целиком. Проблема защиты для подобного рода многомерных данных и ее решение для обеспечения конфиденциальности описывается в [18] и требует особого подхода для задачи обеспечения целостности ТМИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Гузаиров М. Б., Фрид А. И., Вульфин А. М., Берхольц В. В., and Кириллова А. Д. "Анализ защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата" Вестник Уфимского государственного авиационного технического университета. 2019. Т. 23, № 4 (86). С. 132–146.
2. Горбатов, Виктор С; Жуков, Игорь Ю; Мурашов, Олег Н. Криптографический протокол аутентификации и выработки общего ключа контрольных устройств автотранспорта. Безопасность информационных технологий, [S.l.]. Т. 24. № 4. С. 27–34, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/274 (дата обращения: 11.07.2020). DOI: http://dx.doi.org/10.26583/bit.2017.4.03.
3. Чуянов Г.А., Косьянчук В.В., Сельвесюк Н.И., Кравченко С.В. Направления совершенствования бортового оборудования для повышения безопасности полетов воздушного судна // Известия ЮФУ. Технические науки. 2014. №6 (155). С. 219–229. URL: https://cyberleninka.ru/article/n/napravleniya-sovershenstvovaniya-bortovogo-oborudovaniya-dlya-povysheniya-bezopasnosti-poletov-vozdushnogo-sudna (дата обращения: 11.07.2020).
4. Бронников А.М. Эффективность технической эксплуатации необслуживаемой в межсервисный период бортовой системы воздушного судна // Научный вестник МГТУ ГА. 2017. №6. С. 89–98. DOI: https://doi.org/10.26467/2079-0619-2017-20-6-89-98.
5. Guzairov M.B. Frid A.I., Vulfin A.M., Berkholts V.V. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring // Proceedings of 2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). P. 1–6. DOI: https://doi.org/10.1109/ICOECS46375.2019.8950020.
6. Вульфин А.М., Фрид А.И. Нейросетевая модель анализа технологических временных рядов в рамках методологии Data Mining // Информационно-управляющие системы. 2011. №5. URL: https://cyberleninka.ru/article/n/neyrosetevaya-model-analiza-tehnologicheskih-vremennyh-ryadov-v-ramkah-metodologii-data-mining (дата обращения: 11.07.2020).
7. Мелихова А.П., Цикин И.А. Пеленгационный метод контроля целостности поля глобальных навигационных спутниковых систем // Научно-технические ведомости Санкт-Петербургского

государственного политехнического университета. Информатика, телекоммуникации и управление. 2015. №1 (212). С. 37–48.
8. Фазлиахметов Т.И. Фрид А.И. Модель анализа рисков несанкционированной модификации метрологических данных в производственных системах // Вестник УГАТУ = Vestnik UGATU. 2012. №3 (48). С. 187–193.
9. Гольберг Ф.Д. Математические модели авиационных газотурбинных двигателей как объект управления. / Гольберг Ф.Д., Батенин А.В. М.: издательство МАИ, 1999. – 82 с.
10. Фрид А.И., Гузаиров М.Б., Вульфин А.М., Берхольц В.В. Концепция мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата// сборниК докладов XXIII пленума ФУМО ВО ИБ и всероссийской научной конференции "фундаментальные проблемы информационной безопасности в условиях цифровой трансформации" (инфобезопасность - 2019). С. 7–14.
11. Гуревич, О.С., Гольберг, Ф.Д., Селиванов О.Д. Интегрированное управление силовой установкой многорежимного самолета / Под общ. ред. О.С.Гуревича. М.: Машиностроение, 1993. – 304 с.
12. J.S. Armstrong, F. Collopy, Error measures for generalizing about forecasting methods: Empirical comparisons, International Journal of Forecasting 8 (1) (1992). P. 69–80.
13. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. Новосибирск: ИМ СО РАН, 1999. – 270 с.
14. Гузаиров М.Б., Фрид А.И., Вульфин А.М., Берхольц В.В. Поддержка принятия решений в задаче обеспечения информационной безопасности авиационных систем телеметрии// Труды XXV юбилейного симпозиума «Надежность и качество», 25-31 мая 2020 г, Пенза, Россия, Т.1. С. 178–183.
15. Васильев В.И., Вульфин А.М., Берхольц В.В., Кириллова А.Д., Бельский С.М. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования // Вестник УГАТУ. Т. 23. № 4 (86), (2019). С. 122–131. URL: http://journal.ugatu.ac.ru/index.php/Vestnik/article/view/2216 (дата обращения: 11.07.2020).
16. Гузаиров М.Б., Фрид А.И., Вульфин А.М., Берхольц В.В., Кириллова А.Д. Анализ защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата // Вестник УГАТУ. Т. 23. № 4 (86). С. 37–43 (2019). URL: http://journal.ugatu.ac.ru/index.php/Vestnik/article/view/2206(дата обращения: 11.07.2020).
17. Джураев, Р. Х. Методы оценки рисков нарушения целостности информации в сетях передачи данных / Р. Х. Джураев, Б. М. Умирзаков, Д. Б. Абдуллаев. // Молодой ученый. 2017. № 15 (149). С. 46–51.
18. Горлатых, Андрей В.; Запечников, Сергей В. Построение защищенной системы управления многомерными структурами данных. Безопасность информационных технологий, [S.l.]. Т. 25. № 3. С. 16–25, 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136 (дата обращения: 11.07.2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.02.

REFERENCES:
[1] Guzairov M.B., Frid A.I., Vulfin A.M., Berkholts V.V., and Kirillova A.D. "Analysis of the security of the system for collecting, storing and processing telemetric information about the state of on-board systems of the aircraft" Vestnik Ufa State Aviation Technical University. 2019. Vol. 23. No. 4 (86). P. 132–146 (in Russian).
[2] Gorbatov, Victor S.; Zhukov, Igor Y.; Murashov, Oleg N. Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security (Russia), [S.l.]. Vol. 24. No. 4. P. 27–34, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/274 (accessed: 07/11/2020). DOI: http://dx.doi.org/10.26583/bit.2017.4.03 (in Russian).
[3] Chuyanov G.A., Kos'yanchuk V.V., Sel'vesyuk N.I., Kravchenko S.V. Directions for improving on-board equipment to improve aircraft flight safety. Izvestiya SFedU. (News SFU) Technical science. 2014. №6 (155). P. 219–229 URL: https://cyberleninka.ru/article/n/napravleniya-sovershenstvovaniya-bortovogo-oborudovaniya-dlya-povysheniya-bezopasnosti-poletov-vozdushnogo-sudna (accessed: 11.07.2020) (in Russian).
[4] Bronnikov A.M. The effectiveness of the technical operation of the aircraft system onboard unattended during the interservice period. Nauchnyj vestnik MGTU GA (Scientific Herald of the MSTU GA). 2017. №6. P. 89–98. DOI https://doi.org/10.26467/2079-0619-2017-20-6-89-98 (in Russian).
[5] Guzairov M.B. Frid A.I., Vulfin A.M., Berkholts V.V. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring. Proceedings of 2019 International Conference on Electrotechnical Complexes and Systems (ICOECS) P. 1–6. DOI: https://doi.org/10.1109/ICOECS46375.2019.8950020.
[6] Vulfin A.M., Frid A.I Neural network model for the analysis of technological time series in the framework of the Data Mining methodology. Informatsionno-upravlyayushchiye sistemy (Information Management

Systems) 2011. №5. URL: https://cyberleninka.ru/article/n/neyrosetevaya-model-analiza-tehnologicheskih-vremennyh-ryadov-v-ramkah-metodologii-data-mining (accessed: 11.07.2020) (in Russian).

[7] Melikhova A.P., Tsikin I.A. Direction finding method for monitoring the integrity of the field of global navigation satellite systems // Scientific and technical bulletins of the St. Petersburg State Polytechnic University. Computer science, telecommunications and management. 2015. No. 1 (212). P. 37–48.

[8] Fazliakhmetov T.I. Frid A.I. Model of risk analysis of unauthorized modification of metrological data in production systems. Vestnik USATU. 2012. No 3 (48). P. 187–193.

[9] Golberg F.D. Mathematical models of aviation gas turbine engines as an object of control. Golberg F.D., Batenin A.V. M.: MAI publishing house, 1999. – 82 p. (in Russian).

[10] Frid A.I., Guzairov M.B., Vulfin A.M., Berkholts V.V. The concept of monitoring the integrity of telemetric information about the state of the power plant of the aircraft. collection of reports of the XXIII plenum of the FUMO VO IB and the All-Russian scientific conference "fundamental problems of information security in the context of digital transformation" (information security -2019). P. 7–14 (in Russian).

[11] Gurevich, O.S., Golberg, F.D., Selivanov O.D. Integrated control of the power plant of a multi-mode aircraft. Under the general. ed. O.S. Gurevich. M.: Mechanical Engineering, 1993. – 304 p. (in Russian).

[12] J.S. Armstrong, F. Collopy, Error measures for generalizing about forecasting methods: Empirical comparisons, International Journal of Forecasting 8 (1) (1992). P. 69 – 80.

[13] Zagoruyko N.G. Applied methods of data and knowledge analysis. Novosibirsk: IM SB RAS, 1999. – 270 p. (in Russian).

[14] Guzairov M.B. Frid A.I., Vulfin A.M., Berkholts V.V. Decision support in the task of ensuring information security of aviation telemetry systems. Proceedings of the XXV anniversary symposium “Nadezhnost' i kachestvo” (Reliability and Quality), May 25-31, 2020, Penza, Russia, T.1. P. 178–183 p. (in Russian).

[15] Vasilyev V.I., Vulfin A.M. Berholts V.V., Kirillova A.D., Belsky S.M. Risk analysis of ensuring the integrity of telemetric inform.ation using cognitive modeling technology. Vestnik of Ufa State Aviation Technical University. Vol. 23. No. 4 (86). P. 122–131 (2019). URL: http://journal.ugatu.ac.ru/index.php/Vestnik/article/view/2216 (accessed: 11.07.2020) (in Russian).

[16] Guzairov M.B., Frid A.I., Vulfin A.M., Berkholts VV, Kirillova A.D. Analysis of the security of the system for collecting, storing and processing telemetric information on the state of the aircraft's onboard systems // Vestnik of Ufa State Aviation Technical University. Vol. 23. No. 4 (86). P. 37–43 (2019). URL: http://journal.ugatu.ac.ru/index.php/Vestnik/article/view/2206 (accessed: 11.07.2020) (in Russian).

[17] Dzhuraev, R. Kh. Methods for assessing the risks of violation of the integrity of information in data transmission networks R. Kh. Dzhuraev, BM Umirzakov, DB Abdullaev. Young scientist. 2017. No. 15 (149). P. 46–51 (in Russian).

[18] Gorlatyh, Andrey V.; Zapechnikov, Sergey V. Building secure multidimensional data management system. IT Security (Russia), [S.l.]. Vol. 25. No. 3. P. 16–25, 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136 (accessed: 07/11/2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.02 (in Russian).

Поступила в редакцию – 07 октября 2020 г. Окончательный вариант – 23 ноября 2020 г.
Received – October 07, 2020. The final version – November 23, 2020.

Григорий П. Гавдан[1], Рустем В. Пенерджи[2]
[1]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[2]ФГУП «Всероссийский Научно-исследовательский институт метрологической службы», Озерная ул., 46, Москва, 119361, Россия
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

DOI: http://dx.doi.org/10.26583/bit.2020.4.07

Аннотация. Целью написания статьи является рассмотрение вопросов, связанных с обеспечением безопасности информации информационных систем (ИС). Актуальность работы обусловлена, прежде всего, тем, что число кибератак на различные сферы экономики российского государства не уменьшается, а с каждым годом продолжает расти. Наблюдается растущий интерес к информации, циркулирующей в государственных органах управления (всех уровней) и государственных информационных систем (ГИС). Порой важные стратегические (государственные) задачи зачастую приходится отодвигать на «задний» план перед необходимостью решения срочных (важных сиюминутных) тактических задач. ГИС это неотъемлемая часть достаточно сложной системы управления, а (само) управление (фактически) становится ситуационным, а значит, и роль структур государственного управления, и ГИС, в этих условиях не утратила своей актуальности. Предметом исследования в работе является обеспечение безопасности ГИС в условиях неопределенности. Для достижения поставленной цели в работе проводится анализ нормативно правовых актов Российской Федерации. ГИС рассмотрены, как объекты компьютерных атак в условиях неопределенности. Разработана методика категорирования ГИС. В статье рассмотрены основные определения, аргументы и приведены источники, подтверждающие важность оценки угроз безопасности информации ГИС. В результате проведенных в работе исследований подтверждены возрастающая значимость защиты и актуальность разработки методики по оценке угроз безопасности информации. Вывод: правильно поставленная работа (с исходными данными) для проведения исследования в условиях высокой степени их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением информационной безопасности, в том числе и ГИС. Результаты исследования могут быть использованы при разработке методики оценки угроз безопасности государственных информационных систем.

Ключевые слова: безопасность информации, государственная информационная система, государственные органы управления, информационная система, объект компьютерных атак, оценки угроз безопасности информации, управление.

Для цитирования: ГАВДАН, Григорий П.; ПЕНЕРДЖИ, Рустем В. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 77–94, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1308>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.07.

Grigory P. Gavdan[1], Rustem V. Penerdji[2]
[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
[2]All-RUSSIAN RESEARCH INSTITUTE OF METROLOGICAL SERVICE, Ozernaya str., 46, Moscow, 119361, Russia
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221

Ensuring the security of state information systems in conditions of uncertainty

DOI: http://dx.doi.org/10.26583/bit.2020.4.07

Abstract. The paper addresses issues related to information security of information systems (IS). The Relevance of the work is primarily due to the fact that the number of cyber-attacks on various sectors of the Russian economy is not decreasing, but keeps growing every year. There is an increasing interest in the information circulating in government authorities (at all levels) and SIS. Sometimes important strategic (state) tasks often have to be relegated to the "background" before the need to solve urgent (important short-term) tactical tasks. Today, SIS is an integral part of a rather complex management system, and (itself) management (in fact) becomes situational, which means that the role of public administration structures, and SIS, in these conditions has not lost its relevance. The subject of the research is to ensure the security of SIS in conditions of uncertainty. To achieve this goal, the paper uses the method of analysis of regulatory legal acts of the Russian Federation. SIS data are considered as objects of computer attacks under conditions of uncertainty. The structure of the SIS categorization methodology was developed. The paper discusses the main definitions, arguments, and sources that confirm the importance of assessing threats to the security of SIS information. As a result of the research the increasing importance of protection and the relevance of developing a methodology for assessing information security threats are confirmed. Conclusion: correctly set work (with initial data) for conducting research in conditions of a high degree of their uncertainty is a key point in solving any problems related to information security, including SIS. The results of the study can be used to develop a methodology for assessing threats to the security of state information systems.

Keywords: information security, state information system, state management bodies, information system, object of computer attacks, information security threat assessment, management

For citation: GAVDAN, Grigory P.; PENERDJI, Rustem V. Ensuring the security of state information systems in conditions of uncertainty. IT Security (Russia), [S.l.], v. 27, n. 4, p. 77–94, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1308>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.07.

Введение

Всё чаще ведущие мировые эксперты обращают внимание на то, что сегодня мир вступил *в эпоху новой научно-технической революции*. Современное *коммуникационное*, быстро меняющееся общество вступило в информационный (постиндустриальный) период. Таким образом, мы (общество) все становимся свидетелями ситуации, когда проблемы (того или иного вида деятельности) *информационного общества* превосходят проблемы индустриализации производства[1].

Научно-техническая революция изменила очень многое, однако сейчас в обществе назрели перемены, в образе жизни, во внутреннем мире людей, поэтому можно говорить о социально-технологической революции, которая раздвигает рамки давосского проекта [1] и других технократических проектов будущего. Всё это зачастую связано с военными, политическими, конкурентными (борьбой) или экономическими «играми»; с расширением различных систем и сетей; с возможностью несанкционированного доступа к создаваемой, обрабатываемой, передаваемой и хранимой информации; с экономическим и промышленным шпионажем и др. Развитие методов, средств и форм (автоматизация процессов обработки, передачи, хранения и распространение информации; защита информации от незаконного изменения, уничтожения и хищения и др., а также их повсеместное применение) делает защищаемую информацию *более уязвимой* [2]. Действия злоумышленников могут быть направлены на информационные системы, IT-инфраструктуру компании, мобильные

[1]Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2019. – 314 с.

устройства, рабочие компьютеры, другие технические средства и, наконец, на любого человека как на элемент киберпространства [3].

Утверждается, что в прогнозный период развития информационные технологии будут способствовать реализации национальной программы «Цифровая экономика Российской Федерации» (например, налоговый маневр и др.). России (сегодня) предстоит обеспечить решение первоочередных задач[2] формирования цифровой экономики, в том числе:

– совершенствование регуляторной и нормативной среды;

– увеличение внутренних затрат на развитие цифровой экономики Российской Федерации (Министерство экономического развития Российской Федерации);

– обработки и хранения больших объемов данных;

– создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи;

– повышение уровня информационной безопасности во всех сферах деятельности;

– обеспечение подготовки высококвалифицированных кадров для экономики.

Так, например, в [3] за II квартал 2019 г. отмечаются следующие тенденции [3]:

– количество уникальных инцидентов остается высоким (превосходит показатель I квартала на 3%);

– целенаправленные атаки преобладают над массовыми атаками (их доля составила 59%. Это на 12 % пунктов больше, чем в I квартале);

– более половины всех компьютерных преступлений совершаются с целью кражи информации (это прямая финансовая выгода в 42% атак против частных лиц и в 30% атак на юридические лица);

– персональные данные (ПДн) – основной тип украденной информации в атаках на юридические лица (29%) (частные лица наиболее часто рискуют учетными записями и данными своих банковских карт – соответственно 44% и 34% от всего объема информации, украденной у частных лиц);

– уверенный рост курса биткойна, так объемы скрытого майнинга выходят на прежний уровень;

– набирают обороты Атаки MageCart на онлайн-ресурсы;

– специалистами отмечаются вредоносные JavaScript-снифферы, в том числе и на сайтах без функции оплаты;

– не уменьшается доля заражений вредоносным программным обеспечением (ПО) среди государственных учреждений (62% против 44% в I квартале 2019 г.). Наиболее часто в минувшем квартале, например, атакам троянов шифровальщиков;

– группировка RTM продолжает активно атаковать одну из слабо защищенных отраслей (промышленный сектор) [3].

Весьма существенное увеличение зарегистрированных преступлений наблюдается в IT-сфере. За 8 месяцев текущего года правоохранители выявили 180 153 (+66,8 %) преступления, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [4].

К глубокому сожалению, в России многие (изначально) экономические программы и бизнес практики оказались и/или продолжают оказываться трудно реализуемыми, ущербными, а то и вовсе заброшенными. Усложненность и парадоксальность развития экономических программ и бизнес-практик постоянно требует качественного обновления

[2]Прогноз социально-экономического развития Российской Федерации на 2021 год и на плановый период 2022 и 2023 годов. Министерство экономического развития Российской Федерации, 2019. – 94 с. URL: https://www.economy.gov.ru/material/file/956cde638e96c25da7d978fe3424ad87/Prognoz.pdf.

знаний, накопления опыта и навыков [5], чего не происходит. Большинство существующих решений достаточно плохо справляются с выявлением внешне легитимных действий злоумышленников и защитой ИТ-инфраструктуры, а потому в настоящее время активно применяется поведенческий анализ.

Перевод в сотрудников на удаленный режим работы из-за эпидемии COVID-19 привел не только к сокращению рабочих мест, но и к увеличению рисков. Пользователи через общедоступные сети для выполнения своей должностной работы массово заходят в корпоративные информационные системы, которые не обеспечены необходимой защитой.

Злоумышленник становятся изобретательнее, а, поэтому обеспечивать безопасность становится всё сложнее [5]. Он стал более изощренным: ведёт незаметные целевые атаки и может скачивать информацию ограниченного доступа, не привлекая к себе внимания [4]. Следовательно, существующие информационно-технологические разработки и программы должны учитывать и возникающие изменения, например, нарастание угроз, происходящие вокруг изменения и др. Органы государственной власти сегодня не являются исключением, которым для управления важно иметь хорошую и защищенную систему управления, работа которой направлена на разработку и построение целостной модели развития государства для его процветания, существования и выживания, в том числе и *в условиях неопределенности.*

Развитие (на перспективу) будущих теорий и практик общества в условиях неопределенности требует адекватного и ясного целеполагания действий. Так, например, достаточно ясное представление о серьёзных угрозах критической сферы народного хозяйства страны (национальная безопасность) за счет широкого внедрения современных информационных технологий (ИТ) сегодня можно найти в различных источниках[1]. Так, ГИС включают в себя информационно-технологические средства и системы, при создании которых опираются на передовые научные изыскания, такие как знания, передовые технологии (ноу-хау) и др. и являются неотъемлемой частью и достаточно сложной системы государственного управления [5].

Обратимся к определению, *государственные информационные системы* (ГИС) – это федеральные и региональные информационные системы (ИС), созданные на основании (соответственно) федеральных законов, законов субъектов РФ, на основании правовых актов госорганов. Они являются важной и неотъемлемой частью [6] сложной системы государственного управления и (ст.14)[3] созданы в целях реализации полномочий государственных органов и обеспечения обмена информацией.

Органы государственной власти разных уровней имеют в настоящее время значительные объемы информационных фондов, объединяющихся в десятки тысяч (баз данных), которые в области защиты информации (ЗИ) требуют к себе должного внимания. Следовательно, информационная инфраструктура, в том числе и её ГИС, будут продолжать оставаться одним из основных и важных объектов защиты [6].

Меры защиты информации (ЗИ) ГИС реализуются и выбираются с учетом *угроз безопасности информации* применительно к субъектам и объектам доступа (аппаратный, системный, прикладной и сетевой уровни); в среде виртуализации и облачных вычислений и т.д. Здесь необходимо также учитывать:

а) значения всех факторов, влияющих на требуемый уровень защиты информации ГИС (значения таких факторов в лингвистических переменных в виде унифицированной схемы представлены в работе Малюка А.А.[1], табл. XII.1);

[3]Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в редакции от 18 марта 2019 г.

б) организационные и технические меры ЗИ ГИС, которые определяются:

– масштабом ГИС;

– назначением ГИС;

– распределенностью сегментов ГИС.

в) затруднения, возникающие сегодня при обеспечении безопасности информации современных информационных систем, во многом связаны с:

– частым обнаружением новых уязвимостей и угроз в программном и аппаратном обеспечении информационных систем;

– задержкой при включении обнаруженных факторов риска в разные нормативно-правовые акты (НПА) РФ в области обеспечения безопасности информации и отсутствием соответствия между этими НПА;

– субъективностью экспертных оценок, возникающей при формировании модели угроз безопасности информационных систем и увеличивающейся при этом степенью неопределённости модели угроз.

Защита информации ГИС обеспечивается проведением таких мероприятий, как

– формированием требований к ЗИ ГИС;

– разработкой системы ЗИ ГИС;

– внедрением системы ЗИ ГИС;

– проведением аттестации ГИС по требованиям ЗИ;

– обеспечением ЗИ ГИС в ходе эксплуатации аттестованной ГИС;

– обеспечением ЗИ после принятия решения об окончании обработки информации;

– обеспечением ЗИ при выводе из эксплуатации, аттестованной ГИС и др.

Интерес к вопросам обеспечения безопасности информации ГИС продолжает расти. Это связывают, прежде всего, с

– небывалым повышением значимости информации (масштаб) как общественного (государственного) ресурса;

– существенными изменениями в организации информационно-технологических сетей и информационных технологий;

– возникающей опасностью злоумышленных действий по отношению к её законным участникам;

– наличием богатейшего опыта организации различных защитных мер бизнес процесса и др.;

– значимыми достижениями научных исследований в области защитных мер бизнес процессов;

– возросшей ролью государственных информационных ресурсов необходимых для обеспечения управления, жизнедеятельности государства.

Заметно усиление тенденций направленных:

– на повышение квалификации злоумышленников проводящих компьютерные атаки;

– на добывание злоумышленниками любой ограниченного доступа информации (государственной, коммерческой тайн, в том числе компрометирующей информации) ГИС;

– на увеличение частоты самих компьютерных атак на крупные мировые компании;

– на блокирование работы ГИС и вывод их из строя.

Так, в настоящее время, *не многие заказчики и операторы ГИС* понимают важность комплексной защиты информации в ИС. Использование полученной злоумышленником

информации может нанести серьезный ущерб. Именно поэтому необходимо осознанно подходить к выбору средств защиты информации в ГИС [7].

Перейдём к рассмотрению нормативно-правовых актов, регулирующих объекты КИИ и ГИС РФ.

1. Нормативно-правовые акты, регулирующие объекты КИИ и ГИС РФ

1.1 Критерии отбора нормативно-правовых актов

Отбор нормативно-правовых актов выполнялся по следующим критериям:

– областью регулирования НПА должна быть КИИ и ГИС;

– источником НПА должны быть федеральные органы исполнительной власти РФ и регуляторы в части защиты информации;

– НПА должны присутствовать в открытом доступе (документы, содержащие сведения, содержащую государственную тайну и конфиденциальную информацию не анализировались).

В настоящее время в Российской Федерации действуют следующие нормативно–правовые акты, регулирующие критическую информационную инфраструктуру (КИИ).

1.2 Перечень нормативно-правовых актов, применимых к объекту исследований

1.2.1 Законы и указы, применяемые к объекту исследований

В настоящее время в РФ действуют следующие НПА, регулирующие создание и функционирование объектов КИИ.

Так, основными концептуальными документами РФ в сфере информационной безопасности являются:

– Стратегия национальной безопасности РФ № 683 от 31.12.2015;

– Доктрина информационной безопасности РФ № 6646 от 05.12.2016;

– Стратегия развития информационного общества в РФ на 2017 – 2030 годы № 203 от 09.05.2017.

Основополагающими НПА Российской Федерации в указанной области являются:

– Федеральный закон № 187-ФЗ от 26 июля 2017 года;

– Закон Российской Федерации № 5485-1 от 21.07.1993;

– Указ Президента Российской Федерации № 1203 от 30.11.1995.

1.2.2 Подзаконные акты РФ, применяемые к объекту исследований

Во исполнение требований вышеприведенных законодательных актов разработаны, введены в действие и скорректированы следующие нормативные акты:

– Постановление Правительства РФ № 127 от 08.02.2018;

– Постановление Правительства РФ № 162 от 17.02.2018;

– Приказ ФСТЭК России № 31 от 14.03.2014;

– Приказ ФСТЭК России № 227 от 06.12.2017;

– Приказ ФСТЭК России № 235 от 21.12.2017;

– Приказ ФСТЭК России № 236 от 22.12.2017;

– Приказ ФСТЭК России № 239 от 25.12.2017;

– Приказ ФСБ Российской Федерации № 366 от 24.07.2018;

– Приказ ФСБ Российской Федерации № 367 от 24.07.2018;

– Приказ ФСБ Российской Федерации № 368 от 24.07.2018.

1.2.3 Методические документы РФ, применимые к объекту исследований

Помимо действующих нормативных актов необходимо вспомнить ещё и о Методических документах ФСТЭК России, например, таких как:

– «Меры защиты информации в государственных информационных системах»[4];
– «Методика моделирования угроз безопасности информации»[5] (проект).

1.3 Обзор законодательства по ГИС и КИИ основного геополитического противника

Различные отрасли экономики сегодня активно стоят на внедрении новых цифровых решений, которые позволят с помощью автоматизированных систем управления технологическими процессами, информационно-телекоммуникационных систем (сетей) и информационных систем осуществить модернизацию и повысить тем самым свою конкурентоспособность. Чаще всего приобретая такие решения, руководство предприятий или организаций не хотят (или не задумываются) уделять требуемого внимания вопросам обеспечения защиты информации [8] считая, что на этом можно сэкономить деньги.

В настоящее время считается, что основным геополитическим противником для США являются Китай и Российская Федерация. Содержание (является тому подтверждением) актуальной (редакция 2017 г.) Стратегии Национальной Безопасности США: «Китай и Россия бросают вызов американской власти, влиянию и интересам, пытаясь подорвать американскую безопасность и процветание» [9].

В [9] Россия обвиняется (*не обоснованно*) в проведении информационных атак против т.н. «свободного мира»: «Россия (по всему миру) использует информационные операции как часть (наступательные) киберусилий по влиянию на общественное мнение. Её кампании влияния сочетают тайные разведывательные операции и ложные онлайн-персонажи с государственными СМИ, посредниками и платными пользователями социальных сетей или «троллями» [10]. Наряду с сушей, морем, воздухом и космосом, *киберпространство*, признается организацией североатлантического альянса (НАТО) как оперативная область [11]. Эксперты НАТО одобряют развитие, как оборонительного, так и оперативно кибернетического потенциала [12] государства. К слову сказать, США существенно раньше всех озаботились защитой информации, как в ГИС, так и критической информационной инфраструктуре (*Federal Information and Information Systems* и *Critical Infrastructure*).

В США и странах запада на основе финансирования научно-исследовательских проектов различного вида и рода направлений заметно развитие и стремительный подъем информационных технологий (ИТ). К тому же в США сосредоточены ведущие научно-технические кластеры мира. Например, в США с 2015 г. по 2019 г. в области финансирования научных разработок в военной и гражданской сфере продолжает прослеживаться динамика (это сотни млрд долларов) роста вложений [13]. Благодаря такому внедрению научных разработок (значительный объем ИТ в США продается за рубеж) и развитию информационной сферы. Поэтому Америка остаётся (сегодня) абсолютным мировым лидером [13]. В настоящее время возникает большое количество вопросов, на которые необходимо дать точные ответы. Так, примером может послужить, определение критических процессов ГИС в условиях неопределённости и др.[6]

2. Разработка структуры методики категорирования Федеральной ГИС

2.1 Принадлежность объекта исследований к критической информационной

[4]Методический документ. «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.
[5]Проект Методического документа. «Методика моделирования угроз безопасности информации». ФСТЭК России 2020 г.
[6]Проблемные вопросы процедуры категорирования объектов КИИ // Единый портал электронной подписи. URL: https://iecp.ru/news/item/423941-problemnyye-voprosy-protsedura-kategorirovaniya-kiya-obyekty (дата обращения: 12.08.2020).

инфраструктуре

В случае с ФГИС Росстандарта, субъектом КИИ может быть «как юридическое лицо, которому ФГИС принадлежит на праве собственности – Федеральному агентству по техническому регулированию и метрологии, так и оператору информационной системы»[7].

В случае, когда оператор планирует расширение функциональных возможностей ИС, которое может повлечь за собой её отнесение (принадлежность) к КИИ, необходима проверка (изменение) правоустанавливающих документов оператора.

При проверке необходимо удостовериться, что сферы применения 187-ФЗ указанные в Уставе организации-оператора (раздел «Цели и предмет деятельности предприятия») и в Едином государственном реестре юридических лиц (ОКВЭД – Общероссийский классификатор видов экономической деятельности) имеют место.

В данном случае предполагается, что расширение функциональных возможностей ФГИС будет касаться области транспорта и/или связи. Так как у оператора в правоустанавливающих документах данные сферы деятельности отсутствуют, следовательно, необходимо запланировать внесение в них изменений.

Помимо внесения изменений в правоустанавливающие документы, рекомендуется издать внутренний нормативный акт оператора (приказ, распоряжение), подтверждающий планируемое расширение функциональных возможностей эксплуатируемой ИС с подтверждением принадлежности в этом случае к элементам КИИ.

2.2 Содержание работ по категорированию объектов критической информационной инфраструктуры

Структурная схема работ по категорированию объектов КИИ ФСТЭК России приведена на рис. 1 [14]. В соответствии с п. 5[8], процесс категорирования включает :

– определение процессов, выполняющихся в рамках реализации функций субъекта КИИ, а именно:

а) управленческих процессов;

б) технологических процессов;

в) производственных процессов;

г) финансово-экономических процессов;

д) иных процессов.

– выявление среди перечисленных выше так называемых критических процессов, то есть тех, нарушение штатного режима функционирования которых или полное прекращение функционирования может привести к негативным последствиям:

а) в социальной сфере;

б) в политической жизни;

в) в сфере экологии;

г) в экономике государства;

д) в сфере обеспечения обороноспособности и безопасности;

е) в области поддержания правопорядка.

– «выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения функционирования критических процессов, а также могут ими управлять

[7]Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

[8]Постановление Правительства РФ от 08.02.2018 № 127 «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».

или их контролировать»;

– «создание перечня объектов КИИ, которые подлежат категорированию»;

– «в соответствии с перечнем показателей критериев значимости, оценка масштаба последствий к которым могут привести инциденты ИБ на объектах КИИ»;

– «присвоение каждому из объектов КИИ соответствующей категории значимости (возможно представление обоснованного решения об отсутствии необходимости присвоения категорий)».

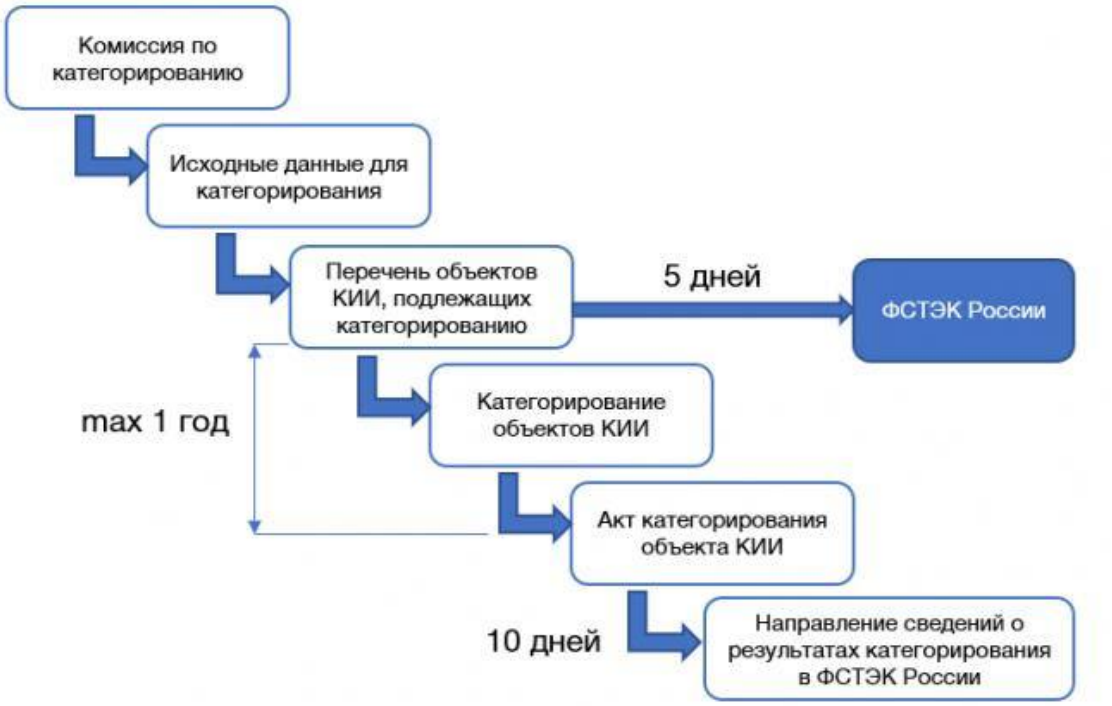

Рис. 1. Схема категорирования объектов КИИ
(Fig. 1. The scheme of categorization of objects CII)

По результатам исследований, ГИС находятся на первом месте среди прочих объектов целенаправленных компьютерных атак (APT), где злоумышленника интересует конкретная компания или государственная организация. Так, отмечено, «главное – это преобладание целенаправленных атак над массовыми атаками, и их доля составила 65% против 59% во II квартале [4].

Наибольший интерес для злоумышленников представляют *государственные учреждения*, промышленные компании, финансовый сектор и сфера науки и образования» [15]. Категории объектов компьютерных атак представлены на рис. 2.

В III квартале 2019 г. доля кибератак, направленных на кражу информации, выросла до 61% в атаках на юридические лица и до 64% в атаках на частных лиц (58% и 55% во втором квартале) [15]. При этом доля финансово мотивированных кампаний не превышает 31%.

Как указано Игорем Ляпуновым на BIS Summit Ekaterinburg, вице-президентом ПАО «Ростелеком» по информационной безопасности [16], «Существенно вырастет число атак, направленных на объекты КИИ и органы государственной власти, в том числе со стороны профессиональных группировок с инструментарием уровня government-stated» или «У атак на объекты КИИ нет монетизации, их задача – *получить контроль над инфраструктурой*».

Прогнозы на 2020 год для ГИС эту тенденцию сохранили [17], [18]: «Атак на критическую инфраструктуру будет больше – в этом сходятся во мнении эксперты *Group-IB, Trend Micro* и *Chronicle*. Промышленный шпионаж, атаки с помощью традиционного вредоносного ПО или вымогателей, атаки на цепочки поставок – варианты могут быть различны [17]. Атаки ожидаются как на предприятия энергетики, промышленные системы и системы жизнеобеспечения, так и на *ресурсы государственной власти*» и т.д.

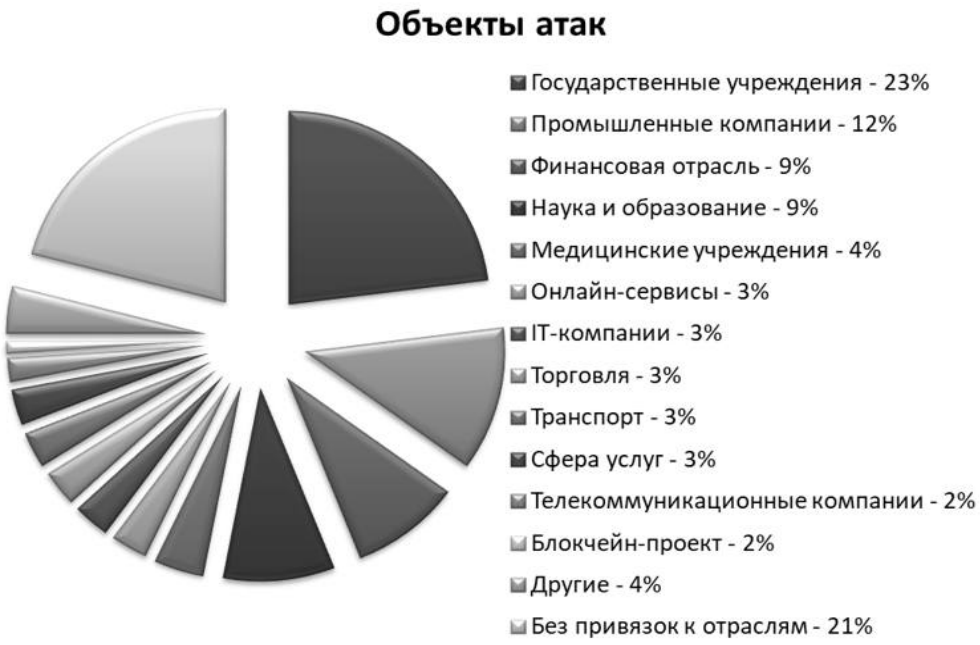

Рис. 2. Категории объектов компьютерных атак
(Fig. 2. Categories of objects of computer attacks)

3. ГИС, как объект компьютерных атак в условиях неопределенности

3.1 Тенденция к увеличению использования понятия неопределённости

Заметно, что число работ, использующих термин «неопределенность», постоянно растёт. Подтверждением данного утверждения служат результаты анализа публикационной активности.

3.2 Анализ публикационной активности

Анализ публикационной активности отечественных ученых и специалистов по теме неопределенности проводился по Российскому индексу научного цитирования (РИНЦ)». Рассмотренная «база научных публикаций ScienceDirect», которая составляет основу, индекса научного цитирования Scopus является тому подтверждением. Например, динамика зарубежных научных публикаций по теме «неопределенность» с 1991 по 2011 гг.

Согласно другим источникам интерес к данной тематике до 2019 г. не пропал и количество научных публикаций по теме «неопределенность» не уменьшилась.

3.3 Введение понятия «неопределённости».

Впервые понятие неопределённости было упомянуто [20] при формулировании понятия «информация». Информация, в соответствии с [20] – «”нечто”, что уменьшает неопределённость», т.е. в первоначальном смысле она являлась некоей мерой информации.

В настоящее время общепризнанного определения данного понятия, пусть даже в какой-либо отдельной области нет. В рамках настоящей работы под неопределённостью предполагается понимать «отсутствие или недостаток информации о чём-либо».

3.3.1 Классификация неопределённости

Для целей настоящего исследования будем использовать классификацию, приведенную в [21]. В настоящее время различают неопределенность *трех видов* (родов):

– «неопределенность среды или первого рода»;

– «неопределенность выбора принятия решения или второго рода»;

– «неопределенность будущей реализации принятого решения, она же третьего рода» [21].

Неопределенность 1-го рода – это неопределённость разнообразия и нестабильности окружающей среды. Данный род неопределенности не подчиняется наблюдателям или лицам, принимающим решение. Это – непрогнозируемое изменение внешних условий.

Неопределенность 2-го рода – это неопределённость выбора решения при необходимости его принятия.

Неопределенность 3-го рода – это неопределённость реализации принятого решения и последствий, наступающих после его принятия.

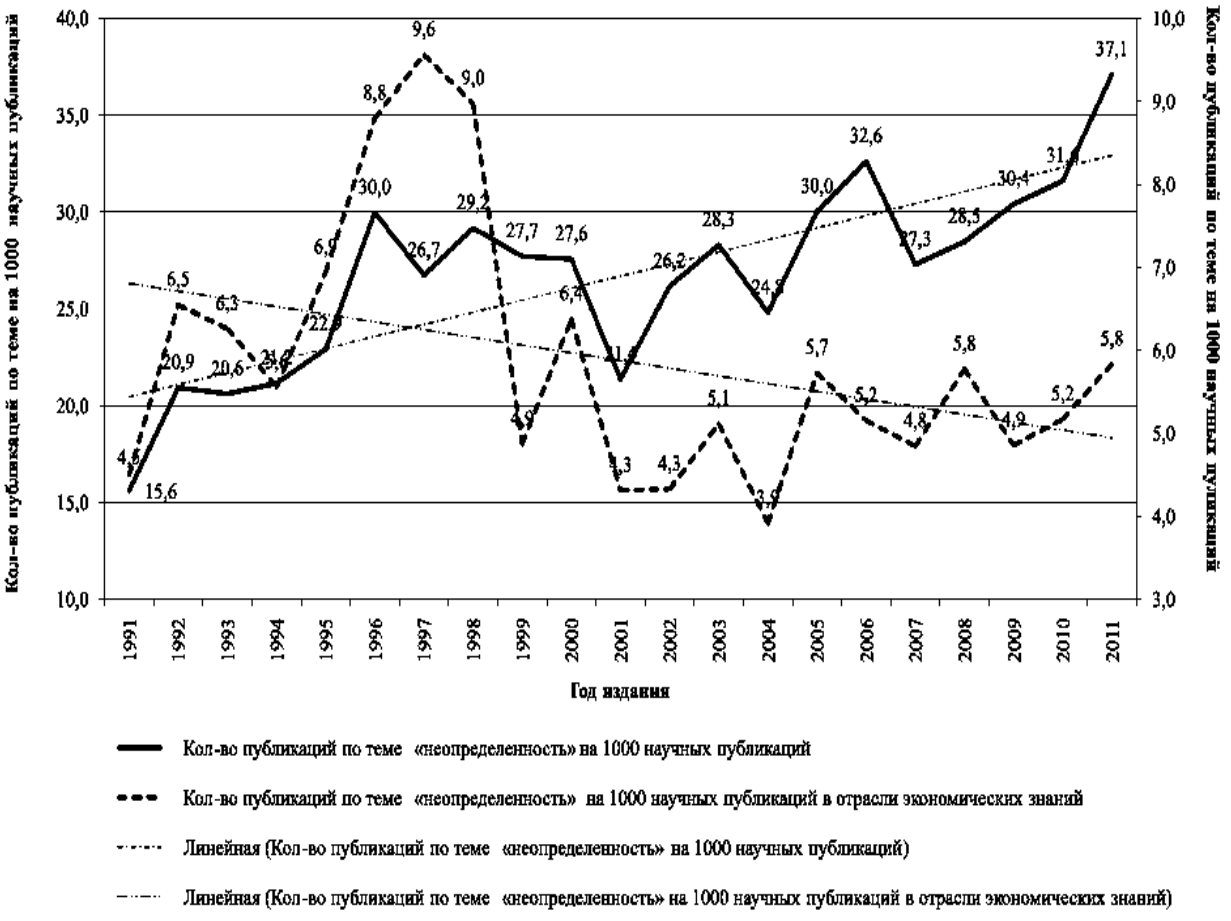

Рис. 3. Динамика зарубежных научных публикаций по теме «неопределенность» с 1991 по 2011 гг. по тематической направленности
(Fig. 3. Dynamics of foreign scientific publications on the topic «uncertainty» from 1991 to 2011 by thematic focus)

3.4 Неопределённость при обеспечении безопасности информации

Применительно к обеспечению безопасности информации термин неопределённость можно использовать следующим образом.

3.4.1 Неопределённости первого рода

К неопределённости первого рода или среды целесообразно отнести неопределённости, возникающие при несоответствии требований НПА как одних к другим, так и внешним условиям.

Проиллюстрировать несоответствие требований различных НПА можно сопоставлением[9,10,11] в части состава мер защиты информации.

К примеру, мера с кодом ЗИС. 21[8,9] сформулирована как «Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и т.п.», а в другом[10] как «Запрет несанкционированной удаленной активации периферийных устройств» и т.д. В качестве примера несоответствия внешним условиям, можно привести используемые для оценки угроз[9,12]. В обоих документах ставится задача уменьшения субъективности и неопределённости экспертных оценок, при отсутствии перечня конкретных мер по реализации. Также к неопределённости первого рода целесообразно отнести быстро меняющуюся ситуацию с разработкой и внедрением новых технологий. В [22] отмечено, что «Эпоха интернета и больших данных несет с собой поток информации, которую можно использовать для принятия решений. В этой ситуации проблемой для своевременного и точного принятия решений является уже не отсутствие информации, а риск невозможности понимания и управления присущей ей неопределенностью, возникающей из-за ненадежности, неполноты, обманчивости и её противоречивости» [22].

Данное обстоятельство ведёт к неопределённости второго рода – формирования решения.

3.4.2 Неопределённости второго рода

При повсеместном стремлении руководства нашего государства к внедрению так называемой цифровой экономики, которая формулируется, как хозяйственная деятельность важно помнить о том, что перегибы во всех областях к хорошим результатам никогда не приводили. Ключевым фактором производства здесь являются данные в цифровом виде (обработки больших объемов и использования результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг)»[13], где неопределённости первого рода возрастают. Например, там же упоминаются туманные вычисления, для которых отсутствует нормативная база по обеспечению безопасности информации. Более простой пример: как, при формировании модели угроз, определить границы защищаемого объекта, если часть вычислений выполняется в облаке.

3.4.3 Неопределённости третьего рода

[9]Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[10]Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

[11]Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ».

[12]Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.

[13]Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы».

К неопределенности третьего рода или неопределённость реализации принятого решения и последствий, наступающих после его принятия целесообразно отнести эксплуатацию информационной системы в условиях вредоносных воздействий. Изучение данного вида неопределённости выходит за пределы темы настоящей работы.

3.4.4 Учёт неопределённости при обеспечении безопасности информации

При наличии неопределённостей первого и второго рода, становится актуальной задача их учёта при обеспечении безопасности информации в ГИС.

Для этого, с учётом неопределённостей, необходимы как разработка математической модели угроз (МУ) безопасности информации, так и проекта методики, позволяющего оценить угрозы безопасности информации в ГИС.

Для постановки задачи можно использовать формулировку: «необходимо разработать методику М, позволяющую по множеству исходных данных сформировать множество актуальных угроз **Ω*** и получить значения субъективной вероятности p(ω) реализации каждой из угроз безопасности информации (УБИ), при этом неопределенность H(**Ω***) состояния безопасности информации в информационной системе с применением методики М должна быть меньше, чем та же неопределенность, но без применения методики М» [23].

3.5 Разработка методики оценки угроз безопасности информации в ГИС

При наличии неопределённостей первого и второго рода, становится актуальной задача их учёта при обеспечении безопасности информации ГИС. Данный проект методики оценки угроз безопасности информации в ГИС предусматривает меры по снижению неопределенности при оценке угроз. В рамках работы ГИС считается автоматизированной системой (АС), созданной в защищённом исполнении.

В соответствии с п. 5.9[14], стадии создания подобной АС соответствуют требованиям документа по стандартизации[15].

3.5.1 Особенности стадий создания информационных систем

Методика содержит перечень работ, выполняемых на следующих стадиях создания ИС[13]:

– «формирования требований к АС»;
– «разработки концепции АС»;
– «техническое задание на создание АС»;
– «эскизный проект АС»;
– «технический проект АС»;
– «рабочая документация на АС»;
– «ввод АС в действие»;
– «сопровождение АС».

При этом создаваемая МУ используется на всех стадиях жизненного цикла ИС.

3.5.2 Снижение неопределённости при моделировании угроз

Создание множества УБИ ГИС (в работе) выполняется на основании исследования выбранных угроз из БДУ ФСТЭК России (*https://bdu.fstec.ru/threat*), анализа используемого в информационной системе программного обеспечения и сопоставления совпадений с использованием экспертных оценок для оценки реализуемости этих угроз.

[14]ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения – Москва. ФГУП «СТАНДАРТИНФОРМ», 2018.
[15]ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» – Москва. ФГУП «СТАНДАРТИНФОРМ», 2009.

При этом угрозы, признанные нереализуемыми, остаются в создаваемой БДУ с присвоением числового показателя, оповещающего о нереализуемости. На каждом этапе создания должна происходить переоценка показателей реализуемости угроз.

3.5.2.1 Снижение неопределенности на этапе формирования требований, разработки концепции и создания технического задания на создание АС.

На данном этапе снижение неопределённости первого рода выполняется:

– формированием баз данных угроз в соответствии с [24];

– экспертной оценкой каждой УБИ из сформированной модели МУ с присвоением признака реализуемости.

Снижение неопределённости второго рода выполняется использованием для формирования экспертного мнения группы экспертов с принятием согласованного решения по каждой УБИ.

3.5.2.2 Снижение неопределенности на этапе создания эскизного и технического проектов и разработки рабочей документации АС.

На данном этапе снижение неопределённости первого рода выполняется:

– актуализацией созданной МУ в соответствии с выбранными БДУ;

– экспертной оценкой каждой УБИ из сформированной МУ с присвоением признака реализуемости.

Снижение неопределённости второго рода выполняется использованием для формирования экспертного мнения группы экспертов с принятием согласованного решения по каждой УБИ.

3.5.2.3 Снижение неопределенности на этапе ввода в действие и эксплуатации АС.

На данном этапе снижение неопределённости первого рода выполняется:

– актуализацией созданной МУ в соответствии с выбранными БДУ и актуальными НПА и методическими документами;

– экспертной оценкой каждой УБИ из сформированной БДУ с присвоением признака реализуемости;

Снижение неопределённости второго рода выполняется выполнением проведением тестирования на проникновение для АС с корректировкой созданной МУ.

Следует отметить отсутствие в ряде исходных данных однозначного соответствия с источниками реестра угроз, упомянутых ранее. Здесь важно помнить, что:

– практическое использование любых моделей оценки уязвимости упирается в ограничения (неполнота и недостоверность исходных данных);

– правильно поставленная работа с исходными данными в условиях их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением ИБ не только ГИС;

– принципиальным моментом практической реализации является построение адекватных моделей рассматриваемых систем (процессов).

Заключение

Анализ эксплуатируемых информационных фондов (ИФ) органов государственной власти РФ выявляет наиболее характерные тенденции проблемного характера, имеющие распространение на:

– информационные ресурсы, информационные системы и ГИС;

– объекты информатизации органов государственной власти РФ и субъектов РФ и др.

Результаты анализа и их оценка состояния эксплуатируемых информационных фондов позволяет сделать выводы, на основании которых можно сказать, что необходима методика оценки угроз безопасности информации ГИС, которая бы предусматривала меры по снижению неопределенности при оценке этих угроз. Для постановки задачи в работе использовалась формулировка: «необходимо разработать методику, позволяющую по множеству исходных данных сформировать множество актуальных угроз и получить значения субъективной вероятности реализации каждой угрозы БИ. При этом важно, чтобы неопределенность $H(\Omega^*)$ состояния безопасности информации в ИС с применением методики M должна быть меньше, чем та же неопределенность, но без применения методики M». Для решения такой задачи требуется учитывать много факторов, например, к основным можно отнести:

- вероятности возникновения различных угроз информации;
- стоимость реализации способов и средств ЗИ;
- наличие заинтересованных сторон;
- подготовка персонала по защите информации ГИС.

Вывод. Выбор методов, способов и средств защиты информации в ГИС является достаточно сложной оптимизационной задачей. Поэтому правильно поставленная работа с исходными данными (для проведения исследования) в условиях высокой степени их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением информационной безопасности, в том числе и ГИС.

СПИСОК ЛИТЕРАТУРЫ:

1. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности // Стратегические приоритеты. 2017. № 2 (14). С. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (дата обращения: 20.09.2020).
2. Малюк, Анатолий А.; Гавдан, Григорий П. Формирование и использование национальных информационных ресурсов – основа развития цифровой экономики. Безопасность информационных технологий, [S.l.]. Т. 26, № 2. С. 67–85, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200/1145/ (дата обращения: 20.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05.
3. Отчет компании PositiveTechnologies: Актуальные киберугрозы: II квартал 2019 года // PositiveTechnologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q2-rus.pdf. (дата обращения: 24.09.2020).
4. Статистические данные о зарегистрированных преступлениях на территории Российской Федерации в январе–августе 2019 года. URL: https://genproc.gov.ru/smi/news/genproc/news-1703326// (дата обращения: 20.11.2019).
5. Пенерджи, Рустем В.; Гавдан, Григорий П. Информационная безопасность государственных информационных систем. Безопасность информационных технологий, [S.l.]. Т. 27, №. 3. С. 26–42, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1290 (дата обращения: 25.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.03.
6. Рудницкий Е. Поведенческий анализ для защиты инфраструктуры: хакеры и коронавирус меняют рынок ИБ решений. URL: http://www.itsec.ru/articles/povedencheskij-analiz-dlya-zashchity-infrastruktury-hakery-i-koronavirus-menyayut-rynok-ib-reshenij?utm_medium=email&_hsmi=98246397&_hsenc=p2ANqtz-8Lx6jOBvC9ynjJlcgSG0fIaacWQafeSfWuo7a8edWxKBXjnbS4e-Sw8S_rlu52-lyunSBIVR3N0qFsxRHV5YcWuqH2aQ&utm_content=98246397&utm_source=hs_email (дата обращения: 26.10.2020).
7. Жумаева А.П., Ялбаева В.А., Селифанов В.В., Макарова Д.Г., Звягинцева П.А., Чернов Д.В. О выборе средств защиты информации для государственных информационных систем. Известия Тульского государственного университета. Технические науки. 2018. №10. С. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998/ (дата обращения: 28.09.2020).
8. Салкуцан, Алексей А.; Гавдан, Григорий П.; Полуянов, Андрей А. Методика определения критических процессов на объектах информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 18–34, 2020. ISSN 2074-7136.

URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187. (дата обращения: 03.09.20200). DOI: http://dx.doi.org/10.26583/bit.2020.2.02.

9. Рябова В. Китай признал существование кибервойск. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (дата обращения: 09.08.2020).
10. National Security Strategy of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 04.09.2019).
11. Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (дата обращения: 02.09.2020).
12. 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (дата обращения: 02.09.2020).
13. Гавдан, Григорий П.; Иваненко, Виталий Г.; Салкуцан, Алексей а. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 69–82, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232/1165 (дата обращения: 03.09.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
14. Щелкачев И.В. Правила категорирования объектов КИИ РФ. URL: https://d-russia.ru/wp-content/uploads/2018/06/2_pravila_kategorirovaniya_obektov_kii.pdf (дата обращения: 26.09.2020).
15. Positive Technologies: «Кибератаки все чаще носят целенаправленный характер». Итоги третьего квартала 2019 года. Журнал ПЛАС. По материалам Positive Technologies. URL: https://plusworld.ru/daily/cat-security-and-id/positive-technologies-kiberataki-vse-chashhe-nosyat-tselenapravlennyj-harakter/ (дата обращения: 26.09.2020).
16. Ляпунов И. Кибер атаки на критически важные для РФ объекты участились в десятки раз. РБК. ДИП. URL: https://www.rbc.ru/ekb/13/02/2019/5c641f829a794756010d719d (дата обращения: 27.09.2020). R-Vision. Прогнозы по информационной безопасности на 2020 года.
17. Anti-Malware.ru «Прогноз развития киберугроз и средств защиты информации 2020» URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast/ (дата обращения: 27.09.2020).
18. Кузьмин Е.А. Организационно-экономические системы в условиях неопределённости и определённости: оценка значений энтропии и негэнтропии // Управленец. 2012. № 11-12. С. 44–54. URL: https://cyberleninka.ru/article/n/organizatsionno-ekonomicheskie-sistemy-v-usloviyah-neopredelennosti-i-opredelennosti-otsenka-znacheniy-entropii-i-negentropii (дата обращения: 26.09.2020).
19. National initiative for cybersecurity education (NICE). URL: https://www.nist.gov/itl/applied-cybersecurity/nice. (дата обращения: 15.09.2020).
20. Авдийский В.И., Безденежных В.М. Неопределённость, изменчивость и противоречивость в задачах анализа рисков поведения экономических систем // Эффективное антикризисное управление. 2011. № 3. С. 46–61. URL: https://elibrary.ru/item.asp?id=16753895 (дата обращения: 15.09.2020). eLIBRARY ID: 16753895.
21. Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions // Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (дата обращения: 12.09.2020).
22. Ильченко А.Н. Математическая модель и методика оценки угроз безопасности информации в информационной системе в условиях неопределенности. С. 60–65 // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции "Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации" (ИНФОБЕЗОПАСНОСТЬ -2019) (дата обращения: 15.06.2020).
23. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (дата обращения: 15.09.2020).

REFERENCES:

[1] Akhromeeva TS, Malinetskiy G.G., Posashkov S.A. Strategies and risks of digital reality. Strategic priorities. 2017. № 2(14). P. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (accessed: 20.09.2020) (in Russian).

[2] Malyuk, Anatoly A.; Gavdan, Grigory P. Development and use of national information resources as the basis for digital economy development. IT Security (Russia), [S.l.]. V. 26, no. 2. P. 67–85, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200 (accessed: 20.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05. (in Russian).

[3] Positive Technologies report: Current cyber threats: Q2 2019. Positive Technologies URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q2-rus.pdf. (accessed: 24.09.2020) (in Russian).

[4] Statisticheskiye dannyye o zaregistrirovannykh prestupleniyakh na territorii Rossiyskoy Federatsii v yanvare–avguste 2019. URL: https://genproc.gov.ru/smi/news/genproc/news-1703326/. (accessed: 20.09.2020).

[5] Penerdji, Rustem V.; Gavdan, Grigory P. Information security of state information systems. IT Security (Russia), [S.l.]. V. 27, no. 3. P. 26–42, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1290 (accessed: 25.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.0 (in Russian).

[6] Rudnitskiy E. Povedencheskiy analiz dlya zashchity infrastruktury: khakery i koronavirus menyayut rynok IB resheniy. URL: http://www.itsec.ru/articles/povedencheskij-analiz-dlya-zashchity-infrastruktury-hakery-i-koronavirus-menyayut-rynok-ib-reshenij?utm_medium=email&_hsmi=98246397&_hsenc=p2ANqtz-8Lx6jOBvC9ynjJlcgSG0fIaacWQafeSfWuo7a8edWxKBXjnbS4e-Sw8S_rlu52-lyunSBIVR3N0qFsxRHV5YcWuqH2aQ&utm_content=98246397&utm_source=hs_email (accessed: 26.10.2020) (in Russian).

[7] Zhumaeva A.P., Erbaeva V.A., Selifanov V.V., Makarov G.D., Zvyagintsev P.A., Chernov D.V. On the choice of means of information security for government information systems. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2018. №. 10. P. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998 (accessed: 28.09.2020) (in Russian).

[8] Salkutsan, Alexei A.; Gavdan, Grigory P.; Poluyanov, Andrey A. The methodology for critical processes identifying at information infrastructure facilities. IT Security (Russia), [S.l.]. V. 27, no. 2. P. 18–34, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187 (accessed: 09.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (in Russian).

[9] Ryabova V. Kitay priznal sushchestvovaniye kibervoysk. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (accessed: 09.08.2020) (in Russian).

[10] National Security Strategy of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed: 04.09.2019).

[11] Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (accessed: 02.09.2020).

[12] 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed: 02.09.2020).

[13] Gavdan, Grigory P.; Ivanenko, Vitaliy G.; Salkutsan, Alexei A. Security of significant objects ofcritical information infrastructure. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 69–82, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (accessed: 03.09.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05 (in Russian).

[14] Shchelkachev I.V. Pravila kategorirovaniya obyektov CII RF of the Russian Federation. URL: https://d-russia.ru/wp-content/uploads/2018/06/2_pravila_kategorirovaniya_obektov_kii.pdf. (accessed: 26.09.2020). (in Russian).

[15] Positive Technologies: «Kiberataki vse chashche nosyat tselenapravlennyy kharakter». Itogi tretyego kvartala 2019. PLUS Journal. On materials Positive Technologies. URL: https://plusworld.ru/daily/cat-security-and-id/positive-technologies-kiberataki-vse-chashhe-nosyat-tselenapravlennyj-harakter/ (accessed: 26.09.2020).

[16] Lyapunov I. Kiber-ataki na kriticheski vazhnyye dlya of the Russian Federation obyekty uchastilis v desyatki raz. RBK. DIP. URL: https://www.rbc.ru/ekb/13/02/2019/5c641f829a794756010d719d (accessed: 27.09.2020). R-Vision. Prognozy po informatsionnoy bezopasnosti na 2020. (in Russian).

[17] Anti-Malware.ru «Prognoz razvitiya kiberugroz i sredstv zashchity informatsii 2020». URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast/ (accessed: 27.09.2020).

[18] Kuzmin E.A. Organizatsionno-ekonomicheskiye sistemy v usloviyakh neopredelennosti i opredelennosti: otsenka znacheniy entropii i negentropii. Upravlenets. 2012. № 11-12. S. 44–54. URL: https://cyberleninka.ru/article/n/organizatsionno-ekonomicheskie-sistemy-v-usloviyah-neopredelennosti-i-opredelennosti-otsenka-znacheniy-entropii-i-negentropii (accessed: 26.09.2020) (in Russian).

[19] National initiative for cybersecurity education (NICE) Workforce Framework Cybersecurity. NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (accessed: 15.09.2020).

[20] Avdiyskiy V.I. Bezdenezhnykh V.M. Neopredelennost, izmenchivost i protivorechivost v zadachakh analiza riskov povedeniya ekonomicheskikh sistem // Effektivnoye antikrizisnoye upravleniye. 2011. № 3. S. 46–61. URL: https://elibrary.ru/item.asp?id=16753895 (accessed: 15.09.2020). eLIBRARY ID: 16753895. (in Russian).

[21] Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions // Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (accessed: 12.09.2020).

[22] Ilchenko A.N. Matematicheskaya model i metodika otsenki ugroz bezopasnosti informatsii v informatsionnoy sisteme v usloviyakh neopredelennosti. S. 60-65. Sbornik dokladov XXIII plenuma FUMO VO IB i Vserossiyskoy nauchnoy konferentsii "Fundamentalnyye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii" (INFOBEZOPASNOST -2019) (accessed: 15.06.2020) (in Russian).

[23] Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (accessed: 15.09.2020) (in Russian).

Поступила в редакцию – 27 октября 2020 г. Окончательный вариант – 09 ноября2020 г.
Received – October 27, 2020. The final version – November 09, 2020.

Никита С. Жданов[1], Андрей В. Матерухин[2]
Московский государственный университет геодезии и картографии,
Гороховский пер., 4, Москва, 105064, Россия
[1]*e-mail: zhdanow3b@ya.ru, https://orcid.org/0000-0002-3687-6843*
[2]*e-mail: a_materuhin@miigaik.ru, https://orcid.org/0000-0002-9576-9925*

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ ЛАБОРАТОРНОЙ СРЕДЫ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАВЫКАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

DOI: http://dx.doi.org/10.26583/bit.2020.4.08

Аннотация. В статье описывается разработанная авторами виртуальная лабораторная среда для обучения навыкам тестирования на проникновение с обоснованием принятых проектных решений, а также результаты проведенного исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность». Показано, что виртуальная лабораторная среда для обучения навыкам тестирования на проникновение вполне может быть реализована с использованием программного обеспечения с открытым исходным кодом. Реализованная программная среда предъявляет достаточно умеренные требования к аппаратной платформе (конкретизированные в тексте статьи), на которой она должна выполняться. Проведенное исследование применимости показало, что разработанная виртуальная лабораторная среда может быть использована в учебном процессе с применением дистанционных образовательных технологий и позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности.

Ключевые слова: виртуальная лабораторная среда, навыки тестирования на проникновение, информационная безопасность, дистанционное обучение.
Для цитирования: ЖДАНОВ, Никита С.; МАТЕРУХИН, Андрей В. ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ ЛАБОРАТОРНОЙ СРЕДЫ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАВЫКАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 95–107, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1309>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.08.

Nikita S. Zhdanov[1], Andrey V. Materukhin[2]
Moscow State University of Geodesy And Cartography,
Gorokhovsky lane, 4, Moscow, 105064, Russia
[1]*e-mail: zhdanow3b@ya.ru, https://orcid.org/0000-0002-3687-6843*
[2]*e-mail: a_materuhin@miigaik.ru, https://orcid.org/0000-0002-9576-9925*

Using a virtual laboratory environment for penetration-testing skills training

DOI: http://dx.doi.org/10.26583/bit.2020.4.08

Abstract. This paper describes the virtual laboratory environment developed by the authors for training penetration-testing skills with justification of the design decisions, as well as the results of the study of the applicability of the developed virtual laboratory environment for teaching penetration-testing skills in the educational process of bachelor's degree in information security program. It has been shown that a virtual lab environment for training penetration-testing skills can be implemented using open source software. The implemented software environment makes rather moderate requirements to the hardware platform (specified in the paper) on which it should be executed. The study of applicability has shown that the developed virtual laboratory environment can be used in the educational process of bachelor's degree in information security program with the use of distance learning technologies and allows students to develop practical skills in using penetration testing methods on examples of objects of various levels of complexity.

Keywords: virtual laboratory environment, penetration-testing skills, information security, distance learning.
For citation: ZHDANOV, Nikita S.; MATERUKHIN, Andrey V. Using a virtual laboratory environment for penetration-testing skills training. IT Security (Russia), [S.l.], v. 27, n. 4, p. 95–107, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1309>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.08.

Введение

При проведении аудита информационной безопасности для оценки уровня защищенности компьютерных систем в последние годы все чаще используется тестирование на проникновение. В монографии [1] достаточно убедительно обосновано, что тестирование на проникновение представляет собой один из основных типов аудита критической информационной инфраструктуры. В монографии в частности сказано, что «…тестирование является более гибким инструментом аудита чем, например, мероприятия оценки соответствия, так как его проведение не ограниченно рамками действующих стандартов и регламентов В [2] отмечено, что использование методов обхода систем безопасности сетевых сервисов и проникновения в открытые информационные системы является основным методом проведения аудита безопасности информационных систем. Это мнение, на наш взгляд, излишне радикально, однако оно отражает возрастающую роль методов тестирования на проникновения в проведении оценки уровня защищенности компьютерных систем. Согласно [3], «контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов». Тестирование на проникновение позволяет реализовать главное назначение превентивной защиты – обнаружить уязвимость в защищаемой системе, что позволит обеспечить ее устранение и тем самым предотвратить возможные атаки с ее использованием.

Таким образом, навыки тестирования на проникновения становятся все более востребованы работодателями в области информационной безопасности, что делает формирование этих навыков в процессе обучения в вузе по направлению «Информационная безопасность» актуальной задачей. Однако использование упражнений, направленных на формирование этих навыков, в обычных компьютерных классах, являющихся частью сети университета, может привести к непредвиденным последствиям для этой сети. В [4] термин «тестирование на проникновение» определяется как метод оценки защищенности компьютерной системы или сети, основанный на имитации действий внешнего злоумышленника (не обладающего правами на доступ к системе) или инсайдера (обладающего определенным уровнем доступа)». Согласно [5], «тестирование на проникновение позволяет в достаточно короткие сроки объективно оценить реальный уровень защищенности информационных активов организации в условиях современного состояния способов несанкционированного доступа к информации». Достаточно очевидно, что использование способов несанкционированного доступа к информации в условиях университетской сети может привести как минимум к затруднениям в ее использования другими службами и учебными подразделениями университета. Это связано с тем, что в такого рода упражнениях студенты применяют различные инструменты, которые можно использовать для взлома систем.

Стандартное решение состоит в том, что потенциально опасные инструменты, вовлеченные в процесс обучения, должны использоваться отдельно от потенциально уязвимых систем, чтобы гарантировать, что эти инструменты не вызовут непредвиденных проблем в этих системах. Такой подход означает создание отдельной сети с атакующим и целевым компьютерами, не связанной с общеуниверситетской сетью. Недостатком этого

подхода, помимо дополнительных расходов на настройку и установку полностью изолированной системы, является невозможность корректно использовать ресурсы сети Интернет при выполнении упражнений.

Альтернативой описанному стандартному решению является создание виртуальной лабораторной среды в сети университета. Такая среда, в случае ее надлежащей реализации, может обеспечить защиту для реальных систем университета, позволяя обучаемым выполнить как полный спектр атак, так и провести оборонительные учения с использованием виртуальных машин.

В настоящей статье описывается разработанная авторами виртуальная лабораторная среда для обучения навыкам тестирования на проникновение с обоснованием принятых проектных решений, а также результаты проведенного исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность».

1. Краткий обзор работ по использованию виртуальных лабораторных сред для обучения студентов навыкам тестирования на проникновение

Использование сетевых виртуальных лабораторий в вузах началось довольно давно. Первые обнаруженные нами публикации на русском языке на данную тему относятся еще к концу 90-х годов прошлого века. Это, например, работа [6], которая описывает программные средства для создания виртуальных лабораторий. Следует заметить, что первоначально виртуальные лаборатории рассматривались как некоторый программно-аппаратный комплекс, позволяющий проводить эксперименты в некоторой предметной области без непосредственного контакта с реальной экспериментальной установкой или при полном отсутствии таковой. Важное преимущество такого подхода, как отмечено в [7], заключается в возможности использования виртуальной лаборатории в дистанционном обучении. Позже использование термина «виртуальная лаборатория» расширилось. В [8] виртуальные лаборатории рассматриваются как реализации интерактивных аттестующих элементов с автоматической проверкой ответов, доступ к которым обеспечивается средствами системы дистанционного обучения.

Несмотря на то, что работ, посвященных различным аспектам разработки и использования виртуальных лабораторий довольно много, почти все они не затрагивают предметную область информационной безопасности. Особенно мало академических работ, в которых рассматриваются аспекты разработки и использования виртуальной лабораторной среды для обучения студентов навыкам тестирования на проникновение.

В [9] описывается разработка и применение лабораторных стендов на основе платформ виртуализации для получения специалистами навыков и знаний о сетевой инфраструктуре объекта перед проведением реального аудита информационной безопасности. В работе обоснованы ограничения существующих готовых лабораторных стендов и средств для их построения в контексте обучения аудиту информационной безопасности, а также описывается разработанная виртуальная лаборатория. Это довольно интересное с нашей точки зрения решение, но оно слишком специализировано и предназначено для использования специалистами, уже обладающими довольно высоким уровнем подготовки, а поэтому не подходит для использования в условиях подготовки бакалавров информационной безопасности.

В [10] описана специализированная виртуальная лаборатория, позволяющая производить настройку и проверку DLP-системы, определять политику безопасности, обеспечивать контроль информационных потоков в компании, а также анализировать

выявленные инциденты. Решение основано на применении программного обеспечения компании InfoWatch, хорошо показывает возможности использования виртуализации в учебном процессе, но также является узкоспециализированным и не может рассматриваться как основа для формирования – навыков тестирования на проникновение.

В [11] приводится разработка Национального исследовательского университета «МИЭТ» – учебно-методический комплекс по подготовке к аудиту информационной безопасности магистрантов по направлению подготовки 10.04.01 «Информационная безопасность» по программе – «Аудит информационной безопасности автоматизированных систем», а также программный комплекс для построения среды виртуализации для моделирования сетевой инфраструктуры на базе симуляторов сетей Netsimulator, IMINES, Core, Mininet. Недостатком такого решения, с нашей точки зрения, является применение проприетарного программного обеспечения, что делает затруднительным настройку виртуальной среды под потребности обучения навыкам тестирования на проникновение.

В [12] при анализе необходимых характеристик лабораторной среды для тестирования на проникновения указано, что основной характеристикой должна быть ее универсальность, позволяющая исследовать различные типы атак. При создании виртуальной лаборатории, по мнению авторов работы [12], следует учитывать ограниченную мощность персонального компьютера (ПК), которая должна позволять проводить тестирование на проникновение. В качестве уязвимой информационной системы используется Metasploitable. По мнению авторов работы [12], уникальность их решения заключается в быстроте, доступности и легкости развертывания по сравнению с более сложными лабораториями, для функционирования которых необходимо более одного ПК. Разработанная ими лабораторная среда поддерживает стабильную работу на среднем по мощности ПК. Это объясняется тем, что основными компонентами являются Unix-подобные операционные системы на базе ядра Linux, обладающие сравнительно небольшими системными требованиями. Благодаря этому качеству лаборатория может быть развернута на ноутбуках и в компьютерных классах для обучения.

В [13] авторы также используют Metasploitable в качестве платформы для обучения студентов эксплуатации уязвимостей. Авторы отмечают, что практически каждый открытый сетевой порт является точкой входа в систему, а преимуществом Metasploitable является высокая удобность и эффективность.

Однако с нашей точки зрения работы [12–13] не позволяют создать на основе описываемых ими решений учебную платформу для студентов, поскольку использование в качестве уязвимой цели Metasploitable, в которой все возможные уязвимости одновременно доступны для возможного использования, затрудняет процесс обучения и контроля правильности выполнения учебных заданий.

В [14] авторы рассматривают возможность использования заданий из популярного ресурса root-me.org в качестве дополнения для разработанных ими лабораторных работ. На ресурсе root-me.org проводятся соревнования по информационной безопасности в формате «Захват флага» (CTF, Capture The Flag)[1]. Ресурс поддерживает английский, немецкий, французский и испанский языки, имеет большую базу уязвимостей, отсортированных по направлениям. Название заданий описывает уязвимость, эксплуатация которой позволит решить задание. Присутствует ранговая система начисления баллов за решенное задание: чем сложнее задание, тем больше за него начисляют баллов. По нашему мнению, ресурс действительно можно использовать в

[1]Root Me: Hacking and Information Security learning platform. URL: https://www.root-me.org (accessed: 10.10.2020).

качестве дополнительного материала в обучении в вузе, но для этого необходимо провести довольно большую предварительную методическую работу.

Ближе всего к нашему представлению о возможной реализации виртуальной лабораторной среды для обучения студентов методам тестирования на проникновения находятся решения, описанные в [15–18], в которых описывается использование в качестве платформы облачного кластера Гродненского государственного университета. Согласно [15], эта платформа используется с 2012 г., реализована на основе OpenNebula, а в качестве системы виртуализации использует Kernel-based Virtual Machine (KVM). В кластере реализовано три учебных лаборатории – начального, среднего и высокого уровня сложности. Работа обучаемого в лабораторной среде осуществляется на основе методики «серый ящик»: перед началом исследования предоставляется информация об инфраструктуре в виде схемы и описания деятельности виртуальной компании. Для автоматизации проверки ответов на задания лабораторий используются уникальные для каждого обучаемого токены (флаги), отмечающие соответствие найденной в результате проникновения уязвимости, требуемым эталонам. Прохождение начального уровня сложности открывает доступ к прохождению среднего уровня сложности, а затем высокого.

В работе [18] авторы выделяют три основных вектора составления заданий, соответствующие уровням сложности:

– сетевая безопасность (начальный уровень сложности);
– безопасность веб-приложений (средний уровень сложности);
– обнаружение атак (высокий уровень сложности).

Очень интересным, с нашей точки зрения, является решение, использованное для создания виртуальной лабораторной среды в Эдинбургском университет имени Нейпира (Edinburgh Napier University), описанное в [19]. В этой работе описано использование двух облачных сред – одна имитировала большой набор серверов и компьютеров обычных пользователей в самых разных сетевых конфигурациях, а другая имитировала набор компьютеров с установленными на них операционными системами семейства Linux с разными незакрытыми известными уязвимостями.

К сожалению, при всей привлекательности решений для создания виртуальной лабораторной среды в [15–19] они не могут быть использованы в нашем университете вследствие недостаточности материально-технической базы для ее реализации. Как нам представляется, это не только проблема нашего университета – в аналогичной ситуации находятся и многие другие российские университеты, реализующие программы по направлению «Информационная безопасность». Поэтому нами была разработана и реализована виртуальная лабораторная среда для обучения навыкам тестирования на проникновение, которая основана на использовании программного обеспечения с открытым исходным кодом и которая не требует наличия в университете дорогостоящего вычислительного кластера.

2. Требования к функционалу виртуальной лабораторной среды

В результате проведенного предварительного анализа были определены следующие обязательные требования к функционалу виртуальной лабораторной среды:

– виртуальная лабораторная среда должна поддерживать выполнение заданий, связанных с тестированием сетевой безопасности;

– виртуальная лабораторная среда должна иметь средства автоматизации проверки правильности выполнения задания;

– задания должны быть разделены по направлениям, соответствующим темам лекционного материала;

– виртуальная лабораторная среда должна обеспечивать разные уровни сложности выполнения заданий и упражнений, при этом начальный уровень сложности должен обеспечить пологость кривой обучаемости.

Использованные инструментальные средства для реализации виртуальной лабораторной среды можно условно разделить на три группы.

В первую группу входят программные средства, реализующие среду реализации. Важно отметить, что поскольку одним из выделенных требований к разрабатываемой среде является сравнительно низкий начальный уровень сложности заданий (кривая обучаемости должна быть пологой), то разумно использовать популярные среды реализации, то есть те, которые обучаемые скорее всего уже знают.

Самой популярной операционной системой для серверов являются системы на базе ядра Linux, поэтому большинство студентов по направлению «Информационная безопасность» уже имеют навыки работы в этой операционной системе. Серверные версии Linux к тому же, полностью соответствуют требованиям по быстроте, доступности и экономичности для системы. Поэтому было решено использовать операционную систему Linux для всех серверов лабораторной среды и среду VirtualBox для виртуализации.

Для реализации многих заданий, связанных с тестированием сетевой безопасности, необходимо использовать веб-сервер. Нами было принято решение использовать программное обеспечение с открытым исходным кодом – веб-сервер Apache. Это один из наиболее популярных веб-серверов[2]. Преимущества Apache в его гибкости, мощности и широкой распространенности. Он хорошо документирован и может быть расширен с помощью системы загружаемых библиотек. Использование этого программного обеспечения позволяет исполнять программы на большом количестве языков программирования без использования внешнего программного обеспечения.

Для хранения учетных данных и результатов обучаемых, было принято решение использовать также программное обеспечение с открытым исходным кодом – систему управления базами данных (СУБД) MySQL. К достоинствам MySQL можно отнести простоту использования, распространенность, а также популярность использования этой СУБД для обучения навыкам работы с базами данных.

Использование PHP в качестве языка веб-разработки обусловлено его популярностью, а также некоторым рядом достоинств:

– PHP специально разработан для веб-разработок и его код может внедряться непосредственно в HTML;

– пользователь не видит исходного PHP кода страницы;

– язык предоставляет широкие возможности программирования и позволяет подключать дополнительные модули и библиотеки;

– язык PHP без подключенных библиотек и модулей уязвим и, вместо создания уязвимостей, достаточно лишь не применять рекомендации по безопасности при разработке веб-приложения.

– связка PHP+MySQL является распространенной связкой для обучения разработке веб-приложений.

Для автоматизации проверки ответов на задания решено было использовать утилиту ncat – форк стандартной сетевой утилиты netcat. Данная утилита позволяет

[2]Usage statistics of web servers. URL: https://w3techs.com/technologies/overview/web_server (accessed: 10.10.2020)

общаться системам в одной сети посредством открытия сетевого порта на прослушивание или передачу информации. Использование ncat обусловлено дополнительными опциями, обеспечивающими защиту данных. Опция allow позволяет подключаться к операционной системе только с разрешенного ip адреса, а опция ssl шифрует соединение, исключая возможность перехвата данных.

Во вторую группу инструментальных средств для реализации виртуальной лабораторной среды входят программные средства для реализации уязвимостей в тестовой лабораторной среде. Классификацией векторов атак и уязвимостей занимается сообщество Open Web Application Security Project (OWASP).

Согласно списку OWASP TOP-10 2017 г. самыми распространенными векторами атак на веб-приложения являются:

1. Внедрение кода.
2. Некорректная аутентификация.
3. Незащищенность конфиденциальных данных.
4. Внедрение внешних XML-сущностей.
5. Нарушение контроля доступа.
6. Небезопасная конфигурация.
7. Межсайтовый скриптинг.
8. Небезопасная десериализация.
9. Использование компонентов с известными уязвимостями.
10. Недостаточное логирование и мониторинг.

Не все из представленных векторов атак представляют интерес для реализации в лабораторной среде. Наш выбор уязвимостей для реализации был основан на том, что задания на их основе должны быть простыми и понятными студенту, который только начал знакомиться с техниками тестирования на проникновение.

Нами были отобраны следующие вектора атак:

– внедрение кода и в качестве реализации данного вектора атаки – использование sql-инъекций в запросы к СУБД MySQL;

– некорректная аутентификация, представленная в виде cookie с именем пользователя;

– нарушение контроля доступа – отсутствие дополнительных проверок доступа к административной панели, кроме пароля;

– небезопасная конфигурация и в качестве реализации данного вектора атаки – простые пароли служб и аккаунтов, а также загрузка исполняемых файлов с PHP кодом из административной панели веб-приложения;

– использование компонентов с известными уязвимостями – уязвимое программное обеспечение FTP службы; уязвимость в команде sudo, позволяющая непривилегированным пользователям запускать команды с правами суперпользователя (уязвимость CVE-2019-14287[3]).

К третьей группе инструментальных средств для реализации виртуальной лабораторной среды относятся программные приложения, при помощи которых можно выявлять и эксплуатировать уязвимости. К этой группе утилиты для работы с возможными уязвимостями. Для нашей виртуальной лабораторной среды мы не стали ограничивать обучаемых в выборе этих средств, ограничившись рекомендацией использовать Kali Linux или любой другой популярный дистрибутив для тестирования на проникновение. В

[3]Potential bypass of Runas user restrictions. URL: https://www.sudo.ws/alerts/minus_1_uid.html (accessed: 10.10.2020)

процессе выполнения заданий студенты пользовались такими утилитами как Nmap, Hashcat, Hydra, BurpSuite, Metasploit Framework.

3. Описание разработанной виртуальной лабораторной среды

Общая структура разработанной тестовой лабораторной среды приведена на рис. 1.

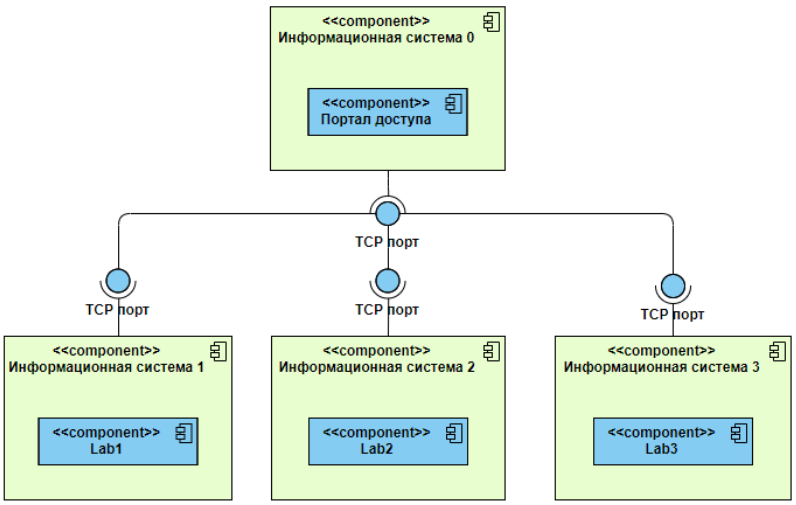

Рис. 1. UML диаграмма структуры тестовой лабораторной среды
(Fig. 1. UML diagram of the test laboratory structure)

Тестовая лабораторная среда состоит из:

– информационной системы с учебным сайтом, на котором расположены учетные записи студентов, задания, рейтинговая таблица;

– информационной системы с установленными уязвимыми компонентами (Lab1, Lab2 и Lab3 соответствующие лабораторным работам);

– канала связи между ними.

В состав тестовой лабораторной среды входят четыре виртуальные машины с установленными ОС Linux Ubuntu 18.04 LTS Server, а также установлен Apache веб-сервер и СУБД MySQL, проведены специальные настройки и установки.

Виртуальная лабораторная среда для обучения навыкам тестирования на проникновение содержит лабораторные работы, соответствующие трем направлениям:

1. Эксплуатация уязвимостей веб-приложения.
2. Эксплуатация уязвимостей сервера.
3. Применение полученных навыков.

Для реализации методики «серый ящик» в названии каждого задания помещена подсказка, позволяющая студенту понять эксплуатация уязвимости какого вида приведет к решению этого задания.

Задания и уязвимости соответствуют темам лекционного материала.

Необходимо было разработать и реализовать такой алгоритм, который отвечает следующим требованиям:

1. Ответ для каждого студента уникален.
2. Поддерживается работа нескольких студентов над одним заданием.
3. Передача данных должна осуществляться по зашифрованному каналу связи.

Решено было использовать утилиту ncat с дополнительными опциями allow для разрешения доступа к каналу связи только порталу доступа и ssl для шифрования

передаваемых данных. Алгоритм валидации ответа был реализован при помощи bash скриптов и php кода внутри страницы задания.

Портал доступа к тестовой лабораторной среде предполагает авторизацию студента для доступа к заданию. Авторизация происходит при помощи подключенного к странице php скрипта, обращающегося к СУБД MySQL, где хранятся учетные данные пользователей и таблица заданий. Авторизовавшись, студент получает доступ к заданиям. Было принято решение не нагружать систему дополнительными программными средствами и ограничиться применением стандартного элемента HTML – фрейма. Использование HTML фреймов обусловлено такими факторами, как удобство использования и возможность динамического расширения контента учебного сайта. На рис. 2 представлен итоговый вид портала доступа после прохождения процедуры авторизации.

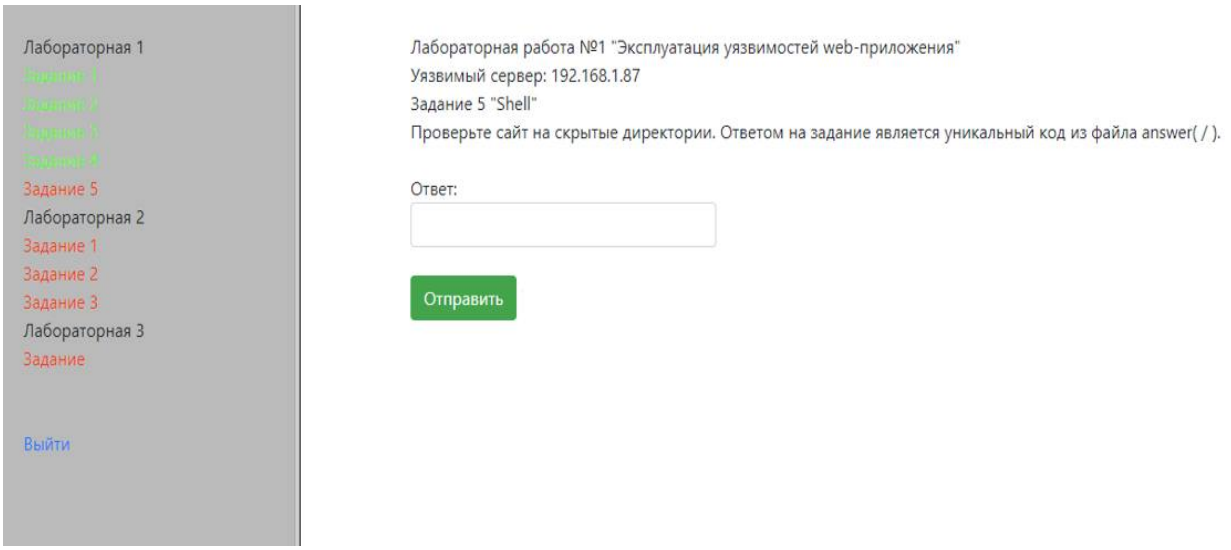

Рис. 2. Общий вид портала доступа
(Fig. 2. General view of the access portal)

Из рис. 2 видно, что страница разделена на 2 основных фрейма – фрейм задания и фрейм меню. В задании есть строчка с указанием адреса уязвимого приложения, а также поле ввода ответа и кнопка проверки ответа.

В меню выполненные задания обозначены зеленым цветом, а не выполненные – красным.

Унификация веб-приложений уязвимых информационных систем и портала доступа к заданиям позволила использовать одинаковые программные конструкции, что позволит упростить планируемое в дальнейшем расширение списка выполняемых лабораторных работ.

4. Исследование применимости и дальнейшее направление развития

Для исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность» программное обеспечение виртуальной лабораторной среды было установлено на аппаратную платформу в следующей конфигурации: 2 процессора Intel Xeon CPU E5-2690, 2.90GHz, 256Gb RAM. С привлечением студентов третьего и четвертого курсов были проверены различные варианты подключения к виртуальной лабораторной среде (из сети

университета, из дома, с использованием различных устройств), а также проведено нагрузочное тестирование с целью определить предельное значение количества одновременно комфортно работающих (то есть без возникновения субъективного чувства «торможения» системы) в виртуальной среде студентов. Исследование показало, что, по крайней мере, 30 студентов в условиях дистанционного обучения могут комфортно работать в системе на использованной аппаратной платформе.

Другим вопросом, на который должно было ответить исследование, был вопрос о том, действительно ли использование разработанной виртуальной среды позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение. Разработанная виртуальная лабораторная среда для тестирования на проникновение была использована для проведения лабораторных работ в течение весеннего семестра 2020 г. по дисциплине «Программно-аппаратные средства защиты информации. В исследовании принимало участие 24 студента (1 группа). Заданием для проверки навыков была выбрана третья лабораторная работа, охватывающая весь спектр уязвимостей, представленных ранее.

Результаты начального тестирования выявили неспособность студентов самостоятельно решить это задание (рис. 3). Итоговое тестирование, проведенное в конце семестра после выполнения в дистанционном режиме лабораторных работ в виртуальной лабораторной среде, показало, что более чем у 80 % студентов, прошедших обучение, были сформированы устойчивые практические навыки использования методов тестирования на проникновение (рис. 4).

Полученные результаты, по нашему мнению, показывают, что использование виртуальной лабораторной среды в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность» действительно позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности

Планируемое дальнейшее развитие разработанной виртуальной лабораторной среды связано с тем, что Московский государственный университет геодезии и картографии (МИИГАиК) является признанным российским центром компетенций как в области обработки геопространственных данных, так и в области обеспечения защиты таких данных.

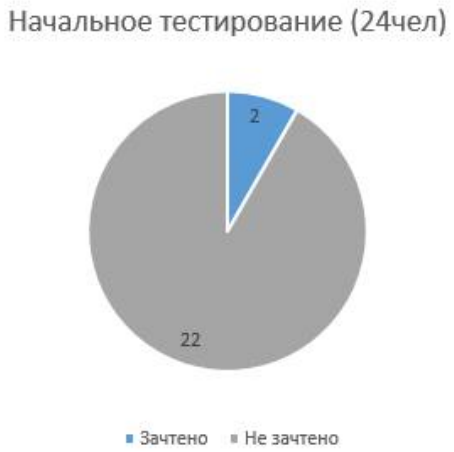

Рис. 3. Диаграмма начального тестирования (Fig. 3. Diagram of primary testing)

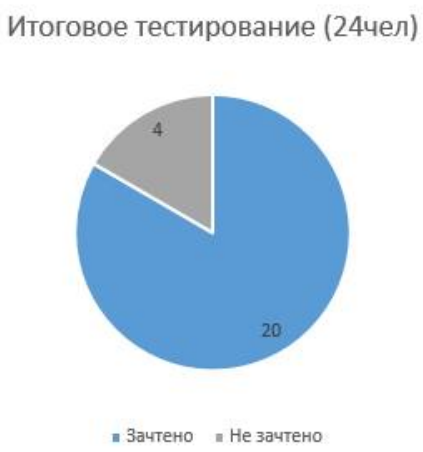

Рис. 4. Диаграмма итогового тестирования (Fig. 4. Diagram of final testing)

В работе [20] уже было указано, что все более широкое распространение как геоинформационных систем, так и систем сбора и обработки пространственных данных, сделало обеспечение безопасности в этой специфической сфере одним из весьма востребованных приложений технологий информационной безопасности. При разработке политики безопасности для геоинформационных систем необходимо учитывать характеристики геопространственных данных, а также то, что набор возможных уязвимостей для геоинформационных систем или систем сбора пространственно-временных данных обладает особенностями, характерными именно для этого типа компьютерных систем.

Заключение

В работе показано, что виртуальная лабораторная среда для обучения навыкам тестирования на проникновение вполне может быть реализована с использованием программного обеспечения с открытым исходным кодом. Реализованная программная среда предъявляет достаточно умеренные требования к аппаратной платформе, на которой она должна выполняться. Проведенное исследование применимости разработанной виртуальной лабораторной среды в условиях дистанционного обучения показало, что для поддержки одновременной работы 30 студентов в этой виртуальной среде вполне достаточно мини-кластера в следующей конфигурации: 2 процессора Intel Xeon CPU E5-2690, 2.90GHz, 256Gb RAM. Исследование также показало, что использование виртуальной лабораторной среды в учебном процессе действительно позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности.

Дальнейшим направлением развития виртуальной лабораторной среды в университете МИИГАиК является разработка тестовых виртуальных машин с установленными на них различными типами геоинформационных систем или систем сбора пространственно-временных данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. СПб.: Наукоемкие технологии, 2018. – 122 с. URL: https://elibrary.ru/item.asp?id=36445362 (дата обращения: 10.10.2020).
2. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. – 272 с. ISBN 978-5-4461-0662-2.
3. Горбатов, Виктор С.; Мещеряков, Алексей А. Сравнительный анализ средств контроля защищенности вычислительной сети. Безопасность информационных технологий, [S.l.]. Т. 20. № 1. С. 43–48, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/354 (дата обращения: 10.10.2020).
4. Котляров В.П. Современный подход к анализу уязвимостей информационных систем / В.П. Котляров, К.А. Ядыменко // Путь науки. 2014. Т. 1, № 9 (9). С. 38–41. URL: https://elibrary.ru/item.asp?id=22509935 (дата обращения: 10.10.2020).
5. Чуб, В. С. Аудит безопасности информационной системы с использованием тестов на проникновение // Молодой исследователь Дона. 2018. № 6 (15). С. 88–90. URL: https://elibrary.ru/item.asp?id=36903527 (дата обращения: 10.10.2020).
6. Дмитриев В.М., Зайченко Т.Н., Шутенков А.В Универсальная моделирующая среда для создания виртуальных лабораторий //В сборнике: Технический университет: дистанционное инженерное образование. Труды Международной научно-практической конференции. Министерство общего и профессионального образования РФ, Ассоциация технических университетов, Томский политехнический университет. 1998. С. 194–195.
7. Трухин А.В. Об использовании виртуальных лабораторий в образовании // Открытое и дистанционное образование. 2002. № 4 (8). С. 81–82. URL: https://elibrary.ru/item.asp?id=14794890 (дата обращения: 10.10.2020).
8. Вашенков О.Е., Волкова А.А., Лямин А.В. Примеры реализации сетевых виртуальных лабораторий в среде системы дистанционного обучения //Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007. № 45. С. 157–163. URL: https://elibrary.ru/item.asp?id=11543701 (дата обращения: 10.10.2020).

9. Иванов А.А., Настинов Э.О. Разработка виртуальной лаборатории для моделирования сетевой инфраструктуры объекта аудита //В сборнике: Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2019. Доклады Всероссийской конференции (с международным участием). Сер. "Научные конференции, посвященные дню Радио" 2019. С. 279–283. URL: https://elibrary.ru/item.asp?id=39137554 (дата обращения: 10.10.2020).
10. Калиберда Е.А., Шабалин А.М Использование современных систем виртуализации для формирования профессиональных компетенций студентов вузов при изучении DLP-систем // Наука о человеке: гуманитарные исследования. 2020. Т. 14. № 2. С. 118–122. URL: https://elibrary.ru/item.asp?id=43811417 (дата обращения: 10.10.2020).
11. Воеводин В.А. Учебно-методический комплекс по подготовке к аудиту информационной безопасности //В сборнике: ПРЕПОДАВАТЕЛЬ ГОДА 2019 сборник статей первого тура Международного научно-методического конкурса. 2019. С. 273–283. URL: https://elibrary.ru/item.asp?id=39132731 (дата обращения: 10.10.2020).
12. Красов А.В. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем / А.В. Красов, С.И. Штеренберг, А.И. Москальчук // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38–46. URL: https://elibrary.ru/item.asp?id=42576548 (дата обращения: 10.10.2020).
13. Стефінко Я. Я. Використання FOSS на платформі KALI Linux та Metasploitable для вивчення процесу етичного хакінгу / Стефінко Я. Я., Піскозуб А. З. // FOSS Lviv 2014, 24-27 квітня 2014 року: – Л.:, 2014. С. 118–121. URL: http://elartu.tntu.edu.ua/handle/123456789/16912 (дата обращения: 10.10.2020).
14. Кобилев, М.А. Опыт создания интерактивной образовательной платформы на основе инструментария соревнований ctf / М.А. Кобилев, Д.С. Зеленский, Е.С. Абрамов // Информационное противодействие угрозам терроризма. 2015. № 24. С. 321–328. URL: https://elibrary.ru/item.asp?id=23603864 (дата обращения: 10.10.2020).
15. Кадан А.М. Облачные лаборатории для задач тестирования на проникновение / А.М. Кадан, А.К. Доронин // Современные информационные технологии и ИТ-образование. 2016. Т. 12. № 3-1. С. 104–110. URL: https://elibrary.ru/item.asp?id=27411981 (дата обращения: 10.10.2020).
16. Кадан А.М. Виртуальные облачные лаборатории в подготовке специалистов направления "Компьютерная безопасность" / А.М. Кадан, С.А. Зайкова // Информатизация образования. 2015. № 2. С. 37–43. URL: https://elibrary.ru/item.asp?id=32844265 (дата обращения: 10.10.2020).
17. Кадан А.М. Облачный кластер университета в подготовке студентов направления "Компьютерная безопасность" // Ученые записки института социальных и гуманитарных знаний. Вып. 1(13): материалы VII международной научн.-практ. конф. "Электронная Казань 2015". Казань: ЮНИВЕРСУМ, 2015. С. 245–250. URL: https://elib.grsu.by/doc/13890 (дата обращения: 10.10.2020).
18. Кадан А.М. Изучение методов тестирования на проникновение в подготовке специалистов по защите информации / А.М. Кадан, А.К. Доронин // Информатизация образования. 2016. № 2. С. 3–11. URL: https://elibrary.ru/item.asp?id=32844238 (дата обращения: 10.10.2020).
19. Buchanan, William & Ramsay, Bruce & Macfarlane, Richard & Smales, Adrian & Russell, Gordon & (Jr, Bill. (2015). Teaching Penetration Testing and Malware Analysis within a Cloud-based Environment. URL:https://www.researchgate.net/publication/281030350_Teaching_Penetration_Testing_and_Malware_Analysis_within_a_Cloud-based_Environment (дата обращения: 10.10.2020).
20. Матерухин А.В. Особенности реализации образовательной программы по направлению подготовки 10.03.01 Информационная безопасность в Московском государственном университете геодезии и картографии с учетом специфики вуза // В сборнике: Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 146–150. URL: https://elibrary.ru/item.asp?id=29725564 (дата обращения: 10.10.2020).

REFERENCES:

[1] Makarenko S.I. Audit bezopasnosti kriticheskoj infrastruktury` special`ny`mi informacionny`mi vozdejstviyami. Monografiya. SPb.: Naukoemkie texnologii, 2018. – 122 s. URL: https://elibrary.ru/item.asp?id=36445362 (accessed: 10.10.2020) (in Russian).
[2] Skabczov N. Audit bezopasnosti informacionny`x sistem. SPb.: Piter, 2018. – 272 s. ISBN 978-5-4461-0662-2 (in Russian).
[3] Gorbatov, Victor S.; Meshcheryakov, Aleksey A. Comparative Analysis of Computer Network Security Scanners. IT Security (Russia), [S.l.]. Vol. 20. no. 1. P. 43–48, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/354 (accessed: 10.10.2020) (in Russian).
[4] Kotlyarov V.P., Yadymenko K.A. Modern approach to the analysis of information system vulnerability. Put` nauki. 2014. T. 1. № 9 (9). P. 38–41. URL: https://elibrary.ru/item.asp?id=22509935 (accessed: 10.10.2020) (in Russian).

[5] Chub, V. S Information system safety audit using penetration testing. Molodoj issledovatel` Dona. 2018. № 6 (15). P. 88–90. URL: https://elibrary.ru/item.asp?id=36903527 (accessed: 10.10.2020) (in Russian).
[6] Dmitriev V.M., Zajchenko T.N., Shutenkov A.V Universal`naya modeliruyushhaya sreda dlya sozdaniya virtual`ny`x laboratorij. V sbornike: Texnicheskij universitet: distancionnoe inzhenernoe obrazovanie. Trudy` Mezhdunarodnoj nauchno-prakticheskoj konferencii. Ministerstvo obshhego i professional`nogo obrazovaniya RF, Associaciya texnicheskix universitetov, Tomskij politexnicheskij universitet. 1998. S. 194–195 (in Russian).
[7] Truxin A.V. Ob ispol`zovanii virtual`ny`x laboratorij v obrazovanii. Otkry`toe i distancionnoe obrazovanie. 2002. № 4 (8). S. 81–82. URL: https://elibrary.ru/item.asp?id=14794890 (accessed: 10.10.2020) (in Russian).
[8] Vashenkov O.E., Volkova A.A., Lyamin A.V. Primery` realizacii setevy`x virtual`ny`x laboratorij v srede sistemy` distancionnogo obucheniya. Nauchno-texnicheskij vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta informacionny`x texnologij, mexaniki i optiki. 2007. № 45. S. 157–163. URL: https://elibrary.ru/item.asp?id=11543701 (accessed: 10.10.2020) (in Russian).
[9] Ivanov A.A., Nastinov E`.O. Development of a virtual laboratory for modeling network infrastructure of audit object. V sbornike: Radioe`lektronny`e ustrojstva i sistemy` dlya infokommunikacionny`x texnologij - RE`US-2019. Doklady` Vserossijskoj konferencii (s mezhdunarodny`m uchastiem). Ser. "Nauchny`e konferencii, posvyashhenny`e dnyu Radio" 2019. S. 279–283. URL: https://elibrary.ru/item.asp?id=39137554 (accessed: 10.10.2020) (in Russian).
[10] Kaliberda E.A., Shabalin A.M The impact of modern virtualization systems on university students' professional competences while studying dlp systems. Nauka o cheloveke: gumanitarny`e issledovaniya. 2020. T. 14. № 2. P. 118–122. URL: https://elibrary.ru/item.asp?id=43811417 (accessed: 10.10.2020) (in Russian).
[11] Voevodin V.A. Uchebno-metodicheskij kompleks po podgotovke k auditu informacionnoj bezopasnosti. V sbornike: PREPODAVATEL` GODA 2019 sbornik statej pervogo tura Mezhdunarodnogo nauchno-metodicheskogo konkursa. 2019. S. 273–283. URL: https://elibrary.ru/item.asp?id=39132731 (accessed: 10.10.2020) (in Russian).
[12] Krasov A.V., Shterenberg S.I., Moskal`chuk A.I. Virtual laboratory creation for distributed information system safety testing. Vestnik Bryanskogo gosudarstvennogo texnicheskogo universiteta. 2020. № 3 (88). S. 38–46. URL: https://elibrary.ru/item.asp?id=42576548 (accessed: 10.10.2020) (in Russian).
[13] Stefinko Ya. Ya., Piskozub A. Z. Using FOSS on the platform KALI Linux and Metasploitable for the study of the Ethical Hacking. FOSS Lviv 2014 (Lviv, 24-27 April 2014). P. 118–121. URL: http://elartu.tntu.edu.ua/handle/123456789/16912 (accessed: 10.10.2020) (in Ukrainian).
[14] Kobilev, M.A., Zelenskij D.S., Abramov E.S. Xperience in working with interactive educational platform based on ctf competition tools. Informacionnoe protivodejstvie ugrozam terrorizma. 2015. № 24. P. 321–328. URL: https://elibrary.ru/item.asp?id=23603864 (accessed: 10.10.2020) (in Russian).
[15] Kadan A.M., Doronin A.K. Oblachny`e laboratorii dlya zadach testirovaniya na proniknovenie. Sovremenny`e informacionny`e texnologii i IT-obrazovanie. 2016. T. 12. № 3-1. S. 104–110. URL: https://elibrary.ru/item.asp?id=27411981 (accessed: 10.10.2020) (in Russian).
[16] Kadan A.M., Zajkova S.A Virtual cloud laboratories in training of specialists of the direction "computer security". Informatizaciya obrazovaniya. 2015. № 2. S. 37–43. URL: https://elibrary.ru/item.asp?id=32844265 (accessed: 10.10.2020) (in Russian).
[17] Kadan A.M. University cloud cluster in the training of students of computer security direction. Ucheny`e zapiski instituta social`ny`x i gumanitarny`x znanij. Vy`p. 1(13): materialy` VII mezhdunarodnoj nauchn.-prakt. konf. "E`lektronnaya Kazan` 2015". – Kazan`: YuNIVERSUM, 2015. S. 245–250. URL: https://elib.grsu.by/doc/13890 (accessed: 10.10.2020) (in Russian).
[18] Kadan A.M., Doronin A.K. The study of methods for penetration testing in training of information security specialists. Informatizaciya obrazovaniya. 2016. № 2. P. 3–11.URL https://elibrary.ru/item.asp?id=32844238 (accessed: 10.10.2020) (in Russian).
[19] Buchanan, William & Ramsay, Bruce & Macfarlane, Richard & Smales, Adrian & Russell, Gordon & (Jr, Bill. (2015). Teaching Penetration Testing and Malware Analysis within a Cloud-based Environment. URL:https://www.researchgate.net/publication/281030350_Teaching_Penetration_Testing_and_Malware_Analysis_within_a_Cloud-based_Environment (accessed: 10.10.2020).
[20] Materuxin A.V. Osobennosti realizacii obrazovatel`noj programmy` po napravleniyu podgotovki 10.03.01 informacionnaya bezopasnost` v Moskovskom gosudarstvennom universitete geodezii i kartografii s uchetom specifiki vuza. V sbornike: Aktual`ny`e problemy` obespecheniya informacionnoj bezopasnosti. Trudy` Mezhvuzovskoj nauchno-prakticheskoj konferencii. 2017. S. 146–150. URL: https://elibrary.ru/item.asp?id=29725564 (accessed: 10.10.2020) (in Russian).

Поступила в редакцию – 10 октября 2020 г. Окончательный вариант – 06 ноября 2020 г.
Received – October 10, 2020. The final version – November 06, 2020.

Сергей В. Запечников[1,2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[2]Всероссийский институт научной и технической информации РАН,
Усиевича ул., 20, Москва, 125190, Россия
e-mail: SVZapechnikov@mephi.ru, https://orcid.org/0000-0002-7975-6040

СИСТЕМЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА, ОБЕСПЕЧИВАЮЩИЕ КОНФИДЕНЦИАЛЬНОСТЬ ТРАНЗАКЦИЙ*

DOI: http://dx.doi.org/10.26583/bit.2020.4.09

Аннотация. Статья посвящена актуальной проблеме обеспечения конфиденциальности информации при выполнении транзакций в системах распределенного реестра. Обсуждаются различные аспекты конфиденциальности транзакций и особенности постановки задачи для систем распределенного реестра с двумя моделями представления балансов участников: UTXO-моделью и моделью аккаунтов. Приводятся определения и обсуждаются свойства основных криптографических примитивов, используемых при решении задачи обеспечения конфиденциальности транзакций: перемешивающих сетей, кольцевой подписи, гомоморфного шифрования, доказательств с нулевым разглашением. Анализируются известные решения для систем распределенного реестра, основанных на UTXO-модели, такие как Zcash, Monero, Zcoin, Dash, CoinShuffle, Verge, Grin и другие, а также для систем, основанных на модели аккаунтов: DSC, Zether, Zeth, BlockMaze. На основе сопоставления достоинств, недостатков и ограничений к применению для существующих решений делаются выводы о перспективах развития систем распределенного реестра, обеспечивающих конфиденциальность транзакций, намечаются новые исследовательские задачи.

Ключевые слова: распределенный реестр, блокчейн-технологии, криптовалюта, консенсус, репликация сервисов, конфиденциальность.

Для цитирования: ЗАПЕЧНИКОВ, Сергей В. СИСТЕМЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА, ОБЕСПЕЧИВАЮЩИЕ КОНФИДЕНЦИАЛЬНОСТЬ ТРАНЗАКЦИЙ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 108–123, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1310>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09.

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

Sergey V. Zapechnikov[1,2]
[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoye shosse, 31, Moscow, 115409, Russia
[2]All-Russian Institute for Scientific and Technical Information of Russian Academy of Sciences (VINITI RAS),
Usievicha str., 20, Moscow, 125190, Russia
e-mail: SVZapechnikov@mephi.ru, https://orcid.org/0000-0002-7975-6040

The distributed ledgers ensuring privacy-preserving transactions*

DOI: http://dx.doi.org/10.26583/bit.2020.4.09

Abstract. The paper is devoted to the actual problem of ensuring privacy during performing transactions in distributed ledgers. We discuss various aspects of transaction privacy, as well as the specifics of setting the problem for distributed ledgers with two main models for representing participants' balances: the UTXO-model and the account model. Based on these results, we outline definitions and consider security properties of the main cryptographic primitives used for preserving the privacy of transactions: mixers, ring signatures, homomorphic encryption, and zero-knowledge proofs. We analyze well-known solutions

for distributed ledgers based on the UTXO-model, such as Zcash, Monero, Zcoin, Dash, CoinShuffle, Verge, Grin, and others, as well as for systems based on the account model: DSC, Zether, Zeth, BlockMaze. Based on the comparison of advantages, disadvantages, and limitations for existing solutions, conclusions are drawn about the future development of distributed ledgers that ensure the privacy of transactions, and new research tasks are outlined.

Keywords: distributed ledger, blockchain technologies, cryptocurrency, consensus, state machine replication, confidentiality.

For citation: ZAPECHNIKOV, Sergey V. The distributed ledgers ensuring privacy-preserving transactions. IT Security (Russia), [S.l.], v. 27, n. 4, p. 108–123, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1310>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09.

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

Введение

Технологии распределенного реестра (блокчейн-технологии) получили широкое распространение в качестве инструмента обеспечения доверия между сообществами пользователей во многих областях человеческой деятельности: от банковского дела и страхования до логистики и здравоохранения. Обзору технологий распределенного реестра как инструмента обеспечения доверия между участниками деловой деятельности посвящена статья автора [1].

Однако дальнейшее распространение блокчейн-технологий во многих областях человеческой деятельности сдерживается нерешенностью проблемы обеспечения безопасности информации. При этом доступность, целостность и подлинность информации обеспечиваются уже самими архитектурными и системотехническими решениями, на которых строятся системы распределенного реестра. «Слабым звеном» в информационной безопасности является конфиденциальность.

Проблема обеспечения конфиденциальности в системах распределенного реестра преимущественно проявляется в двух аспектах: в отношении данных транзакций, записываемых в реестр, а также в отношении кода исполняемых при этом смарт-контрактов. Настоящая статья посвящена первой из этих задач, для которой имеется целый ряд содержательных решений. Ограничение доступа к коду смарт-контрактов – это гораздо менее изученная и далёкая от решения задача, которая заслуживает отдельного исследования.

При анализе проблем обеспечения безопасности транзакций в системах распределенного реестра целесообразно использовать два понятия: конфиденциальность и приватность.

Первое из них хорошо знакомо специалистам в области информационной безопасности, закреплено во многих нормативно-технических и правовых документах. Конфиденциальность в самом общем понимании этого слова подразумевает гарантии того, что содержание информации ограниченного распространения не станет известно лицам, для которых это не предусмотрено политикой управления доступа к этой информации.

Второе понятие – приватность (privacy) – широко распространено в зарубежной литературе, но практически не используется в отечественных источниках и тем более не имеет сколько-нибудь официального статуса. Тем не менее, на нём стоит остановиться в контексте рассматриваемой темы.

Под приватностью в зарубежной литературе обычно понимают гарантии того, что никто не сможет узнать о владельце какой-либо информации больше того, что он сам

желает. Каждый владелец вправе регулировать, кто и какие сведения о нём получает. В то же время имеется много как легитимных, так и нелегитимных способов узнать о человеке больше, чем он сам того пожелает: прямые утечки данных, восстановление информации по косвенным признакам, интеллектуальный анализ данных с применением машинного обучения, что позволяет выявить «тонкие» и скрытые закономерности в данных. Это свойство применимо не только к конфиденциальным данным. Приватность включает в себя такие аспекты как разграничение доступа к информации, анонимность (когда она требуется), несвязываемость и неразличимость транзакций. Скорее всего, наиболее адекватным русскоязычным аналогом термина «приватность» можно считать фразу «обеспечение тайны частной жизни». В связи со сказанным представляется, что рано или поздно необходимость закрепления понятия «приватность» в отечественной нормативно-правовой базе будет осознана, и оно состоится.

Таким образом, применительно к транзакциям, совершаемым участниками деловой деятельности, сведения о которых сохраняются в системах распределенного реестра, использование понятия «приватность» выглядит оправданным и необходимым. Однако в связи с отсутствием установившейся практики применения этого термина в рамках данной статьи далее будет использоваться термин «конфиденциальность транзакций», подразумевая под ним, в том числе, аспекты, связанные с приватностью.

Рассмотрение систем распределенного реестра, обеспечивающих конфиденциальность транзакций, в статье начинается с характеристики в п. 1 двух основных моделей представления балансов в системах распределенного реестра, так как от них существенно зависит инструментарий и приёмы решения задачи. Далее, в п. 2 рассматриваются наиболее употребительные криптографические конструкции, помогающие обеспечивать конфиденциальность транзакций, даются их определения и обсуждаются требования к наличию защитных свойств. Пп. 3 и 4 посвящены анализу существующих систем, обеспечивающих конфиденциальность транзакций в UTXO-модели и модели аккаунтов соответственно.

1. Модели представления балансов в системах распределенного реестра

В ныне существующих системах распределенного реестра распространены две модели представления балансов участников: UTXO-модель (Unspent Transaction Output) и модель аккаунтов (account model).

Первая модель предполагает схему данных реестра в виде ориентированного ациклического двудольного графа, описывающего перемещение активов между участниками деловой деятельности. Пример такого графа показан на рис. 1. Модель основана на понятии непотраченного выхода транзакций (UTXO), т.е. такого подмножества вершин графа в каждый момент времени, который описывает состояние активов, перешедших в новое состояние в результате предыдущих транзакций, но ещё не послуживших «входом» для новых транзакций. Чтобы узнать баланс конкретного пользователя системы, нужно отследить и просуммировать все его непотраченные выходы транзакций. Первой системой распределенного реестра, построенной по UTXO-модели, стала криптовалюта Bitcoin [2]. В дальнейшем абсолютное большинство криптовалютных платформ, которые относятся к системам распределенного реестра открытого типа [1], также стало строиться на основе UTXO-модели.

Модель аккаунтов использует привычную для пользователей и интуитивно понятную модель учётной записи с привязанным к ней «личным кабинетом», что даёт возможность удобно управлять движением учитываемых в реестре активов. Для этой модели характерна широкая функциональность, обусловленная возможностью связывать

транзакции со смарт-контрактами. Первой системой распределенного реестра, в которой реализована эта идея, стала платформа открытого типа Ethereum [3]. Впоследствии модель аккаунтов распространилась и на платформы закрытого типа, такие как Hyperledger Fabric [4]. Вместе с тем, блокчейн-платформы закрытого типа не следует однозначно связывать с моделью аккаунтов, так как поверх них может быть реализована и UTXO-модель.

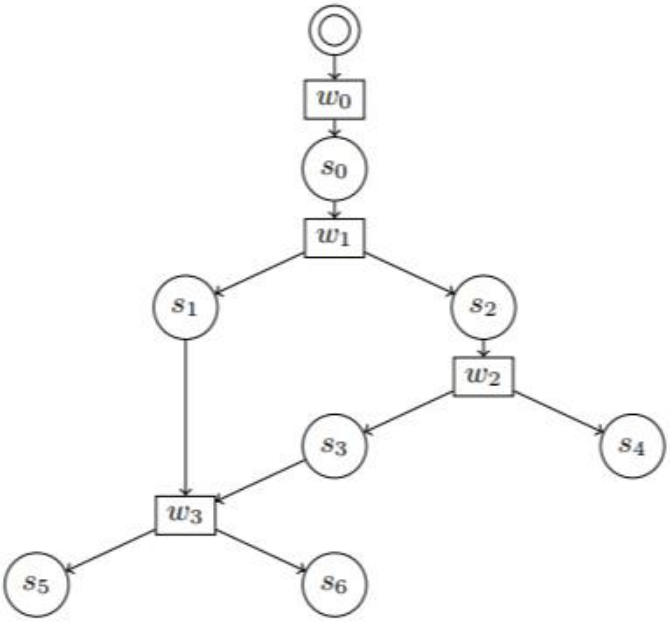

Рис. 1. Пример графа транзакций в UTXO-модели: s_i – состояния активов, w_i – транзакции (операции) с активами, приводящие к изменению их состояний
(Fig. 1. Example of a transaction graph in the UTXO model: s_i – asset states, w_i – transactions (operations) with assets that lead to changes in their states))

Достоинства и недостатки обеих моделей довольно очевидны и хорошо известны. Преимущества UTXO-модели – это полная прозрачность движения активов, принципиальная возможность параллельной и даже многопоточной обработки транзакций, недостатки – невозможность пользователям сохранять своё состояние между транзакциями и, как следствие, поддерживать смарт-контракты (вместо них на некоторых платформах реализованы скрипты с ограниченной функциональностью), ограниченная пропускная способность по обработке транзакций, высокие требования к объёму памяти узлов блокчейн-сети, называемых нодами (от англ. слова “node”), для хранения реестра. Преимущества модели аккаунтов – интуитивная понятность для пользователей, возможность запрограммировать в смарт-контрактах почти любую бизнес-логику, Тьюринг-полнота вычислений, недостатки – необходимость постоянно хранить состояния всех аккаунтов, относительная трудность проверки движения активов между аккаунтами, угроза нанесения значительного ущерба пользователям в случае компрометации их аккаунтов.

Обе модели в базовом варианте страдают от отсутствия встроенных в них механизмов обеспечения конфиденциальности и открытости распределенного реестра. Во-первых, любой нарушитель может получить все данные транзакций, загрузив себе копию реестра. Во-вторых, анализируя данные транзакций в реестре, можно прослеживать взаимосвязи между транзакциями и учетными записями. Новые транзакции непрерывно добавляются в реестр, а прежние не удаляются. Поэтому, как только какая-либо транзакция раскрывает реальную личность её участника, информация о нём

автоматически будет раскрыта во всей цепочке транзакций, которая может быть прослежена от этой транзакции как вперёд, так и назад. В-третьих, помимо данных из реестра, злоумышленники могут использовать любую внесистемную, косвенную информацию для определения личности владельцев аккаунтов [5].

Простейший способ обеспечить конфиденциальность транзакций в UTXO-модели для любого участника системы – это генерировать множество случайных адресов своих электронных кошельков, в пределе – для каждой новой транзакции открывать новых кошелёк. Однако хранение большого количества кошельков (адресов с их балансами) крайне неудобно для пользователя и создает для них риски утраты контроля движения принадлежащих им активов. Для решения проблем конфиденциальности в системах распределенного реестра на основе UTXO-модели в разное время было предложено несколько решений, реализованных в таких платформах как Dash, Zerocoin, Zerocash, Monero, CoinJoin.

Вместе с тем, известно немного предложений по обеспечению конфиденциальности транзакций для модели аккаунтов. Баланс аккаунта обновляется всякий раз, когда связанная с ним транзакция добавляется в реестр. Таким образом, в любой момент времени баланс – это накопленный результат всех связанных с аккаунтом операций. А это, в свою очередь, приводит к большей концептуальной сложности защиты аккаунтов по сравнению с защитой графа транзакций и к большей сложности реализации защиты. Требования к защищённости модели аккаунтов выше ещё и по той причине, что раскрытие идентичности отправителя или получателя хотя бы в одной транзакции приводит к утрате анонимности владельца аккаунта.

2. Инструментарий обеспечения безопасности транзакций

В качестве инструментов обеспечения конфиденциальности транзакций в системах распределенного реестра используется ряд криптографических схем. Далее рассмотрим основные из них.

1. ***Криптографические перемешивающие сети.*** Назначение криптографических перемешивающих сетей – разрушение логических связей между пакетом входящих сообщений и идентификаторами их отправителей. Первая перемешивающая сеть предложена Шаумом [6] (описание приводится по [7]). Рассмотрим её конструкцию в качестве примера.

Пусть $S_1, \dots, S_{n_S}$ – множество отправителей, $M_1, \dots, M_{n_{M_S}}$ – множество перемешивающих серверов, B – общедоступная доска объявлений, на которую можно только добавлять новые записи, $T_1, \dots, T_{n_T}$ – множество доверенных лиц. Предполагается, что каждому отправителю S_i доступен аутентифицированный канал связи с B.

Криптосхема включает в себя три последовательных фазы: установку начальных параметров, подачу сообщений отправителями, перемешивание сообщений серверами. Основная идея схемы состоит в следующем. Каждый отправитель S_i итеративно зашифровывает открытый текст своего сообщения m_i на открытых ключах $pk_1, \dots, pk_{n_{M_S}}$ перемешивающих серверов $M_1, \dots, M_{n_{M_S}}$ в обратном порядке и пересылает получившийся шифртекст C_i первому перемешивающему серверу M_1. Этот сервер, используя свой секретный ключ sk_1, снимает верхний уровень шифрования всех шифртекстов, перемешивает все сообщения в случайном порядке и отправляет их второму перемешивающему серверу M_2. Второй и каждый последующий сервер обрабатывают пакет сообщений аналогично тому, как это делал сервер M_1. Последний из перемешивающих серверов $M_{n_{M_S}}$ выдает открытые тексты сообщений, первоначально

поданных отправителями, в случайном порядке. Для реализации схемы в качестве криптографических примитивов используются стойкие схемы открытого шифрования и цифровой подписи.

Впоследствии было предложено множество усовершенствованных конструкций, например, проверяемые перемешивающие сети [7].

2. ***Кольцевая подпись*** – криптографическая схема, состоящая из трёх алгоритмов, выполнимых за полиномиальное время: RS=(KeyGen, Sign, Verify) [8].

Алгоритм генерации ключей $\mathrm{KeyGen}(\lambda) \to (VK, SK)$ по заданному параметру безопасности λ генерирует пару ключей схемы цифровой подписи: секретный ключ подписи SK и соответствующий ему открытый ключ проверки подписи VK.

Алгоритм генерации подписи $\mathrm{Sign}(SK, m, R) \to \Sigma$, используя секретный ключ подписи SK, для заданного сообщения m и списка ключей проверки подписи $R = (VK_1, \dots, VK_l)$ вырабатывает цифровую подпись Σ.

Алгоритм проверки подписи $\mathrm{Verify}(R, m, \Sigma) \to b$ для заданных списка ключей проверки подписи $R = (VK_1, \dots, VK_l)$, сообщения m и подписи Σ вырабатывает бит b=1, если проверка подписи прошла успешно, и b=0 в противном случае.

Схема кольцевой подписи позволяет подписывать сообщения любому участнику криптосистемы, принадлежащему заранее определённой группе участников, но таким образом, что при проверке подписи возможно подтвердить её корректность, но невозможно будет различить, кто именно из членов группы её создал.

3. ***Гомоморфное шифрование***. Схемы гомоморфного шифрования – особый вид схем открытого шифрования, которые позволяют выполнять операции с данными «под шифром», т.е. вычислять функции или выполнять алгоритмы над зашифрованными данными. Различают частично и полностью гомоморфное шифрование. Частично гомоморфное шифрование позволяет выполнять над зашифрованными данными только одну операцию: сложение либо умножение. Полностью гомоморфное шифрование обеспечивает возможность вычислить произвольную функцию, представленную в виде булевой либо арифметической схемы. В контексте рассматриваемой темы интерес представляет полностью гомоморфное шифрование.

Схема гомоморфного шифрования – это совокупность четырех алгоритмов FHE=(Gen, Enc, Eval, Dec) [9], где Gen, Enc, Dec соответствуют стандартной схеме шифрования с открытым ключом: алгоритмы генерации ключей, зашифрования и расшифрования, а алгоритм Eval принимает на вход вектор шифртекстов и функцию, представленную в виде булевой либо арифметической схемы C, а на выходе выдает зашифрованный результат применения этой функции к вектору шифртекстов. При этом обеспечивается следующее свойство, называемое корректностью:

$$\mathrm{Dec}_{sk}\left(\mathrm{Eval}\left(C, \mathrm{Enc}_{pk}(x_1), \dots, \mathrm{Enc}_{pk}(x_n)\right)\right) = C(x_1, \dots, x_n),$$

где $(pk, sk) \leftarrow \mathrm{Gen}(k)$, k – параметр безопасности (как правило, длина секретного ключа шифрования).

Практическая значимость полностью гомоморфного шифрования состоит в том, что оно позволяет реализовать модель вычислений «вслепую», т.е. сторона вычислительного процесса, которой доверена обработка данных, сможет выполнять любые вычислительные операции, не видя открытый текст. Основная проблема практического применения гомоморфного шифрования связана с низкой производительностью схем, так как вычисление функции требует низкоуровневого представления её в виде булевой или арифметической схемы (в зависимости от схемы

гомоморфного шифрования). Сложные функции могут приводить к чрезвычайно большим булевым схемам и, как следствие, к «астрономической» сложности вычислений при реализации гомоморфного шифрования. Представление в виде арифметической схемы более выгодно, так как позволяет построить схему, оперирующую не с отдельными битами, а с многоразрядными числами.

4. ***Доказательства с нулевым разглашением*** – криптографические протоколы, которые позволяют одной стороне – доказывающему P – доказать второй стороне – проверяющему V какое-либо утверждение, не сообщая проверяющему никаких дополнительных сведений, кроме факта истинности этого утверждения. Например, можно доказать, что в двух шифртекстах зашифрован один и тот же открытый текст, не разглашая сам открытый текст. В самом общем виде доказательства с нулевым разглашением позволяют доказывать истинность утверждений st вида:

$$\text{st: } \{(a,b,c,\ldots;\ x,y,z,\ldots):\ f(a,b,c,\ \ldots\ ,x,y,z,\ \ldots)=\text{true}\},$$

где $a,b,c,\ldots$ – общеизвестные величины, $x,y,z,\ldots$ – секретные величины, известные только доказывающему.

Среди доказательств с нулевым разглашением выделяется множество взаимопроникающих классов протоколов. Одним из важнейших классов доказательств являются Σ-протоколы [10]. Это интерактивные протоколы специального вида, которые позволяют конструировать доказательства для очень широкого класса алгебраических отношений. Методика Фиата – Шамира [11] позволяет стандартным образом преобразовывать Σ-протоколы в неинтерактивные доказательства с нулевым разглашением. В некоторых системах распределенного реестра удается использовать такие относительно простые классы доказательств, однако в большинстве случаев интерес для создания конфиденциальных систем распределенного реестра представляют протоколы, позволяющие построить доказательства для функций произвольного вида, представимых в виде булевой или арифметической схемы. К ним относятся краткие неинтерактивные доказательства знания с нулевым разглашением (zk-SNARK – zero-knowledge succinct non-interactive arguments of knowledge), доказательства типа Bulletproof, а также масштабируемые прозрачные доказательства знания с нулевым разглашением (zk-STARK – zero-knowledge scalable transparent arguments of knowledge). Подобные криптографические конструкции обладают высокой сложностью и заслуживают отдельного исследования.

В качестве примера далее рассмотрим определение доказательства типа zk-SNARK [12] (описание приводится по [13]). Это криптографическая схема, состоящая их четырех алгоритмов, выполнимых за полиномиальное время: $\Pi_Z = (\text{Setup}, \text{KeyGen}, \text{GenProof}, \text{VerProof})$, которая обладает свойствами полноты (completeness), состоятельности (soundness), краткости (succinctness) и совершенно нулевого разглашения (perfect zero-knowledge). Она позволяет создать доказательство с нулевым разглашением для произвольного утверждения вида $\vec{x} = C(\vec{a})$, где C – арифметическая схема, описывающая функцию, которая принимает на вход вектор $\vec{a}$ и выдаёт на выходе вектор $\vec{x}$.

Алгоритм генерации начальных параметров $\text{Setup}(\lambda) \rightarrow pp_Z$ по заданному параметру безопасности λ генерирует список открытых параметров pp_Z. Все остальные алгоритмы по умолчанию используют pp_Z как открытые общедоступные параметры.

Алгоритм генерации ключей $\text{KeyGen}(C) \rightarrow (pk_Z, vk_Z)$ по заданной арифметической схеме C, используя общедоступные параметры pp_Z, генерирует пару ключей (pk_Z, vk_Z), где pk_Z – открытый ключ генерации доказательства, vk_Z – секретный ключ проверки доказательства.

Алгоритм генерации доказательства $\mathrm{GenProof}(pk_Z, \vec{x}, \vec{a}) \to \pi$ по заданному открытому вектору $\vec{x}$, называемому утверждением (statement), который является входом для арифметической схемы C, секретному вектору $\vec{a}$, называемому свидетельством (witness), который служит дополнительным входом для схемы C, используя ключ генерации доказательства pk_Z, создаёт совокупность данных, называемую криптографическим доказательством π, со свойством нулевого разглашения, которое доказывает, что векторы $\vec{x}$ и $\vec{a}$ связаны алгебраическим отношением, задаваемым схемой C: $(\vec{x}, \vec{a}) \in R_C$. Здесь $\vec{x}$ и π являются общедоступными наборами данных.

Алгоритм проверки доказательства $\mathrm{VerProof}(vk_Z, \vec{x}, \pi) \to b$ позволяет, используя ключ проверки доказательства vk_Z и открытый вектор $\vec{x}$, использованный для генерации доказательства π алгоритмом GenProof, проверить это доказательство. Алгоритм вырабатывает бинарный ответ вида b=1, если проверка прошла успешно, и b=0 в противном случае.

3. Обеспечение конфиденциальности транзакций в UTXO-модели

Криптовалютная платформа ***Zerocash*** [14] и её современная версия ***Zcash*** стали одними из первых систем обеспечения конфиденциальности распределенных реестров. Эта система обеспечивает конфиденциальность как содержания транзакций, так и сведений об отправителе и получателе. Для этого в первой версии платформы использовалась децентрализованная перемешивающая сеть (миксер), через которую участники платформы могли периодически «отмывать» свои биткоины с помощью протокола Zerocoin, но повседневные транзакции должны были проводиться обычным порядком, используя криптовалюту биткоин, главным образом, по причине более высокой производительности.

В современной версии используются криптографические доказательства типа zk-SNARK, которые, однако, требуют наличия доверенной третьей стороны для выработки начальных параметров. Это само по себе противоречит концепции блокчейн-платформы как децентрализованной системы, а кроме того, процедура выработки начальных параметров предполагает выработку так называемых «токсичных отходов» (toxic waste), компрометация которых способна поставить под угрозу безопасность такой системы.

Другая широко известная криптовалютная платформа ***Monero*** [15] также обеспечивает конфиденциальность и содержания, и участников транзакций, но основана на идеях использования одноразовых адресов электронных кошельков и аутентификации транзакций посредством кольцевой подписи. Она позволяет добиться несвязываемости транзакций, но с ограниченной защитой конфиденциальности и большим размером данных для каждой транзакции. Кроме схем цифровой подписи со специальными свойствами, в Monero используются обязательства Педерсена и интервальные доказательства с нулевым разглашением. Во всех криптографических примитивах используется арифметика в группе точек эллиптической кривой, что позволяет добиться высокоэффективной реализации.

Ещё одна криптовалютная платформа ***Zerocoin*** [16] и её современная версия ***Zcoin*** обеспечивает конфиденциальность участников транзакций, не защищая содержание транзакций. Для этого в ней используются доказательства с нулевым разглашением на основе вычислительно сложной задачи дискретного логарифмирования, однако они характеризуются значительным объёмом данных, составляющих доказательство, и большим временем его проверки.

Система ***Lelantus*** [17, 18], являясь дальнейшим развитием платформы Zerocoin, добавляет к исходной конструкции этой платформы несколько новых идей. Для

участников создаются секретные балансы, позволяющие им эмитировать электронные монеты произвольного номинала, а затем анонимно тратить их, превращая в новые монеты произвольных номиналов. Чтобы гарантировать, что сумма входящих и исходящих монет для каждой транзакции равна, используются специальные доказательства с нулевым разглашением. Конструкция доказательства допускает неограниченное число входящих и исходящих монет для каждой транзакции. Пользователям также предоставляется возможность открывать так называемые экранированные адреса, с которых можно совершать экранированные платежи в адрес заранее предопределённых получателей. В системе Lelantus используется высокоэффективный метод пакетной верификации транзакций, который позволяет сетевым валидаторам проверять сотни или даже тысячи различных транзакций одновременно, значительно снижая среднюю стоимость проверки одной транзакции. Построенное таким образом решение имеет множество преимуществ перед альтернативными системами, а именно:

- она не требует каких-либо доверенных процессов настройки, а безопасность криптографических протоколов основывается только на стандартных и проверенных временем вычислительно сложных задачах;
- система обеспечивает анонимность участников транзакций, позволяя им быть неразличимыми среди больших множеств других участников (размером 65536 и более);
- транзакции поддерживают прямые анонимные платежи и могут принимать произвольное количество входящих и исходящих монет, которые могут быть объединены, разделены или выкуплены в произвольных пропорциях;
- коммуникационная сложность транзакций имеет сложность, выражаемую логарифмом от количества участников, среди которых скрывается анонимный участник, вычислительная сложность верификации транзакций линейна по тому же параметру, но может быть ещё больше ускорена за счёт пакетной верификации.

Система ***Dash*** [19] повторяет конструкцию криптовалютной платформы Bitcoin, но содержит встроенные функции защиты, которые обеспечивают конфиденциальность участников транзакций, но не скрывают содержание транзакций. В основе лежит криптографическая перемешивающая сеть. Dash обеспечивает несвязываемость транзакций, но процесс перемешивания в этой системе очень медленный.

Платформа ***CoinShuffle*** [20] – ещё один вариант реализации перемешивающей сети для обеспечения конфиденциальности участников, но не содержания транзакций. Она обеспечивает истинную анонимность для переводов биткоинов с баланса на баланс (а не псевдонимность, как на исходной платформе Bitcoin) и не требует наличия какой бы то ни было доверенной третьей стороны.

Система ***Verge*** [21] занимает особое место среди рассматриваемых решений, поскольку, в отличие от всех остальных систем, обеспечивает конфиденциальность участников транзакций не разрывая логическую связь между идентификаторами участников и адресами их электронных кошельков, а скрывая их IP-адреса, для чего используются технологии анонимных децентрализованных сетей Tor и I2P.

Система ***Grin*** [22, 23] – одна из двух современных реализаций криптографической схемы MimbleWimble, предложенной анонимным автором в 2016 г. (второй реализацией является малоизвестная система Beam). Она обеспечивает конфиденциальность как содержания транзакций, так и участников. Система использует множество криптографических примитивов, в том числе обязательства Педерсена, схему цифровой подписи Шнорра, агрегированные цифровые подписи, доказательства с нулевым разглашением. Криптографические конструкции системы Grin хорошо исследованы, для

них получены строго доказанные результаты. Достоинством системы Grin является хорошая масштабируемость, недостатком – требование наличия защищённых коммуникационных каналов между участниками.

Все вышеупомянутые решения предназначаются для блокчейн-платформ открытого типа. Особый подход к решению задачи обеспечения конфиденциальности транзакций содержится в работе [24]. Предлагаемое в ней решение позволяет обеспечить конфиденциальность для UTXO-модели представления балансов, но на блокчейн-платформе закрытого типа. Это решение включает в себя несколько компонентов. Первый из них – специальный способ кодирования токенов, позволяющий совершать анонимные транзакции. Каждый токен представлен обязательством Педерсена, которое содержит идентификатор владельца токена, значение токена и его тип. Жизненный цикл токена регулируется транзакциями эмиссии и передачи его между балансами. При эмиссии создается токен заданного типа и номинала, право владения им и присваивается автору транзакции. Эмиссия токенов может осуществляться только уполномоченными эмитентами. Впоследствии токен может сменить владельца только через транзакцию передачи. Поскольку рассматриваемый метод основан на UTXO-модели, транзакция передачи состоит из набора входящих токенов, которые должны быть аннулированы, и набора исходящих токенов, которые должны быть созданы. При этом валидность транзакции проверяется в соответствии со следующими правилами:

- автор транзакции является законным владельцем входящих токенов;
- владельцы исходящих токенов являются зарегистрированными участниками системы;
- тип и номинал токенов сохраняются;
- входящие токены могут быть проверены по реестру, чтобы гарантировать, что они созданы в результате валидных транзакций;
- входящие токены не были потрачены ранее.

В рассматриваемой системе предлагается использовать целый ряд криптографических примитивов: неинтерактивные доказательства с нулевым разглашением Грота – Сахаи, обязательства Педерсена, проверяемые псевдослучайные функции, «слепую» цифровую подпись, схему открытого шифрования Эль-Гамаля, что обеспечивает в целом приемлемую для практики вычислительную сложность транзакций.

Описанный подход развивается в работе [25], где предлагается схема, обеспечивающая совершение анонимных транзакций с возможностями отзыва полномочий пользователей и аудита проводимых транзакций. Авторы этой работы создали прототип такой системы с открытым исходным кодом для блокчейн-платформы Hyperledger Fabric.

4. Обеспечение конфиденциальности транзакций в модели аккаунтов

Обеспечение конфиденциальности транзакций в модели аккаунтов, как правило, требует более сложных криптографических конструкций. В связи с этим предложенные решения сравнительно малочисленны. Рассмотрим четыре решения, известных автору статьи.

Система ***DSC*** [26] – пожалуй, самая простая среди известных схем для модели аккаунтов. Она обеспечивает конфиденциальность балансов пользователей и содержания транзакции, но не способна разорвать логическую связь между отправителями и получателями транзакций, т.е. решает задачу обеспечения конфиденциальности лишь частично.

В качестве криптографических примитивов в схеме используются неинтерактивные доказательства с нулевым разглашением в модели общей ссылочной строки (CRS – common reference string), а также (в комплексе с ним) гомоморфная схема шифрования специального вида. Идея построения этого доказательства основана на том, что для каждой транзакции формулируется набор утверждений одного из двух типов: либо утверждения об алгебраической связи между набором величин, среди которых есть как секреты, известные только участникам транзакции, так и открытые параметры и шифртексты, либо о том, что некоторая величина принимает значения из заданного интервала неотрицательных целых чисел. Для реализации доказательств первого типа используются сигма-протоколы, преобразованные в неинтерактивные доказательства при помощи методики Фиата – Шамира. Для утверждений второго типа используются интервальные доказательства (range proofs).

Особенностью системы DSC является малое время генерации доказательства за счёт относительно большого объёма данных, составляющих доказательство. К сожалению, система DSC имеет лишь экспериментальную реализацию, не привязанную к какой-либо конкретной блокчейн-платформе. По-видимому, практический интерес к ней сдерживается невозможностью обеспечить конфиденциальность участников транзакций.

Система ***Zether*** [27] предлагает более полное решение, позволяя обеспечить конфиденциальность как содержания транзакций, так и идентификаторов участников транзакций. Решение ориентировано на блокчейн-платформу Ethereum и предполагает выпуск в обращение специальных Zether-токенов (ZTH). Для операций с ними разработаны специальные смарт-контракты и используются специальные аккаунты. Аккаунты идентифицируются при помощи открытых ключей схемы открытого шифрования Эль-Гамаля и, таким образом, не ассоциированы с адресами аккаунтов платформы Ethereum. Владельцы аккаунтов могут конвертировать «родную» криптовалюту платформы Ethereum – эфир – в эти токены и обратно при предъявлении соответствующих ключей аккаунта. Аккаунты также имеют механизмы защиты от повторной траты токенов, в некотором смысле подобные аналогичным механизмам платформы Ethereum, а именно последовательная нумерация транзакций на каждом аккаунте и подписание содержания каждой транзакции её инициатором. Чтобы перевести токены с баланса одного аккаунта на баланс другого аккаунта, их необходимо зашифровать при помощи открытых ключей обоих аккаунтов, приложив криптографические доказательства утверждений двух типов: во-первых, доказательство того, что в обоих шифртекстах зашифрована одна и та же сумма активов, вовлеченных в транзакции, и во-вторых, того, что на балансе отправителя имеется достаточно активов для совершения транзакции. Для реализации столь нетривиальных доказательств авторы предлагают оригинальную гибридную конструкцию, составленную из сигма-протоколов и доказательств типа Bulletproofs, названную ими «Σ-Bullets».

Однако такого рода доказательства порождают проблему, связанную с тем, что они генерируются для фиксированных состояний балансов аккаунтов отправителей и получателей. Если за время ожидания и исполнения смарт-контракта состояние хотя бы одного аккаунта изменится, доказательство окажется недействительным, а внутренняя криптовалюта, используемая для оплаты работы майнеров, – газ окажется потраченной впустую. Чтобы преодолеть эти сложности, к функциональности смарт-контрактов добавляются операции блокировки и разблокировки аккаунтов.

Базовый механизм обеспечения конфиденциальности транзакций системы Zether реализован на языке программирования смарт-контрактов Solidity. На основе этого механизма может быть реализован целый ряд прикладных программ: электронные

аукционы, платёжные каналы, электронное голосование, а также обеспечивающий конфиденциальность балансов участников механизм консенсуса посредством «доказательства обладания долей» (proof-of-stake).

Система ***ZETH*** [28] предлагает другой путь решения проблемы, также позволяющий обеспечить конфиденциальность как содержания, так и участников транзакций. Предлагаемая авторами криптосхема в значительной мере основана на идеях, почерпнутых из криптовалютной платформы Zerocash, но ориентирована на блокчейн-платформы Ethereum. Участники, желающие совершать транзакции конфиденциально, депонируют свои активы в обязательства, называемые zethNotes, и используют специальный смарт-контракт, реализующий функции перемешивающей сети, – миксер.

Участники миксера могут конфиденциально обмениваться активами между собой. Аккаунт участников миксера привязан только к сгенерированной ими паре ключей: секретному и открытому. Секретный ключ нужен для распоряжения активами на своём балансе, открытый – для зачисления активов на свой баланс от других участников миксера. Им не нужно после каждой транзакции конвертировать свои средства обратно в исходную криптовалюту, так как любая цепочка из нескольких подряд выполненных конфиденциальных транзакций также обеспечивает конфиденциальность. Количество активов на балансе участника раскрывается только для транзакций по депонированию криптовалюты в миксер и обратного снятия её оттуда. Последнее обстоятельство несколько снижает свойства конфиденциальности системы ZETH по сравнению с её прототипом – криптовалютой Zerocash. Поскольку аккаунты участников привязаны только к сгенерированным ими самими ключам, а миксер разрывает логическую связь между отправителями и получателями транзакций для любых сторонних наблюдателей, кроме самих участников транзакций, такой механизм обеспечивает анонимность каждого отдельно взятого участника миксера среди всех его участников.

В качестве основных криптографических примитивов в системе ZETH используются схемы обязательств (commitments) Педерсена, доказательства с нулевым разглашением типа zk-SNARK, криптографические хэш-функции, схемы шифрования с открытым ключом.

Система ZETH реализована в виде прототипа на языке C++ с использованием библиотеки libsnark для реализации доказательств типа zk-SNARK. В реализации используется встроенный в новые версии платформы Ethereum механизм предварительно откомпилированных смарт-контрактов на основе аппарата эллиптических кривых.

Система ***BlockMaze*** [13] демонстрирует иной подход к решению проблемы. В ней предлагается модель двойного баланса: к аккаунту каждого участника блокчейн-платформы привязываются два баланса, один из которых ведётся в открытом виде, а другой носит название баланса с нулевым разглашением. Этот второй баланс ассоциируется с обязательствами (commitments), производными от состояния первого баланса. Оба баланса могут взаимно конвертироваться, а баланс с нулевым разглашением может использоваться для совершения транзакций между аккаунтами с использованием доказательств типа zk-SNARK.

Однако взаимосвязи между отправителями и получателями не могут быть скрыты при использовании такого подхода. Для этой цели в BlockMaze реализуется двухэтапная процедура перевода активов с баланса на баланс при выполнении транзакции. На первом шаге отправитель создаёт обязательство для переводимого актива, выполняя транзакцию Send. Чтобы обновить баланс с нулевым разглашением и предотвратить повторную трату одного и того же актива, каждой такой транзакции присваивается свой порядковый номер, который привязывается к обязательству. После подтверждения транзакции Send

блокчейн-платформой, получатель связывает предназначенное ему обязательство для переводимых активов с другими обязательствами, в результате чего формируется дерево Меркле. После этого получатель генерирует доказательство с нулевым разглашением, чтобы получить на свой баланс переводимый актив, но не разгласить, из какой именно транзакции берётся переводимый ему актив.

Таким образом, система BlockMaze имеет следующие характерные особенности:

- балансы аккаунтов и содержание транзакций скрыты от посторонних участников при помощи криптографических обязательств;
- взаимосвязь между транзакциями опосредуется через двухэтапную процедуру перевода активов;
- чтобы гарантировать валидность транзакций и корректность обновления балансов, применяются доказательства типа zk-SNARK.

Недостатком системы BlockMaze является высокая степень интерактивности протоколов, что приводит к высоким вычислительным и коммуникационным затратам. Авторы системы рассматривают возможность её усовершенствования путём замены протоколов на неинтерактивные доказательства, что, однако, является нетривиальной задачей.

Заключение

Проблема обеспечения конфиденциальности транзакций в системах распределенного реестра находится в стадии активной научно-практической разработки, но далека от полного решения. Усилия исследователей направлены на создание механизмов и систем, обеспечивающих как конфиденциальность содержания транзакций, так и приватность участников транзакций. Они предназначаются для работы на платформах как открытого, так и закрытого типов, поддерживающих как UTXO-модель транзакций, так и модель аккаунтов.

В настоящее время значительно больше решений создано для *UTXO-модели*, что объясняется относительной её простотой и ясностью требований, предъявляемых к механизмам обеспечения конфиденциальности. Существующие решения демонстрируют совершенно разные, порою несовместимые подходы к обеспечению конфиденциальности. Не все известные решения способны обеспечить защиту и содержания транзакций, и сведений об их участниках одновременно. Системы, предоставляющие максимальные возможности защиты, страдают от слишком высоких вычислительных, емкостных и коммуникационных требований к участникам протоколов.

Вместе с тем анализ известных из литературы решений по обеспечению конфиденциальности транзакций для *модели аккаунтов* позволяют сделать вывод, что ни одно из них не решает эту проблему целиком. Самый распространённый инструмент решения этой задачи – доказательства с нулевым разглашением. Несмотря на попытки использования разных типов доказательства (как правило, в сочетании с другими криптографическими примитивами), ни один из методов не предоставляет удовлетворительного решения с точки зрения производительности и объёма создаваемых участниками протокола данных.

Существующие решения, даже внутри одной модели представления балансов, трудно непосредственно сравнивать между собой, в том числе из-за слишком разных подходов к реализации, что затрудняет даже простое сравнение конкурирующих решений по производительности и времени выполнения алгоритмов.

В то же время, от полноты и успешности решения задачи обеспечения конфиденциальности транзакций в системах распределенного реестра зависят

перспективы широкого применения блокчейн-технологий в сферах, связанных с циркуляцией сведений ограниченного распространения, в частности, содержащих охраняемую законом тайну: коммерческую, банковскую, врачебную и иную. В связи с этим представляется, что исследования в обозначенной сфере должны получить большую глубину и содержательность. В частности, перспективы продолжения исследований могут быть связаны со следующими исследовательскими задачами:

- расширение номенклатуры требований по обеспечению конфиденциальности и других аспектов информационной безопасности систем распределенного реестра, а также реализующих эти требования свойств криптографических конструкций, которые возможно обосновать формальными доказательствами;
- поиск возможностей применения ранее не использовавшихся криптографических примитивов или разработка совершенно новых примитивов, которые помогут снизить сложность выполнения криптографических протоколов и криптосхем;
- поиск новых моделей представления балансов, а также новых моделей коммуникации участников системы распределённого реестра при совершении транзакций.

СПИСОК ЛИТЕРАТУРЫ:

1. Запечников, Сергей В. Системы распределенного реестра как инструмент обеспечения доверия между участниками бизнес-процессов. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 37–53, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1230 (дата обращения: 07.11.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.03.
2. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S. Nakamoto. 2006. – 9 p. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 07.11.2020).
3. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Petersburg version G. Wood. GitHub repository. 2020. – 39 p. URL: https://ethereum.github.io/yellowpaper/paper.pdf (дата обращения: 07.11.2020).
4. Hyperledger project site. 2020. URL: https://www.hyperledger.org/ (дата обращения: 07.11.2020).
5. DuPont, J. Toward De-Anonymizing Bitcoin by Mapping Users Location J. DuPont, A.C. Squicciarini. Proc. 5th ACM Conference on Data and Application Security and Privacy. ACM, 2015. P. 139–141.
6. Chaum, D. Untraceable electronic mail, return addresses, and digital D. Chaum. Communications of the ACM. Vol. 24, No. 2 (Feb. 1981). P. 84–88.
7. Haines, T. SoK: Techniques for verifiable mix nets T. Haines, J. Muller. Proc. 2020 IEEE 33rd computer security foundations symposium (CSF), Boston, MA, USA, 2020. P. 49–64.
8. Backes, M. Ring Signatures: Logarithmic-Size, No Setup - from Standard Assumptions M. Backes, N. Döttling, L. Hanzlik, et al. Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Vol. 11478, Springer, Cham. P. 281–311.
9. Armknecht, F. A guide to fully homomorphic encryption F. Armknecht, C. Boyd, C. Carr, et al. 2017. – 35 p. URL: https://www.semanticscholar.org/paper/A-Guide-to-Fully-Homomorphic-Encryption-Armknecht-Boyd/7ee670d05930c034d2224a42b37db8862a566810 (дата обращения: 08.11.2020).
10. Hazay, C. Sigma protocols and efficient zero-knowledge C. Hazay, Y. Lindell. Efficient secure two-party protocols. Information security and cryptography. Springer, Berlin, Heidelberg. 2010. P. 147–175.
11. Fiat, A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. A. Fiat, A. Shamir. Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science. Springer Berlin Heidelberg. Vol. 263. P. 186–194.
12. Bitansky, N. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again N. Bitansky, R. Canetti, A. Chiesa, et al. ITCS '12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, January 2012. P. 326–349.
13. Guan, Z. BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs Z. Guan, Z. Wan, Y. Yang, et al. IEEE Transactions on Dependable and Secure Computing, 2020. DOI: http://dx.doi.org/10.1109/TDSC.2020.3025129.
14. Ben-Sasson, E. Zerocash: Decentralized anonymous payments from Bitcoin E. Ben-Sasson, A. Chiesa, C. Garman et al. Proc. IEEE Symposium on Security and Privacy (SP), 2014. P. 459–474.
15. Alonso, K. Monero: Privacy in the blockchain K. Alonso, J. Joancomarti. IACR eprint archive. 2018. – 47 p. URL: https://eprint.iacr.org/2018/535.pdf (дата обращения: 08.11.2020).

16. Miers, I. Zerocoin: Anonymous Distributed E-Cash from Bitcoin I. Miers, C. Garman, M. Green et al. Proc. IEEE Symposium on Security and Privacy (SP), 2013. P. 397–411.
17. Jivanyan, A. Lelantus: A new design for anonymous and confidential cryptocurrencies A. Jivanyan. Zcoin project site, 2020. – 18 p. URL: https://zcoin.io/papers/lelantusv2.pdf (дата обращения: 08.11.2020).
18. Jivanyan, A. Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions A. Jivanyan. IACR eprint archive. 2019. – 23 p. URL: https://eprint.iacr.org/2019/373.pdf (дата обращения: 08.11.2020).
19. Duffield, E. Dash: A privacy-centric cryptocurrency E. Duffield, D. Diaz. GitHub repository. 2015. URL: https://github.com/dashpay/dash/wiki/Whitepaper (дата обращения: 08.11.2020).
20. Ruffing, T. Coinshuffle: Practical decentralized coin mixing for bitcoin T. Ruffing, P. Moreno-Sanchez, A. Kate. Proc. European Symposium on Research in Computer Security. Springer, 2014. P. 345–364.
21. Blackpaper: Verge Currency, 5th ed. VergeCurrency site, 2020. – 30 p. URL: https://vergecurrency.com/static/blackpaper/verge-blackpaper-v5.0.pdf (дата обращения: 08.11.2020).
22. Peverell, I. Introduction to MimbleWimble and Grin I. Peverell. GitHub repository. 2020. URL https://github.com/mimblewimble/grin/blob/master/doc/intro.md (дата обращения: 08.11.2020).
23. Fuchsbauer, G. Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble G. Fuchsbauer, M. Orrù, Y. Seurin. Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Vol 11476. Springer, Cham. P. 657–689.
24. Androulaki, E. Privacy-preserving auditable token payments in a permissioned blockchain system E. Androulaki, J. Camenisch, A. De Caro, et al. Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. ACM, 2020. P. 255–267.
25. Bogatov D. Anonymous transactions with revocation and auditing in Hyperledger Fabric D. Bogatov, A. De Caro, K. Elkhiyaoui. IACR e-archive. 2019. – 18 p. URL: https://eprint.iacr.org/2019/1097.pdf (дата обращения: 08.11.2020).
26. Ma, S. An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain S. Ma, Y. Deng, D. He, et al. IEEE Transactions on Dependable and Secure Computing, 2020. DOI: http://dx.doi.org/10.1109/TDSC.2020.2969418.27
27. Bünz, B. Zether: Towards Privacy in a Smart Contract World B. Bünz, S. Agrawal, M. Zamani, et al. Bonneau J., Heninger N. (eds) Financial Cryptography and Data Security (FC 2020). Lecture Notes in Computer Science. Vol 12059. Springer, Cham. P. 423–443.
28. Rodelet, AQ. ZETH: On integrating Zerocash on Ethereum A. Rondelet, M. Zajac. arXiv.org publication, 2019. – 39 p. URL: https://arxiv.org/abs/1904.00905v2 (дата обращения: 08.11.2020).

REFERENCES:

[1] Zapechnikov, Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 37–53, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1230 (accessed: 07.11.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.03 (in Russian).
[2] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. S. Nakamoto. 2006. – 9 p. URL: https://bitcoin.org/bitcoin.pdf (accessed: 07.11.2020).
[3] Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Petersburg version G. Wood. GitHub repository. 2020. – 39 p. URL: https://ethereum.github.io/yellowpaper/paper.pdf (accessed: 07.11.2020).
[4] Hyperledger project site. 2020. URL: https://www.hyperledger.org/ (accessed: 07.11.2020).
[5] DuPont, J. Toward De-Anonymizing Bitcoin by Mapping Users Location J. DuPont, A.C. Squicciarini. Proc. 5th ACM Conference on Data and Application Security and Privacy. ACM, 2015. P. 139–141.
[6] Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms D. Chaum. Communications of the ACM. Vol. 24, No. 2 (Feb. 1981). P. 84–88.
[7] Haines, T. SoK: Techniques for verifiable mix nets T. Haines, J. Muller. Proc. 2020 IEEE 33rd computer security foundations symposium (CSF), Boston, MA, USA, 2020. P. 49–64.
[8] Backes, M. Ring Signatures: Logarithmic-Size, No Setup - from Standard Assumptions M. Backes, N. Döttling, L. Hanzlik, et al. Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Vol. 11478, Springer, Cham. P. 281–311.
[9] Armknecht, F. A guide to fully homomorphic encryption F. Armknecht, C. Boyd, C. Carr, et al. 2017. – 35 p. URL: https://www.semanticscholar.org/paper/A-Guide-to-Fully-Homomorphic-Encryption-Armknecht-Boyd/7ee670d05930c034d2224a42b37db8862a566810 (accessed: 08.11.2020).
[10] Hazay, C. Sigma protocols and efficient zero-knowledge C. Hazay, Y. Lindell. Efficient secure two-party protocols. Information security and cryptography. Springer, Berlin, Heidelberg. 2010. P. 147–175.

[11] Fiat, A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems A. Fiat, A. Shamir. Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science. Springer Berlin Heidelberg. Vol. 263. P. 186–194.
[12] Bitansky, N. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again N. Bitansky, R. Canetti, A. Chiesa, et al. ITCS '12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, January 2012. P. 326–349.
[13] Guan, Z. BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs Z. Guan, Z. Wan, Y. Yang, et al. IEEE Transactions on Dependable and Secure Computing, 2020. DOI: http://dx.doi.org/10.1109/TDSC.2020.3025129.
[14] Ben-Sasson, E. Zerocash: Decentralized anonymous payments from Bitcoin E. Ben-Sasson, A. Chiesa, C. Garman et al. Proc. IEEE Symposium on Security and Privacy (SP), 2014. P. 459–474.
[15] Alonso, K. Monero: Privacy in the blockchain K. Alonso, J. Joancomarti. IACR eprint archive. 2018. – 47 p. URL: https://eprint.iacr.org/2018/535.pdf (accessed: 08.11.2020).
[16] Miers, I. Zerocoin: Anonymous Distributed E-Cash from Bitcoin I. Miers, C. Garman, M. Green et al. Proc. IEEE Symposium on Security and Privacy (SP), 2013. P. 397–411.
[17] Jivanyan, A. Lelantus: A new design for anonymous and confidential cryptocurrencies A. Jivanyan. Zcoin project site, 2020. – 18 p. URL: https://zcoin.io/papers/lelantusv2.pdf (accessed: 08.11.2020).
[18] Jivanyan, A. Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions A. Jivanyan. IACR eprint archive. 2019. – 23 p. URL: https://eprint.iacr.org/2019/373.pdf (accessed: 08.11.2020).
[19] Duffield, E. Dash: A privacy-centric cryptocurrency E. Duffield, D. Diaz. GitHub repository. 2015. URL: https://github.com/dashpay/dash/wiki/Whitepaper (accessed: 08.11.2020).
[20] Ruffing, T. Coinshuffle: Practical decentralized coin mixing for bitcoin T. Ruffing, P. Moreno-Sanchez, A. Kate. Proc. European Symposium on Research in Computer Security. Springer, 2014. P. 345–364.
[21] Blackpaper: Verge Currency, 5th ed. VergeCurrency site, 2020. – 30 p. URL: https://vergecurrency.com/static/blackpaper/verge-blackpaper-v5.0.pdf (accessed: 08.11.2020).
[22] Peverell, I. Introduction to MimbleWimble and Grin I. Peverell. GitHub repository. 2020. URL https://github.com/mimblewimble/grin/blob/master/doc/intro.md (accessed: 08.11.2020).
[23] Fuchsbauer, G. Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble G. Fuchsbauer, M. Orrù, Y. Seurin. Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Vol 11476. Springer, Cham. P. 657–689.
[24] Androulaki, E. Privacy-preserving auditable token payments in a permissioned blockchain system E. Androulaki, J. Camenisch, A. De Caro, et al. Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. ACM, 2020. P. 255–267.
[25] Bogatov D. Anonymous transactions with revocation and auditing in Hyperledger Fabric D. Bogatov, A. De Caro, K. Elkhiyaoui. IACR e-archive. 2019. – 18 p. URL: https://eprint.iacr.org/2019/1097.pdf (accessed: 08.11.2020).
[26] Ma, S. An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain S. Ma, Y. Deng, D. He, et al. IEEE Transactions on Dependable and Secure Computing, 2020. DOI: http://dx.doi.org/10.1109/TDSC.2020.2969418.27
[27] Bünz, B. Zether: Towards Privacy in a Smart Contract World B. Bünz, S. Agrawal, M. Zamani, et al. Bonneau J., Heninger N. (eds) Financial Cryptography and Data Security (FC 2020). Lecture Notes in Computer Science. Vol 12059. Springer, Cham. P. 423–443.
[28] Rodelet, AQ. ZETH: On integrating Zerocash on Ethereum A. Rondelet, M. Zajac. arXiv.org publication, 2019. – 39 p. URL: https://arxiv.org/abs/1904.00905v2 (accessed: 08.11.2020).

Поступила в редакцию – 08 ноября 2020 г. Окончательный вариант – 18 ноября 2020 г.
Received – November 18, 2020. The final version – November 18, 2020.

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 оформления аннотации**);

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

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

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

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

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

Правила оформления аннотации

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

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

Аннотация включает следующие аспекты содержания статьи**:**

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

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

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

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

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

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

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

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

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

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

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 8277

Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 8277
E-mail: BIT@mephi.ru
https://bit.mephi.ru

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

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

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Ответственный редактор И.М. Ядыкин
Технический редактор П.А. Золотухина

Подписано в печать 27.11.2020. Формат 60x84 1/8
Печ. л. 16. Уч.-изд. л. 16. 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»
ул. Кантемировская, 60, Москва, 115477, Россия