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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

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

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

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

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

Основные тематические направления журнала:

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

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

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

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

Papers in Russian and English are equally welcome.

Focus topics:

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

СОДЕРЖАНИЕ

CONTENT

Анна В. Бацких[1], Ирина Г. Дровникова[2], Евгений А. Рогозин[3]
[1,2,3]Воронежский институт министерства внутренних дел Российской федерации,
пр-т Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: svatikova96@mail.ru, https://orcid.org/0000-0001-5564-168X
[2]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

АНАЛИЗ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОСНОВНЫЕ АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DOI: http://dx.doi.org/10.26583/bit.2020.2.01

Аннотация. В статье представлены результаты анализа научно-технической литературы и открытых нормативно-распорядительных документов международного, федерального и ведомственного уровней, посвященных процессу функционирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных системах (АС) на объектах информатизации органов внутренних дел (ОВД). На примере типовой сертифицированной СЗИ от НСД «Страж NT 4.0» рассмотрены функциональные возможности действующих в защищенных АС ОВД СЗИ от НСД, выявлены недостатки и определены основные аспекты совершенствования подсистем управления доступом данных систем на основе использования новых информационно-телекоммуникационных технологий, связанных с повышением реальной защищенности АС на объектах информатизации ОВД. В качестве перспективной технологии предложена дополнительная биометрическая аутентификация, основанная на распознавании субъекта доступа по индивидуальной динамике клавиатурного набора (клавиатурному почерку).
Ключевые слова: защита информации, система защиты информации, подсистема управления доступом, несанкционированный доступ, аутентификация пользователя, клавиатурный почерк.
Для цитирования: БАЦКИХ, Анна В.; ДРОВНИКОВА, Ирина Г.; РОГОЗИН, Евгений А. АНАЛИЗ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОСНОВНЫЕ АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 6-17, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1267>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.01.

Anna V. Batskih[1], Irina G. Drovnikova[2], Evgeni A. Rogozin[3]
[1,2,3]Voronezh Institute of the Ministry of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: svatikova96@mail.ru, https://orcid.org/0000-0001-5564-168X
[2]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Analysis of the process of functioning of subsystems of access control systems to protect information from unauthorized access and basic aspects their perfection in automated systems of internal affairs bodies

DOI: http://dx.doi.org/10.26583/bit.2020.2.01

Abstract. The paper presents the results of the analysis of scientific and technical literature and open regulatory and administrative documents of the international, Federal and departmental levels devoted to the process of functioning of information protection systems (SPI) from unauthorized access (UA) in automated systems (AS) at the objects of Informatization of internal Affairs bodies (ATS). Using the

example of a typical certified SPI from UA «Strazh NT 4.0» the functionality of SPI from UA operating in protected ATS is analyzed, shortcomings are identified and the key aspects of improving subsystems of access control systems based on the use of new information and telecommunication technologies related to improving real security as on the objects of Informatization Department are defined. As a promising technology additional biometric authentication based on realization of recognition of the access subject on individual dynamics of a keyboard set (keyboard handwriting) is offered.
Keywords: information protection, information security system, access control subsystem, unauthorized access, authenticate users, keyboard handwriting.
For citation: BATSKIH, Anna V.; DROVNIKOVA, Irina G.; ROGOZIN, Evgeni A. Analysis of the process of functioning of subsystems of access control systems to protect information from unauthorized access and basic aspects their perfection in automated systems of internal affairs bodies. IT Security (Russia), [S.l.], v. 27, n. 2, p. 6-17, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1267>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.01.

Введение

Характерной особенностью настоящего времени является ускоренный темп развития новых информационно-телекоммуникационных технологий и их широкое проникновение практически во все сферы человеческой деятельности. Это активно используется различного рода злоумышленниками, несанкционированное воздействие которых на информационный ресурс АС приводит к нарушению целостности, конфиденциальности или доступности хранящейся, обрабатываемой и передаваемой информации и в результате – к нарушению надежности функционирования АС в целом по ее прямому назначению. Согласно статистическим данным Генеральной прокуратуры Российской Федерации отмечается ежегодный рост преступлений, связанных с использованием информационно-коммуникационных технологий: по итогам за январь–август 2019 года число преступлений в сфере компьютерной информации выросло более чем в полтора раза (+66,8 %), правоохранители выявили 180 153 преступления [1]. В результате таких преступных действий наносится ощутимый ущерб объектам информатизации, эксплуатирующим АС различного назначения. Это в первую очередь относится к АС на объектах информатизации критического применения, характеризующихся неприемлемыми для народного хозяйства размерами ущерба, а также других последствий, возникающих по причине нарушения их работоспособности, сбоев или отказов в работе. К такого рода объектам в полной мере следует отнести и объекты информатизации, эксплуатирующие АС ОВД.

Динамика киберпреступности диктует необходимость повышения эффективности противодействия ей, что относится к стратегическим направлениям деятельности правоохранительных органов. Таким образом, вопросы, связанные обеспечением надежности функционирования АС на объектах информатизации ОВД и, в частности, их информационной безопасности (ИБ), являются весьма актуальными. Их актуальность основывается на основных положениях Доктрины ИБ, в которой отмечается необходимость как повышения защищенности критической информационной структуры и устойчивости ее функционирования, так и развития механизмов обнаружения, защиты и предупреждения информационных угроз [2]. Концепция обеспечения информационной безопасности ОВД Российской Федерации до 2020 года определяет комплекс мер, направленных на обеспечение защиты информации (ЗИ), информационных ресурсов и информационных систем ОВД Российской Федерации от специальных программно-технических воздействий, средств технических разведок, НСД, а также утечки информации по техническим каналам [3].

Опыт эксплуатации современных АС ОВД показал, что наибольший вклад в нарушение надежности их функционирования вносят угрозы, связанные с НСД к

конфиденциальному информационному ресурсу [4, 5]. С целью ЗИ от НСД используют СЗИ от НСД – важнейшую и обязательную составляющую механизма защиты современных АС на объектах информатизации ОВД [6]. Одной из ключевых функций СЗИ от НСД является управление доступом к информации, реализуемой ее важнейшей подсистемой – подсистемой управления доступом [7]. Результаты проведенного в [4] анализа эффективности функционирования СЗИ в АС, функционирующих в защищенном исполнении на объектах информатизации ОВД, с учетом современной мировой тенденции приоритетного развития средств аутентификации в программных продуктах ИБ [8, 9], требований руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [7] и нормативных актов МВД России [3] позволяет сделать вывод об актуальности задач разработки новых подсистем управления доступом в СЗИ от НСД защищенных АС ОВД или усиления уже существующих подсистем путем объединения стандартной процедуры аутентификации с процедурой дополнительной аутентификации субъектов доступа на основе использования современных информационно-телекоммуникационных технологий (в первую очередь, при обращении к особо важному информационному ресурсу).

1. Постановка задачи

Для определения основных аспектов совершенствования действующих подсистем управления доступом СЗИ от НСД в АС ОВД необходимо решить следующие задачи:

1. На основе результатов анализа открытой нормативно-распорядительной документации международного, федерального и ведомственного уровней, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, определить основные направления формирования требований, предъявляемых к функционированию их СЗИ от НСД.

2. Рассмотреть состав СЗИ от НСД в АС ОВД и определить базовые функции ее подсистемы управления доступом.

3. Раскрыть назначение и основные функции типовой широко используемой в защищенных АС ОВД СЗИ от НСД «Страж NT 4.0», провести ее классификацию по условиям функционирования с точки зрения ЗИ в АС на объектах информатизации ОВД для уточнения требований, предъявляемых к подсистеме управления доступом, с целью разработки и применения обоснованных мер по достижению требуемого уровня защищенности служебной информации.

4. Выявить недостатки функционирования подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» на объектах информатизации ОВД с целью определения функциональных возможностей подсистемы и направлений ее совершенствования для достижения требуемого уровня ЗИ.

2. Теоретический анализ

Анализ международных и отраслевых стандартов Российской Федерации по ИБ АС [8–10], Руководящих документов ФСТЭК России [5–7, 11–13], а также ведомственных нормативных актов по вопросам ЗИ на объектах информатизации ОВД [3] показал, что оценка эффективности функционирования систем и средств ЗИ на этапе эксплуатации АС и разработка адекватных существующим угрозам перспективных образцов этих систем является одним из важнейших моментов в процессе эксплуатации АС ОВД в защищенном исполнении. Следовательно, оценка эффективности СЗИ от НСД в АС ОВД может быть положена в основу формирования требований по ЗИ в данных системах.

Результаты анализа нормативно-распорядительных документов, используемых для

оценки эффективности СЗИ от НСД в АС ОВД [2, 3, 5, 10, 14–22], подробно представленные в [4, 23, 24], показали:

– необходимость доработки существующих в настоящее время требований по ЗИ в АС ОВД, основанных на функциональных требованиях к оценке эффективности СЗИ от НСД без учета поведения данных систем в динамическом (временном) диапазоне;

– необходимость совершенствования существующих СЗИ в АС ОВД в направлении управления процессами ЗИ от НСД с помощью управляемых параметров на основе количественной оценки эффективности функционирования СЗИ от НСД.

В соответствии с [6] СЗИ от НСД представляет собой комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от НСД к информации в АС. Применительно к объекту информатизации ОВД СЗИ от НСД следует рассматривать как функционально самостоятельную подсистему всех необходимых мероприятий, методов и средств, выделяемых (предусматриваемых) в АС ОВД с целью решения актуальных задач ЗИ от НСД. Программные средства ЗИ, входящие в состав СЗИ от НСД АС ОВД, образуют отдельную ее подсистему, обладающую рядом достоинств: надежностью, гибкостью, универсальностью, возможностью модификации и развития, простотой реализации [25]. Это позволяет совершенствовать существующие СЗИ на объектах информатизации ОВД для обеспечения требуемого уровня защищенности служебной информации от угроз НСД, повышая при этом общую надежность функционирования АС ОВД в защищенном исполнении.

На основе анализа структур СЗИ от НСД, действующих в защищенных АС на объектах информатизации ОВД [4, 26], и руководящих документов [7, 9] определено, что типовая СЗИ от НСД АС ОВД включает в свой состав пять основных подсистем: подсистему управления доступом («Включение ПК и идентификация пользователя»), подсистему разграничения доступа («Инициализация прав пользователя на работу в системе и доступ к каталогу файлов»), подсистему регистрации и учета («Работа пользователя с файлами и программами»), криптографическую подсистему («Работа пользователя с прикладным программным обеспечением»), подсистему обеспечения целостности («Деструктивное воздействие на СЗИ от НСД»).

В соответствии с [7] к базовым функциям подсистемы управления доступом СЗИ от НСД АС ОВД относятся идентификация и аутентификация (проверка подлинности) субъектов доступа.

Согласно [6] идентификация понимается как присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов, а аутентификация – как проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Посредством идентификации субъекту доступа (пользователю, действующему от имени определенного пользователя процессу, другому аппаратно-программному компоненту) предоставляется возможность сообщать свое имя (назвать себя). Аутентификация позволяет другой стороне убеждаться в том, что субъект доступа действительно является тем, за кого себя выдает. Основными методами аутентификации субъектов доступа в настоящее время являются: парольная аутентификация, маркеры аутентификации (смарт-карты), биометрическая аутентификация [27].

Парольная аутентификация осуществляется с использованием устройств идентификации и проверки подлинности субъекта доступа, представляющих собой USB-устройства, на которых записываются персональные данные субъекта доступа, позволяющие СЗИ от НСД по введенному вручную паролю определить данного субъекта и его привилегии входа в систему. Основными достоинствами парольной аутентификации

являются ее простота и привычность, связанные со встроенностью паролей в современные операционные системы и другие сервисы, что при правильном использовании паролей позволяет обеспечить приемлемый во многих случаях уровень ИБ. В то же время парольную аутентификацию следует признать самым слабым средством проверки подлинности по совокупности характеристик (ограничения на длину пароля, связанные с ограниченностью человеческой памяти; влияние длины пароля на время аутентификации и др.).

Более надежной альтернативой паролям можно считать маркеры аутентификации (смарт-карты), однако использование данного метода аутентификации связано с серьезными дополнительными расходами и не исключает возможности маскировки нарушителя под легального пользователя АС в случае утери или кражи смарт-карты. Смарт-карты также не способны предотвратить сетевую атаку с использованием уязвимых мест, поскольку рассчитаны на правильный вход субъекта доступа в систему.

Наиболее точной технологией аутентификации субъектов доступа является биометрическая аутентификация. Биометрия представляет собой комплекс автоматизированных методов аутентификации человека, основанных на анализе его физиологии (отпечатки пальцев, сетчатка и роговица глаз, геометрия руки и лица и др.) и поведения (динамика ручной подписи, стиль работы с клавиатурой). На стыке физиологических особенностей и поведенческих характеристик находятся анализ особенностей голоса и распознавание речи [27].

3. Обсуждение результатов

Для ЗИ на объектах информатизации, эксплуатирующих защищенные АС ОВД, в настоящее время используются СЗИ от НСД «Dallas Lock», «Dallas Lock Linux», «Secret Net», «Secret Net Studio», «Страж NT» и др. Наиболее широкое применение в АС ОВД для защиты конфиденциальной информации и сведений, составляющих государственную тайну, нашла СЗИ от НСД «Страж NT 4.0», на примере которой рассмотрим функциональные возможности СЗИ от НСД, действующих в АС ОВД, выявим существующие недостатки их функционирования для определения направлений совершенствования подсистем управления доступом данных систем с целью повышения реальной защищенности АС на объектах информатизации ОВД.

СЗИ от НСД «Страж NT 4.0» является сертифицированным (сертификат ФСТЭК России № 3553, выдан 20.04.2016, действует до 20.04.2024) программным средством защиты от НСД к информации и соответствует требованиям руководящих документов [11] по 3-му классу защищенности средств вычислительной техники (СВТ) и [13] по 2-му уровню контроля отсутствия недекларированных возможностей. Она предназначена для комплексной защиты информационных ресурсов от НСД в соответствии с требованиями законодательства Российской Федерации: в АС до класса защищенности 1Б включительно, в государственных информационных системах до 1-го класса защищенности включительно, в информационных системах персональных данных до 1-го уровня защищенности включительно. Функционирует в среде 32-х и 64-разрядных операционных систем Microsoft Windows, поддерживая новейшие версии Microsoft до Windows 10 включительно (в АС ОВД используются версии Microsoft до Windows 7 включительно).

СЗИ от НСД «Страж NT 4.0» обладает рядом ощутимых преимуществ по сравнению с ее предыдущими версиями и представляет собой многофункциональную систему, реализующую следующие основные функции [28, 29]:

– двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов (USB-идентификаторов типа Guardant ID, Rutoken, eToken, JaCarta, ESMART Token) и смарт-карт

(Рутокен, eToken, JaCarta, ESMART);

– дискреционный и мандатный принципы контроля доступа к ресурсам системы;

– создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений;

– регистрация событий безопасности, в том числе и действий администратора.

– маркировка выдаваемых на печать документов независимо от печатающего их приложения;

– гарантированная очистка;

– контроль целостности защищаемых ресурсов и компонентов СЗИ;

– управление пользователями, носителями информации и устройствами;

– преобразование информации на отчуждаемых носителях;

– тестирование СЗИ.

Проведем классификацию СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ в АС ОВД для уточнения требований идентификации и аутентификации субъектов доступа, предъявляемых к подсистеме управления доступом.

Для подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД класса защищенности 1Б в соответствии с пп. 2.10, 2.14 Руководящего документа ФСТЭК России [7] должны быть реализованы требования идентификации и аутентификации, представленные в таблице 1.

Для используемой в АС ОВД подсистемы управления доступом СЗИ от НСД «Страж NT 4.0», сертифицированной по 3-го классу защищенности СВТ, в соответствии с руководящим документом [11] должны выполняться требования к показателям защищенности в части идентификации и аутентификации, представленные в таблице 2.

Результаты исследования качества функционирования подсистем управления доступом СЗИ от НСД современных защищенных АС ОВД, представленные в [4, 25], показали: их высокую значимость в решении проблемы ЗИ на объектах информатизации, эксплуатирующих данные системы, особенно в условиях возрастания угроз НСД; зависимость сложности целесообразных для применения в АС ОВД процедур и средств идентификации и аутентификации субъектов доступа от уровня конфиденциальности защищаемой служебной информации; важность проведения контроля физического состояния субъекта доступа к информационному ресурсу высокого уровня конфиденциальности в процессе аутентификации, поскольку его ошибочные действия могут привести к потерям, неприемлемым для ОВД и общества в целом.

Результаты проведенной классификации СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ в АС ОВД, а также результаты изучения опыта эксплуатации СЗИ от НСД «Страж NT 4.0» в защищенных АС на объектах информатизации ОВД с осуществлением стандартных процедур идентификации и аутентификации субъектов доступа, основанных на парольной аутентификации и использовании смарт-карт, представленные в [30], позволяют констатировать, что функциональные возможности подсистемы управления доступом СЗИ от НСД «Страж NT 4.0», определяемые требованиями действующей нормативно-распорядительной документации, датированной 1992 годом [7, 11], не соответствуют как возможностям современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, так и потребности подразделений ОВД, занимающихся обработкой конфиденциальной информации. Следовательно данная подсистема нуждается в существенной доработке на основе применения новых информационно-телекоммуникационных технологий в области ЗИ для достижения требуемого уровня защищенности служебной информации без нарушения эффективности функционирования АС ОВД по прямому назначению. В первую очередь это

касается особо важного информационного ресурса, требующего повышенной защищенности (информация высокого уровня конфиденциальности, наиболее важные параметры функционирования АС ОВД и др.). Как правило данный информационный ресурс предназначен для узкого круга санкционированных субъектов доступа и характеризуется малой частотой обращений к нему.

Таблица 1. Требования к подсистеме управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД по идентификации и аутентификации субъектов доступа в соответствии с [7]

Наличие/отсутствие требований	Требования	Расшифровка требований
+	Идентификация, аутентификация субъектов доступа в систему	Идентификация и аутентификация субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов
+	Идентификация, аутентификация субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	Идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам)
+	Идентификация, аутентификация субъектов доступа к программам	Идентификация программ по именам
+	Идентификация, аутентификация субъектов доступа к томам, каталогам, файлам, записям, полям записей	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам

Обозначения: «–» – требования отсутствуют; «+» – есть требования.

Таблица 2. Требования к показателям защищенности подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД в части идентификации и аутентификации в соответствии с [11]

Наличие/отсутствие требований	Наименование показателя защищенности	Требования
=	Идентификация и аутентификация	Требование от субъектов доступа идентифицировать себя при запросах на доступ, проверка подлинности идентификатора субъекта — осуществление аутентификации. Подсистема должна располагать необходимыми данными для идентификации н аутентификации и препятствовать входу в систему неиденфицированного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась. Подсистема должна обладать способностью надежно связывать полученную идентификацию со всеми действиями данного субъекта доступа.

Обозначения: «–» – требования отсутствуют; «+» – новые либо дополнительные требования; «=» – требования совпадают с требованиями к СВТ предыдущего класса.

Управление эффективностью функционирования подсистемы управления доступом СЗИ от НСД для достижения требуемого уровня ЗИ в АС ОВД может быть осуществлено за счет усложнения процедуры аутентификации субъектов доступа и сокращения

необходимого для ее реализации временного диапазона. Поэтому с целью повышения защищенности АС, эксплуатируемых на объектах информатизации ОВД, предлагается при обращении к особо важному информационному ресурсу использовать подсистему многоуровневого управления доступом в систему, выполняющую помимо стандартной процедуры аутентификации субъектов доступа процедуру их дополнительной аутентификации. Это наиболее значимо для многопользовательских АС ОВД, относящихся к первой группе классов защищенности от НСД [7], имеющих широкую номенклатуру субъектов доступа с разными полномочиями к конфиденциальному информационному ресурсу, способных одновременно обрабатывать и (или) хранить информацию различных уровней конфиденциальности.

Перспективным направлением реализации процедуры дополнительной аутентификации может стать использование биометрической технологии, основанной на распознавании субъекта доступа к информационному ресурсу АС ОВД по индивидуальной динамике клавиатурного набора (клавиатурному почерку). Целесообразность применения аутентификации субъектов доступа по клавиатурному почерку по сравнению с другими технологиями биометрической аутентификации объясняется ее основными достоинствами: достаточно высокая степень эффективности, возможность контроля физического состояния субъектов доступа, скрытость использования, быстродействие, простота реализации и дешевизна [31, 32].

Заключение

Таким образом, в статье на основе анализа открытой разно уровневой нормативно–распорядительной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, определен состав СЗИ от НСД данных систем и выявлены основные направления формирования требований к их функционированию на объектах информатизации ОВД.

Раскрыты назначение, основные функции и проведена классификация типовой широко используемой в АС ОВД СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ. На основе проведенной классификации и изучения опыта эксплуатации СЗИ от НСД «Страж NT 4.0» в защищенных АС на объектах информатизации ОВД определены недостатки стандартной процедуры аутентификации и возможности ее совершенствования путем введения процедуры дополнительной биометрической аутентификации субъектов доступа по клавиатурному почерку для достижения требуемого уровня ЗИ.

Использование в типовых СЗИ от НСД защищенных АС на объектах информатизации ОВД подсистем многоуровневого управления доступом, основанных на реализации совокупной процедуры аутентификации субъектов доступа, при обращении к особо важному информационному ресурсу позволит обеспечить высокий уровень защищенности АС ОВД от угроз НСД к служебной информации указанного уровня конфиденциальности, не нарушая при этом требуемой эффективности ее функционирования по прямому назначению.

СПИСОК ЛИТЕРАТУРЫ:

1. Статистические данные о зарегистрированных преступлениях на территории Российской Федерации в январе–августе 2019 года. URL: https://www.genproc.gov.ru/smi/news/genproc/news–1703326/ (дата обращения: 20.11.2019).
2. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. URL:http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 14.12.2019).
3. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169. URL: http://policemagazine.ru/forum/showthread.php?t=3663 (дата обращения: 28.11.2019).
4. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел: дис. ... канд. техн. наук: 05.13.19 / Попов Антон Дмитриевич. – Воронеж, 2018. – 163 с.
5. ФСТЭК России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. URL: https://fstec.ru/component/attachments/download/299 (дата обращения: 13.12.2019).
6. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 13.12.2019).
7. ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. URL: https://fstec.ru/component/attachments/download/296 (дата обращения: 14.12.2019).
8. ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1 Revision 4, September 2012. – 93 p. URL: https://commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (дата обращения: 10.12.2019).
9. ГОСТ Р ИСО/МЭК 15408–2–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные компоненты безопасности. URL: http://docs.cntd.ru/document/1200105710 (дата обращения: 10.12.2019).
10. ГОСТ Р 51583–2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 11.12.2019).
11. ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. URL: http://fstec.ru/tekhnicheskaya–zashchita–informatsii/dokumenty/114–spetsialnye–normativnye–dokumenty/383–rukovodyashchij–dokument–reshenie–predsedatelya–gostekhkomissii–rossii–ot–25–iyulya–1997–g (дата обращения: 11.12.2019).
12. ФСТЭК России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. URL: http://docs.cntd.ru/document/901817221 (дата обращения: 28.11.2019).
13. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. URL: http://meganorm.ru/Index2/1/4293808/4293808514.htm (дата обращения: 28.11.2019).
14. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149–ФЗ (в ред. от 19.12.2016) (с изм. и доп., вступ. в силу с 13.12.2019). URL: https://legalacts.ru/doc/FZ–ob–informacii–informacionnyh–tehnologijah–i–o–zawite–informacii/ (дата обращения: 02.12.2019).
15. О государственной тайне: закон Российской Федерации от 21.07.1993 № 5485–1 (в ред. от 08.03.2015) // СПС «КонсультантПлюс» (дата обращения: 12.12.2019).
16. О сертификации средств защиты информации: постановление Правительства РФ от 26.06.1995 № 608 (ред. от 21.04.2010) // СПС «КонсультантПлюс» (дата обращения: 03.12.2019).
17. Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну…: постановление Правительства РФ от 21.04.2010 № 266 (в ред. от 03.11.2014) // СПС «КонсультантПлюс» (дата обращения: 10.12.2019).
18. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/gost–r–50922–2006 (дата обращения: 02.12.2019).

19. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // СПС «КонсультантПлюс» (дата обращения: 10.12.2019).
20. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21 (в ред. от 23.03.2017) // СПС «КонсультантПлюс» (дата обращения: 02.12.2019).
21. Об утверждении Наставления по технической защите информации в системе Министерства внутренних дел: приказ МВД России от 06.03.2013 № 010.
22. ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200075565 (дата обращения: 02.12.2019).
23. Каднова А.М. Система показателей качества функционирования при создании системы информационной безопасности на объекте информатизации ОВД / О.И. Бокова, А.М. Каднова, Е.А. Рогозин, А.С. Серпилин // Приборы и системы, управление, контроль, диагностика. 2019. № 1. С. 26–33.
24. Каднова, Айжана М. et al. Алгоритм создания автоматизированных систем в защищенном исполнении. Безопасность информационных технологий, [S.l.], Т. 26, № 4. С. 93–100, dec. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1235> (дата обращения: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.07.
25. Формирование требований к системам защиты информации от несанкционированного доступа в автоматизированные системы органов внутренних дел на основе генетического алгоритма: монография / Дровникова И.Г. [и др.]. Воронеж: Воронеж. ин-т МВД России, 2019. – 128 с.
26. Бокова, Оксана И. Et al. Разработка имитационной модели системы защиты информации от несанкционированного доступа с использованием программной среды cpn tools. Безопасность информационных технологий, [S.l.], Т. 26, № 3. С. 80–89, sep. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1220> (дата обращения: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.07.
27. Мартынова Л.Е. Исследование и сравнительный анализ методов аутентификации / Мартынова Л.Е. [и др.] // Молодой ученый. 2016. № 19. С. 90–93.
28. Система защиты информации от несанкционированного доступа «Страж NT 4.0». URL: https://www.guardnt.ru/gnt_40.html (дата обращения: 30.11.2019).
29. Страж NT. Система защиты информации от несанкционированного доступа. Версия 4.0. Руководство администратора. URL: https://labvs.ru/upload/iblock/390/390a1a477039748 e3f745132c08172a6.pdf (дата обращения: 30.11.2019).
30. Рогозин Е.А. Проблемы и пути их решения при проектировании систем защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов, Т.В. Мещерякова // Информационные технологии, связь и защита информации МВД России. 2017. Ч. 1. С. 115–118.
31. Аверин А.И. Аутентификация пользователей по клавиатурному почерку / А.И. Аверин, Д.П. Сидоров. URL: http://cyberleninka.ru/article/n/autentifikatsiya–polzovateley–po–klaviaturnomu–pocherku (дата обращения: 02.12.2019).
32. Яндиев И.Б. Исследование временных характеристик клавиатурного почерка для быстрой аутентификации личности / И.Б. Яндиев // Молодой ученый. 2017. № 14. С. 154–157.

REFERENCES:

[1] Statistical data on registered crimes in the territory of the Russian Federation in January–August. URL: https://www.genproc.gov.ru/smi/news/genproc/news–1703326/ (accessed: 20.11.2019) (in Russian).
[2] About the statement of the Doctrine of information security of the Russian Federation: the decree of the President of the Russian Federation of 05.12.2016 № 646. URL:http://publication.pravo.gov.ru/ Document/View/0001201612060002 (accessed: 14.12.2019) (in Russian).
[3] About the statement of the Concept of ensuring information security of law–enforcement bodies of the Russian Federation till 2020: the order of the Ministry of internal Affairs of Russia of 14.03.2012 № 169. URL: http://policemagazine.ru/forum/showthread.php?t=3663 (accessed: 28.11.2019) (in Russian).
[4] Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against unauthorized access taking into account their temporal characteristics in automated systems of internal Affairs: dis. ... cand. tech. sciences: 05.13.19. Popov Anton Dmitrievich. – Voronezh, 2018. – 163 p. (in Russian).
[5] FSTEC of Russia. Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information. URL: https://fstec.ru/component/attachments/ download/299 (accessed: 13.12.2019) (in Russian).

[6] FSTEC of Russia. Guidance document. Protection against unauthorized access to information. Terms and definitions. URL:https://fstec.ru/component/attachments/download/298 (accessed: 13.12.2019) (in Russian).
[7] FSTEC of Russia. Guidance document. Automated system. Protection against unauthorized access to information. Classification of automated systems and information security requirements. URL: https://fstec.ru/component/attachments/download/ 296 (accessed: 14.12.2019) (in Russian).
[8] ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1 Revision 4, September 2012. – 93 p. URL: https://commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (accessed: 10.12.2019).
[9] GOST R ISO / IEC 15408–2–2013. Information technology. Methods and means of security. Information technology security assessment criteria. Part 2: Functional components of safety. URL: http://docs.cntd.ru/document/1200105710 (accessed: 10.12.2019) (in Russian).
[10] GOST R 51583–2014. National standard of the Russian Federation. Information protection. Order of creation of the automated systems in the protected execution. URL: http://docs.cntd.ru/document/1200108858 (accessed: 11.12.2019) (in Russian).
[11] FSTEC of Russia. Guidance document. Computer aids. Protection against unauthorized access to information. Indicators of protection against unauthorized access to information. URL: http://fstec.ru/ tekhnicheskaya–zashchita–informatsii/dokumenty/114–spetsialnye–normativnye–dokumenty/383–rukovodyashchij– dokument–reshenie–predsedatelya–gostekhkomissii–rossii–ot–25–iyulya–1997–g (accessed: 11.12.2019) (in Russian).
[12] FSTEC of Russia. Guidance document. Temporary position on the organization of development, production and operation of software and technical means of information protection from unauthorized access in automated systems and computer equipment. URL: http://docs.cntd.ru/document/901817221 (accessed: 28.11.2019) (in Russian).
[13] FSTEC of Russia. Guidance document. Protection against unauthorized access to information. Part 1: information security software. Classification by the level of control of the absence of undeclared opportunities. URL: http://meganom.ru/Index2/1/4293808/4293808514.htm (accessed: 28.11.2019) (in Russian).
[14] On information, information technologies and information protection: Federal law № 149–FZ of 27.07.2006 (as amended on 19.12.2016) (with ed. and extra, intro. effective from 13.12.2019). URL:https://legalacts.ru/doc/FZ–ob–informacii–informacionnyh–tehnologijah–i–o–zawite–informacii/ (accessed: 02.12.2019) (in Russian).
[15] On state secrets: law of the Russian Federation № 5485–1 of 21.07.1993 (as amended on 08.03.2015). SPS «ConsultantPlus» (accessed: 12.12.2019) (in Russian).
[16] On certification of information security tools: decree of the Government of the Russian Federation of 26.06.1995 № 608 (ed. of 21.04.2010) SPS «ConsultantPlus» (accessed: 03.12.2019) (in Russian).
[17] About features of conformity assessment of products (works, services) used for protection of information constituting a state secret...: resolution of the Government of the Russian Federation of 21.04.2010 № 266 (as amended from 03.11.2014) SPS «ConsultantPlus» (accessed: 10.12.2019) (in Russian).
[18] GOST R 50922–2006. Information protection. Basic terms and definitions. URL: http://docs.cntd.ru/document/gost–r–50922–2006 (accessed: 02.12.2019) (in Russian).
[19] GOST R 51275–2006. Information protection. Object of Informatization. Factors that affect information. Generalities. SPS «ConsultantPlus» (accessed: 10.12.2019) (in Russian).
[20] On approval of the composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems: order of the FSTEC of Russia dated 18.02.2013 № 21 (as amended on 23.03.2017) SPS «ConsultantPlus» (accessed: 02.12.2019) (in Russian).
[21] About the approval of the Instruction on technical protection of information in the system of the Ministry of internal Affairs: order of the Ministry of internal Affairs of Russia of 06.03.2013 № 010 (in Russian).
[22] GOST R 53114–2008 information Protection. Ensuring information security in the organization. Basic terms and definitions. URL: http://docs.cntd.ru/document/ 1200075565 (accessed: 02.12.2019) (in Russian).
[23] Kadnova A.M. System of indicators of the quality of functioning when creating an information security system on the object of informatization of ATS. O.I. Bokova, A.M. Kadnova, E.A. Rogozin, A.S. Serpilin. Devices and systems, management, control, diagnostics. 2019. № 1. P. 26–33 (in Russian).
[24] Kadnova, Aizhana M. et al. Algorithm for creation of automated systems in protected performance. IT Security (Russia), [S.l.], v. 26, n. 4. P. 93–100, dec. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1235> (accessed: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.07.
[25] Formation of requirements to information protection systems from unauthorized access to automated systems of internal Affairs bodies on the basis of genetic algorithm: monograph Drovnikova I.G. [and others]. – Voronezh: Voronezh. Institute of MIA of Russia, 2019. – 128 p. (in Russian).
[26] Bokova, Oksana I. et al. Development of an imitation model of information protection system from unauthorized access using the cpn tools software. IT Security (Russia), [S.l.], v. 26, n. 3. P. 80-89, sep. 2019. ISSN 2074-7136.

URL: https://bit.mephi.ru/index.php/bit/article/view/1220 (accessed: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.07 (in Russian).

[27] Martynova L.E. Research and comparative analysis of authentication methods Martynova L.E. [and others]. Young scientist. 2016. № 19. P. 90–93 (in Russian).

[28] Information protection system from unauthorized access «Strazh NT 4.0». URL:https://www.guardnt.ru/gnt_40.html (accessed: 30.11.2019) (in Russian).

[29] Strazh NT. The system of information protection from unauthorized access. Version 4.0. Administrator's guide. URL:https://labvs.ru/upload/iblock/390/390a1a477039748 e3f745132c08172a6.pdf (accessed: 30.11.2019) (in Russian).

[30] Rogozin E. A. Problems and ways to solve them when designing information protection systems from unauthorized access in automated information systems of the police Department E.A. Rogozin, A.D. Popov, T.V. Meshcheryakova. Information technologies, communication and information protection of the Ministry of internal Affairs of Russia. 2017. Part 1. P. 115–118 (in Russian).

[31] Averin A.I. Authentication of users by keyboard handwriting A.I. Averin, D.P. Sidorov. URL: http://cyberleninka.ru/article/n/autentifikatsiya–polzovatelya–po–klaviaturnomu–pocherku (accessed: 02.12.2019) (in Russian).

[32] Yandiev I.B. Study of temporal characteristics of keyboard handwriting for rapid authentication of personality I.B. Yandiev. Young scientist. 2017. № 14. P. 154–157 (in Russian).

Поступила в редакцию – 5 февраля 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – February 05, 2020. The final version – May 25, 2020.

Алексей А. Салкуцан[1], Григорий П. Гавдан[2], Андрей А. Полуянов[3]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[3]ТЭЦ-8 филиал ПАО «Мосэнерго»,
Остаповский пр-д, 1, Москва, 109316, Россия
[1]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: andreapol_tec8@mail.ru, https://orcid.org/0000-0001-8648-5915

МЕТОДИКА ОПРЕДЕЛЕНИЯ КРИТИЧЕСКИХ ПРОЦЕССОВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org /10.26583/bit.2020.2.02

Аннотация. Целью статьи является попытка разработки методики определения критических процессов для упрощения деятельности субъектов критической информационной инфраструктуры (КИИ) по проведению категорирования объектов информационной инфраструктуры на примере химической промышленности. Актуальность рассматриваемых проблем обусловлены тем, что с каждым годом не уменьшается число кибератак на различные сферы деятельности государств, в том числе, и на значимые объекты (ЗО) КИИ. Для защиты национальных информационных ресурсов РФ в 2017 году был выбран вектор действий в направлении защиты объектов КИИ принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который определил важные направления политики российского государства в информационной сфере, и как минимум, на ближайшее десятилетие. Так, в ходе его выполнения, многим субъектам критической информационной инфраструктуры уже пришлось столкнуться с различного уровня трудностями. В статье разобраны некоторые фрагменты решения задач, поставленных при разработке методики определения критических процессов на объектах информационной инфраструктуры, устойчивое функционирование которых регламентировано рядом основополагающих нормативных правовых документов РФ. В работе установлены некоторые особенности определения критических процессов на объектах КИИ, например, химической промышленности, которые нашли свое применение в разработке авторами методики определения критических процессов информационной инфраструктуры.

Ключевые слова: значимые объекты, категорирование объектов, критические процессы, критическая информационная инфраструктура (КИИ), национальные информационные ресурсы, *субъекты КИИ.*

Для цитирования: САЛКУЦАН, Алексей А.; ГАВДАН, Григорий П.; ПОЛУЯНОВ, Андрей А. МЕТОДИКА ОПРЕДЕЛЕНИЯ КРИТИЧЕСКИХ ПРОЦЕССОВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 18-34, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1268>. Дата доступа: 27 may 2020. doi: http://dx.doi.org/10.26583/bit.2020.2.02.

Alexei A. Salkutsan[1], Grigory P. Gavdan[2], Andrey A. Poluyanov[3]
[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[3]CHPP-8 branch of «Mosenergo» PJSC,
1 Ostapovsky Ave., Moscow, 109316, Russia
[1]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: andreapol_tec8@mail.ru, https://orcid.org/0000-0001-8648-5915

The method of identifying critical processes at information infrastructure facilities

DOI: http://dx.doi.org /10.26583/bit.2020.2.02

Abstract. The aim of the study is to develop a methodology for determining critical processes in order to simplify the activities of critical information infrastructure (CII) entities for categorizing information infrastructure objects on the example of the chemical industry. The actuality of the problems under consideration is based on the fact that the number of cyber attacks in various areas of state activity, including significant objects (ZO) of CII, is not decreasing. To protect the national information resources of the Russian Federation in 2017, the actions have been chosen in the direction of protecting CII objects with the adoption of the Federal law "on the security of critical information infrastructure of the Russian Federation", which defined important directions of the Russian state policy in the information sphere for the next decade. Thus during its implementation, many subjects of critical information infrastructure have already had to face difficulties of various levels. The paper analyzes some fragments of solving the tasks set in the development of methods for determining critical processes at information infrastructure facilities, the sustainable functioning of which is regulated by a number of fundamental regulatory legal documents of the Russian Federation. In the course of the study, some features of determining critical processes at CII facilities, for example, in the chemical industry, were established. These features were later used in the development of a unique methodology for determining critical processes in the information infrastructure.

Keywords: significant objects, object categorization, critical processes, critical information infrastructure (CII), national information resources, CII subjects.

For citation: 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, n. 2, p. 18-34, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1268>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.02.

Введение

Непрерывное функционирование значимых объектов критической информационной инфраструктуры (КИИ) и состояние её безопасности в XXI веке играет ключевую роль в России в критических сферах экономики [1] и обеспечении национальной безопасности ведущих стран мира, включая и Российскую Федерацию (РФ). В настоящее время, обладая достаточными знаниями, ресурсами и используя современные технологии (ноу-хау) на мировой арене (и не только на уровне государств), появилась возможность проводить различного рода и вида специальные операции, как оборонительного, так и наступательного характера для достижения целей (политического, экономического, военного и др.) [2].

Для субъектов КИИ критических сфер экономики (государства), которые в своем составе имеют сотни и даже тысячи объектов КИИ выполнение Федерального закона (ФЗ) № 187 от 26 июля 2017 года[1] является не простой задачей.

В настоящее время возникает большое количество вопросов, на которые необходимо дать ответы, например, определение критических процессов в условиях неопределённости и др.[2] На IT&Security Forum Kazan 2019 представителем Национальным координационным центром по компьютерным инцидентам (НКЦКИ) Кореловым С. был представлен доклад на тему: «О практике взаимодействия с НКЦКИ».

Так, например, согласно данным НКЦКИ в 2019 году было выявлено:

6800 адресатов вредоносного программного обеспечения (ВПО);

215 рассылок ВПО с взломанных почтовых адресов;

[1]Федерального закона от 26.072017 года № 187 от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», принят Государственной Думой 12.07.2017 года.

[2]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: 12.12.2019).

186 случаев внедрения ВПО;
53 случая использования ресурсов для проведения DDoS-атаки;
51 случай подмены заглавной страницы сайта;
5 случаев внедрения майнеров и др.

Современные отрасли экономики активно внедряют новейшие цифровые решения, которые позволяют с помощью различных объектов информационной инфраструктуры, таких как: информационные системы (ИС) [3], автоматизированные системы управления технологическими процессами (АСУ ТП) [4] и информационно-телекоммуникационные сети (ИТКС) [5] повысить конкурентоспособность и модернизацию с целью ускорения своего инновационного развития. Чаще всего приобретая такие решения, предприятие или организация не задумываются или не хотят уделить должное внимание вопросам должного обеспечения защиты информации [6].

Например, авторами Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke в статье «Кибербезопасность критических инфраструктур» отмечается, что «современные АСУ ТП в последние годы подвергаются большому числу компьютерных атак, вследствие чего представляется серьезная угроза национальной безопасности государств» [7].

Так, согласно отчету Kaspersky ICS-CERT, в мире количество компьютерных атак с попытками внедрения вредоносных объектов на компьютеры АСУ в первом полугодии 2019 по сравнению с первым полугодием 2018 выросли незначительно, однако все равно находятся на высоких отметках (рис. 1). Так, работа химических предприятий в Российской Федерации основана на использовании различных технологических схем, методов и расчетов (химических формул, превращений одних веществ в другие вещества, изменениях свойств материалов, их строения и др.). В качестве примера в АСУ ТП (химическая отрасль) можно привести всем известную систему SCADA применяемую на базе устройств фирмы SIEMENS. Повсеместное внедрение таких систем в АСУ ТП, с одной стороны, способствовало (в отрасли) увеличению возможностей (отвечающих общим мировым стандартам): качеству конечного продукта, обеспечению его экологической безопасности и др., а с другой стороны, привело к увеличению угроз, способных нанести непоправимый ущерб не только самому предприятию, но зависимым и взаимозависимым с данным предприятием организациям из других сфер экономики [7].

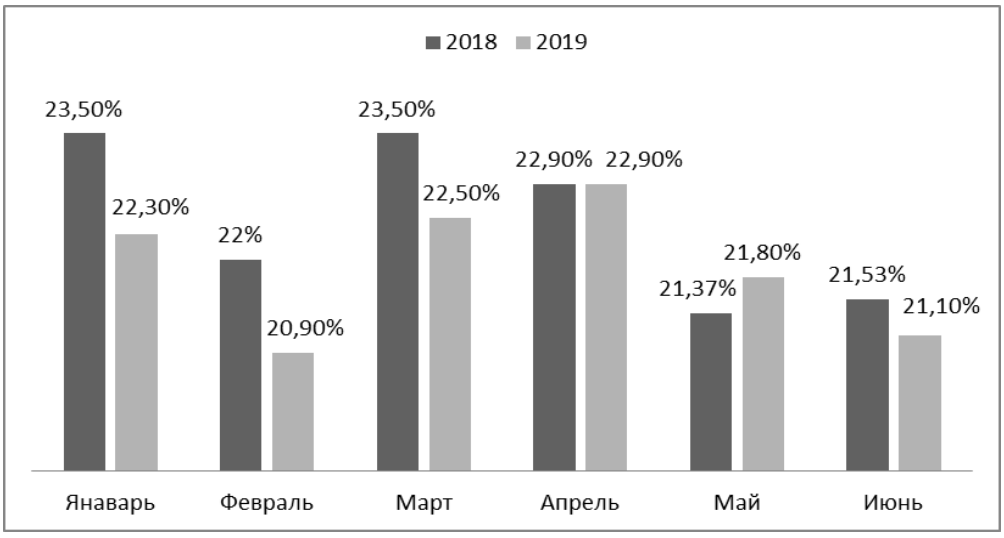


Рис. 1. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам, первые полугодия 2018 и 2019 годов [8]
(Fig. 1. Percentage computers of vulnerable automatic process control systems where malicious objects were blocked by month, first half of 2018 and 2019 [8])

Так, при реализации угроз безопасности информации, например, «Угроза перехвата управления автоматизированной системой управления технологическими процессами» № 183[3] может привести к частичной или полной остановам технологических процессов (без выхода или с выходом оборудования из строя). Как следствие, произойдёт нарушение штатного хода технологических процессов на значимом объекте КИИ (ЗОКИИ).

Принятие Федерального закона № 187[4] от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», и появление связанных с ним других подзаконных актов, направлено именно на защиту ЗОКИИ государства, включая информационные системы органов власти. Поэтому для субъектов КИИ критических сфер экономики, имеющих сегодня сотни и даже тысячи значимых объектов КИИ, выполнение этого законодательства является не простой задачей. Так, например, при проведении мероприятий по категорированию нет утвержденной со стороны Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) методики определения критических процессов. При этом также, необходимо отметить, что приказы о создании комиссии по категорированию и специальной комиссии по инвентаризации объектов КИИ и определению критических процессов (КП) являются внутренними нормативными документами предприятия (субъекта КИИ), где состав и форма определяется с субъектом[5].

В результате этого некоторые субъекты КИИ столкнулись с важной проблемой правильности отнесения того или иного объекта к категории значимого объекта КИИ, где в ряде случаев возврат документов со стороны ФСТЭК России происходит вследствие некорректности применения критериев значимости к объекту ИИ.

Отсутствие для сфер деятельности в РФ утвержденных методик для ЗОКИИ со стороны ФСТЭК России и Федеральной службой безопасности (ФСБ России) вынуждает многих представителей субъектов КИИ (в настоящее время) привлекать аутсорсинговые компании. В свою очередь аутсорсинговые компании (АК) для определения критических процессов в информационной инфраструктуре в своей работе применяют (наработанные) свои методы и подходы. Такое сотрудничество не всегда позволяет достигнуть требуемых гарантией в определении критических процессов у потенциально значимых объектов КИИ (ЗО КИИ) для этих субъектов. И здесь субъекту КИИ приходится делать свой выбор.

Необходимо также отметить, что многие отечественные методики и подходы по категорированию опираются только на метод экспертных оценок с последующим анализом полученных результатов для формирования отчета и включением в акт по категорированию того или иного объекта КИИ [9]. При этом в них не учитываются зависимости и взаимозависимости между объектами информационной инфраструктуры с другими объектами и их процессами, влияющими на появление рисков, например, возникновения каскадных и эскалационных сбоев в одном или нескольких регионах РФ из-за компьютерной атаки и т.д. И это достаточно важная проблема на ряду и с проблемой правильного определения значимости.

---

[3]Банк угроз информации ФСТЭК России // ФСТЭК России. URL: https://bdu.fstec.ru/threat/ubi.183 (дата обращения: 27.03.2020).

[4]Федерального закона № 187 от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации».

[5]Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования» //. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1606-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 27.03.2020).

Если обратимся к опыту рубежных специалистов, то обнаружим, что многими учеными, активно проводятся исследования и обсуждения в области КИИ, которые направлены на разработку комплексных инструментов для определения важнейших услуг информационной инфраструктуры [10]; методов выявления взаимозависимостей отказов инфраструктурных служб [11]; разработке оценок каскадированого (и др.) воздействия на системы КИИ [12]; комплексных подходов к оценке устойчивости критически важных элементов инфраструктуры [13]. Предполагается, что разрабатываемая методика позволит субъектам КИИ правильно определить имеющейся критические процессы, тем самым повысить ситуационную осведомленность государственных органов управления по наличию (у субъектов) объектов КИИ, что даёт возможность предвидеть (предупредить) сбои на ЗО КИИ для случаев с воздействием на КИИ. Так, важность этих объектов (химическая промышленность) для любого государства не требует доказательств, так как несет огромный ущерб людям, экономики и экологии [14].

Главной на сегодня трудностью, по мнению авторов, является отсутствие разработанных и утвержденных методик. Так, есть только отдельные как зарубежные, так и отечественные подходы и методы, которые освещались в научных статьях и конференциях по ИБ. Поэтому некоторые субъекты КИИ вынуждены (хотя и временно) заниматься анализом в отношении своих объектов КИИ без какой-либо утвержденной методической базы со стороны регуляторов.

Всё это послужило и легло в основу разрабатываемой авторами методики. Так, на рис. 2 представлены основные этапы предполагаемой авторами методики по определению значимости объекта (критических процессов) на объектах информационной инфраструктуры. В статье акцентировано внимание на некоторых её моментах.

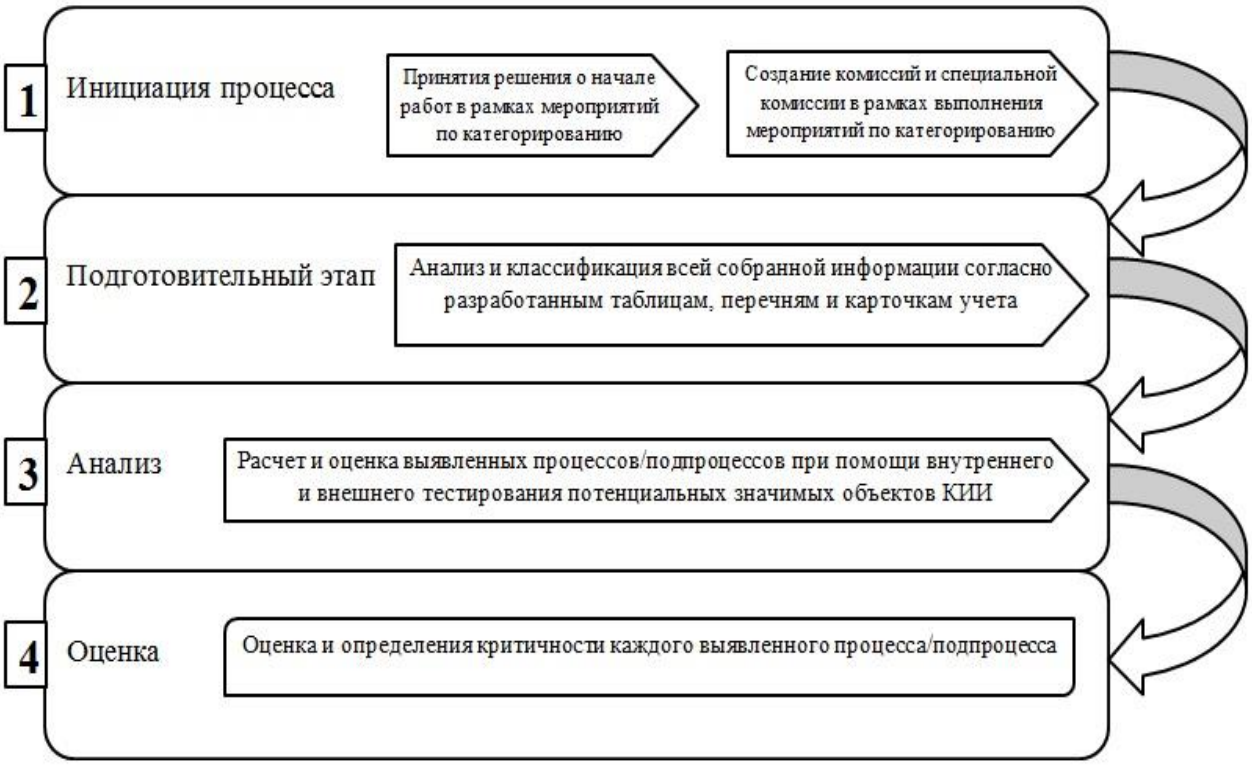


Рис. 2. Основные этапы методики определения критических процессов
(Fig. 2. The main stages of the methodology for determining critical processes)

1. Инициация процесса

После того, как субъект КИИ принял решение о начале работ по выполнению ФЗ №187, он создаёт комиссию по категорированию, которая начинает процесс инициации работ по выполнению мероприятий и одновременно принимает решения о начале работ по определению и обоснованию всех выявленных процессов в организации. Чтобы их выполнить, необходимо нанять соответствующих персонал, имеющий право в соответствии с законодательством РФ на ведение такой деятельности.

Здесь необходимо отметить, что содержать отдел по ИБ и ИТ, сотрудники которого смогли бы на достаточно высоком уровне проводить необходимые мероприятия на объектах КИИ (определять критические процессы, давать обоснованные решения на основе правильно полученных и оформленных результатах в ходе работы, выполнении обслуживания, проведении мониторинга (данных) объектов [15] и др.) с точки зрения финансирования вышестоящими министерствами и ведомствами для многих субъектов КИИ не представляется возможным. При этом, отдадим должное, некоторые субъекты КИИ имеют достаточные финансовые средства на содержание отдела (ИБ и ИТ), и как правило, предпочтения в этом случае отдают аутсорсинговым организациям [16] обладающим подготовленным персоналом, и опытом на рынке ИБ, готовых провести соответствующие мероприятия в рамках выполнения законодательства по КИИ (не безвозмездно) и это их законное право.

Первый этап. Инициация процесса по категорированию объектов КИИ. Для того чтобы избежать ошибок на первом этапе методики, авторами рекомендуется взять за основу нижеприведенную схему (рис. 3).

Рис. 3. Инициация процесса категорирования объектов критической информационной инфраструктуры
(Fig. 3. Initiating the process of categorizing critical information infrastructure objects)

Субъекты КИИ, у которых потенциально значимые объекты (ЗО) имеют выход в сеть Интернет, подвергают свои объекты угрозам. Это не означает, что необходимо отказаться от информационных Интернет-технологий в производстве и других сферах человеческой деятельности.

Важно при этом помнить, что в таких ситуациях в процессе эксплуатации (в последствии ЗОКИИ) существуют риски, например, от компьютерных атак, последствия которых могут наносить ущерб государству (приводить к жертвам среди населения, срыву государственного оборонного заказа, или к недоступности той или иной значимой системы и др.) [15].

2. Специальная комиссия по инвентаризации значимых объектов и определению критических процессов

Второй этап. Субъектом издается приказ о проведении инвентаризации всех информационных активов, после чего специальная комиссия приступает к выполнению возложенных на нее задач, которые представлены на рис.4 в виде схемы. Создание базы данных всех информационных активов находящейся на балансе предприятия основывается на тщательном сборе данных, на предприятии со всех структурных подразделении (таблица 1) может основываться как на зарубежных методах, например CRAMM, FRAP, OCTAVE, RiskWatch, Microsoft и т.д., так и на отечественных экспертных методах. Независимо от применения того или иного метода или подхода, главное, чтобы была собрана достаточная информация для заполнения базы данных обо всех выявленных информационных активах.

Таблица 1. База данных всех информационных активов на балансе предприятия

№ п.п.	Наименование актива	Адрес размещения	Назначение объекта	Количество	Документация на актив
1					
…					
n					

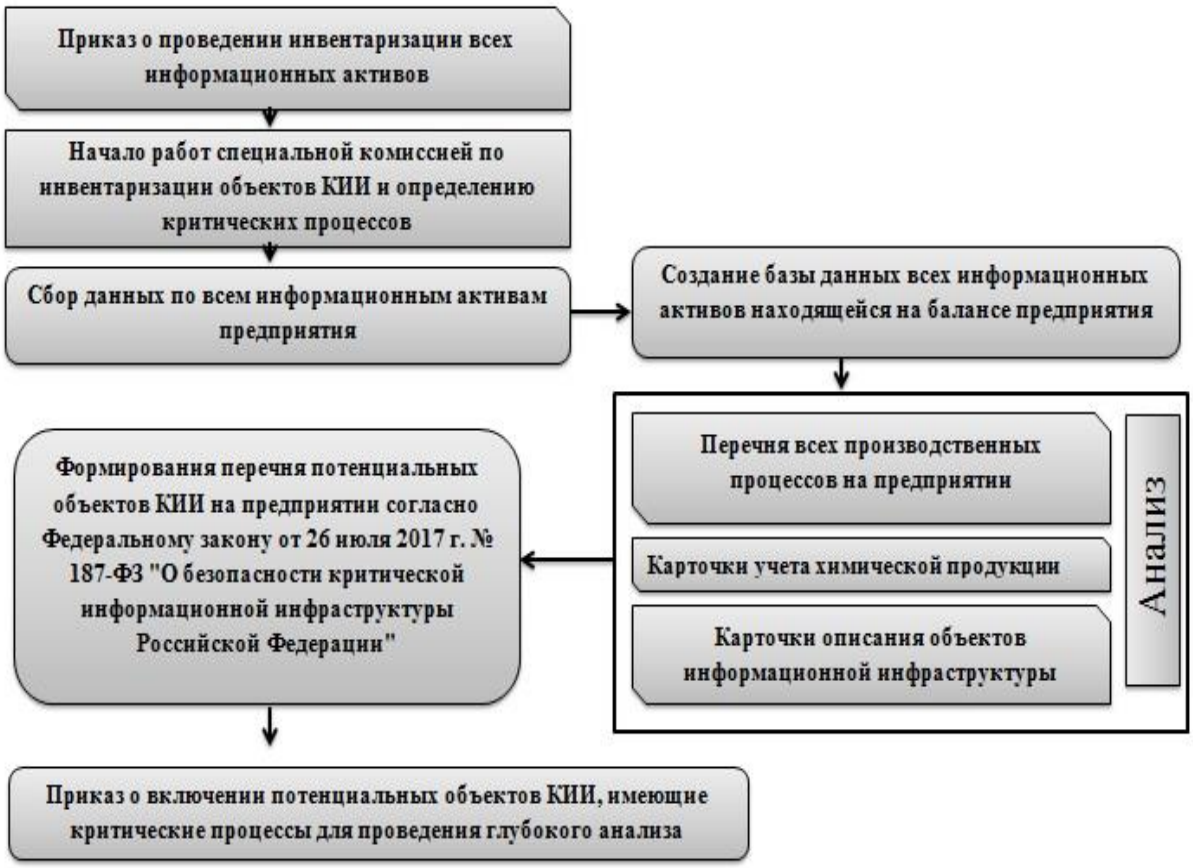


Рис. 4. Основные задачи специальной комиссии на подготовительном этапе
(Fig.4. The main tasks of the special commission at the preparatory stage)

После того, как специальной комиссией сформирована база данных всех информационных активов, далее формируется перечень потенциальный объектов КИИ на предприятии согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ[6]. Для того чтобы его сформировать необходимо, провести тщательный анализ всей технической документации, которая имеется на химическом предприятии, для того, чтобы разобраться какие объекты информационной инфраструктуры влияют или могут повлиять на технологические процессы [16]. Для этого необходимо:

1. Сформировать перечень всех производственных процессов на предприятии. Пример приведен в табл. 2.

Таблица 2. Перечень всех производственных процессов на предприятии

Критерии			**Описание**
Классификация химико-технологических процессов	Группа химических процессов		
	Тип процесса		
	Подтип процесса		
	По способу организации основные процессы		
Описание процесса	Вход (ресурсы преобразующейся в ходе процесса в выходы процесса)		
	Управление (условия выполнения процесса (документация, на основе которой осуществляется выполнение процесса)		
	Механизмы	Название оборудования	
		Серия и номер оборудования	
		Серия и номер лицензии	
		Количество	
		Наименование подразделения и № помещения	
		Ответственное лицо	
	Выход результаты (продукция)		

Результатом любого производственного процесса является выпуск определенной продукции. Однако здесь необходимо отметить, что в данном случае химическая продукция является очень специфичной. И поэтому для каждой химической продукции на предприятии необходимо создавать карточку учета (табл. 3).

Таблица 3. Карточка учета химической продукции на предприятии

№ п.п.	**Название химической продукции**	**Класс опасности [7]**	**Номер паспорта безопасности химической продукции**
1			
…			
n			

[6]Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // ФСТЭК России. Доступно на: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 10.02.2020).

[7]ГОСТ 12.1.007-76 Система стандартов безопасности труда (ССБТ). Вредные вещества. Классификация и общие требования безопасности (с Изменениями № 1,2) // Электронный фонд правовой и нормативно-технической документации. Доступно на: http://docs.cntd.ru/document/5200233 (дата обращения: 14.03.2020).

К карточке учета химической промышленности обязательно прикладывается приложение опасностей химической продукции согласно ГОСТ 32419-2013[8] «Классификация опасности химической продукции. Общие требования» информация представлена в табл. 4–6.

Таблица 4. Классификация химической продукции, опасность которой обусловлена ее физико-химическими свойствами

Критерии		**Описание**
Классификация опасности взрывчатой химической продукции	Классы опасности взрывчатой химической продукции	
Классификация опасности сжатых, сжиженных и растворенных под давлением газов	Классы опасности газов под давлением	
Классификация опасности воспламеняющихся газов, в том числе химически неустойчивых	Классы опасности воспламеняющихся газов	
	Дополнительные классы опасности для химически неустойчивых воспламеняющихся газов	
Классификация опасности химической продукции в аэрозольной упаковке	Классы опасности химической продукции в аэрозольной упаковке	
Классификация опасности химической продукции, представляющей собой воспламеняющуюся жидкость	Классы опасности химической продукции, представляющей собой воспламеняющуюся жидкость	
Классификация опасности химической продукции, представляющей собой воспламеняющееся твердое вещество	Классы опасности химической продукции, представляющей собой воспламеняющееся твердое вещество	
Классификация опасности саморазлагающейся химической продукции	Классы опасности саморазлагающейся химической продукции	
Классификация опасности пирофорной химической продукции	Классы опасности пирофорной химической продукции	
Классификация опасности самонагревающейся химической продукции	Классы опасности самонагревающейся химической продукции	
Классификация опасности химической продукции, выделяющей воспламеняющиеся газы при контакте с водой	Классы опасности химической продукции, выделяющей воспламеняющиеся газы при контакте с водой	
Классификация опасности окисляющей химической продукции	Классы опасности окисляющей химической продукции	
Классификация опасности органических пероксидов	Классы опасности органических пероксидов	
Классификация опасности химической продукции, вызывающей коррозию металлов	К химической продукции, вызывающей коррозию металлов, относится продукция, которая вызывает скорость коррозии стальной или алюминиевой поверхности > 6,25 мм в год при температуре 55 °С.	

[8]ГОСТ 32419-2013 Классификация опасности химической продукции. Общие требования // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200107879 (дата обращения: 14.03.2020).

Таблица 5. Классификация опасности химической продукции по воздействию на организм человека

Критерии (Классы опасности химической продукции)		**Описание**
Классификация опасности химической продукции, обладающей по воздействию на организм острой токсичностью	Обладающей острой токсичностью по воздействию на организм	
Классификация опасности химической продукции, вызывающей поражение (некроз)/раздражение кожи	Вызывающей поражение (некроз) / раздражение кожи	
	Вызывающей поражение (некроз)/раздражение кожи	
Классификация опасности химической продукции, вызывающей серьезные повреждения/раздражение глаз	Вызывающей серьезные повреждения / раздражение глаз	
	Вызывающей серьезное повреждение / раздражение глаз	
Классификация опасности химической продукции, обладающей сенсибилизирующим действием	Обладающей сенсибилизирующим действием	
Классификация опасности мутагенов	Классы опасности мутагенов	
Классификация опасности канцерогенов	Классы опасности канцерогенов	
Классификация опасности химической продукции, воздействующей на функцию воспроизводства	Классы опасности химической продукции, воздействующей на функцию воспроизводства	
Классификация опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при однократном воздействии	Классы опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при однократном воздействии	
Классификация опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при многократном / продолжительном воздействии	Классы опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при многократном/ продолжительном воздействии	
Классификация опасности химической продукции, представляющей опасность при аспирации	Классы опасности химической продукции, представляющей опасность при аспирации	

Таблица 6. Классификация опасности химической продукции по воздействию на окружающую среду

Критерии		**Описание**
Классификация опасности химической продукции, разрушающей озоновый слой		
Классификация опасности химической продукции, обладающей острой токсичностью для водной среды	Классы опасности химической продукции, обладающей острой токсичностью для водной среды	
Классификация опасности химической продукции, обладающей хронической токсичностью для водной среды	Классы опасности химической продукции, обладающей хронической токсичностью для водной среды	

Важно при проведении анализа понять, как устроена иерархия химико-технологических систем на химическом предприятии. Иерархия химического предприятия состоит из трех ступеней (рис. 5) [17].

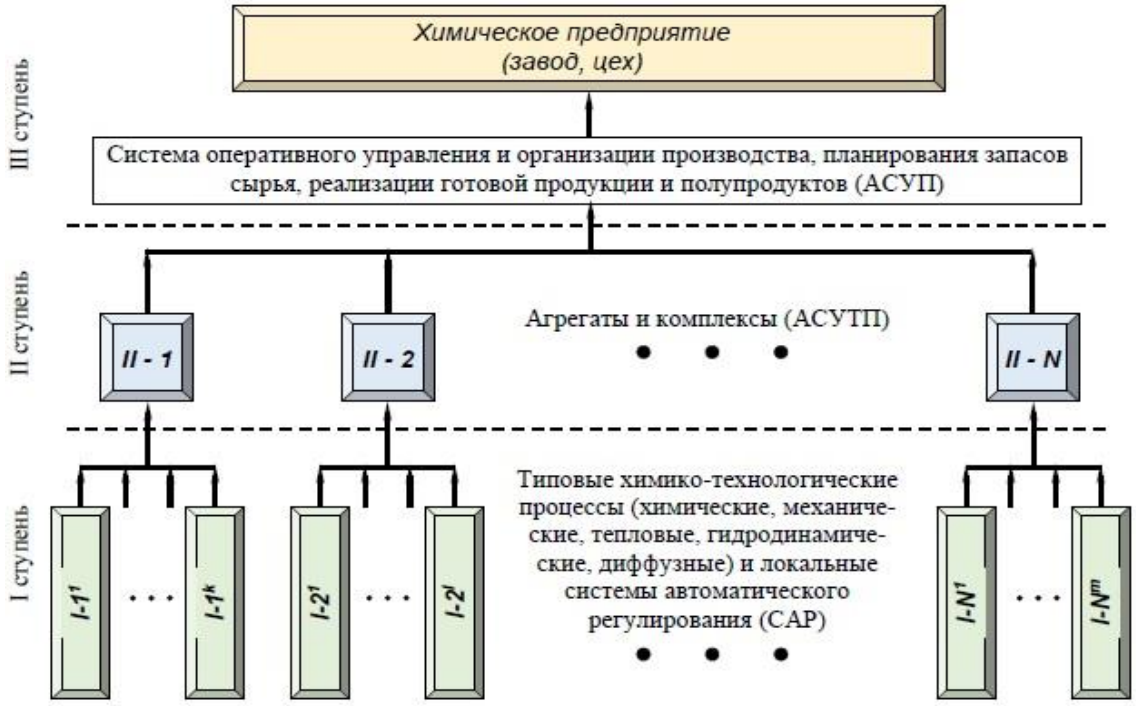


Рис. 5. Иерархия химического производства [17]
(Fig 5. Hierarchy of chemical production) [17]

На сегодняшний день цифровизация российских промышленных предприятий идет большими темпами, благодаря чему происходит положительное влияние на качественные [18] и количественные показатели деятельности [19], в том числе и химической отрасли [20].

2. Сформировать перечень потенциальный объектов КИИ согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (таблица 7).

Таблица 7. Перечень потенциальный объектов КИИ на предприятии

№ п.п.	Наименование объекта	Адрес размещения	Тип объекта	Вид права собственности	Количество	Номер карточки описания объекта

Для того чтобы заполнить вышеприведённую таблицу необходимо, чтобы каждый объект информационной инфраструктуры имел свою (заполненную) карточку описания (составлено на базе приказа № 236[9]) представленной в табл.8.

[9] Приказ от 22.12.2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (в ред. приказа ФСТЭК России от 21 марта 2019 г. № 59).

Таблица 8. Учетная карточка описание объекта информационной инфраструктуры

Критерии		**Описание**
Общие сведения по объекту	Наименование объекта	
	Производитель	
	Серия и номер лицензии	
	Год поставки объекта	
	Количество	
	Описание	
Сведения о взаимодействии объекта и сетей электросвязи	Категория сети электросвязи или сведения об отсутствии взаимодействия объекта с сетями электросвязи	
	Наименование оператора связи и (или) провайдера хостинга	
	Цель взаимодействия с сетью электросвязи	
	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия	
Сведения о силах обеспечения безопасности объекта	Структурное подразделение (работники) ответственные за обеспечение безопасности объекта	
	Структурное подразделения (работники), эксплуатирующие объект	
	Структурное подразделение (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) объекта	
Сведения о программных и программно-аппаратных средствах, используемых на объекте	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации - при наличии)	
	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются)	
	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки) или сведения об отсутствии средств защиты информации	
Организационные и технические меры, применяемые для обеспечения безопасности объекта	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	
Дополнительная информация по объекту	Документация на объект	
	Общая схема инфраструктуры производства на предприятии и архитектура объекта в этой схеме	

Также к вышеперечисленной таблице прилагается приложение, в котором прописаны технические данные, а именно системные и технические компоненты (табл. 9). Для каждого компонента заполнение таблицы происходит отдельно.

Таблица 9. Описание системных и технических компонентов объекта

<table>
<tr><th colspan="3">Критерии</th><th colspan="3">Описание компонентов (1,2,3..n)</th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th></tr>
<tr><td colspan="3">Название компонента</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Описание</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование объекта, с которым косвенно или прямо происходит взаимодействие</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование процесса или процессов, которые включены в системные / технические компоненты</td><td></td><td></td><td></td></tr>
<tr><td rowspan="6">Наименование процесса или процессов, которые включены в системные/ технические компоненты</td><td colspan="2">Наименование процесса и его схема</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Наименование подпроцесса и его схема</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Информация по программно-логические контроллеры (ПЛК)</td><td>Название</td><td></td><td></td><td></td></tr>
<tr><td>Серия и номер лицензии</td><td></td><td></td><td></td></tr>
<tr><td>Схема размещение</td><td></td><td></td><td></td></tr>
<tr><td>Перечень технической документации</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Перечень технической документации</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование производственного процесса, над которым установлены компоненты</td><td></td><td></td><td></td></tr>
</table>

Следует отметить, что после сбора всей исходной информации последующее проведение процедуры анализа должно строго контролироваться (со стороны комиссией по категорированию) так, как сформированные отчеты будут использованы на последующих этапах методики. В ряде после неправильного предоставления данных (специальной комиссией), предприятие рискует увеличить сроки реализации мероприятий по категорированию.

Неправильное определение (в организации) ЗОКИИ – это шанс попасть под санкции со стороны регулирующих органов исполнительной власти РФ [21]. Это особенно важно на фоне громких заявлений (в средствах массовой информации) о проведенных кибератаках [22] со стороны различных преступных группировок в информационном пространстве. Такая преступная активность способна приводить к нарушению работы ЗОКИИ (вызвать дестабилизацию социальной, политической, экономической и др. систем государства). Так, например, государственные органы в РФ сегодня отказываются от использования иностранного ПО и оборудования, отдавая предпочтение отечественным разработкам (ПО, средствам защиты информации и другие) [23].

Данная мера помогает государственным структурам и российским компаниям не только снизить уровень угроз КИИ, но и оказывает поддержку отечественному производителю в условиях острого экономического и политического кризиса [24].

Заключение

Решение субъектами информационной инфраструктуры задач выявления значимых объектов на основе определения критических процессов остается на сегодня одним из важных направлений работы по защите ЗОКИИ, а значит и обеспечения национальной безопасности Российской Федерации. Отсутствие методик определения критических процессов субъекты ИИ заставляет субъекты КИИ испытывать определенные трудности, возникающие в ходе категорировании своих объектов для последующей их эксплуатации.

Необходимо отдать должное, что ФЗ-187 и пакет связанных с ним нормативных документов, дали запуск процессу позитивных изменений в сфере обеспечения безопасности КИИ и позволили в Российской Федерации пройти за два года в этом направлении путь, который занимал в некоторых государствах десятилетия. Доклады руководителей государственных структур и субъектов КИИ (на форумах, конференциях, совещаниях и др.) конечно же, вносят свою неоценимую пользу, но тоже не решают эту проблему в полной мере.

В настоящей работе приведены этапы проведения работ необходимых при определении категорирования и некоторые их особенности, нашедшие применение в разрабатываемой авторами методике по определению критических процессов субъектов (химическая промышленность) информационной инфраструктуры, где в основу методики был положен опыт Национальной образовательной инициативы США в области кибербезопасности. Только проведение дальнейших исследований, а затем и применение комплексных инструментов для определения важнейших услуг информационной инфраструктуры; методов выявления взаимозависимостей отказов инфраструктурных служб; комплексный подход к оценке устойчивости критически важных элементов инфраструктуры; разработок оценки каскадированого воздействия на системы позволит качественно выполнять категорирование объектов информационной инфраструктуры и эксплуатацию значимых объектов КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Козырева А.А., Тарасов Д.А. Современное состояние государственной политики в сфере информационной безопасности. Вестник Воронежского института МВД России. 2018. № 4. С. 243–247. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-gosudarstvennoy-politiki-v-sfere-informatsionnoy-bezopasnosti (дата обращения: 12.12.2019).
2. Родачин В.М. Гибридные войны и обеспечение национальной безопасности России. Гуманитарные науки. Вестник Финансового университета. 2019. № 4. С. 93–99. DOI: https://doi.org/10.26794/2226-7867-2019-9-4-93-99.
3. Жернова В.М. Информационные системы как источник повышенной опасности в условиях цифровизации. Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19. № 3. С. 67–71. DOI: https://doi.org/10.14529/law190310.
4. Батьковский М. А., Кравчук П. В., Судаков В. А. Информационная система управления диверсификацией интегрированных структур оборонно-промышленного комплекса. Бюллетень науки и практики. 2020. Т. 6. № 1. С. 237–247. DOI: https://doi.org/10.33619/2414-2948/50/26.
5. Асалханова С.А. Формирование единого информационного пространства в цифровой экономике. Известия Санкт-Петербургского государственного экономического университета. 2020. № 1. С. 144–147. URL: https://cyberleninka.ru/article/n/formirovanie-edinogo-informatsionnogo-prostranstva-v-tsifrovoy-ekonomike (дата обращения: 27.03.2020).
6. Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz. Cyber security of critical infrastructures. ICT Express, Vol. 4, Issue 1, March. 2018. P. 42–45. DOI: https://doi.org/10.1016/j.icte.2018.02.001.
7. Грачков, Игнатий А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты. Безопасность информационных технологий, [S.l.], Т. 25, № 1. С. 90–98, mar. 2018. ISSN 2074-

7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1097/1091 (дата обращения: 28.03.2020). DOI: http://dx.doi.org/10.26583/bit.2018.1.09.

8. Отчет Kaspersky ICS-CERT. Kaspersky ICS-CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения: 27.03.2020).
9. Вавичкин, Александр Н. et al. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений. Безопасность информационных технологий, [S.l.], Т. 26, № 2. С. 44–57, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1198> (дата обращения: 28.03.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
10. Herrera, Luis-Carlos & Maennel, Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
11. Hannes Seppänen, Pekka Luokkala, Zhe Zhang, Paulus Torkki, Kirsi Virrantaus. Critical infrastructure vulnerability– A method for identifying the infrastructure service failure interdependencies. International Journal of Critical Infrastructure Protection. 2018. Vol. 22. P. 25–38. DOI: https://doi.org/10.1016/j.ijcip.2018.05.002.
12. Rehak, David & Senovsky, Pavel & Hromada, Martin & Lovecek, Tomas & Novotny, Petr. (2018). Cascading Impact Assessment in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection. Vol. 22. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2018.06.004.
13. David Rehak, Sciprofile linkPavel Šenovský, Martin Hromada, Tomas Lovecek. An integrated approach to assessing the stability of critical infrastructure elements. International Journal of Critical Infrastructure Protection, Vol. 25. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003.
14. Кулясова Е. В. Химическая промышленность России: Современное состояние и проблемы развития. Вестник университета. 2019. № 5. С. 93–100. DOI: https://doi.org/10.26425/1816-4277-2019-5-93-100.
15. Миннуллина К.А. Смирнова А.Е. Стрелков Е.С. Татаринова Е.П. Договор как стратегия минимизации инновационных рисков. Вестник Волжского университета им. В.Н. Татищева. 2019. № 2. С. 122–128. URL: https://cyberleninka.ru/article/n/dogovor-kak-strategiya-minimizatsii-innovatsionnyh-riskov (дата обращения: 28.03.2020).
16. Остроцкая С.В., Калуцкий И.В. К вопросу анализа угроз безопасности критическим информационным инфраструктурам // Материалы II Всероссийской научной конференции с международным участием. В 2 частях. 2019 Издательство: Издатель Качалин Александр Васильевич. - Курск: Информационные технологии в моделировании и управлении: подходы, методы, решения, 2019. С. 212–217. URL: https://www.elibrary.ru/item.asp?id=39542201 (дата обращения: 23.03.2020).
17. Калашников А.О, Сакрутина Е.А. Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры. Информация и безопасность. 2018. № 4. С. 466–471. URL: https://www.elibrary.ru/item.asp?id=36739588 (дата обращения: 28.03.2020).
18. Надеждина М.Е. Модель химико-технологических систем на принципах «Индустрии 4.0». Безопасность транспорта и сложных технических систем глазами молодежи. Материалы Всероссийской молодежной научно-практической конференции. Иркутск, 10-13 апреля 2018 г. - Иркутск: Иркутский государственный университет путей сообщения, 2018. С. 132–134. URL: https://www.elibrary.ru/item.asp?id=35307860 (дата обращения: 28.03.2020).
19. Кулясова Е.В., Вдовенко З.В. Цифровизация промышленных предприятий: возможности и угрозы новой реальности. Ученые записки российской академии предпринимательства. 2019. Том 18. № 3. С. 98–110. URL: https://www.elibrary.ru/item.asp?id=41311983 (дата обращения: 28.03.2020).
20. Кулясова Е.А, Вдовенко З.В. Перспективные инструменты цифровизации предприятий химического комплекса. Сборник методических рекомендаций по вопросам теоретических и практических разработок в области прикладных общественно-гуманитарных и технических наук. 2019. С. 128–133. URL: https://www.elibrary.ru/item.asp?id=38521969 (дата обращения: 28.03.2020).
21. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Психопедагогика в правоохранительных органах. 2018. № 2(73). С. 25–29. DOI: https://doi.org/10.24411/1999-6241-2018-12004.
22. Cyber Polygon Международный тренинг по борьбе с глобальными киберугрозами. Cyber Polygon. URL: https://cyberpolygon.com/upload/Cyber-Polygon-ru.pdf (дата обращения: 28.03.2020).

23. 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://cyberleninka.ru/article/n/o-vybore-sredstv-zaschity-informatsii-dlya-gosudarstvennyh-informatsionnyh-sistem (дата обращения: 28.03.2020).
24. Габричидзе Т.Г., Куделькин В.А., Зайцев А.М., Болтовский А.В., Лебедева Т.Г. Анализ систем управления базами данных, используемых на территории Российской Федерации. Известия Самарского научного центра Российской академии наук. 2016. №1. С. 5–12. URL: https://cyberleninka.ru/article/n/analiz-sistem-upravleniya-bazami-dannyh-ispolzuemyh-na-territorii-rossiyskoy-federatsii (дата обращения: 28.03.2020).

REFERENCES:

[1] Kozyrev A. A., Tarasov D. A. Modern state policies in the field of information security. Vestnik Voronezhskogo instituta MVD Rossii. 2018. No. 4. P. 243–247. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-gosudarstvennoy-politiki-v-sfere-informatsionnoy-bezopasnosti (accessed: 12.12.2019) (in Russian).
[2] Reducin V. M. Hybrid war and the national security of Russia. Gumanitarnye nauki. Vestnik finansovogo universitetam. 2019. No. 4. P. 93–99. DOI: https://doi.org/10.26794/2226-7867-2019-9-4-93-99 (in Russian).
[3] Zhernova V. M. Information systems as a source of increased danger in digitalization conditions. Bulletin of the South Ural State University. 68 Ser. Law. 2019. Vol. 19. No. 3. P. 67–71. DOI: https://doi.org/10.14529/law190310 (in Russian).
[4] Batkovskiy, M., Kravchuk, P., & Sudakov, V. (2019). Diversification Management Information System Integrated Structures of the Military-Industrial Complex. Bulletin of Science and Practice, 6(1). P. 237–247. DOI: https://doi.org/10.33619/2414-2948/50/26 (in Russian).
[5] Asalkhanova S. A. Formation of a single information space in the digital economy. Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta. 2020. No 1. P. 144–147. URL: https://cyberleninka.ru/article/n/formirovanie-edinogo-informatsionnogo-prostranstva-v-tsifrovoy-ekonomike. (accessed: 27.03.2020) (in Russian).
[6] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz. Cyber security of critical infrastructures. ICT Express, Vol. 4, Issue 1, March 2018. P. 42–45. DOI: https://doi.org/10.1016/j.icte.2018.02.001.
[7] Grachkov, Ignatiy A. Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.], v. 25, n. 1. P. 90–98, mar. 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1097> (accessed: 20.04.2020) DOI: http://dx.doi.org/10.26583/bit.2018.1.09.
[8] Kaspersky ICS-CERT report. Kaspersky ICS-CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (accessed: 27.03.2020).
[9] Vavichkin, Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.], v. 26, n. 2. P. 44–57, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1198> (accessed: 20.04.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
[10] Herrera, Luis-Carlos & Maennel, Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
[11] Hannes Seppänen, Pekka Luokkala, Zhe Zhang, Paulus Torkki, Kirsi Virrantaus. Critical infrastructure vulnerability—A method for identifying the infrastructure service failure interdependencies. International Journal of Critical Infrastructure Protection. 2018. Vol. 22. P. 25–38. DOI: https://doi.org/10.1016/j.ijcip.2018.05.002.
[12] Rehak, David & Senovsky, Pavel & Hromada, Martin & Lovecek, Tomas & Novotny, Petr. (2018). Cascading Impact Assessment in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection. Vol. 22. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2018.06.004.
[13] David Rehak, Sciprofile linkPavel Šenovský, Martin Hromada, Tomas Lovecek. An integrated approach to assessing the stability of critical infrastructure elements/ / International Journal of Critical Infrastructure Protection, Vol. 25. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003.
[14] Kulyasova E.V. Chemical industry of Russia: Current state and development problems. Bulletin of the University. 2019. No. 5. P. 93–100. DOI: https://doi.org/10.26425/1816-4277-2019-5-9-100 (in Russian).

[15] Minnullina K. A., Smirnova A. E., Strelkov E. S., Tatarinova E. P. Treaty as innovative risks minimization strategy. Vestnik Volzhskogo universiteta im. V.N. Tatishcheva. 2019. Vol. 2. P. 122–128. URL: https://cyberleninka.ru/article/n/dogovor-kak-strategiya-minimizatsii-innovatsionnyh-riskov (accessed: 28.03.2020) (in Russian).
[16] Ostrotskaya S. V., Kalutsky I. V. On the issue of analyzing security threats to critical information infrastructures. Materials of the II all-Russian scientific conference with international participation. In 2 parts. 2019 Publisher: Publisher Alexander Kachalin. - Kursk: Information technologies in modeling and management: approaches, methods, solutions, 2019. P. 212–217. URL: https://www.elibrary.ru/item.asp?id=39542201 (accessed: 28.03.2020) (in Russian).
[17] Kalashnikov A. O, Sakrutina E. A. Model of predicting risk potential of significant plants of critical information infrastructure. Informatsiya-i-bezopasnost. 2018. Vol. 4. P. 466–471. URL: https://www.elibrary.ru/item.asp?id=36739588 (accessed: 28.03.2020) (in Russian).
[18] Nadezhdina M.E. Model of chemical and technological systems based on the principles of "Industry 4.0". All-Russian youth scientific and practical conference. Irkutsk: Irkutsk state University of railway transport, 2018. P. 132–134. URL: https://www.elibrary.ru/item.asp?id=35307860 (accessed: 28.03.2020) (in Russian).
[19] Kulyasova E.V., Vdovenko Z.V. Digitalization of industrial enterprises: opportunities and threats of new reality. Uchenye zapiski rossijskoj akademii predprinimatel'stva. 2019. Vol. 18. No 3. P. 98–110. URL: https://www.elibrary.ru/item.asp?id=41311983 (accessed: 28.03.2020) (in Russian).
[20] Kulyasova E.A, Vdovenko Z.V. Promising directions of digitalization of chemical enterprises. Sbornik metodicheskih rekomendacij po voprosam teoreticheskih i prakticheskih razrabotok v oblasti prikladnyh obshchestvenno-gumanitarnyh i tekhnicheskih nauk. 2019. P. 128–133. URL: https://www.elibrary.ru/item.asp?id=38521969 (accessed: 28.03.2020) (in Russian).
[21] Novichkov V.E., Pykhtin I.G. Social and Legal Grounds providing Criminal Liability for Illegal Influence on Vital Informational Infrastructure of the Russian Federation. Psychopedagogy in Law Enforcement. No. 2(73). 2018. P. 25–29 DOI: https://doi.org/10.24411/1999-6241-2018-12004 (in Russian).
[22] Cyber Polygon international training to combat global cyber threats. Cyber Polygon. URL: https://cyberpolygon.com/upload/Cyber-Polygon-ru.pdf (accessed: 28.03.2020).
[23] 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. No. 10. P. 52–58. URL: https://cyberleninka.ru/article/n/o-vybore-sredstv-zaschity-informatsii-dlya-gosudarstvennyh-informatsionnyh-sistem (accessed: 02.12.2019) (in Russian).
[24] Gabrichidze T.G., Kudelkin V.A., Zaitsev A.M., Boltovskii A.V., Lebedeva T.G. Analysis of database management systems, used in the Russian Federation. Izvestiya Samarskogo nauchnogo centra Rossijskoj akademii nauk. 2016. No. 1. P. 5–12. URL: https://cyberleninka.ru/article/n/analiz-sistem-upravleniya-bazami-dannyh-ispolzuemyh-na-territorii-rossiyskoy-federatsii (accessed 02.12.2019) (in Russian).

Поступила в редакцию – 23 марта 2020 г. Окончательный вариант – 20 мая 2020 г.
Received – March 23, 2020. The final version – May 20, 2020.

Кристина В. Наташова[1], Сергей С. Соколов[2], Олег Н. Губернаторов[3],
Анатолий П. Ныркова[4], Антон В. Кириков[5]
[1-5]Государственный университет морского и речного флота имени адмирала С.О. Макарова, ул. Двинская, 5/7, Санкт-Петербург, 198035, Россия
[1]e-mail: natashov1397@mail.ru, https://orcid.org/0000-0003-4322-3223
[2]e-mail: sssokolov@mail.ru, https://orcid.org/0000-0002-4581-2518
[3]e-mail: ovel82@mail.ru, https://orcid.org/0000-0002-4581-2518
[4]e-mail: nyrkowap@gumrf.ru, https://orcid.org/0000-0002-9803-6284
[5]e-mail: tony-68@yandex.ru, https://orcid.org/0000-0002-2556-0915

К ВОПРОСУ О КАТЕГОРИРОВАНИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МОРСКИХ ПОРТОВ

DOI: http://dx.doi.org/10.26583/bit.2020.1.03

Аннотация. Целью статьи является рассмотрение проблемных вопросов, возникающих при проведении категорирования объектов критической информационной инфраструктуры (КИИ). Морские порты имеют стратегическое значение для развития экономики Российской Федерации и транспортного обеспечения внешней торговли. Морские порты в соответствии с Федеральным законом №187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» являются субъектами КИИ в сфере транспорта. Выполнение требований указанного закона, в частности решение вопросов по категорированию объектов КИИ в соответствии с Постановлением Правительства РФ от 8 февраля 2018 года № 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», требует тщательной проработки и оценки, по причине того, что субъекты КИИ все чаще сталкиваются с многогранностью процессов и необходимостью учета специфики той или иной сферы их деятельности. В данной статье рассмотрен субъект КИИ «Калининградский морской торговый порт» и проведено категорирование одной из информационных систем как авторские рекомендации по исполнению Постановления Правительства Российской Федерации №127 от 8 февраля 2018 года для информационных систем морских портов. В заключении авторы отмечают важность разработки отраслевых регламентов по категорированию и обеспечению защищенности КИИ, важность разработки типовых моделей нарушителей, которые бы учитывали отраслевые особенности, и необходимость привлечения к работе комиссии узконаправленных специалистов, как из состава организации, так и сторонних.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, категорирование, водный транспорт, морской порт.

Для цитирования: НАТАШОВА, Кристина В. et al. К ВОПРОСУ О КАТЕГОРИРОВАНИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МОРСКИХ ПОРТОВ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 35-46, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1269>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.03.

Kristina V. Natashova[1], Sergey S. Sokolov[2], Oleg N. Gubernatorov[3],
Anatoliy P. Nyrkov[4], Anton V. Kirikov[5]
[1–5]Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya Str., 5/7, St. Petersburg, 198035, Russia
[1]e-mail: natashov1397@mail.ru, https://orcid.org/0000-0003-4322-3223
[2]e-mail: sssokolov@mail.ru, https://orcid.org/0000-0002-4581-2518
[3]e-mail: ovel82@mail.ru, https://orcid.org/0000-0002-4581-2518
[4]e-mail: nyrkowap@gumrf.ru, https://orcid.org/0000-0002-9803-6284
[5]e-mail: tony-68@yandex.ru, https://orcid.org/0000-0002-2556-0915

On the issue of categorization of objects of critical information infrastructure of seaports

DOI: http://dx.doi.org/10.26583/bit.2020.1.03

Abstract. The purpose of the article is to consider the problematic issues that arise during the categorization of CII objects. Seaports are of strategic importance for the development of the Russian Federation's economy and transport support for foreign trade. In accordance with Federal law No. 187-FZ of July 26, 2017 "on security of critical information infrastructure of the Russian Federation", seaports are subjects of CII in the field of transport. Compliance with the requirements of this law, in particular, addressing issues related to the categorization of CII objects in accordance with Russian Government Resolution No. 127 of February 8, 2018 "on approval of the rules for categorizing critical information infrastructure objects of the Russian Federation, as well as the list of indicators of the criteria for the significance of critical information infrastructure objects of the Russian Federation and their values", requires careful study and evaluation, because, that CI subjects are increasingly faced with the complexity of processes and the need to take into account the specifics of a particular area of their activities.

This article considers the subject of the Kaliningrad commercial sea port CII and categorizes one of the information systems as the author's recommendations for the implementation of the Decree of the Government of the Russian Federation No. 127 of February 8, 2018 for information systems of seaports. In conclusion, the authors note the importance of developing industry regulations for categorizing and ensuring the security of CII, the importance of developing standard models of violators that would take into account industry characteristics, and the need to attract narrowly focused specialists to the work of the Commission, both from the organization and from outside.

Keywords: information security, critical information infrastructure, categorization, water transport, seaport.

For citation: NATASHOVA, Kristina V. et al. On the issue of categorization of objects of critical information infrastructure of seaports. IT Security (Russia), [S.l.], v. 27, n. 2, p. 35-46, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1269>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.03.

Введение

Сегодня морское портовое хозяйство почти невозможно представить без комплекса информационных систем и технологий, обеспечивающих его успешное функционирование. Процесс автоматизации информационных процессов водного транспорта продолжается, поэтому вопросы обеспечения информационной безопасности, как никогда актуальны [1].

Поскольку морской порт – это важный транспортный узел, обеспечивающий международные связи, необходимо организационно-правовое сопровождение решения вопросов по выполнению требований по обеспечению безопасности [2]. Одним из таких в части категорирования объектов КИИ, функционирующих в сфере транспорта является Приказ Министерства транспорта РФ от 14 декабря 2018 года № 449 «О создании Комиссии Министерства транспорта Российской Федерации по согласованию перечней объектов критической информационной инфраструктуры подведомственных Минтрансу России службы, агентств, предприятий, учреждений и организаций», изданный в рамках обеспечения реализации требований Федерального закона от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Морские порты имеют важное значение в международной торговле и экономике России. Согласно Федеральному закону №187-ФЗ информационные системы и сети, автоматизированные системы управления морского порта могут быть отнесены к объектам КИИ. В ходе реализации требований Федерального закона №187-ФЗ обозначился ряд проблемных вопросов, которые будут рассмотрены в данной статье.

1. Морской порт как субъект критической информационной инфраструктуры

Субъектами критической информационной инфраструктуры являются «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматизированные системы управления (АСУ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей». При этом различают два вида субъектов КИИ: владельцы объектов КИИ и организации, обеспечивающие взаимодействие объектов КИИ.

Для проведения категорирования решением руководителя субъекта КИИ создается постоянно действующая комиссия по категорированию.

При определении принадлежности организации к понятию «Субъект КИИ» следует оценивать не принадлежность ИС, ИТКС и АСУ к перечисленным сферам, а виды деятельности организации.

Основные и вспомогательные виды деятельности организации отражены в учредительных документах организации (Устав) и лицензиях, сертификатах, и иных разрешительных документах на эти виды деятельности [3].

Согласно Общероссийскому классификатору видов экономической деятельности (ОКВЭД) к сфере транспорта могут относиться виды деятельности под классами 49, 50, 51, 52, 53. Морским портам характерны виды деятельность классов:

49. Деятельность сухопутного и трубопроводного транспорта;
50. Деятельность водного транспорта;
52. Складское хозяйство и вспомогательная транспортная деятельность.

2. Категорирование объектов критической информационной инфраструктуры морского порта

Первым шагом категорирования объектов КИИ является создание постоянно действующей комиссии по категорированию приказом руководителя морского порта, в которую должны входить:

а) Руководитель морского порта;

б) Руководитель критичных направлений деятельности, процессы которых автоматизируются одной из систем;

в) Руководитель подразделения информационных технологий;

г) В случае наличия – руководитель автоматизации;

д) Ответственный за промышленную безопасность;

е) В случае наличия – ответственный за контроль за опасными веществами и материалами;

ж) Руководитель подразделения защиты информации либо администратор информационной безопасности;

з) В случае наличия – руководитель подразделения по защите государственной тайны;

и) В случае наличия – руководитель отдела по гражданской обороне и чрезвычайным ситуациям;

к) Иные работники по решению Руководителя морского порта;

л) По согласованию с Федеральным органом или юридическим лицом, который определяет политику, нормативно-правовое регулирование в установленной сфере деятельности, могут быть включены представители данного юридического лица. Если субъект осуществляет деятельность водного транспорта, то по согласованию с Министерством транспорта РФ и (или) Федеральным агентством морского и речного транспорта, их представители могут быть включены в комиссию субъекта.

Следующие действия выполняет сформированная комиссия по категорированию. У комиссии нет ограничений по привлечению других работников.

Второй шаг категорирования – формирование перечня критических процессов. Критическими процессами морского порта являются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности Субъекта КИИ в сфере транспорта.

Для определения критических процессов необходимо вновь обратиться к учредительным и разрешительным документам для выписки выполняемых организацией функций и видов деятельности [4]. Для каждой функции/вида деятельности формируется перечень процессов. После чего можно использовать перечень критериев значимости из Постановления Правительства РФ от 8 февраля 2018 года №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» для определения критичности процесса, т.е. повлечет ли нарушение процесса последствия, соответствующие этим критериям значимости.

Третьим шагом является определение объектов КИИ, обеспечивающих выполнение критических процессов, выделенных на предшествовавшем этапе. Для каждого критического процесса необходимо определить системы, осуществляющие обработку, управление, контроль или мониторинг этого процесса. Результатом данного шага является формирование перечня объектов КИИ, подлежащих категорированию, который согласовывается с Комиссией Министерства транспорта РФ [п. 15 Постановление Правительства РФ №127], после чего отправляется в ФСТЭК России согласно рекомендуемой форме [Информационное сообщение ФСТЭК России от 24.08.2018 №240/25/3752] в течение 10 дней со дня утверждения перечня [п. 15 Постановление Правительства РФ №127]. Согласно Постановлению Правительства РФ от 13 апреля 2019 года №452 «О внесении изменений в Постановление Правительства Российской Федерации от 8 февраля 2018 года №127» государственные органы и государственные учреждения были обязаны до 1 сентября 2019 года утвердить перечни объектов КИИ. Что касается российских юридических лиц данный срок несет рекомендательный характер. Со дня утверждения перечня объектов КИИ устанавливается максимальный срок не более 1 года со дня утверждения перечня для последующего категорирования этих объектов, т.е. не позднее 1 сентября 2020 года в случае соблюдения указанных выше сроков по представлению перечней объектов КИИ [п. 15 Постановление Правительства РФ №127].

На *четвертом шаге* осуществляется анализ уязвимостей и актуальных угроз безопасности. Для составления перечня уязвимостей исходными данными являются сведения о программном обеспечении, аппаратных платформах, операционных системах, используемых на рассматриваемых объектах.

Анализ угроз необходим для последующей оценки возможного ущерба при компьютерных инцидентах. Можно использовать уже существующие модели угроз безопасности информации, если они разрабатывались ранее для рассматриваемого объекта.

В отсутствии разработанных моделей угроз для получения исходных данных по угрозам безопасности информации рекомендуется использование банка данных угроз безопасности информации ФСТЭК России [4].

Данный этап включает в себя оценку возможного ущерба при возникновении компьютерного инцидента на объекте КИИ. Необходимо ориентироваться на последствия, которые соответствуют показателям значимости из Правил категорирования. В соответствии с оцененным ущербом присваивается категория значимости по данному показателю.

Пятый шаг – это присвоение категории значимости, которая является наивысшей из определенных на предшествовавшем шаге. Этот шаг оформляется актом категорирования, в котором перечислены сведения о самом объекте КИИ, присвоенной категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Акт подписывается комиссией и в течение 10 дней со дня его утверждения в ФСТЭК России представляются Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий по утвержденной форме в соответствии с Приказом ФСТЭК России № 236 от 22 декабря 2017 года.

3. Практический пример категорирования

В качестве примера субъекта КИИ рассмотрим Калининградский морской торговый порт (ОАО «КМТП»).

Основным видом деятельности ОАО «КМТП» по коду ОКВЭД является транспортная обработка грузов (код 52.24), что в соответствии с пунктом 8 статьи 2 Федерального закона № 187-ФЗ означает, что морской порт функционирует в сфере транспорта. Кроме данного способа определения принадлежности к субъектам КИИ можно обратиться к разрешительным и учредительным документам организации. Так в Уставе Калининградского морского порта в разделе 3 пункте 4 перечислены основные виды деятельности. Также стоит ответить на вопрос, есть ли у организации системы, автоматизирующие эти виды деятельности. Так, транспортно-экспедиторское обслуживание и складские операции автоматизированы системами управления грузовым и контейнерным терминалами [5]. Таким образом, можно принять решение о признании ОАО «КМТП» субъектом КИИ.

Первый шаг. Создается комиссия по категорированию.

Второй шаг. Для формирования перечня процессов Калининградского морского торгового порта выпишем основные виды деятельности:

а) Погрузо-разгрузочные работы (стивидорная деятельность);

б) Шипчандлерское обслуживание (снабжение) судов, прибывающих в порт;

в) Транспортно-экспедиторское обслуживание и складские операции;

г) Перевозки грузов, багажа, почты, на судах порта, а также другими видами транспорта;

д) Агентское обслуживание судов;

е) Перевозочная и транспортно-экспедиционная деятельность;

ж) Осуществление швартования морских судов в морских портах;

з) Учреждение склада временного хранения[1]. [6]

[1] Устав Акционерного Общества «Морской торговый порт»
URL: http://www.kscport.ru/index.php/ru/aktsioneram/ustav-oao-kmtp/

Далее для каждого осуществляемого вида деятельности сформируем перечень процессов, реализуемых в рамках этого вида деятельности для получения полного перечня процессов Калининградского морского торгового порта.

Для каждого процесса из перечня определим критичность его нарушения (табл. 1).

Таблица 1. Выделение критических процессов

№ п/п	Наименование	Негативные последствия				
		Социальная значимость	**Политическая значимость**	**Экономическая значимость**	**Экологическая значимость**	**Значимость для обеспечения обороны страны, безопасности государства и правопорядка**
1.	Бухгалтерский и налоговый учет	-	-	-	-	-
2.	Кадровый учет и расчет заработной платы	-	-	-	-	-
3.	Оперативный учет с планированием поставок, отгрузок и внутрипортовых операций	+	-	+	-	-
4.	Планирование и учет погрузочно-разгрузочных работ	+	-	+	-	-
5.	Подготовка и оформление документации на размещение и отгрузку груза	+	-	+	-	-
6.	Получение информации по переработанным грузам и контейнерам	-	-	-	-	-
7.	Получение отчетов	-	-	-	-	-
8.	Погрузка и выгрузка судов	+	-	+	-	-

№ п/п	Наименование	Негативные последствия				
		Социальная значимость	**Политическая значимость**	**Экономическая значимость**	**Экологическая значимость**	**Значимость для обеспечения обороны страны, безопасности государства и правопорядка**
9.	Тарификация и биллинг услуг	+	-	+	-	-
10.	Учет и адресное хранение грузов	-	-	-	-	-
11.	Учет и адресное хранение контейнеров	-	-	-	-	-
12.	Электронный обмен с клиентами	-	-	-	-	-

Таким образом, критическими процессами порта являются:

- Оперативный учет с планированием поставок, отгрузок и внутрипортовых операций;
- Планирование и учет погрузочно-разгрузочных работ;
- Подготовка и оформление документации на размещение и отгрузку груза;
- Погрузка и выгрузка судов;
- Тарификация и биллинг услуг.

Третий шаг. Для определения объектов КИИ необходимо провести инвентаризацию информационных, программных и технических ресурсов [7] и отобрать те, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов:

1. Информационные системы:
   1.1. Береговые информационные системы;
   1.2. Бортовые информационные системы;
   1.3. Электрокартографические системы;
   1.4. Портовые технологические системы.
2. Информационно-телекоммуникационные сети;
3. Автоматизированные системы управления[2].

Для обеспечения критических процессов необходимую информацию обрабатывает: автоматизированная система управления грузовым терминалом ОАО «Калининградский морской торговый порт» (АСУ ГТ КМТП). На основе этих данных формируется перечень объектов КИИ [8].

Четвертый шаг. Рассмотрим возможные действия нарушителей и угрозы безопасности информации в отношении АСУ ГТ КМТП [5] (Табл. 2).

[2] Отчёты// ОАО «КМТП» URL: http://www.scport.ru/index.php/ru/aktsioneram/otchety

Таблица 2. Возможные действия нарушителей и угрозы безопасности информации

1.	Категория нарушителя, краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	1. Внешний нарушитель со средним потенциалом, обладающий следующими возможностями: − Информация о системе из общедоступных источников; − Общедоступная информация об уязвимостях отдельных компонент ИС. Данный тип нарушителя может использовать следующие каналы реализации угроз: − Общедоступные каналы передачи данных, имеющие подключение к ИС; − Реализация атак посредством направленных воздействий на работников организации (социальная инженерия). 2. Внутренний нарушитель со средним потенциалом, обладающий следующими возможностями: − Осведомленность о мерах защиты информации, применяемых в ИС; − Осведомленность о структурно-функциональных характеристиках и особенностях функционирования ИС Данный тип нарушителя может использовать следующие каналы реализации угроз: − Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический); − Использование штатных средств доступа к ИС.
2.	Основные угрозы безопасности информации или обоснование их неактуальности	− Угроза внедрения вредоносного ПО; − Угроза несанкционированного доступа с использованием компрометированных/подобранных данных идентификации и аутентификации пользователей и администраторов; − Угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); [9] − Угроза доступа к информации в обход или с использованием ошибок в настройке средств разграничения доступа; − Угроза несанкционированного удаления данных, обрабатываемых в системе; − Угроза нарушения работоспособности системного ПО; − Угроза нарушения работоспособности прикладного ПО; − Угроза проведения атак типа «отказ в обслуживании» на каналы связи; [10] − Угроза проведения атак типа «отказ в обслуживании» на компоненты системы; − Угроза использования недекларированных возможностей/закладок прикладного ПО; − Угроза использования недекларированных возможностей/закладок системного ПО; − Угроза несанкционированного доступа к конфигурации системы/раскрытия данных технологического процесса; − Угроза создания нештатных режимов работы; − Угроза блокирования передаваемых управляющих команд; − Угроза несанкционированного удаления конфигурационных файлов.

Пятый шаг. На основании показателей критериев значимости осуществим категорирование объекта КИИ (табл. 3).

Таблица 3. Категорирование объекта КИИ

1.	Категория значимости объекта	III категория
2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Далее номер – это порядковый номер Показателя. **1.** ***Показатель к объекту КИИ не применим*****;** **2.** ***Показатель к объекту КИИ не применим*****;** **3.** ***а) в пределах одной внутригородской территории города федерального значения. Данное значение дает основу для присвоения III категории объекту по данному показателю. б) показатель к объекту КИИ не применим;*** **4-7.** ***Показатель к объекту КИИ не применим*****;** **8.** ***0,06% от годового объема доходов, усредненного за прошедший 5-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** **9.** ***0,00000006% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** **10.** ***Показатель к объекту КИИ не применим*****;** **11.** ***а) в пределах одной внутригородской территории города федерального значения. Данное значение дает основу для присвоения III категории объекту по данному показателю. б) до 300 чел. Значения недостаточно для присвоения категории по данному показателю;*** **12-14.** ***Показатель к объекту КИИ не применим*** **[11]**
3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	1. ***Объект КИИ не управляет процессами, связанными с причинением ущерба жизни и здоровью людей.*** 2. ***Нарушение функционирования объекта КИИ не оказывает влияние на нарушение функционирования объектов обеспечения жизнедеятельности населения, так как объект КИИ не участвует в каких-либо процессах обеспечения жизнедеятельности населения.*** 3. ***а) В пределах одной внутригородской территории города федерального значения; б) Нарушение функционирования объекта КИИ не оказывает влияние на недоступность предоставление транспортных услуг пассажирам.*** 4. ***Объект КИИ не обеспечивает функционирование сетей электросвязи.*** 5. ***Объект КИИ единолично не обеспечивает доступ к государственной услуге.*** 6. ***Объект КИИ не обеспечивает функционирование государственных органов*** 7. ***Объект КИИ не обеспечивает соблюдение условий международного договора, заключенного Российской Федерацией с иностранным государством либо с международной организацией.*** 8. ***0,06% от годового объема доходов, усредненного за прошедший 5-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** 9. ***0,00000006% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период.***

		Данного значения недостаточно для присвоения категории по данному показателю; 10. ***Объект КИИ не обеспечивает поведение банковских операций.*** 11. ***а) В пределах одной внутригородской территории города федерального значения; б) вредным воздействиям в случае нарушения функционирования могут подвержены до 300 человек. Данного значения недостаточно для присвоения категории.*** *12.* ***Нарушение функционирования объекта не может привести к прекращению или нарушению функционирования пункта управления (ситуационного центра), так как объект не участвует в управлении или мониторинге процессов пунктов управления (ситуационных центров).*** *13.* ***Нарушение функционирования объекта не может привести к снижению показателей государственного оборонного заказа, так как объект не з в процессах реализации, управления или контроля данных процессов.*** *14.* ***Нарушение функционирования объекта не может привести к прекращению или нарушению функционирования информационной системе в области обеспечения обороны страны, безопасности государства и правопорядка, так как объект не задействован в процессах реализации, управления и контроля данных процессов.***

Для расчета показателей экономической значимости объектов КИИ (8 и 9 показатель) необходимо участие специалистов финансово-экономического отдела, поскольку у комиссии по категорированию могут возникнуть трудности в связи с недостатком сведений и профессиональной специфики вопроса.

Заключение

В данной статье были рассмотрены проблемные вопросы, возникающие при проведении категорирования объектов КИИ. Новое законодательство определило новые меры и средства обеспечения защищенности наиболее важных объектов. Однако, при категорировании, субъекты все чаще сталкиваются с многогранностью процессов и необходимостью учета специфики транспортной отрасли. Субъекты КИИ в ходе категорирования сталкиваются с необходимостью привлечения специалистов, не входящих в комиссию по категорированию как внутри Организации (как расчет 8 и 9 экономического показателя), так и сторонних (услуги аутсорсинга по обеспечению защиты значимых объектов КИИ: как категорирование, так и проектирование систем защиты). Категорирование КИИ – это лишь первый этап. Далее следует проектирование подсистемы безопасности значимого объекта и разработка рабочей документации на значимый объект.

В соответствии с законодательством, ответственность за результаты категорирования объектов КИИ несет непосредственно субъект КИИ. Это определяет важность разработки отраслевых регламентов по категорированию и обеспечению защищенности КИИ, важность разработки типовых моделей нарушителей, которые бы учитывали, например, такие отраслевые особенности как трансграничное взаимодействие с иностранными контрагентами. Обеспечение информационной безопасности – это процесс и его нельзя завершать, им необходимо централизованно управлять на всех уровнях, начиная с создания федеральных центров отраслевых компетенций в области информационной защищенности ключевых активов. Это ставит новые задачи и определяет перспективы развития направления обеспечения безопасности КИИ, в том числе на водном транспорте.

СПИСОК ЛИТЕРАТУРЫ:

1. Sokolov, S., Glebov, N., Natashova, K., Gubernatorov, O. Categorization of objects of critical information infrastructure of water transport // E3S Web of Conferences Volume 110, 9 August 2019. DOI: 10.1051/e3sconf/201911002003.
2. Соколов С.С., Ныркoв А.П, Глебов Н.Б. Кибербезопасность на водном транспорте// Сборник тезисов докладов. Национальная научно-практическая конференция профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ ИМЕНИ АДМИРАЛА С.О. МАКАРОВА». 2018.
3. Соколов С.С. Методы и модели обеспечения информационной безопасности объектов транспортной инфраструктуры, отнесенных к критически важным для национальной безопасности РФ объектам // Современные проблемы науки и образования. 2015. № 1-1. URL: http://science-education.ru/ru/article/view?id=18583 (дата обращения: 23.10.2020).
4. Ныркoв А.П., Кислов Р.И., Белов А.В. К вопросу о категорировании объектов критической информационной инфраструктуры водного транспорта. // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. \ СПОИСУ. – СПб, 2018. – 631 с. ISBN 978–5–907050–44–0.
5. Банк данных угроз безопасности информации//ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» URL: https://bdu.fstec.ru (дата обращения: 16.10.2019).
6. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. The Safety Assessment of Critical Infrastructure Control System// Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018. DOI: 10.1109/ITMQIS.2018.8524948.
7. Ли И.В., Наташова К.В., Проблемы обеспечения информационной безопасности автоматизированных систем на водном транспорте. //Сборник трудов «Региональная информатика и информационная безопасность», Выпуск 5 / СПОИСУ. – СПб., 2018. – 549 с.
8. Ли И.В., Наташова К.В., Нормативно-правовое регулирование информационной безопасности на водном транспорте.// Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. \ СПОИСУ. – СПб, 2018. – 631 с. ISBN 978–5–907050–44–0.
9. Наташова К.В., Ли И.В., Современное состояние ИТС и ИТ на водном транспорте.//Материалы IX межвузовской научно-практической конференции аспирантов, студентов и курсантов «Современные тенденции и перспективы развития водного транспорта России» 23 мая 2018 года. – СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова, 2018. – 928 с.
10. Glebov N., Zhilenkov A., Chernyi S., Sokolov S., "Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis", Procedia Computer Science. Vol. 150. P. 609–615 (2019).
11. Наташова К.В., Об основных темах для обсуждения и итогах 11-й межссесионной встречи регионального форума АСЕАН по безопасности на море.// Современные тенденции и перспективы развития водного транспорта России: материалы X межвузовской научно-практической конференции аспирантов, студентов и курсантов. 22 мая 2019 года. – СПб.: Изд-во ГУМРФ им. адм. С. О. Макарова, 2019. – 777 с.

REFERENCES:

[1] Sokolov, S., Glebov, N., Natashova, K., Gubernatorov, O. Categorization of objects of critical information infrastructure of water transport. E3S Web of Conferences Volume 110, 9 August 2019. DOI: 10.1051/e3sconf/201911002003.
[2] S.S. Sokolov, A.P. Nyrkov, N.B. Glebov. Cybersecurity on water transport. CONFERENCE ABSTRACTS. National scientific and practical conference of teaching staff Admiral Makarov State University of Maritime and Inland Shipping. 2018.
[3] Data Bank of threats to information security of FSTEC of Russia. URL: https://bdu.fstec.ru (accessed: 16.10.2019) (in Russian).
[4] S.S. Sokolov. Methods and models for ensuring information security of transport infrastructure objects classified as critically important for the national security of the Russian Federation. Modern problems of science and education. 2015. No. 1 (part 1).
[5] A.P. Nyrkov, R.I. Kislov, A.V. Belov. On the issue of categorization of objects of critical information infrastructure of water transport. Proceedings of the XVI St. Petersburg International Conference “Regional Informatics (RI-2018).
[6] Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. The Safety Assessment of Critical Infrastructure Control System. Proceedings of the 2018 International Conference "Quality Management, Transport and

Information Security, Information Technologies", IT and QM and IS 2018. DOI: 10.1109/ITMQIS.2018.8524948.

[7] Li I.V., Natashova K.V. Problems of ensuring information security of automated systems for water transport. Regional Informatics and Information Security. Proceedings. Vol. 5. SPOISU. SPb., 2018. – 549 p.

[8] Li I.V., Natashova K.V. Legal regulation of information security in marine transport. Proceedings of the XVI St. Petersburg International Conference “Regional Informatics (RI-2018). SPOISU. SPb., 2018. – 631 p.

[9] Natashova K.V., Li I.V. Current status of its and it on water transport. Materials of the IX interuniversity scientific and practical conference of postgraduates, students and cadets “Current trends and prospects for the development of water transport in Russia” May 23, 2018. – 928 p.

[10] Glebov N., Zhilenkov A., Chernyi S., Sokolov S., "Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis", Procedia Computer Science, vol. 150. P. 609–615 (2019).

[11] Natashova K.V., On the main topics for discussion and the results of the 11th inter-session meeting of the ASEAN regional forum on Maritime security. Materials of the XI interuniversity scientific and practical conference of postgraduates, students and cadets “Current trends and prospects for the development of water transport in Russia” May 22, 2019.

Поступила в редакцию – 18 января 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – January 18, 2020. The final version – May 25, 2020.

Дмитрий А. Мельников[1], Юрий Ф. Релеев[2], Леонид Д. Кварацхелия[3]
[1]Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, Москва, 119333, Россия
[2,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]e-mail: r3le@yandex.ru, https://orcid.org/0000-0001-9352-541X
[3]e-mail: kvarleon1997@gmail.ru, https://orcid.org/0000-0002-9199-3903

МОДЕЛЬ ДОВЕРИЯ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Аннотация. В статье представлено исследование современных моделей доверия на основе инфраструктуры открытых криптографических ключей (*Public Key Infrastructure* – PKI), целью которого является разработка российской национальной модели доверия. Для достижения поставленной цели была обоснована необходимость создания национальной инфраструктуры доверия в условиях перехода к цифровой экономике. Вместе с тем, в работе проведён анализ текущего состояния российской PKI, которое характеризуется отсутствием единой структуры удостоверяющих центров (УЦ) и единого федерального органа регулирования в области обеспечения криптографическими ключами (сертификатами открытых ключей). Анализ зарубежных PKI-моделей доверия позволил сделать вывод о том, что ни одна из таких моделей не может быть эталонной, и не может быть реализована в Российской Федерации. Основу предлагаемой модели составляет концепция распределённой системы центров подтверждения подлинности, которая имеет иерархическую структуру и позволит объединить все государственные и частные УЦ в единую динамическую систему, способную удовлетворить самые разнообразные потребности цифровой экономики и граждан Российской Федерации по обеспечению информационной безопасности. Реализация разработанной авторами модели доверия позволит, в первую очередь, предотвратить многие киберпреступления и попытки нанесения финансово-экономического ущерба субъектам информационного взаимодействия.

Ключевые слова: инфраструктура открытых ключей, доверие, целостность, неотказуемость, удостоверяющий центр, центр подтверждения подлинности, сертификат открытого ключа, электронная подпись.

Для цитирования: МЕЛЬНИКОВ, Дмитрий А.; РЕЛЕЕВ, Юрий Ф.; КВАРАЦХЕЛИЯ, Леонид Д. МОДЕЛЬ ДОВЕРИЯ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 47-64, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1270>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.04.

Dmitry A. Melnikov[1], Yury F. Releev[2], Leonid D. Kvaratskheliya[3]
[1]Federal Research Center "Computer Science and Control" of Russian Academy of Sciences,
Vavilov Str., 44/2, Moscow, 119333, Russia
[2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]e-mail: r3le@yandex.ru, https://orcid.org/0000-0001-9352-541X
[3]e-mail: kvarleon1997@gmail.ru, https://orcid.org/0000-0002-9199-3903

Trust Model for the Russian Federation Digital Economy

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Abstract. The paper presents a study of modern trust models based on the Public Key Infrastructure (PKI) infrastructure, the purpose of which is to develop a Russian national trust model. To meet this goal, the necessity of creating a national infrastructure of trust in the transition to a digital economy was

substantiated. At the same time, the analysis of the current state of the Russian PKI, which is characterized by the absence of a unified structure of the certification authorities (CA) and a unified federal regulatory authority in the field of cryptographic key management (public key certificates), is carried out. An analysis of foreign PKI models of trust allowed us to conclude that none of these models can be used as reference and implemented in the Russian Federation. The basis of the proposed model is the concept of a distributed system of the validation authorities, which has a hierarchical structure and will allow combining all public and private CAs into a single dynamic system that can meet the most diverse needs of the digital economy and citizens of the Russian Federation to manage information security. The implementation of the trust model developed by the authors will allow, first of all, preventing many cybercrimes and attempts to cause financial and economic damage on the subjects of information interaction.

Keywords: public key infrastructure, trust, integrity, nonrepudiation, certificate authority, validation authority, public key certificate, digital signature.

For citation: MELNIKOV, Dmitry A.; RELEEV, Yury F.; KVARATSKHELIYA, Leonid D. Trust Model for the Russian Federation Digital Economy. IT Security (Russia), [S.l.], v. 27, n. 2, p. 47-64, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1270>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.04.

Введение

В современных информационно-технологических системах (ИТС) самого широкого спектра назначения для обеспечения конфиденциальности, целостности, неотказуемости и установления авторства используются методы, способы и средства криптографической защиты информации. Наиболее характерным примером такого использования является электронная (цифровая) подпись (ЭП/ЭЦП) [1]. Применение ЭП позволяет проверить отсутствие искажения информации (целостность) принадлежность подписи владельцу сертификата ключа подписи (авторство), и в случае успешной проверки проверить факт подписания электронного документа (неотказуемость). При этом, в отличие от обычных рукописных подписей, её невозможно подделать, не получив закрытый ключ автора подписи.

Задача распределения и обмена ключами между участниками защищённого взаимодействия в рамках ИТС решается на основе асимметричных криптографических систем. Однако, при использовании таких криптосистем существует проблема, которая заключается в доверии к тому или иному открытому ключу. Что «мешает» злоумышленнику сформировать собственную пару ключей и выдавать себя за другого владельца? Решение этой проблемы выходит за рамки теоретической криптографии и относится к сфере организации системы обеспечения криптоключами, в частности, созданию инфраструктуры PKI [1–3]. Идея состоит в том, что есть третья сторона, которой доверяют взаимодействующие стороны. Доверенная третья сторона (ДТС) осуществляет привязку (*binding*) открытых ключей к уникальным идентификаторам (или параметрам подлинности (ПРП), *identity*) физических и юридических лиц (организаций). Привязка осуществляется путём регистрации клиентов (формирование их цифрового образа, т.е. ПРП) и выдачи им сертификатов ($СЕРТ_{ОК}$) удостоверяющим центром (УЦ, *certification authority* – CA), в которых параметр подлинности криптографически связан (с помощью ЭП УЦ) с открытым ключом. В дальнейшем при взаимодействии принадлежность открытого ключа конкретному клиенту может быть проверена в УЦ ДТС. В Российской Федерации УЦ выполняют все перечисленные задачи – регистрацию, выдачу $СЕРТ_{ОК}$ и их проверку [3].

Тем не менее, даже после внедрения PKI, проблема доверия остается нерешённой [4]. В общем случае неизвестно, насколько доверенными можно считать УЦ и субъекты, имеющие их $СЕРТ_{ОК}$. Каждый УЦ должен иметь политику сертификации, в которой

отражается порядок выдачи $СЕРТ_{ОК}$ и процедуры проверки физических и юридических лиц, получающих $СЕРТ_{ОК}$. Однако, с точки зрения неквалифицированного в соответствующей предметной области пользователя, проверка политики сертификации на её полноту и корректность является проблематичной. Ещё сложнее проверка того, что УЦ действительно реализует свою политику и является надёжным. В работе описывается способ решения данных проблем – формирование структуры доверия на основе PKI. В первом разделе обосновывается необходимость такой структуры. Во втором разделе приводятся обзор зарубежного опыта и анализ существующих моделей доверия на основе PKI. В третьем разделе обосновывается выбор и приводится описание предлагаемой национальной структуры модели доверия для цифровой экономики Российской Федерации.

1. Обоснование необходимости национальной инфраструктуры доверия

1.2 Определение доверия

Ключевым фактором обеспечения ИБ при взаимодействии субъектов (людей, организаций, ИТС) является доверие – взаимосвязь между двумя сторонами, называемыми доверяющей стороной (доверитель) и доверенной стороной (доверяемый). Доверитель проводит оценку и принимает решение о доверии, основываясь на личном опыте и полученной информации, то есть он является в некотором смысле «мыслящим» субъектом. Доверяемая же сторона может быть физическим лицом и организацией, а также, например, информацией, криптографическим ключом.

У доверительной связи есть своя «область действия», обозначающая цель её применения. Например, «быть доверенным» относительно предоставляемых услуг и товаров, или же «быть подлинным» пользователем ИТС. Так как существует множество различных определений термина «доверие», не всегда понятно, что подразумевается под ним в том или ином контексте. В силу этого, всегда необходимо уточнять и определять значение термина в конкретной ИТС.

1.3 Доверие в PKI

Как доверие к оценке, так и доверие к принятому решению означают положительную убеждённость в чём-либо, от чего (в перспективе или на текущий момент) зависит благосостояние доверителя. Доверие к оценке наиболее естественно измеряется как дискретный или непрерывный уровень надёжности (убеждённости), тогда как доверие к принятому решению лучше представить в виде выбора между двумя вариантами. Одним из возможных решений проблемы доверия в PKI является отражение рассчитанного каким-либо образом уровня доверия в $СЕРТ_{ОК}$ [3]. Однако, реализация такого подхода на практике весьма проблематична – пользователи неохотно будут приобретать $СЕРТ_{ОК}$ с низким уровнем доверия.

УЦ выдают $СЕРТ_{ОК}$ в соответствии с политикой сертификации, описывающей требования к получателям, и детальное описание процедур проверки получателей. Доверяющая сторона должна оценивать достаточность этих требований и проверок. Также, доверяющая сторона должна быть убеждена в том, что УЦ действительно следует этой политике. Даже подлинный $СЕРТ_{ОК}$ не может дать полную гарантию того, что открытый ключ является подлинным – злоумышленник может каким-либо образом заставить УЦ выпустить $СЕРТ_{ОК}$ с поддельным именем. С этой угрозой связано множество компьютерных инцидентов и атак [5].

В масштабах Российской Федерации проблема доверия в инфраструктуре PKI существенно усложняется. Так, согласно перечню аккредитованных УЦ Министерства

связи и массовых телекоммуникаций, по состоянию на 19.12.2019 аккредитованы 502 УЦ[1]. На сегодняшний день злоумышленники активно пользуются несовершенством (а точнее, отсутствием) национальной структуры доверия к PKI. Возникло несколько прецедентов неправомерного использования УЦ электронных подписей застрахованных лиц и оформления документов без участия гражданина[2]. Например, таким образом была осуществлена незаконная продажа квартиры без участия собственника[3]. Ряд УЦ предлагают услугу дистанционного выпуска $СЕРТ_{ОК}$ без личного контакта заявителя и центра регистрации (ЦР). Фактически, это облегчает задачу злоумышленников по получению поддельного $СЕРТ_{ОК}$, что может трактоваться как нарушение действующего законодательства[4]. Для предотвращения возникновения подобных проблем и развития цифровой экономики в России необходимо формирование структуры национальной структуры доверия PKI.

2. Анализ существующих моделей доверия на основе PKI

2.1 Издание сертификатов и подтверждении подлинности

$СЕРТ_{ОК}$ показывает степень доверия между УЦ и владельцем открытого ключа. Зачастую, эта степень отражает лишь то, что владелец открытого ключа правомочно владеет уникальным именем, указанным в $СЕРТ_{ОК}$. Помимо этого, в $СЕРТ_{ОК}$ может быть указана и другая информация.

Доверие к параметрам, указанным в $СЕРТ_{ОК}$, формируется доверяющей стороной из доверия к УЦ. Связанная таким образом последовательность $СЕРТ_{ОК}$ называется *цепочкой доверия*. А совокупность взаимосвязанных $СЕРТ_{ОК}$ называется *сетью доверия*. Формально, любую сеть доверия, основанную на $СЕРТ_{ОК}$ можно назвать PKI, однако на практике используются лишь определённые модели.

Структура доверия при создании $СЕРТ_{ОК}$ представлена на рис. 1. При этом подразумевается, что ЦР является составной частью УЦ.

В нижней части рисунка отражены процедуры формирования доверия. Доверительная связь, отмеченная индексом 1, показывает, что корневой УЦ безусловно и полностью доверяет подлинности своей собственной пары открытого и закрытого ключей. Необходимо отметить, что подлинность корневого открытого ключа невозможно подтвердить соответствующим $СЕРТ_{ОК}$, так как эта проверка выполняется тем же самым ключом (если бы ключ сам мог подтверждать свою подлинность, то в инфраструктуре не было бы смысла). Таким образом, доверие к корневой ключевой паре следует из внешних по отношению к PKI-инфраструктуре источников. Индекс 2 указывает на формирование самоподписанного $СЕРТ_{ОК}$. Индексы 3–6 отражают формирование прямого доверия привязке ключей путём выпуска $СЕРТ_{ОК}$ промежуточного УЦ и пользователя. При этом

[1]Перечень аккредитованных удостоверяющих центров (по состоянию на 19.12.2019) сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, URL: https://digital.gov.ru/ru/activity/govservices/certification_authority/ (дата обращения: 22.12.2019).

[2]Счётная палата Российской Федерации Бюллетень Счетной палаты №12 (декабрь) 2017 г. Пресс-центр счетной палаты Российской Федерации, URL: http://audit.gov.ru/activities/bulleten/bulletin-of-the-accounting-chamber-12-2017.php (дата обращения: 15.12.2019).

[3]Аракелян Е., Хожателова Ю. Новый вид мошенничества: Оставили без квартиры, подделав электронную подпись. 2019 // Комсомольская правда, URL: https://www.kp.ru/daily/26979/4038526/ (дата обращения: 15.12.2019).

[4]Письмо Министерства связи и массовых коммуникаций РФ от 9 октября 2017 г. № П15-1-200-24056 «О разъяснении некоторых положений Федерального закона «Об электронной подписи».

УЦ выпускают СЕРТ$_{ОК}$ согласно своим политикам сертификации, и этим подтверждают подлинность соответствующих привязок.

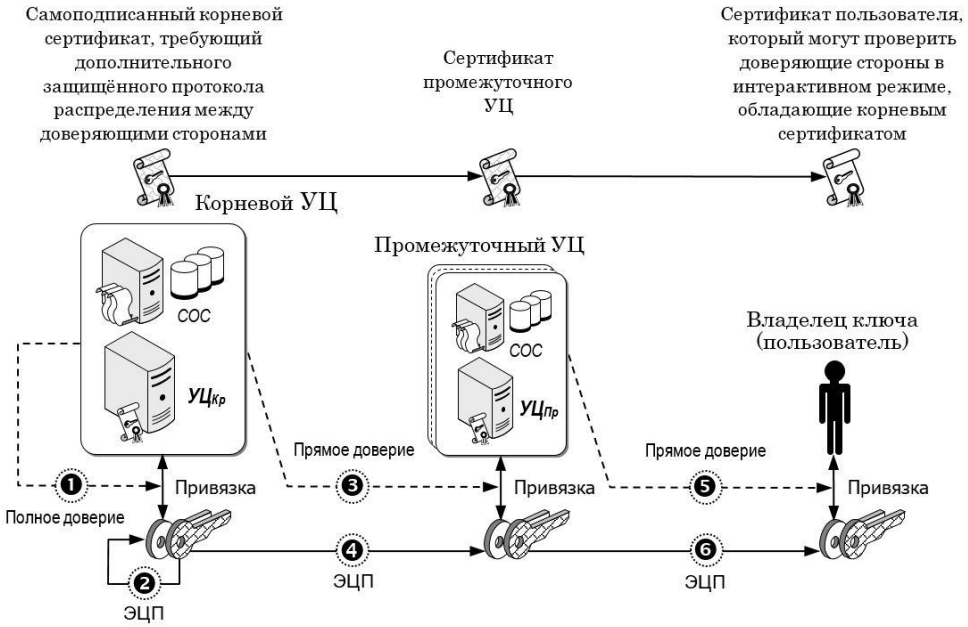


Рис. 1. Структура доверия при создании СЕРТ$_{ОК}$ (СОС[5] – список отозванных СЕРТ$_{ОК}$)
(Fig. 1. The trust structure for a issuing certificates (CRL – certificate revocation list))

На рис. 2 приведена структура доверия при подтверждении подлинности (ПП) СЕРТ$_{ОК}$. Если доверяющая сторона имеет прямое доверие (индекс 1) к корневому УЦ, то с помощью его СЕРТ$_{ОК}$ она может сформировать косвенное доверие (индекс 4) к открытому ключу контрагента. Способы формирования доверительных взаимосвязей определяются соответствующими политиками сертификации УЦ. Процедура проверки подлинности, как правило, осуществляется путём проверки электронной подписи: СЕРТ$_{ОК}$ пользователя подписан ключом промежуточного УЦ, а его СЕРТ$_{ОК}$, в свою очередь, подписан ключом корневого УЦ, к которому доверяющая сторона имеет прямое доверие.

2.2 Одиночная иерархическая PKI

Это – наиболее часто встречающийся вид PKI. В данном случае все пользователи доверяют одному корневому УЦ, которому подчиняются остальные нижестоящие УЦ (рис. 3). Преимущество такой структуры заключается в том, что необходимо распространить между доверяющими сторонами лишь один открытый ключ корневого УЦ по стороннему защищенному каналу связи. Имея этот открытый ключ, и СЕРТ$_{ОК}$ всех промежуточных УЦ, доверяющая сторона может проверить конкретную цепочку доверия от СЕРТ$_{ОК}$ пользователя к СЕРТ$_{ОК}$ УЦ, и сформировать косвенное доверие к открытому ключу пользователя.

Корневой УЦ должен быть доверенным в представлении общепризнанной организации, компетентность которой в вопросах регистрации пользователей и проверке открытых ключей подтверждается, например, аккредитацией.

[5]RFC 5280. IETF, May 2008; RFC 6818. IETF, January 2013.

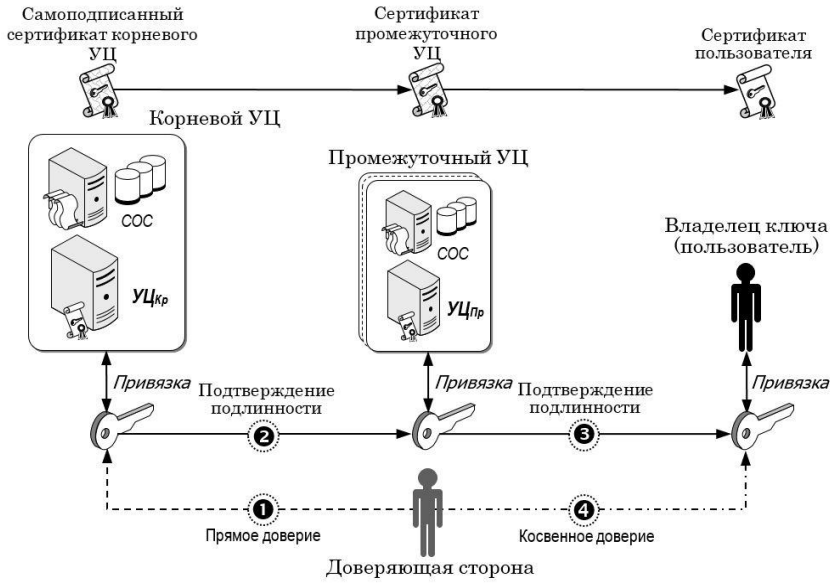


Рис. 2. Структура доверия при подтверждении подлинности СЕРТ$_{ОК}$
(Fig. 2. The trust structure for a validating the certificates)

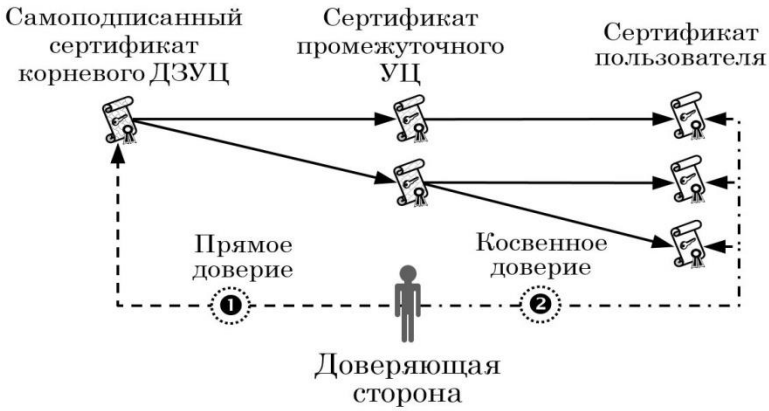


Рис. 3. Структура доверия в одиночной иерархической PKI
(Fig. 3. The trust structure in a single hierarchic PKI)

2.3 Многоиерархическая PKI

Отличием многоиерархической инфраструктуры является то, что СЕРТ$_{ОК}$ пользователей могут принадлежать к различным PKI-иерархиям. Для того чтобы доверяющая сторона могла сформировать доверие к СЕРТ$_{ОК}$ пользователя из любой иерархии, все корневые УЦ должны быть доверенными «замыкающими» (*anchor*) УЦ (ДЗУЦ), как показано на рисунке 4. У доверяющей стороны должно быть прямое доверие к ним.

При такой структуре доверия пропорционально возрастает нагрузка на проверяющую сторону, которая должна получить все СЕРТ$_{ОК}$ корневых УЦ по дополнительным защищённым каналом связи. Это – следствие того, что данная структура плохо масштабируется. Проблема усугубляется ещё и тем, что множество СЕРТ$_{ОК}$ корневых УЦ постоянно изменяется.

Одной из реализаций такой модели можно считать инфраструктуру, реализованную в современных Web-обозревателях. В ней СЕРТ$_{ОК}$ корневых УЦ встраиваются в комплекс программного обеспечения (КПО) Web-клиента и регулярно обновляются. Такое

встраивание СЕРТ$_{ОК}$ позволяет осуществлять автоматическое подтверждение подлинности открытых ключей, используемых для информационного взаимодействия с помощью TLS-протокола (*Transport Layer Security* [7]), и проверки ЭП прикладных КПО.

У такой модели есть и серьёзные уязвимости. Защищённость PKI Web-обозревателей определяется защищённостью наиболее уязвимой отдельной PKI, входящей в её состав. Защищённость последней определяется наиболее уязвимым УЦ такой инфраструктуры. Следовательно, чем больше корневых СЕРТ$_{ОК}$ и промежуточных УЦ, тем менее защищённой становится вся инфраструктура Web-обозревателей. Существует множество способов злонамеренного выпуска фальшивых СЕРТ$_{ОК}$ [8,9]:

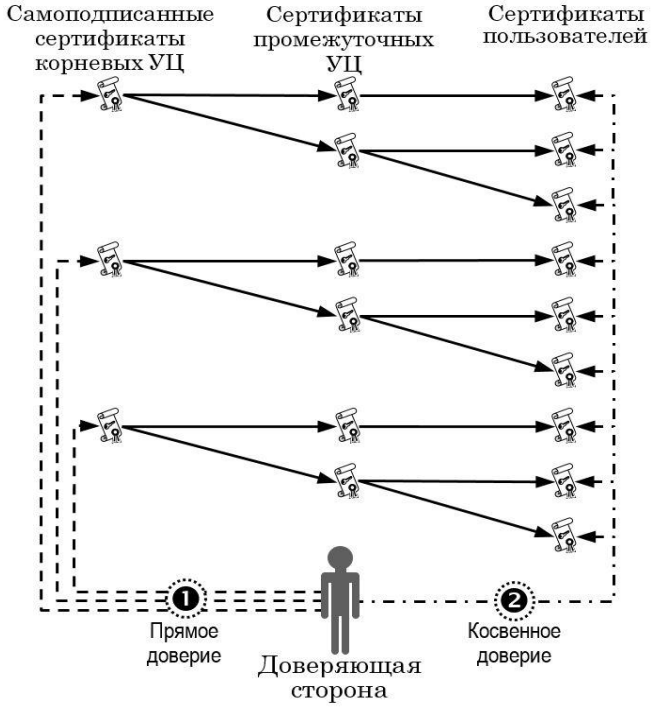


Рис. 4. Структура доверия в многоиерархической PKI
(Fig. 4. The trust structure in a multiple hierarchic PKI)

1. **Атака на УЦ**. В результате таких атак злоумышленники создают ложные СЕРТ$_{ОК}$ известных компаний и используют их для обмана пользователей, перехвата и анализа трафика. Реализации таких атак различны: от внедрения и работы вредоносного КПО в ИТС самих УЦ, до обмана с помощью фальшивых документов в ходе проверки ПРП при регистрации транзакций.

2. **Давление, шантаж УЦ**. Существует высокая вероятность того, что некоторые тайваньские компании-разработчики КПО (Realtek и JMicron) под давлением использовали свои подлинные СЕРТ$_{ОК}$ для подписи вредоносного КПО Win32/Stuxnet [10]. Эти подписи позволили внедрить вредоносный КПО в промышленных ИТС ряда предприятий атомной отрасли Ирана.

3. **Нелегальные УЦ**. С технической точки зрения, любой УЦ в рамках Web-PKI способен сформировать фиктивные СЕРТ$_{ОК}$ и ЭП. Нелегальные УЦ или недобросовестные сотрудники легальных УЦ могут получить большую выгоду, выпуская фальшивые СЕРТ$_{ОК}$, так как подобные СЕРТ$_{ОК}$ будут автоматически признаваться всеми известными операционными системами.

Многие люди произвольно запрашивают выпуск для них различных СЕРТ$_{ОК}$, причём на основе самостоятельных случайных решений, то есть имеет место быть избираемое прямое доверие (рис. 5).

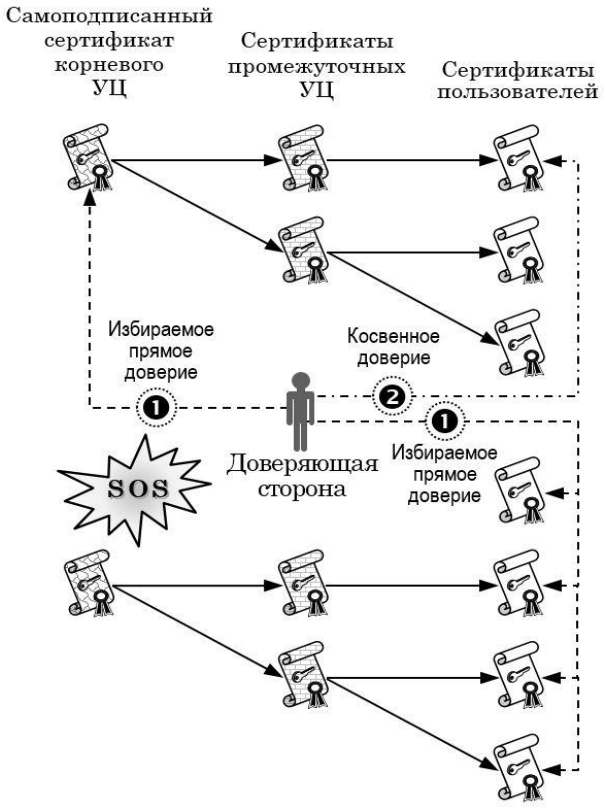


Рис. 5. Структура избираемого прямого доверия
(Fig. 5. The discretionary direct trust structure)

В таком случае игнорируется не только требование наличия защищенных дополнительных каналов получения СЕРТ$_{ОК}$ корневых УЦ, но и надёжность корневого УЦ как ДЗУЦ [11]. Данная модель применима в ситуациях с небольшими рисками в некритичных прикладных ИТС. Например, возникают случаи, когда подлинность СЕРТ$_{ОК}$ не может быть подтверждена в силу того, что отсутствует корневой СЕРТ$_{ОК}$, или же, когда невозможно соблюсти политику ПП в силу того, что срок действия с СЕРТ$_{ОК}$ корневого УЦ истёк. Однако, таким же образом принимаются решения, когда возможен реальный ущерб, например, при установке прикладных КПО. В таких случаях нельзя исходить из одного лишь удобства и низкой стоимости.

Необходимо отметить, что подобная проблема может быть присуща всем моделям доверия PKI, ведь доверяющая сторона из соображений удобства зачастую просто игнорирует факт существования корневых СЕРТ$_{ОК}$. И даже если доверяющая сторона знает о них, она далеко не всегда обладает достаточными компетенциями и информацией необходимой для принятия решения о доверии таким СЕРТ$_{ОК}$.

2.4 Взаимная сертификация нескольких корневых УЦ

Для того чтобы снизить нагрузку на доверяющие стороны можно позволить корневым УЦ осуществлять взаимную (обоюдную) сертификацию (*cross certification*). В такой структуре доверия для подтверждения подлинности доверяющей стороне

необходим всего лишь один СЕРТ$_{ОК}$ любого из корневых УЦ. На рис.6 показано, как доверяющая сторона формирует доверие к открытым ключам пользователей множества PKI-иерархий с взаимно сертифицированными корневыми УЦ.

Недостатком такой модели является увеличение нагрузки на сами корневые УЦ, так как каждый из них должен провести процедуру сертификации со всеми другими корневыми УЦ такой иерархии. В соответствии с теоремой Эйлера (лемма «о рукопожатиях») [12], необходимое число всех таких процедур составляет:

$$\frac{n*(n-1)}{2}, \quad (1)$$

где n – число отдельных корневых УЦ.

Для каждой такой процедуры необходимо согласие корневых УЦ и изменения и дополнение их политики, поэтому данная модель плохо масштабируется и применяется лишь в очень ограниченных случаях.

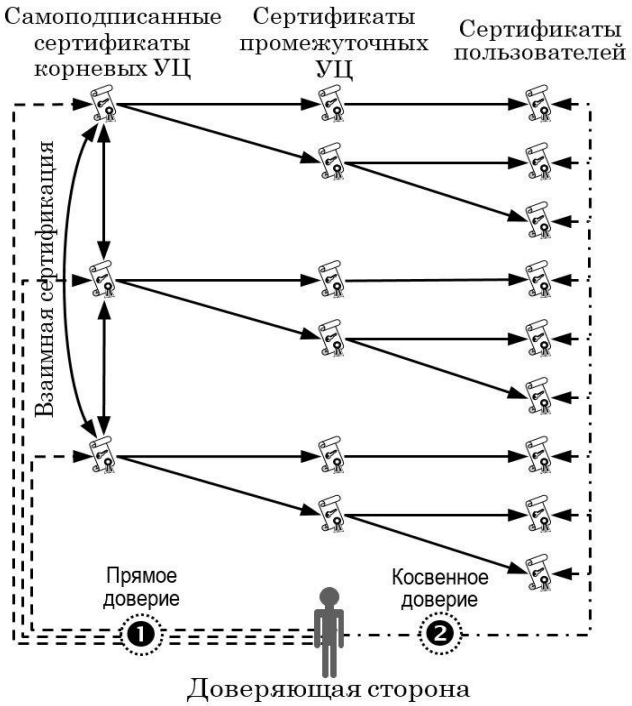


Рис. 6. Структура доверия при взаимной сертификации
(Fig. 6. The cross-certification trust structure)

2.5 Использование связующего УЦ

В качестве улучшения предыдущей модели можно использовать связующий (*bridge*) УЦ между множеством корневых УЦ (рис. 7). Преимущества такого решения в том, что доверяющим сторонам необходимо получить лишь один корневой СЕРТ$_{ОК}$ по дополнительному защищённому каналу, и что каждому корневому УЦ необходима взаимная сертификация лишь с одним связующим УЦ.

Как и в предыдущем случае, недостатком является необходимость согласия всех сторон на взаимную сертификацию со связующим УЦ, и наоборот, согласие связующего УЦ на сертификацию со всеми корневыми УЦ.

2.6 PKI-инфраструктура с центром подтверждения подлинности

С точки зрения доверяющей стороны наиболее проблематичными задачами являются безопасное получение $СЕРТ_{ОК}$ корневого УЦ по дополнительным каналам и ПП $СЕРТ_{ОК}$ пользователей. Возможно выделение этих функций и включение в модель нового участника, берущего на себя такие обязательства, ещё одного «якоря» доверия (ДЗУЦ) – центра ПП (ЦПП, *validation authority* – VA). Такая модель доверия приведена на рис. 8.

При этом ЦПП не обязательно должен выполнять функции УЦ – одна организация может представлять либо функции УЦ, либо ЦПП, либо выполнять обе функции одновременно. Для такой ПП необходимо защищённое соединение между доверяющей стороной и ЦПП, а для этого, в свою очередь, необходим безопасный обмен криптографическими ключами по дополнительному каналу. Процедуры сертификации и ПП отдельны друг от друга, поэтому защищённый канал необязательно должен основываться на асимметричной криптографии.

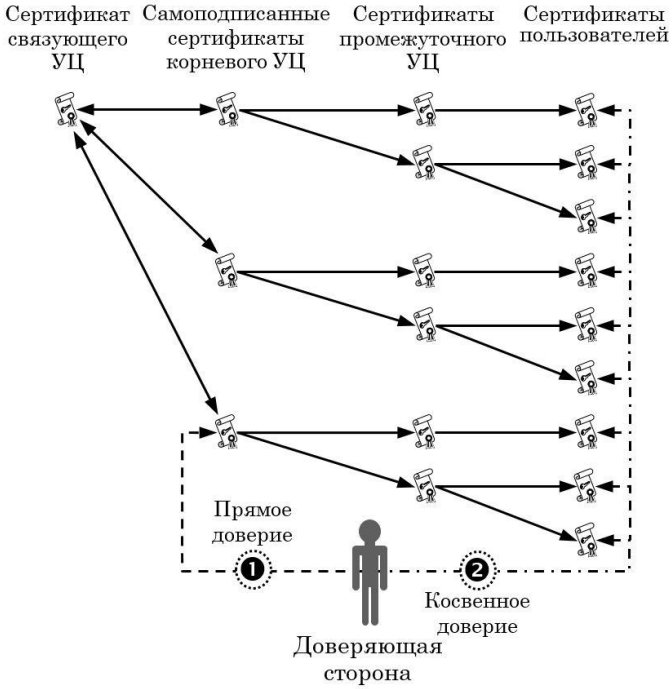


Рис. 7. Структура доверия на основе связующего УЦ
(Fig. 7. The bridge certification authority trust structure)

В такой модели существуют два важных аспекта ИБ: доверяющая сторона должна иметь возможность аутентифицировать ЦПП, чтобы доверять процедуре ПП $СЕРТ_{ОК}$. И напротив, ЦПП может аутентифицировать доверяющую сторону для предоставления ей доступа к процедуре ПП.

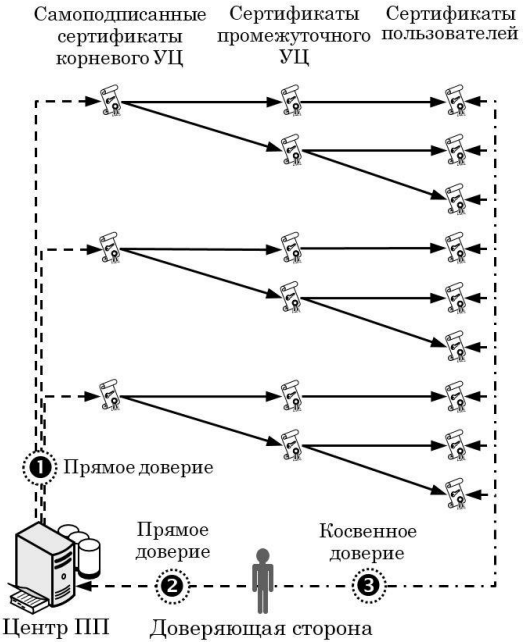


Рис. 8. Структура доверия на основе многоиерархической PKI с ЦПП
(Fig. 8. The validation authority trust structure)

Модель с ЦПП снимает нагрузку с доверяющих сторон и отражает одну из главных тенденций в PKI-технологии [13]. Так как ЦПП независимы от УЦ, то с помощью них возможно соединение множества независимых PKI-инфраструктур.

3. Обоснование выбора и разработка национальной структуры модели доверия

3.1 Зарубежный опыт формирования национальных структур моделей доверия

США

Развитие национальной PKI в США было обусловлено принятием двух важнейших законодательных актов:

1. HIPAA[6] – закон о мобильности и подотчётности в здравоохранении принятый в 1996 году, требовавший в том числе создания национальных стандартов для электронного документооборота в здравоохранении и общих идентификаторов для поставщиков, медицинского страхования, и работодателей;

2. GPEA[7] – закон о прекращении бумажного документооборота в правительстве, принятый в 1998 году. Закон требовал, чтобы за 5 лет система предоставления информации (услуг) гражданам федеральными органами и службами, а также все процедуры были переведены в электронный формат. Также закон устанавливал юридический статус ЭП, и обязывал ведомства внедрить процедуры электронной аутентификации.

[6]The Health Insurance Portability and Accountability Act of 1996. HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996.
[7]The Government Paperwork Elimination Act. GPEA, Pub. L. 105-277, Approved October 21, 1998.

Структура модели доверия федеральной PKI (FPKI) включает в себя федеральный связующий УЦ (ФСУЦ). Основной его задачей является создание цепочки доверия как между федеральными ведомствами, объединяя их в одну государственную сеть доверия, так и создание связи с негосударственной сетью доверия [14, 15]. Очевидно, что как УЦ федеральных ведомств, так и частные УЦ должны удовлетворять определенным требованиям для того, чтобы провести взаимную сертификацию с ФСУЦ (рис. 9)[8].

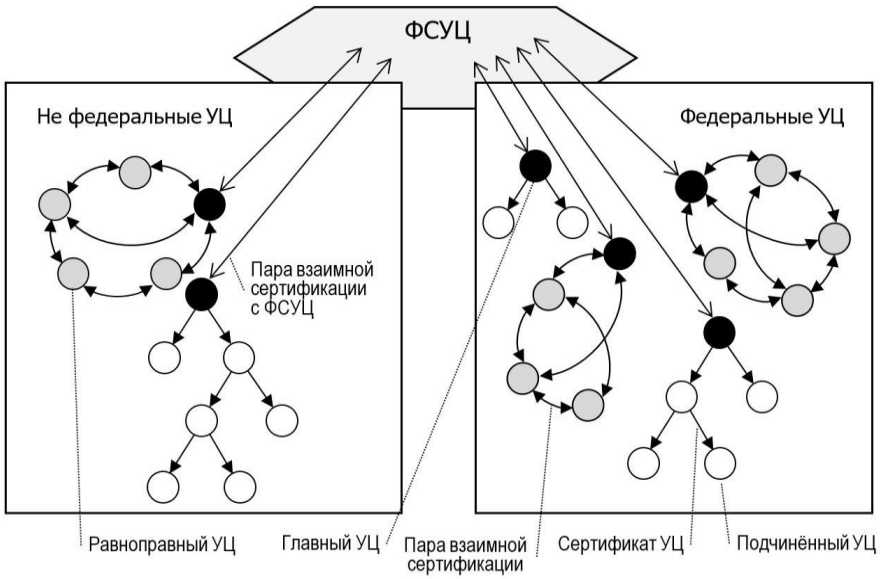


Рис. 9. Взаимодействие между федеральной и частной PKI в США
(Fig. 9. Interoperation between federal and non-federal PKIs)

Необходимо отметить, что ФСУЦ не является корневым для всех остальных, он не выпускает $СЕРТ_{ОК}$ и не является ДТС, а выступает лишь в качестве «моста доверия» между различными сетями доверия.

Европейский союз (ЕС)

В Европейском союзе развитие PKI связано с директивой 1999/93/ЕС «Об использовании электронных подписей в электронных контрактах в рамках Евросоюза»[9]. Важным отличием от модели США является то, что в ЕС существует множество языков государственного уровня. Это потребовало введения новых элементов в инфраструктуру – национальных ЦПП и реестра состояния доверенных служб (РСДС)[10].

Сложностью в создании такой инфраструктуры является то, что прикладные ИТС, которые обрабатывают ЭП, должны устанавливать взаимосвязь с каждым УЦ на территории ЕС, а их насчитывается несколько сотен. В связи с этим такие системы должны обеспечивать:

1. подтверждение подлинности $СЕРТ_{ОК}$ напрямую с выдавшим его УЦ (когда он известен);

[8]National Institute of Standards and Technology. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST Special Publication 800-32, 26 February 2001.
[9]Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[10]IDABC. Study on European Federated Validation Service (EFVS): Analysis and Assessment. Common Solution Model. Contract № 1, Framework contract ENTR/05/58-SECURITY, Specific contract № 14. September 2009.

2. поиск адреса ЦПП который может обработать СЕРТ$_{ОК}$, который выдан УЦ, обозначенном в СЕРТ$_{ОК}$;

3. отправка запроса в известный ЦПП, выполняющий функцию перенаправления. Этот ЦПП получит адрес целевого ЦПП и отправит запрос ему. Перенаправляющим ЦПП может быть, как коммерческий, так и государственный ЦПП на уровне отдельной страны или всего Евросоюза.

Эти требования привели к следующей модели системы обслуживания СЕРТ$_{ОК}$ (рис. 10). Данная структура основывается на использовании национальных ЦПП. В первом случае система передает запросы в ЦПП напрямую (модели 3 и 4), во втором случае (модель 1) запросы передаются на Web-сервер, который связывается с ЦПП. В последнем случае всё происходит через инфраструктуру ЭП для соединения с ЦПП (модель 2).

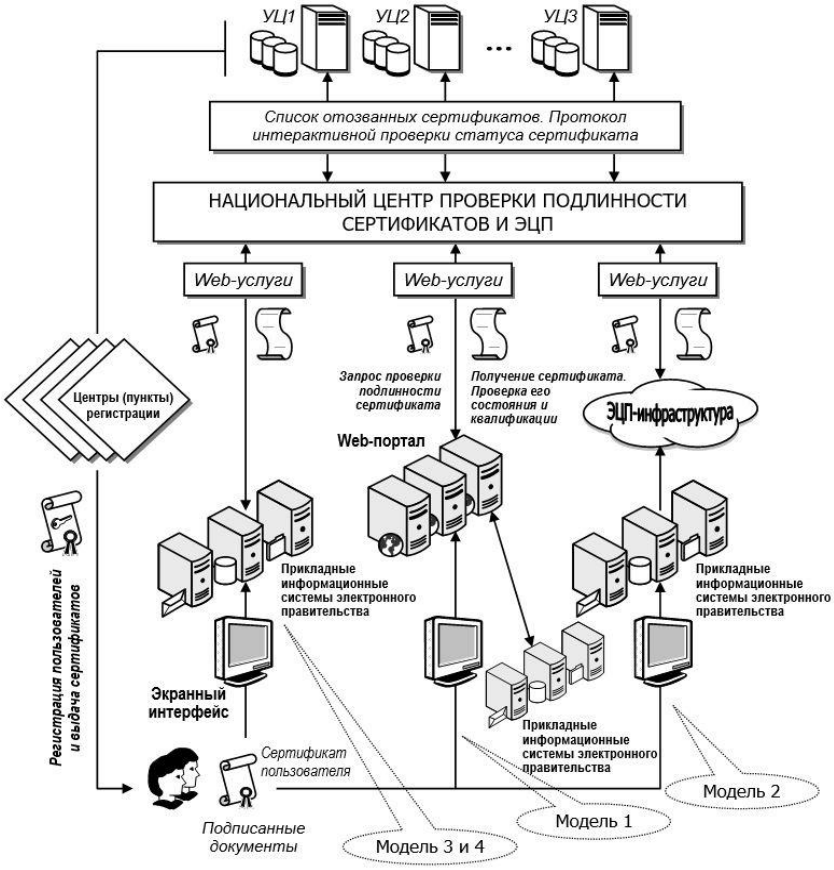


Рис. 10. Модель подтверждения подлинности СЕРТ$_{ОК}$ в режиме «одного окна»
(Fig. 10. The certificate validation by VA («one-stop-shop» mode))

В общем виде модель ПП в ЕС приведена на рис. 11. Отправитель, находящийся в стране $\mathcal{A}$, подписывает документа и отправляет его получателю в стране $\mathcal{B}$ (1). Получатель обращается в национальный ЦПП своей страны (2). ЦПП в стране $\mathcal{B}$ обращается в общеевропейский оператор РСДС (*PPRS*) и получает адрес целевого ЦПП в стране $\mathcal{A}$, который «отвечает» за УЦ, выпустивший СЕРТ$_{ОК}$ отправителя (3). После чего ЦПП в стране $\mathcal{B}$ отправляет запрос ЦПП в стране $\mathcal{A}$ на ПП СЕРТ$_{ОК}$ отправителя (4). ЦПП

в стране $\mathcal{A}$ осуществляет ПП с помощью соответствующего УЦ (5) и возвращает результат промежуточному ЦПП (6), который транслирует ответ получателю.

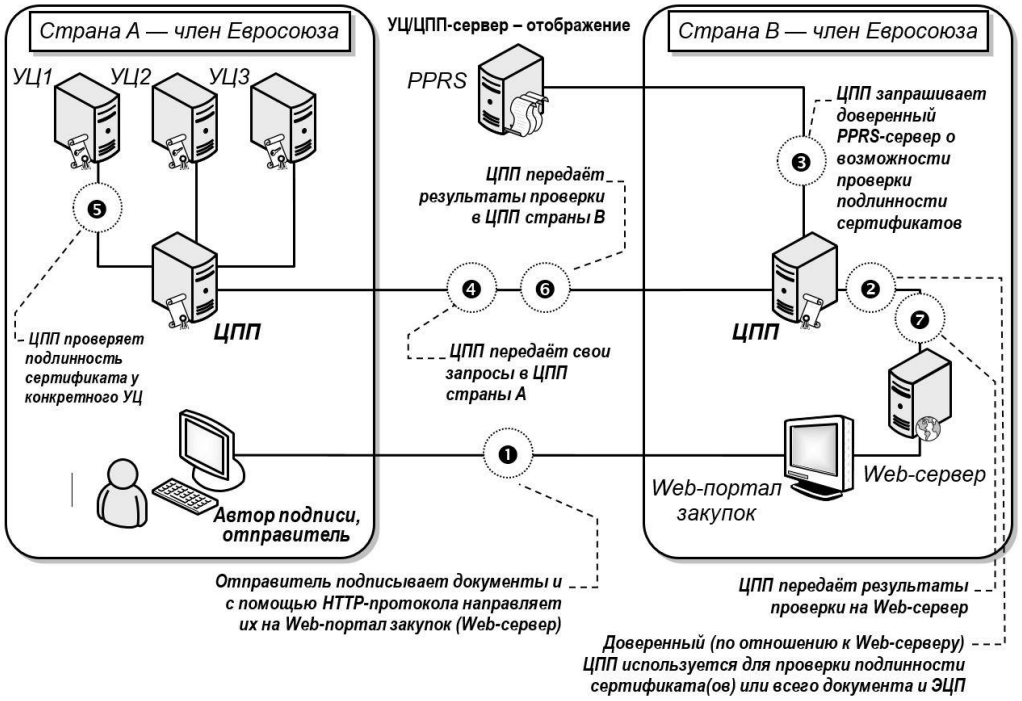


Рис. 11. Процедура ПП в модели ЕС
(Fig. 11. The certificate validation procedure in the EU model)

3.2 Современное состояние PKI в Российской Федерации

Согласно постановлению Правительства РФ №976 от 22.11.2011 федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь). Правовой статус ЭП определен в Федеральном законе №63 ФЗ от 6 апреля 2011 г. «Об электронной подписи».

На сегодняшний день существует порядка 500 аккредитованных Минкомсвязью[11], и большое количество не аккредитованных УЦ, обслуживающих конкретные организации. В 2004 году была разработана Федеральная целевая программа «Электронная Россия» и созданы Общероссийский государственный информационный центр, головной УЦ РФ, текущая структура доверия включает в себя головной (корневой) Федеральный УЦ и несколько УЦ первого уровня, обслуживающих государственные организации. Все аккредитованные УЦ также включены в структуру доверия, а их первичные $\text{СЕРТ}_{\text{ОК}}$ должны издаваться головным УЦ. Однако, в настоящее время существующая в России структура доверия не способна удовлетворить потребности цифровой экономики и должна совершенствоваться и развиваться в рамках Национального проекта «Цифровая экономика Российской федерации»[12].

[11]Перечень аккредитованных удостоверяющих центров (по состоянию на 19.12.2019) // сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, URL: https://digital.gov.ru/ru/activity/govservices/certification_authority/ (дата обращения: 22.12.2019).
[12]Национальная проект «Цифровая экономика Российской Федерации». Паспорт проекта утверждён протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. N 7.

3.3 Предлагаемая модель

В [16] была впервые предложена национальная система ПП СЕРТ$_{ОК}$ и проверки ЭП на основе PKI. На рис. 12 представлена национальная структура доверия на основе PKI. В этой структуре выстраивание иерархий частных УЦ или их взаимная сертификация необязательны, что означает неприкосновенность частного бизнеса. Обязательным условием функционирования национальной структуры доверия – это согласие каждого частного УЦ на подключение к Национальной системе ЦПП (НСЦПП), а также их аккредитация.

Аналогично западноевропейской модели, при ПП СЕРТ$_{ОК}$ и проверке ЭП в рамках одного муниципального образования (или региона) не будет необходимости перенаправления запроса на более высокий уровень, что снизит общую нагрузку на систему. Такая многоуровневая иерархия позволяет освободить корневые УЦ и ЦПП от необходимости вести постоянно изменяющийся перечень всех частных УЦ.

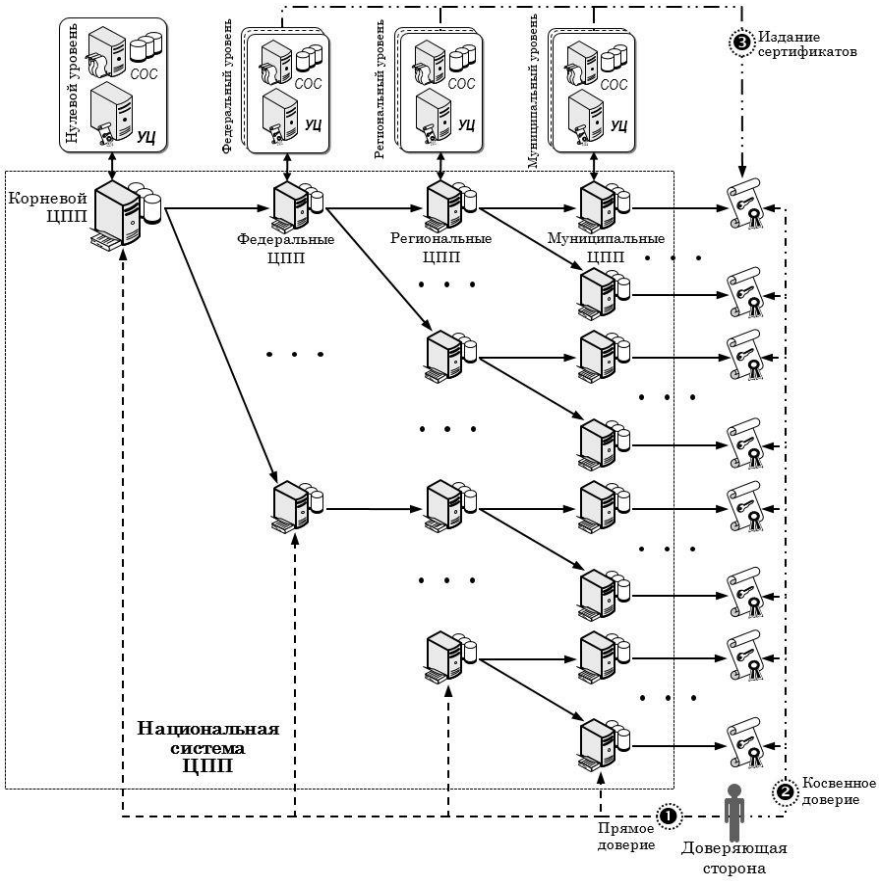


Рис. 12. Модель национальной структуры доверия
(Fig. 12. The national trust structure model)

НСЦПП – это ядро всей национальной структуры доверия, ПП СЕРТ$_{ОК}$ и проверки ЭП, которая представляет собой иерархическую и распределённую структуру ЦПП, включающую несколько уровней ЦПП (федеральный, региональный и муниципальный). С точки зрения государственного управления, НСЦПП представляет собой государственную «надстройку», которая осуществляет регулирование в области ЭП и обеспечивает доверие и функционирование соответствующих государственных и

коммерческих транзакций в различных отраслях цифровой экономики, включая частно-государственное партнёрство.

На федеральном уровне НСЦПП возможно создание отдельных ведомственных и отраслевых ЦПП иерархий и соответствующих сети доверия, которые могут быть организованы не только по географическому принципу, но и по ведомственному, экономическому или иному принципу. При этом частные УЦ разделяются по территориальному признаку. Каждый частный УЦ будет добровольно входить в реестр муниципального или регионального ЦПП. Таким образом, национальная структура доверия Российской Федерации будет самостоятельным сегментом критической информационной инфраструктуры, который потребует создания необходимых систем обеспечения безопасности.

Заключение

Несовершенство PKI в Российской Федерации, т.е. фактическое отсутствие национальной структуры доверия, является источником проблем использования ЭП пользователями, в частности, узковедомственное использование ЭП, и повышает вероятность возникновения различных инцидентов и противоправных действий со стороны злоумышленников в информационно-технологической сфере. При развитии таких инфраструктур основное внимание уделялось модернизации технологической базы и ИТС, а не семантическим аспектам доверия. А ведь именно из-за неправильной трактовки $СЕРТ_{ОК}$ и ПРП происходит большая часть преступлений в данной сфере, особенно когда дело касается глобальной Интернет-сети.

Существует множество теоретических моделей структур доверия на основе PKI, так или иначе нашедших применение на практике. Несмотря на то, что в последние годы предпринимается множество попыток по развитию и регулированию PKI, было введено предоставление многих государственных услуг в электронной форме и т.д., анализ зарубежных национальных структур доверия показал, что текущая ситуация в области PKI в Российской Федерации далека от совершенства.

Предлагаемая национальная модель доверия объединяет все существующие УЦ страны в единую национальную структуру доверия на основе PKI, иерархия которой позволит существенно снизить накладные расходы электронного документооборота, как на государственном, так и на коммерческом уровне, и создаст благоприятные условия для дальнейшего развития цифровой экономики Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. М.: Горячая Линия – Телеком., 2004. – 248 с. ISBN 5-93517-154-6. URL: https://elibrary.ru/item.asp?id=19582746 (дата обращения: 15.01.2020).
2. Раджендран В., "Эволюция экосистемы PKI", 2017 Международная конференция по инфраструктуре открытых ключей и ее приложениям (PKIA), Бангалор, 2017. С. 9–10. DOI: 10.1109/PKIA.2017.8278951. URL: https://ieeexplore.ieee.org/abstract/document/8278951 (дата обращения: 20.01.2020).
3. Мельников, Дмитрий А. et al. Практическая реализация различных моделей инфраструктуры открытых ключей. Безопасность информационных технологий, [S.l.], Т. 23, №. 1. С. 100-114, mar. 2016. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/38> (дата обращения: 07.03.2020).
4. Kaimov A.T., Kaimov A.T. Public key infrastructure: a survey. – 2018. URL: https://repository.kbtu.kz/bitstream/handle/123456789/75/Вестник%201-2018%20для%20библиотеки-92-99.pdf?sequence=1&isAllowed=y (дата обращения: 09.03.2020).
5. Radif M. J. Vulnerability and Exploitation of Digital Certificates, 2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT). IEEE, 2018. P. 88–92. URL: https://ieeexplore.ieee.org/abstract/document/8681179 (дата обращения: 25.01.2020).
6. Kohlas R., Jonczy J., and Haenni R. A Trust Evaluation Method Based on Logic and Probability Theory. In The Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and Security

(IFIPTM 2008), Trondheim, June 2008. DOI:10.1007/978-0-387-09428-1_2. URL: https://link.springer.com/chapter/10.1007/978-0-387-09428-1_2 (дата обращения: 07.03.2020).
7. Rescorla E. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018. DOI: RFC 8446. URL: https://www.hjp.at/doc/rfc/rfc8446.html (дата обращения: 05.03.2020).
8. Hayes J.M. The problem with multiple roots in web browsers – certificate masquerading. In 7th Workshop on Enabling Technologies, Infrastructure for Collaborative Enterprises (WETICE '98). CAUSA Proceedings. P. 306–313. IEEE Computer Society, Palo Alto, 17–19 June 1998. DOI: 10.1109/ENABL.1998.725710. URL: https://ieeexplore.ieee.org/abstract/document/725710 (дата обращения: 01.03.2020).
9. Soghoian C. and Stamm S. Certified lies: Detecting and defeating government interception at-tacks against SSL (short paper). In Financial Cryptography. P. 250–259, 2011. DOI: 10.1007/978-3-642-27576-0_20. URL: https://link.springer.com/chapter/10.1007/978-3-642-27576-0_20 (дата обращения: 02.03.2020).
10. Shakarian P. Stuxnet: Cyberwar revolution in military affairs. – Military Academy West Point NY, 2011. URL: https://apps.dtic.mil/docs/citations/ADA546439 (дата обращения: 01.03.2020).
11. Jøsang A. PKI trust models. In Atilla Elçi *et al.* (editors), Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS). – IGI Global, 2013. P. 279–301. ISBN13: 9781466640306. DOI: 10.4018/978-1-4666-4030-6.ch012. URL: https://www.igi-global.com/chapter/content/76520 (дата обращения: 10.02.2020).
12. Омельченко А.В. Теория графов. – М.: МЦНМО, ISBN 978-5-4439-1247-9. 2018. – 416 с.
13. Ølnes J. PKI Interoperability by an Independent, Trusted Validation Authority. In Proceedings of the 5th Annual PKI R&D Workshop, NIST, Gaithersburg MD, April 2006. URL: https://pdfs.semanticscholar.org/63ed/e2298104b2a71083406f04c4ba071e048499.pdf (дата обращения: 10.02.2020).
14. Freeburg M., McCaughan A. HIPAA for dummies: A practitioner's guide // Compelling counseling interventions: Celebrating VISTAS'fifth anniversary. 2008. P. 305–312. URL:https://www.counseling.org/resources/library/VISTAS/2008-V-Print-complete-PDFs-for-ACA/Freeburg_Article_29.pdf (дата обращения: 10.02.2020).
15. Fletcher P.D. The government paperwork elimination act: Operating instructions for an electronic government // International Journal of Public Administration. 2002. Т. 25. №. 5. P. 723–736. URL:https://www.researchgate.net/publication/247530761_The_Government_PaperWork_Elimination_Act_Operating_Instructions_For_An_Electronic_Government (дата обращения: 15.02.2020).
16. Melnikov D.A., Durakovsky A.P., Gorbatov V.S., Modestov A.A. and Ivanenko V.G. Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust. In Proceedings of the 4rd International Conference on Future Internet of Things and Cloud (FiCloud 2016). 2016. P. 123–130. DOI:10.1109/FiCloud.2016.25.URL:https://www.researchgate.net/publication/322288892_Russian_Model_of_Public_Keys_and_Validation_Infrastructure_as_Base_of_the_Cloud_Trust (дата обращения: 16.02.2020).

REFERENCES:

[1] Gorbatov V.S., Poljanskaja O.Ju. Osnovy tehnologii PKI. M.: Gorjachaja Linija – Telekom., 2004.– 248 p. ISBN 5-93517-154-6. URL: https://elibrary.ru/item.asp?id=19582746 (accessed: 15.01.2020) (in Russian).
[2] Rajendran B. Evolution of PKI ecosystem, 2017 International Conference on Public Key Infrastructure and its Applications (PKIA). IEEE, 2017. P. 9–10. URL: https://ieeexplore.ieee.org/abstract/document/8278951 (accessed: 20.01.2020).
[3] MELNIKOV, Dmitriy A. et al. Practical Implementation of Various Public Key Infrastructure Models. IT Security (Russia), [S.l.], v. 23, n. 1, p. 100-114, mar. 2016. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/38> (accessed: 07.03.2020). (in Russian).
[4] Kaimov A.T., Kaimov A.T. Public key infrastructure: a survey. – 2018. URL: https://repository.kbtu.kz/bitstream/handle/123456789/75/Вестник%201-2018%20для%20библиотеки-92-99.pdf?sequence=1&isAllowed=y (accessed: 09.03.2020).
[5] Radif M. J. Vulnerability and Exploitation of Digital Certificates, 2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT). IEEE, 2018. P. 88–92. URL: https://ieeexplore.ieee.org/abstract/document/8681179 (accessed: 25.01.2020).
[6] Kohlas R., Jonczy J., and Haenni R. A Trust Evaluation Method Based on Logic and Probability Theory. In The Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008), Trondheim, June 2008. DOI:10.1007/978-0-387-09428-1_2. URL: https://link.springer.com/chapter/10.1007/978-0-387-09428-1_2 (accessed: 07.03.2020).
[7] Rescorla E. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018. DOI: RFC 8446. URL: https://www.hjp.at/doc/rfc/rfc8446.html (accessed: 05.03.2020).

[8] Hayes J.M. The problem with multiple roots in web browsers – certificate masquerading. In 7th Workshop on Enabling Technologies, Infrastructure for Collaborative Enterprises (WETICE '98). P. 306–313. DOI: 10.1109/ENABL.1998.725710. URL: https://ieeexplore.ieee.org/abstract/document/725710 (accessed: 01.03.2020)

[9] Soghoian C. and Stamm S. Certified lies: Detecting and defeating government interception at-tacks against SSL (short paper). In Financial Cryptography. P. 250–259, 2011. DOI:10.1007/978-3-642-27576-0_20. URL: https://link.springer.com/chapter/10.1007/978-3-642-27576-0_20 (accessed: 02.03.2020).

[10] Shakarian P. Stuxnet: Cyberwar revolution in military affairs. – Military Academy West Point NY, 2011. URL: https://apps.dtic.mil/docs/citations/ADA546439 (accessed: 01.03.2020).

[11] Jøsang A. PKI trust models. In Atilla Elçi *et al.* (editors), Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS). – IGI Global, 2013. P. 279–301. ISBN13: 9781466640306. DOI: 10.4018/978-1-4666-4030-6.ch012. URL: https://www.igi-global.com/chapter/content/76520 (accessed: 10.02.2020).

[12] Omelchenko A.V. Teoriya grafov. – M.: MCNMO, ISBN 978-5-4439-1247-9. 2018. – 416 p. (in Russian).

[13] Ølnes J. PKI Interoperability by an Independent, Trusted Validation Authority. In Proceedings of the 5th Annual PKI R&D Workshop, NIST, Gaithersburg MD, April 2006. URL: https://pdfs.semanticscholar.org/63ed/e2298104b2a71083406f04c4ba071e048499.pdf (accessed: 10.02.2020).

[14] Freeburg M., McCaughan A. HIPAA for dummies: A practitioner's guide. Compelling counseling interventions: Celebrating VISTAS'fifth anniversary. 2008. P. 305–312. URL:https://www.counseling.org/resources/library/VISTAS/2008-V-Print-complete-PDFs-for-ACA/Freeburg_Article_29.pdf (accessed: 10.02.2020).

[15] Fletcher P.D. The government paperwork elimination act: Operating instructions for an electronic government. International Journal of Public Administration. 2002. Т. 25. №. 5. P. 723–736. URL:https://www.researchgate.net/publication/247530761_The_Government_PaperWork_Elimination_Act_Operating_Instructions_For_An_Electronic_Government (accessed: 15.02.2020).

[16] Melnikov D.A., Durakovsky A.P., Gorbatov V.S., Modestov A.A. and Ivanenko V.G. Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust. In Proceedings of the 4rd International Conference on Future Internet of Things and Cloud (FiCloud 2016). 2016. P. 123–130. DOI:10.1109/FiCloud.2016.25.URL:https://www.researchgate.net/publication/322288892_Russian_Model_of_Public_Keys_and_Validation_Infrastructure_as_Base_of_the_Cloud_Trust (accessed: 16.02.2020).

Поступила в редакцию – 08 марта 2020 г. Окончательный вариант – 22 мая 2020 г.
Received – March 08, 2020. The final version – May 22, 2020.

Виктор В. Ерохин[1], Лариса С. Притчина[2]
[1,2]Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации,
пр-т Вернадского, 76, Москва, 119454, Россия
[1]e-mail: erohinvv@mail.ru, https://orcid.org/0000-0002-8754-0012
[2]e-mail: larisa.pritchin@gmail.com, https://orcid.org/0000-0001-6566-8894

МОДЕЛИРОВАНИЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ОХРАНЯЕМОГО ОБЪЕКТА НА ОСНОВЕ ТЕОРИИ АВТОМАТОВ И СЕТЕЙ ПЕТРИ

DOI: http://dx.doi.org/10.26583/bit.2020.1.05

Аннотация. В статье рассматриваются задачи по оценке и моделированию действий подразделений ОВД или других охранных структур по организационной защите охраняемого объекта на основе теории автоматов и сетей Петри. Решением задачи по созданию модели действий злоумышленника на охраняемом объекте на базе теории автоматов является определение времени пребывания злоумышленника на охраняемом объекте. Решением задачи по моделированию организационной защиты охраняемого объекта с использованием сетей Петри является нахождение параллельно реализующихся взаимосвязанных процессов действия охранных подразделений при осуществлении специальных операций. Рассмотрены методы решения защищаемого объекта от действий злоумышленника: модель организационной защиты охраняемого объекта от действий злоумышленника на основе теории автоматов; модель организационной защиты на основе сетей Петри. Проведено моделирование системы защиты объекта во времени с учётом особенностей угроз, как от субъектов уголовного мира, так и при чрезвычайных ситуациях. Представленные подходы и методы моделирования действий охранных структур позволяют оценить их действия.

Ключевые слова: защита информации, сети Петри, теория автоматов.
Для цитирования: ЕРОХИН, Виктор В.; ПРИТЧИНА, Лариса С. МОДЕЛИРОВАНИЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ОХРАНЯЕМОГО ОБЪЕКТА НА ОСНОВЕ ТЕОРИИ АВТОМАТОВ И СЕТЕЙ ПЕТРИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 65-77, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1271>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.05.

Viktor V. Erokhin[1], Larisa S. Pritchina[2]
[1,2]Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs,
76 Vernadsky Ave., Moscow, 119454, Russia
[1]e-mail: erohinvv@mail.r, https://orcid.org/0000-0002-8754-0012
[2]e-mail: larisa.pritchin@gmail.com, https://orcid.org/0000-0001-6566-8894

Simulation of organizational protection of a protected object based on the theory of automata and Petri nets

DOI: http://dx.doi.org/10.26583/bit.2020.1.05

Abstract. The paper discusses the tasks of evaluating and modeling the actions of police units or other security structures for the organizational protection of a guarded object based on the theory of automata and Petri nets. The solution to the problem of creating a model of an attacker's actions on a guarded object on the basis of the theory of automata is to determine the time of an attacker's stay on a guarded object. The solution to the problem of modeling the organizational protection of a protected facility using Petri nets is to find parallel-to-work interconnected processes of security units during special operations. The methods of solving the protected object from the actions of an attacker are considered: a model of organizational protection of the protected object from the actions of an attacker based on the theory of automata; model of organizational protection based on Petri nets. This allows simulating the object's

protection system in time taking into account the specifics of threats both from the subjects of the criminal world and in emergency situations. In addition the presented approaches and modeling methods for the actions of security structures allow the most accurate assessment and optimization of their actions.
Keywords: information protection, Petri nets, automata theory.
For citation: EROKHIN, Viktor V.; PRITCHINA, Larisa S. Simulation of organizational protection of a protected object based on the theory of automata and Petri nets. IT Security (Russia), [S.l.], v. 27, n. 2, p. 65-77, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1271>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.05.

Введение

Деятельность злоумышленников оказывают достаточное сильное влияние на ущемление прав и свобод человека, на его стремление к комфортной жизни и на функционирование организационных систем в целом. Для эффективной борьбы с деятельностью злоумышленников необходимо принять упреждающие его деятельность специальные меры по организационной защите охраняемого объекта и его субъектов и объектов функционирования.

Последствиями действий злоумышленника обычно являются возникновение угроз жизнеобеспечению человека, его правам и свободам, нанесению материально-финансового ущерба организационной системе или отдельному человеку, по нарушению условий жизни населения и работы правительственных органов и т.д.

Основной объём специальных мероприятий по борьбе с угрозами охраняемых объектов проводится подразделениями УВД. Например, такими мерами могут быть:

- пресечение деятельности уголовных элементов и незаконных вооруженных формирований;
- розыск и задержание злоумышленников и преступников;
- охрана объектов и субъектов;
- сдерживание восстаний и массовых беспорядков;
- освобождение заложников;
- ликвидация последствий чрезвычайных ситуаций.

1. Постановка задачи исследования

Для результативного предупреждения и устранения угроз, а также последствий чрезвычайных ситуаций, необходимо создать математические модели действий охранных подразделений и его персонала при возникновении чрезвычайных обстоятельств. Характер таких действий имеет зависимость от особенностей развития угроз объекту защиты (от злоумышленников, чрезвычайных ситуаций). В связи с чем появляется задача – необходимость в оценивании результативности и оптимизации действий охранных подразделений с учётом различных видов угроз и имеющихся людских и технических ресурсов.

Угрозы охраняемому объекту могут иметь следующие особенности:

- уникальны в совокупности по характеру, физической и социальной среде реализации;
- быстрота развития и реализации;
- как правило, нечеткая определенность исходных данных;
- неполнота и нецелостность исходных данных;
- поэтапное развитие и реализация;
- стохастичность действий.

На основе анализа указанных особенностей развития и реализации угроз на охраняемом объекте, можно определиться с математическим аппаратом по моделированию действий охранных подразделений и их структур. Так как развитие чрезвычайной ситуации на охраняемом объекте происходит поэтапно, то это обусловливает осуществление дискретизации описания такой ситуации посредством методов теории конечных автоматов, сетей Петри, графов. Если в организационной системе охраны объекта присутствует стохастичная сменность состояний, тогда дополнительно к указанным методам необходимо применить модели Марковских и полумарковских цепей и вероятностных автоматов [1–4].

На выбор математических методов моделирования организационной системы по охране объекта могут оказывать следующие характеристики:

- количество охранных структур и групп, которые принимают участие в устранении чрезвычайных ситуаций;
- допустимость риска;
- точность экстраполяции развития чрезвычайных ситуаций на охраняемом объекте;
- сложный или простой характер развития чрезвычайных ситуаций.

На основе этих характеристик можно применять при охране объекта различные виды математического моделирования действий охранных структур по охране объекта и поимке нарушителей (злоумышленников). Присутствие большого количества охранных структур обусловливает при моделировании организационных систем охраны объекта использовать методы теории автоматов. Для чрезвычайных ситуаций с небольшим количеством охранных структур для математического моделирования их действий оптимально использовать Марковские модели или методы теории сетей Петри. Если в организационной системе охраны объекта основной характеристикой является допустимость риска, тогда для моделирования действий охранных структур уже оптимально использовать методы теорий конфликта и игр [5]. В системе охраны объекта, где необходимо обеспечить точность экстраполяции развития чрезвычайных ситуаций на охраняемом объекте, наиболее оптимально для моделирования действий охранных структур использовать методы теории сетей Петри (обеспечение точного результата), Марковские модели (приближенная экстраполяция). При сложном характере развития чрезвычайных ситуаций на объекте охраны оптимальным является применении комбинации методов: сетей Петри, теории автоматов, Марковских моделей, нечетких множеств, теории игр и т.д.

Существуют большие возможности в выборе моделей, которые учитывают динамику изменений состояний моделируемой организационной системы. Особенно эффективными являются модели на основе [1, 4, 6]:

- теории автоматов, которые позволяют оценить разнообразные показатели функционирования моделируемой организационной системы в виде охраняемого объекта;
- сетей Петри.

Использование теории автоматов основано на характеристиках преобразователей – дискретность функционирования и конечность описываемых ими диапазонов параметров [1, 7]. Еще одна важная особенность дискретных моделей заключается в том, что они не используют количественные, а только качественные характеристики для определения текущего состояния модели. Изменения в состоянии дискретной модели от момента к моменту могут быть либо детерминированными, либо недетерминированными.

Первоначально рассмотрим задачу разработки модели действий злоумышленника на охраняемом объекте на основе теории автоматов. Решением задачи является определение времени пребывания злоумышленника на охраняемом объекте.

Далее рассмотрим задачу определения параллельно реализующихся взаимосвязанных процессов действия охранных подразделений при осуществлении специальных операций по организационной защите охраняемого объекта с использованием моделирования на основе сетей Петри.

2. Методы решения защищаемого объекта от действий злоумышленника

2.1. Модель организационной защиты охраняемого объекта от действий злоумышленника на основе теории автоматов.

Повышенный уровень организационной защиты охраняемых объектов от криминального вмешательства обеспечивается применением необходимых технических средств в сочетании с высококачественным оборудованием систем безопасности и сигнализации. Охраняемые объекты в зависимости от важности, количества и типа значений делятся на две категории и четыре подкатегории. Для всех подкатегорий охраняемых объектов имеются разнообразные способы их организационной защиты, что предполагает использование нескольких линий защиты. При анализе охраняемого объекта, как правило, рассматриваются три типа линии защиты:

1) осуществление контроля периметра охраняемого объекта или его элементов;
2) проведение контроля помещений;
3) контролирование хранилищ ценных объектов.

Несколько рубежей указанных типов может присутствовать на охраняемом объекте [1]. При этом злоумышленники преодолевают линии защиты последовательно, и на каждой из линий защиты совершаются или не совершаются какие-либо события, которые являются следствием действий злоумышленников или организационной системы охраняемого объекта. В частности [8, 9]:

- система охраны может либо обнаружить или не обнаружить преступника (злоумышленника);
- в зависимости от вида организационной системы охраняемого объекта злоумышленник при его выявлении может быть информирован или не информирован;
- после обнаружения злоумышленника сигнал от системы защиты объекта поступает на центральную станцию безопасности. Группа задержания или охрана выдвигается к охраняемому объекту для пресечения правонарушения либо для поимки злоумышленника.

При этом на центральную станцию безопасности может поступить ложный сигнал тревоги, который в большинстве случаев обусловливается внешними какими-либо воздействиями или явлениями искусственного/естественного происхождения.

Для математического моделирования организационной защиты охраняемого объекта требуется задать её параметры (g, s, v, $\underline{z}$), такие как:

- если нарушитель преодолел j-ю (j = 1, 2, 3) линию защиты, тогда $g_j = 1$;
- если нарушитель отступил через j-ю линию защиты, тогда $\overline{g}_j = 1$;
- если нарушитель не обнаружен на j-й линии защиты, тогда $s_j = 1$;
- если нарушителя не обнаружили при отступлении через j-ю линию защиты, тогда $\overline{s}_j = 1$;
- если нарушителя не задержали, тогда $v_1 = 1$;
- если были похищены или повреждены ценности, тогда $v_2 = 1$;
- если на j-й линии защиты сработал ложный сигнал тревоги, тогда $z_j = 1$.

- во всех иных случаях параметры g, s, v, z равняются нулю.

С использованием назначенных параметров логики g, s, v, z возможно смоделировать любые действия нарушителя, а также на эти действия реакцию организационной системы защиты охраняемого объекта:

- если нарушитель преодолел первую линию защиты и система охраняемого объекта его обнаружила, тогда $g_1 \,\&\, \bar{s}_1 = 1$;
- если нарушитель перешёл первую и вторую линию защиты, но не смог преодолеть третью линии защиты, и отступил через вторую линию защиты, был выявлен при преодолении второй линии защиты, тогда $g_1 \,\&\, s_1 \,\&\, g_2 \,\&\, \bar{s}_2 \,\&\, \bar{g}_2 \,\&\, \bar{s}_2 = 1$.

Далее приведены результаты математическое моделирование действий нарушителя на объекте охраны на основе конечного аппарата Мура:

$M = (P, X, Y, \delta, \chi)$,

где M – конечный аппарат Мура, описываемый пятиместным кортежем; P – алфавит действий нарушителя на объекте охраны и реакция организационной системы защиты охраняемого объекта; X – входной алфавит воздействий, обусловливающих смену действий нарушителя; Y – выходной алфавит оценивания времени пребывания нарушителя в каждом своем действии на объекте охраны; $\delta: P \times X \to P$ – функция переходов; $\chi: P \to Y$ – функция выходов [1, 10–12].

Автоматная модель охраняемого объекта описывает переходы в промежуточное состояние по параметру P_{ji}, где j – номер преодолеваемой линии защиты, которую преодолел нарушитель, если нарушитель не преодолел линию защиты или отступает через соответствующую линию защиты, тогда перед j ставиться знак минус; i – тип реакции организационной системы охраны объекта: $i = 1$ – нарушитель линии защиты не выявлен; $i = 2$ – нарушитель линии защиты выявлен; $i = 3$ – сработала ложная сигнализация; $i = 4$ – нарушитель смог скрыться с охраняемого объекта; $i = 5$ – информация о задержании нарушителя.

Например, смена действия нарушителя фиксируется компонентами входного алфавита, который определяется следующими логическими выражениями:

- модель $X_{0,12} = \langle g_1 \,\&\, \bar{P}_1 = 1 \rangle$ определяет переход действия нарушителя P_0 в P_{12};
- модель $X_{22,42} = \langle \bar{g}_2 \,\&\, \bar{s}_2 = 1 \rangle$ определяет переход действия нарушителя P_{22} в P_{42}.

В автоматной модели Мура выходные элементы (Y_j) определяются только действиями нарушителя.

При перемещении нарушителя по охраняемому объекту происходит смена его действий от первоначального P_0 (состояние «нормы») до одного из конечных действий, например:

- если нарушителем были похищены ценности, и он смог скрыться, тогда $P_4 = 1$;
- если нарушителем не были похищены ценности, и он смог скрыться, тогда $P_4 = 0$;
- если нарушителя задержали, тогда $P_5 = 1$;
- если нарушителя не задержали, тогда $P_5 = 0$.

Автоматная модель описывает потенциальные вариации для нарушителя, проходящего охрану объекта, как с техническими средствами защиты, так и без них, с учетом времени, затрачиваемого для преодоления каждой линии защиты. Поскольку существует несколько способов организации защиты объектов, необходимо осуществить синтез моделей Мура. Синтез модели конечного автомата выполняется за счет определения последовательности изменений действий нарушителя в зависимости от его точки проникновения, потенциального поведения, использования технических средств защиты, сигнализации, вероятности поимки нарушителя и т.д. На рис. 1 представлен

пример последовательности изменений в автоматной модели, которая имитирует действия нарушителя, который преодолевает последовательно все линии защиты охраняемого объекта. При этом нарушитель был выявлен при пересечении второй линии защиты и захвачен охраной объекта после пересечения им третьей линии защиты.

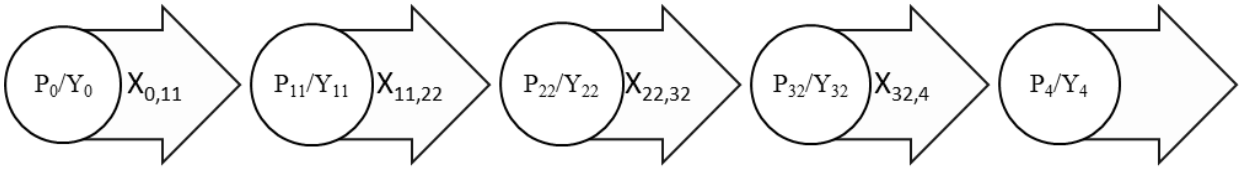


Рис. 1. Последовательность действий в автоматной модели системы защиты
(Fig. 1. Sequence of actions in the automatic security system model)

Для большей детализации организационной системы защиты охраняемого объекта необходимо применить дополнительные логические параметры. Однако это повысит размерность автоматной модели, что скажется на времени реагирования системы на действия нарушителя.

Для оценивания времени преодоления нарушителем организационной системы защиты охраняемого объекта зададим следующие параметры: t_j – время пребывания организационной системы защиты объекта охраны в состоянии P_j (стохастический параметр). На параметр t_j по преодолению нарушителем каждой из линии защиты влияет совокупность стохастических факторов, таких как тип и качественные характеристики инженерно-технической защиты охраняемого объекта, вероятность выявления нарушителя, вид объекта защиты и его площадь или объем и др. Применяя теорему Ляпунова и из источников [1, 7, 10, 13], можно задать, что Y_j имеет нормальный закон распределения с математическим ожиданием m_j и дисперсией d_j.

Посредством предложенной модели организационной защиты охраняемого объекта на основе теории автоматов можно определить время нахождения злоумышленника на охраняемом объекте.

Предложенные аспекты по построению автоматной модели организационной защиты охраняемого объекта позволяют:

- анализировать длительности пребывания нарушителя на объекте охраны с учетом его времени преодоления каждой линии защиты;
- преобразовать автоматную модель в имитационную посредством определения вероятностных значений параметров g_j, s_j, v_j, z_j.

Построим динамическую модель действий охранных структур для ликвидации чрезвычайных ситуаций на охраняемом объекте (рис. 2). При развитии чрезвычайной ситуации охранные структуры реализуют следующие действия: P_0 – повседневная деятельность охранных структур; P_1 – сбор, группировка, классификация и анализ данных о потенциальной чрезвычайной ситуации, их уточнение и предварительное оценивание ситуации; P_2 – предварительные директивы или приказы охранным структурам; P_3 – формирование решений, определение тактических действий охранным структурам, выбор управляющих действий, организация сил и средств для ликвидации чрезвычайных ситуаций, постановка задач охранным структурам; P_4 – управление охранными структурами, определение порядка взаимодействия с другими силами; P_5 – осуществление решения поставленной задачи охранными структурами; P_6 – охранные структуры

завершают действия по охране объекта; P_7 – подведение итогов в работе охранных структур.

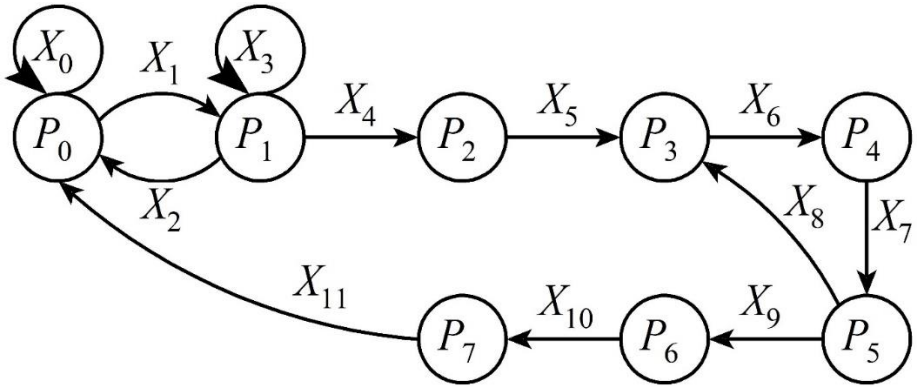
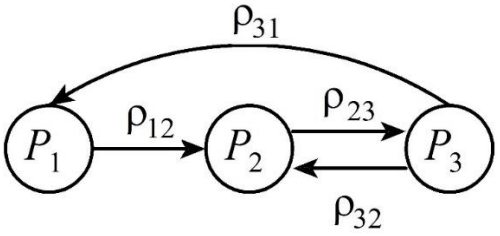


Рис. 2. Автоматная модель действий охранных структур при ликвидации чрезвычайной ситуации на охраняемом объекте
(Fig. 2. Automatic model of actions of security structures in the event of an emergency at a protected object)

Представим моделирование действий охранных структур при проведении мероприятия по поиску и аресту вооруженных нарушителей (рис. 3): P_1 – охранная структура выдвигается на охраняемый объект; P_2 – охранной группой был перекрыт подступ в зону охраняемого объекта, P_3 – охранная структура выдвигается на опорный пункт. На рис. 3 представлен граф рассматриваемой организационной системы охраны с тремя состояниями (P_1, P_2, P_3) и его матричное отображение. Состояния и действия охранных структур известны. Смена этих состояний осуществляется достаточно быстро, чтобы считать такую смену дискретной, и в заданное время.



$$\left[\rho_{ij}\right]=\begin{Vmatrix} 0 & \rho_{12} & 0 \\ 0 & 0 & \rho_{23} \\ \rho_{31} & \rho_{32} & 0 \end{Vmatrix}$$

Рис. 3. Граф состояний и переходов действий охранных структур при проведении мероприятия по поиску и аресту вооруженных нарушителей и его матричное отображение
(Fig. 3. Graph of States and transitions of actions of security structures during the search and arrest of armed violators and its matrix representation)

Для каждого перехода из одного состояния в другое пусть будут заданы вероятности ρ_{ij} системы состояний P. Задачей данного моделирования является расчет вероятностей $\rho_j(k)$ нахождения организационной системы охраны объекта после k-го шага в каждом j-м состоянии. В форме ориентированного графа состояний и переходов представляется организационная система охраны объекта. Вершинами графа являются состояния организационной системы. Дуги графа определяют направления потенциального перехода системы из какого-либо состояния в другое. Дуги на графе не изображаются в случаях, если вероятность перехода организационной системы из одного состояния в другое равняется нулю. Например, для рассматриваемой системы

нейтрализации вооруженных нарушителей вероятность перехода ρ_{12} из состояния P_1 в состояние P_2 будет зависеть от качества постановки задач охранной структуре. Вероятность перехода ρ_{23} из состояния P_2 в состояние P_3 будет зависеть от распоряжения о выдвижении сотрудников охранной структуры на опорный пункт. Вероятность перехода ρ_{31} из состояния P_3 в состояние P_1 будет зависеть от распоряжения о выдвижении сотрудников охранной структуры на охраняемый объект.

2.2. Моделирование организационной защиты на основе сетей Петри

Быстрота формирования чрезвычайных ситуаций на охраняемом объекте при лимитированном времени на исполнение охранных задач или мероприятий, а также неполные исходные данные обусловливают невозможность принятия результативных решений по управлению организационной защитой объекта охраны. Для таких систем рационально использовать методы адаптивного управления организационными системами [1, 14, 15]. В большинстве случаев действия охранных структур на охраняемом объекте при появлении чрезвычайных ситуаций являются кибернетическими, где осуществляется действие управляющего органа на управляемый объект охраны для обеспечения требуемого уровня охраны или перевода процессов в охраняемом объекте в желаемые.

Для моделирования параллельно действующих взаимосвязанных процессов в больших организационных системах (например, действия охранных структур при осуществлении специальных операций при устранении чрезвычайных ситуаций) наиболее широко применяются сети Петри. Сети Петри позволяют учитывать структурность организационной системы охраны объекта и действующие в ней процессы, а также её функционал.

Рассмотрим устоявшуюся организационную систему охраняемого объекта в виде трёх её компонентов (рис. 4): оперативный штаб; охранные структуры или группы (ОГ); чрезвычайные ситуации на охраняемом объекте. В организационной системе охраны объекта управляемыми объектами являются единицы совокупности чрезвычайных ситуаций [4, 12].

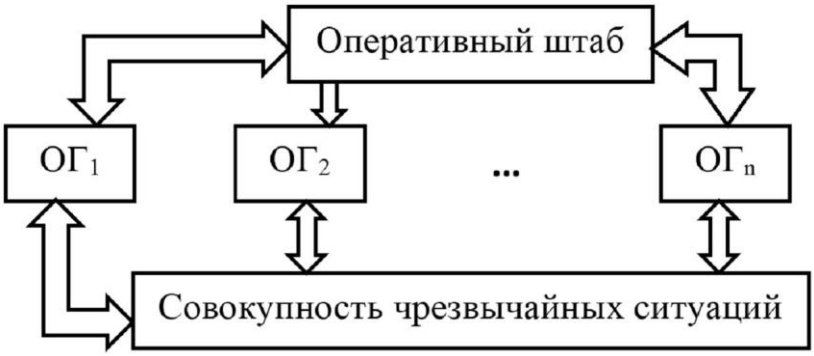


Рис. 4. Модель организационной системы охраняемого объекта
(Fig. 4. Model of the organizational system of the protected object)

Для ликвидации чрезвычайных ситуаций, как проникновение нарушителя или иное, должны использоваться управляющие воздействия – проведение специальных мероприятий и действий охранными структурами. Путем изменений состояний управляемого объекта охраны обеспечивается модификация действий в организационной системе защиты объекта, т.е., например, видоизменение тактических действий охранных подразделений.

Прогнозным или экспертным оцениванием можно компенсировать частичную стохастичность и неполноту исходных данных. Для получения исходных данных, как правило, применяют методы теории вероятности и математической статистики, теории нечетких множеств. Например, при проникновении на охраняемом объекте неизвестного количества нарушителей, их вооружение, интересы и т.д., для описания такой чрезвычайной ситуации на охраняемом объекте необходимо воспользоваться методами теории нечетких множеств. Анализируя данные криминогенных ситуаций по охраняемым объектам, можно утверждать, что количество нарушителей не менее 2 человек и не более 11, но вероятнее всего 4 или 5 человек (рис. 5).

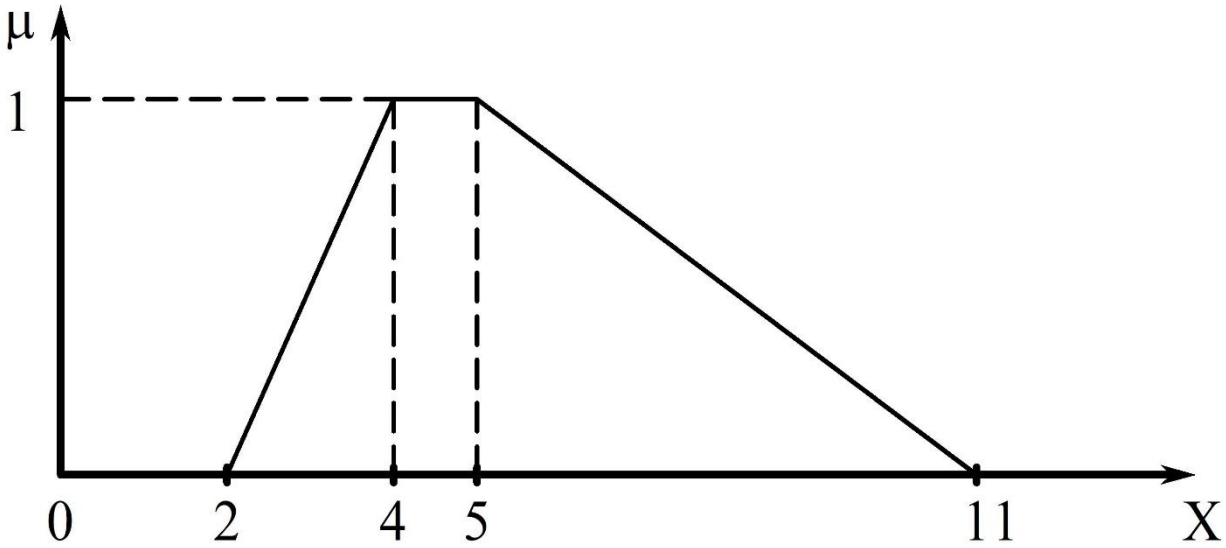


Рис. 5. Трапециевидный закон распределения нарушителей на охраняемом объекте)
(Fig. 5. Trapezoidal law of distribution of the number of violators of the protected object)

Аналитическая форма задания функции $\mu(X)$ следующая:

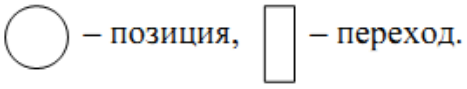
$$\mu = \begin{cases} 0, if \;\; x \le 2 \; or \; x \ge 11, \\ 0{,}5x - 1, if \;\; 2 \le x < 4, \\ 1, if \;\; 4 \le x < 5, \\ -\frac{1}{6}x + 1\frac{5}{6}, if \;\; 5 \le x < 11. \end{cases}$$

Если система охраны объекта располагает совокупностью даже приблизительных параметров чрезвычайных ситуаций, тогда появляется возможность рассчитать функции принадлежности $\mu(x)$.

Сети Петри описывают системы, которые состоят из набора взаимодействующих подсистем. Подсистемы работают в последовательном и параллельном режимах. Принимается во внимание, что каждая подсистема состоит из подсистем нижнего уровня – иерархическая структура. Сети Петри позволяют описать независимое поведения подсистем. Однако при этом необходима объективная информация о взаимодействии между подсистемами одного и того же уровня. С использованием сетей Петри можно не только осуществлять имитирование функционирования систем, но и представлять

информационные процессы, такие как управление организационной системой охраны объекта [10].

В графическом отображении сети Петри зададим два вида узла:



В любой момент времени каждая охранная группа может находиться в некотором состоянии. В соответствии с распоряжениями, приказами, директивами вышестоящей структуры охраны объекта осуществляется переход из одного состояния в другое. После перехода в следующее состояние руководитель охранной группы рапортует об исполнении (неисполнении) поставленной перед группой задачи.

Модель действий охранной группы (ОГ) при осуществлении мероприятий по поимке нарушителя на объекте охраны приведена на рис. 6.

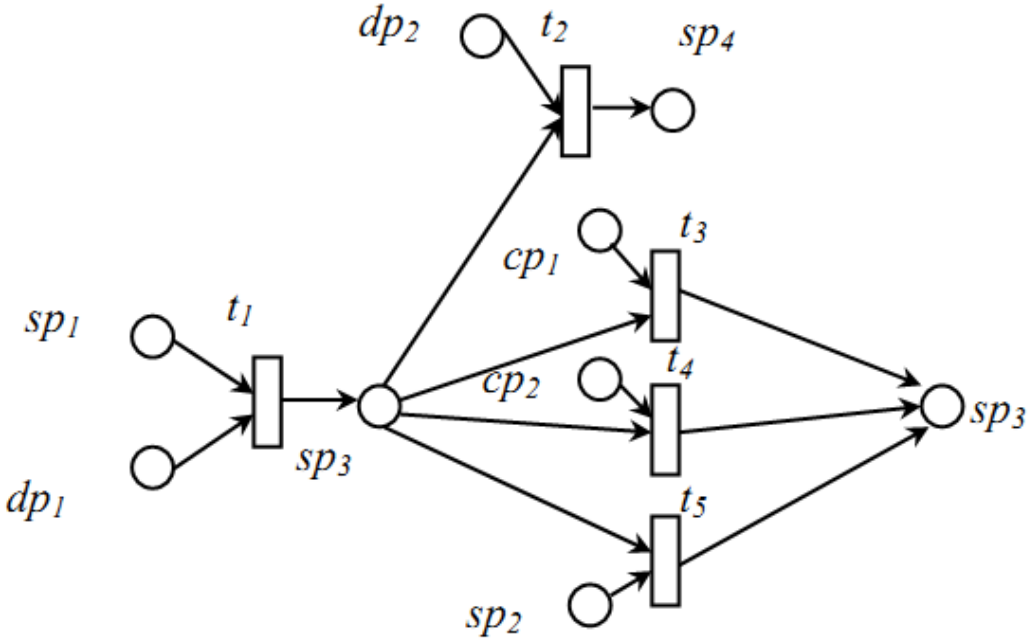


Рис. 6. Модель действий охранной группы
(Fig. 6. Security group action model)

На рис. 6 представлены следующие позиции и переходы данной модели:
*sp*1 – создана охранная группа;
*sp*2 – объект охраны покидает обслуживающий персонал;
*sp*3 – охранная группа осуществляет контроль доступа на объект охраны;
*sp*4 – расформирована или переформирована охранная группа;
*cp*1 – на охранный объект происходят попытки проникновения нарушителей;
*cp*2 – охраняемый объект пытаются покинуть нарушители;
*dp*1 – перед охранной группой поставлены задачи по охране объекта;
*dp*2 – приказ о расформировании или переформировании охранной группы;
*t*1 – охраняемая группа заняла позиции;
*t*2 – расформирование или переформирование охранной группы;

*t*3 – охранная группа препятствует продвижению нарушителей на охраняемый объект или пересечение ими линий защиты;

*t*4 – охраняемой группой пойманы и нейтрализованы нарушители;

*t*5 – охраняемая группа возвращает украденные ценности с охраняемого объекта.

Если при ликвидации чрезвычайных ситуаций на охраняемом объекте привлекаются в большом количестве различные по своему функциональному назначению охранные группы, тогда применение моделирования на основе сетей Петри дает менее точный результат из-за громоздкости. В этом случае целесообразно применять моделирование на основе теории автоматов.

Заключение

Предложенная автоматная модель имеет следующие преимущества: мониторинг продолжительности пребывания нарушителей на охраняемом объекте по каждому рубежу; модель может использовать стохастические значения алфавита действий нарушителя на объекте охраны и реакции организационной системы защиты охраняемого объекта, что позволит рассмотреть эту модель, как имитационную, которая позволит решать оптимизационные задачи.

Представленные подходы и методы моделирования действий охранных структур на охраняемом объекте учитывают характеристики выполняемых задач в случаях появления чрезвычайных ситуаций, что позволяет оценить действия охранных структур.

СПИСОК ЛИТЕРАТУРЫ:

1. Абрамов П.Б. Моделирование динамики сложных систем на основе Марковских форм с внешними потоками событий / П.Б. Абрамов. – Воронеж: ВУНЦ ВВС ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина, 2013. – 156 с.
2. Motallebi H., Abdollahi Azgomi M. Translation from Multisingular Hybrid Petri Nets to Multisingular Hybrid Automata // Fundamenta Informaticae, Vol. 130, No. 3, IOS Press, Feb. 2014. P. 275–315. DOI: 10.3233/FI-2014-993.
3. Chang L., He X., Shatz S. M. A methodology for modeling multi-agent systems using nested petri nets // International Journal of Software Engineering and Knowledge Engineering, Vol. 22, No. 2012. P. 891–925. DOI: 10.1142/S0218194012500246.
4. Pla A., Gay P., Melendez J., Lopez B. Petri net-based process monitoring: A workflow management system for process modelling and monitoring // Journal of Intelligent Manufacturing, Vol. 25, No. 3, 2014. P. 539–554. DOI: 10.1007/s10845-012-0704-z.
5. Orojloo H., Abdollahi Azgomi M. A game-theoretic approach to model and quantify the security of cyber-physical systems // Computers in Industry, Vol. 88, Elsevier, 2017. P. 44–57. DOI: 10.1016/j.compind.2017.03.007.
6. Соломатин М.С., Рогозин Е.А., Дровникова И.Г. Создание модели информационного конфликта "Нарушитель - система защиты" на основе сети Петри-Маркова // Вестник Воронежского института МВД России. 2019. № 2. С. 93–100.
URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik2_2019.pdf (дата обращения: 20.02.2020).
7. Jan N.M., Fong W.H., Sarmin N.H. State machine of place-labelled petri net controlled grammars // Malaysian Journal of Fundamental and Applied Sciences 13(4), 2017. P. 649–653.
8. Занина Т.М. Некоторые аспекты административно-правового регулирования защиты информации на режимных объектах // Вестник воронежского института МВД России, 2018, 3. С. 124–127. URL: https://ви.мвд.рф/upload/site132/document_journal/vestnik_2018_3(2).pdf (дата обращения: 20.02.2020).
9. Козьминых С.И. Организация защиты информации в российской полиции / С.И. Козьминых. – М.: «Издательство «Юнити-Дана», 2017. – 407 с.
10. Zaitsev D.A., Shmeleva T.R., Retschitzegger W., Pröll B. Security of grid structures under disguised traffic attacks // Cluster Computing, 19(3) 2016, 1183–1200. Online 17 June 2016. DOI: 10.1007/s10586-016-0582-9. URL: https://link.springer.com/article/10.1007/s10586-016-0582-9 (дата обращения: 20.02.2020).
11. Мурзаханова Е.В., Пищухин А.М. Оптимальное распределение ресурсов в системе защиты информации в организации // Вопросы защиты информации. 2019. 2(125). С. 36–40.

URL:http://izdat.ntckompas.ru/editions/for_readers/archive/article_detail.php?SECTION_ID=155&ELEMENT_ID=24535 (дата обращения: 20.02.2020).

12. Солодянников А.В. Организация и управление службой защиты информации / А.В. Солодянников. – СПб.: Санкт-Петербургский государственный экономический университет, 2018. – 89 с. URL: https://elibrary.ru/item.asp?id=37310180 (дата обращения: 20.02.2020).
13. Мустафаев В.А., Салманова М.Н. Моделирование динамических взаимодействующих процессов с применением нечетких сетей Петри типа V_F // Вестник Воронежского государственного технического университета. 2019. Т. 15. № 3. С. 28–33. DOI: 10.25987/VSTU.2019.15.3.004. URL: https://cchgeu.ru/science/nauchnye-izdaniya/vestnik-voronezhskogo-gosudarstvennogo-tekhnicheskogo-universiteta-/fayly/vypuski/15_3.pdf (дата обращения: 20.02.2020).
14. Zaitsev D.A., Shmeleva T.R., Groote J.F. Verification of Hypertorus Communication Grids by Infinite Petri Nets and Process Algebra // IEEE/CAA Journal of Automatica Sinica, 6(3), 2019, 733–742. DOI: 10.1109/JAS.2019.1911486. URL: https://ieeexplore.ieee.org/document/8707130 (дата обращения: 20.02.2020).
15. Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. 4(17). С. 61–71. URL: https://elibrary.ru/item.asp?id=27441076 (дата обращения: 20.02.2020).

REFERENCES:

[1] Abramov P.B. Modelirovanie dinamiki slozhnyh sistem na osnove Markovskih form s vneshnimi potokami sobytij. P.B. Abramov. – Voronezh: VUNC VVS VVA im. prof. N.E. Zhukovskogo i Ju.A. Gagarina, 2013. – 156 s. (in Russian).
[2] Motallebi H., Abdollahi Azgomi M. Translation from Multisingular Hybrid Petri Nets to Multisingular Hybrid Automata. Fundamenta Informaticae, Vol. 130, No. 3, IOS Press, Feb. 2014. P. 275–315. DOI: 10.3233/FI-2014-993.
[3] Chang L., He X., Shatz S.M. A methodology for modeling multi-agent systems using nested petri nets. International Journal of Software Engineering and Knowledge Engineering, Vol. 22, No. 2012. P. 891–925. DOI: 10.1142/S0218194012500246.
[4] Pla A., Gay P., Melendez J., Lopez B. Petri net-based process monitoring: A workflow management system for process modelling and monitoring. Journal of Intelligent Manufacturing, Vol. 25, No. 3, 2014. P. 539–554. DOI: 10.1007/s10845-012-0704-z.
[5] Orojloo H., Abdollahi Azgomi M. A game-theoretic approach to model and quantify the security of cyber-physical systems. Computers in Industry, Vol. 88, Elsevier, 2017. P. 44–57. DOI: 10.1016/j.compind.2017.03.007.
[6] Solomatin M.S., Rogozin E.A., Drovnikova I.G. The creation of a model of the information conflict "Intruder - protection system" on the basis of Petri-Markov network. The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia. 2019. № 2. P. 93–100.
URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik2_2019.pdf (accessed: 20.02.2020) (in Russian).
[7] Jan N.M., Fong W.H., Sarmin N.H. State machine of place-labelled petri net controlled grammars. Malaysian Journal of Fundamental and Applied Sciences 13(4), 2017. P. 649–653.
[8] Zanina T.M. Some aspects of administrative legal regulation of information security on regime objects. The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia, 2018, 3. P. 124–127. URL: https://ви.мвд.рф/upload/site132/document_journal/vestnik_2018_3(2).pdf (accessed: 20.02.2020) (in Russian).
[9] Koz'minyh S.I. Organizacija zashhity informacii v rossijskoj policii / S.I. Koz'minyh. – M.: «Izdatel'stvo «Juniti-Dana», 2017. – 407 s. (in Russian).
[10] Zaitsev D.A., Shmeleva T.R., Retschitzegger W., Pröll B. Security of grid structures under disguised traffic attacks. Cluster Computing, 19(3) 2016, 1183–1200. Online 17 June 2016. DOI: 10.1007/s10586-016-0582-9. URL: https://link.springer.com/article/10.1007/s10586-016-0582-9 (accessed: 20.02.2020).
[11] Murzakhanova E.V., Pishchukhin A.M. Optimal allocation of resources in the information security system of the organization. Information security questions, 2019, 2(125), P. 36–40. URL:http://izdat.ntckompas.ru/editions/for_readers/archive/article_detail.php?SECTION_ID=155&ELEMENT_ID=24535 (accessed: 20.02.2020) (in Russian).
[12] Solodjannikov A.V. Organizacija i upravlenie sluzhboj zashhity informacii. A.V. Solodjannikov. – SPb.: Sankt-Peterburgskij gosudarstvennyj jekonomicheskij universitet, 2018. – 89 s. URL: https://elibrary.ru/item.asp?id=37310180 (accessed: 20.02.2020) (in Russian).

[13] Mustafaev V.A., Salmanova M.N. Modeling dynamic interaction processes using fuzzy petri nets of V_F type. Bulletin of Voronezh state technical University. 2019. Vol. 15. No 3. P. 28–33. DOI: 10.25987/VSTU.2019.15.3.004. URL: https://cchgeu.ru/science/nauchnye-izdaniya/vestnik-voronezhskogo-gosudarstvennogo-tekhnicheskogo-universiteta-/fayly/vypuski/15_3.pdf (accessed: 20.02.2020) (in Russian).

[14] Zaitsev D.A., Shmeleva T.R., Groote J.F. Verification of Hypertorus Communication Grids by Infinite Petri Nets and Process Algebra. IEEE/CAA Journal of Automatica Sinica, 6(3), 2019, 733–742. DOI: 10.1109/JAS.2019.1911486. URL: https://ieeexplore.ieee.org/document/8707130 (accessed: 20.02.2020).

[15] Chucklyaev I.I. Methodical Providing Complex Management of Risks of Informational Security of Function-Oriented Information Resources Management Information Systems. Voprosy kiberbezopasnosti, 2016, 4(17). P. 61–71. URL: https://elibrary.ru/item.asp?id=27441076 (accessed: 20.02.2020) (in Russian).

Поступила в редакцию – 29 февраля 2020 г. Окончательный вариант – 22 мая 2020 г.
Received – February 29, 2020. The final version – May 22, 2020.

Анастасия В. Береснева[1], Анна В. Епишкина[2]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115522, Россия
[1]e-mail: anastasiya3161@gmail.com, http://orcid.org/0000-0002-6214-6393
[2]e-mail: avepishkina@mephi.ru, http://orcid.org/0000-0001-7681-0382

ПОДХОДЫ К ОНЛАЙН-ВЕРИФИКАЦИИ СОБСТВЕННОРУЧНОЙ ПОДПИСИ

DOI: http://dx.doi.org /10.26583/bit.2020.2.06

Аннотация. Собственноручная подпись – один из наиболее распространенных методов биометрической аутентификации, где статические и динамические характеристики подписи используются для подтверждения личности пользователя. Целью исследования является анализ алгоритмов верификации собственноручной подписи и методов извлечения характеристик. Существующие разработки используют в основе различные технологии, такие как нейронная сеть, скрытая модель Маркова и алгоритмы машинного обучения. Помимо этого, на точность алгоритма верификации оказывает влияние метод извлечения характеристик подписи, а также, какие именно характеристики подписи принимаются во внимание в процессе классификации. Данная тематика бурно развивается, новые подходы и алгоритмы для решения задачи улучшают точность верификации и скорость обучения. По результатам исследования выбран алгоритм с наименьшим количеством ошибок первого и второго рода. Наиболее перспективный алгоритм положен в основу разрабатываемой системы аутентификации на основе собственноручной подписи.

Ключевые слова: верификация, аутентификация, биометрическая аутентификация, собственноручная подпись, машинное обучение, нейронная сеть.
Для цитирования: БЕРЕСНЕВА, Анастасия В.; ЕПИШКИНА, Анна В. ПОДХОДЫ К ОНЛАЙН-ВЕРИФИКАЦИИ СОБСТВЕННОРУЧНОЙ ПОДПИСИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 78-85, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1272>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.06.

Anastasia V. Beresneva[1], Anna V. Epishkina[2],
[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115522, Russia
[1]e-mail: anastasiya3161@gmail.com, http://orcid.org/0000-0002-6214-6393
[2]e-mail: avepishkina@mephi.ru, http://orcid.org/0000-0001-7681-0382

Approaches to online handwritten signature verification

DOI: http://dx.doi.org /10.26583/bit.2020.2.06

Abstract. Handwritten signature is one of the most common methods of biometric authentication, where static and dynamic signature characteristics are used to confirm the user's identity. The existing developments are based on various technologies, such as the neural network, the hidden Markov model, and machine learning algorithms. This topic is rapidly developing, new approaches and algorithms for solving the problem improve the accuracy of verification and learning speed. The purpose of this study is to analyze existing approaches to the signature verification. The most promising algorithm will be used as the basis for the developed authentication system based on a handwritten signature.

Keywords: verification, authentication, biometric authentication, handwritten signature, machine learning, neural network.
For citation: BERESNEVA, Anastasia V.; EPISHKINA, Anna V. Approaches to online handwritten signature verification. IT Security (Russia), [S.l.], v. 27, n. 2, p. 78-85, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1272>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.06.

Введение

Одной из приоритетных задач в области информационной безопасности является аутентификация и верификация личности пользователя. Система верификации – это

совокупность методов, используемых с целью проверки правильности предоставленного идентификатора, сопоставляя его с эталонными образцами. Многие системы верификации основаны на биометрических технологиях, которые используют биологические характеристики человека для верификации.

Верификация собственноручной подписи – это биометрическая технология, которая использует подпись для идентификации личности с целью авторизации. Задача верификации подписи связана с определением того, действительно ли та или иная подпись принадлежит конкретному лицу или нет. Подписи особенно полезны для идентификации, так как подпись каждого человека уникальна, особенно если ее динамические характеристики рассматриваются вместе со статическим изображением. Алгоритмы, основанные на анализе динамических признаков, называются онлайн алгоритмами верификации подписи.

1. Система верификации собственноручной подписи

Основные этапы работы системы верификации собственноручной подписи включают в себя предварительную обработку, извлечение признаков и классификацию (рис. 1). В статье рассмотрены различные подходы к реализации данных этапов и проведено сравнение их эффективности.

Рис.1. Этапы системы верификации собственноручной подписи
(Fig. 1. Stages of the handwritten signature verification system)

На первом этапе система верификации обрабатывает эталонный набор подписей автора. На основе данного набора происходит анализ и обучение классификатора [1].

После обучения следует этап оценки (тестирования). Во время оценки система верификации принимает на вход собственноручные подписи, чтобы определить, являются ли они подлинными или поддельными. Происходит сравнение эталонного набора с подписями, подлежащими верификации. Предварительная обработка, извлечение признаков одинаковы для подписей в эталонном и тестовом наборе, но эталонные наборы используются для задания характеристик метода (тонкой настройки параметров, например, увеличения или уменьшения порога и регулировки весов) и увеличения производительности [2].

На этапе классификации происходит принятие решения, является ли представленный образец оригинальным или поддельным относительно эталонного набора.

1.1 Ввод подписи

Собственноручная подпись для онлайн-верификации вводится на мобильном устройстве. Современные мобильные устройства обладают необходимым аппаратным обеспечением для извлечения динамических признаков собственноручной подписи,

описывающих процесс совершения подписи – изменение координат пера в зависимости от времени, показания гироскопа и акселерометра.

1.2 Обработка исходных данных

Шаг предварительной обработки требуется перед извлечением признаков подписи главным образом для того, чтобы удалить шум. Предварительная обработка обычно включает фильтрацию, шумоподавление и сглаживание и часто выполняется с использованием преобразования Фурье [3, 4], гауссовых функций [5] или математической морфологии [6]. Нормализация подписей – это процесс приведения всех образцов к единому виду, который также является методом предварительной обработки. Обычно она включает смещение в сторону центра масс, который определяется как координата подписи, равноудаленная от краевых точек по вертикали и горизонтали, или начала координат [7]. В процессе обработки подпись разбивается на конечное число сегментов с приблизительно равным числом точек данных в каждом сегменте, таким образом, если подпись имеет T точек и разделим ее на S сегментов, то сегменты будут иметь приблизительно T/S точек в каждом сегменте. Сегментация сильно влияет на производительность верификации, поэтому хорошая техника сегментации может улучшить результаты верификации. Подпись разбивается на сегменты в местах резких перегибов, как приведено на рис. 2.

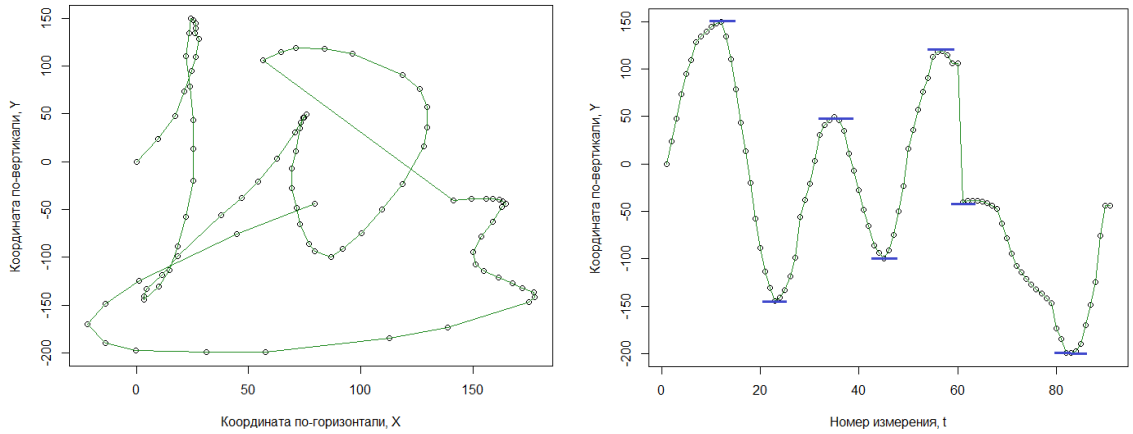


Рис. 2. Собственноручная подпись и зависимость y-координаты от времени
(Fig. 2. Handwritten signature and y-coordinate dependence on time)

1.3 Извлечение характеристик

Для того, чтобы определить, какие именно характеристики необходимо использовать в итоговом алгоритме для достижения максимальной точности верификации, необходимо провести исследование метода извлечения характеристик.

На данный момент различают три основных подхода к извлечению характеристик подписи [8]:

- Методы на основе локальных и глобальных параметров. Глобальные параметры извлекаются из всей подписи, а локальные – из ограниченной области подписи. В параметрических подходах для описания шаблона подписи выбирается набор параметров, затем параметры эталонных и тестовых подписей сравниваются, и выявляется подлинность подписи.
- Функциональные методы. Образец подписи представляется как функция времени, характеристики подписей локально сравниваются по принципу точка-точка или сегмент-сегмент [9]. В этом подходе динамические признаки подписи регистрируются как

временные последовательности, содержащие информацию об изменениях во времени признаков подписи.

- Комбинированные (гибридные) методы. Этот подход основан на комбинировании разных методов из числа вышеприведенных [10].

В ходе исследования проанализированы различные методы выделения характеристик рукописной подписи:

- дискретное преобразование Фурье [3, 4];
- дискретное преобразование Радона [3];
- дискретное вейвлет-преобразование [5];
- извлечение характеристик подписи [2].

1.4 Классификация

В базовом сценарии при классификации подписи есть только несколько эталонных подписей от автора и тестируемая подпись. Цель состоит в том, чтобы решить, принадлежит ли тестируемая подпись автору, который совершил эталонные подписи, или нет. Этот сценарий называется классификацией одного класса. Для классификации могут быть использованы различные методы, рассмотренные ниже.

1.4.1 Классификация на основе расстояний

Данный метод классификации используется в сочетании с параметрическим методом извлечения признаков, в которых подпись представлена в виде набора векторов. Пусть D – расстояние, которое проходит перо при написании собственноручной подписи. Иначе говоря, евклидово расстояние между всеми точками:

$$D(Q,R) = \sqrt{\sum_{i=1}^{n}(q_i - r_i)^2},$$

где $R = (r_1, r_2, ..., r_n)$ это характеристический вектор подписи автора, $Q = (q_1, q_2, ..., q_n)$ – характеристический вектор подписи, подлежащей классификации, n – количество характеристик. Если евклидово расстояние меньше определенного порога, то подпись считается авторской.

1.4.2 Алгоритм динамической трансформации временной шкалы

Алгоритм позволяет оценить расстояние между двумя временными последовательностями разной длины, вычисляет матрицу преобразования и расстояние динамической трансформации [11]. На основании значения расстояния классификатор решает, является ли подпись подлинной или поддельной. Для выделения признаков при применении данного метода классификации используется функциональный метод извлечения признаков.

Таким образом, согласно алгоритму динамической трансформации, для двух векторов $u = (u_1, u_2, ..., u_n)$ и $v = (v_1, v_2, ..., v_n)$ расстояние трансформации может быть вычислено за $O(n^2)$. Матрица трансформации $C \in R^{((m+1)\times(n+1))}$ строится следующим образом:

$$C_{0,0} = 0,\ C_{i,0} = \infty,\ C_{0,j} = \infty;\ i = 1,...n;\ j = 1,...n;$$

$$C_{i,j} = |u_i - v_j| + \min(C_{i-1,j}, C_{i,j-1}, C_{i-1,j-1}),$$

где $|u_i - v_j|$ определяет абсолютное расстояние между координатой i вектора u и координатой j вектора v. После построения матрицы C, можно вычислить наикратчайшее расстояние трансформации между векторами u и v.

Алгоритм динамической трансформации временной шкалы был неоднократно улучшен в ряде исследований [12–13].

1.4.3 Скрытая модель Маркова

В этом методе классификации подпись может быть представлена в виде скрытой марковской модели (СММ), диаграмма перехода состояний которой приведена на рис. 3. Согласно этой статистической модели, скрытая цепь переходит из состояния i в состояние i+1 с вероятностью $a_{i,i+1}$ или возвращается в состояние i с вероятностью a_{ii} =1-$a_{i,i+1}$. Пусть q_t – состояние цепи в момент времени t; вероятность того, что вектор наблюдения O_t внутри некоторой области R_j, когда цепь находится в состоянии i, определяется условной вероятностью состояния системы: $b_i(j) = P\{ O_t \in R_j \mid q_t = i\}$.

В процессе обучения параметры исследуемой подписи оцениваются с помощью набора, содержащего эталонные подписи. Во время проверки вычисляется вероятность того, что подпись является подлинной. Если эта вероятность выше определенного порога, подпись принимается, в противном случае она отклоняется.

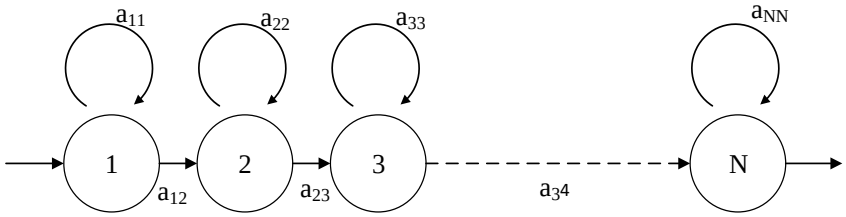


Рис.3. Диаграмма переходов состояний СММ
(Fig. 3. Diagram of HMM state transitions)

Этот подход можно рассматривать как статистическое соответствие между проверяемой подписью и подписью, основанной на СММ.

1.4.5 Персептронная нейронная сеть

Одним из методов классификации подписей является использование персептронной нейронной сети. Нейронная сеть – это система, состоящая из нейронов, их связей и ребер с определенными весами. Нейронная сеть получает вектор, содержащий значения характеристик подписи. Нейроны располагаются во входном и выходном слоях, а также в одном или нескольких скрытых слоях. Последний слой – это выход, который вычисляется суммированием и функцией активации.

В процессе обучения нейронная сеть учится корректировать веса ребер на основе известных классов данных обучения. Веса синапсов настраиваются таким образом, чтобы минимизировать ошибку – разницу между решенным выходом и выходом, вычисленным сетью на недавнем этапе на обучающем наборе. Применение нейронных сетей описывается в большом количестве исследований [14–15]. Для тестирования была реализована простая нейронная сеть персептрона, которая имеет 12 входов, два скрытых уровня по шесть нейронов в каждом и один выход.

1.4.6 Метод опорных векторов

Метод машинного обучения на основе опорных векторов классифицирует представленные образцы на основе обучающего набора данных. Основная идея метода состоит в том, чтобы перевести начальные векторы в пространство большей размерности и найти оптимальную гиперплоскость с максимальным зазором в этом пространстве. Этот

классификационный подход используется в ряде работ [13–15]. Для извлечения признаков подписей могут быть использованы как функциональные, так и параметрические методы.

2. Тестирование

Для анализа эффективности указанных подходов к верификации собственноручных подписей были реализованы соответствующие алгоритмы. Кроме того, мобильное приложение для платформы Android на языке Java реализовано для сбора тестовых подписей пользователей и подписей злоумышленников.

Все реализованные алгоритмы основаны на предварительном обучении. Пользователь выполняет несколько подписей, из которых извлекаются необходимые характеристики.

Для оценки систем верификации используются коэффициенты ошибок 1-го и 2-го рода, которые называются коэффициентами ложного отклонения и ложного принятия соответственно:

– частота ложных пропусков – процент решений аутентификации, разрешающих доступ нелегитимному пользователю;

– частота ложных отказов – процент решений аутентификации, запрещающих доступ легитимному пользователю:

$$FAR = \frac{N_{FA}}{N_F} \times 100\%$$

где N_{FA} и N_{FR} – число ложно принятых и число ложно отклоненных собственноручных подписей на тестовом наборе, N_F – число поддельных подписей, N_T – число оригинальных подписей [5].

По результатам тестирования на наборе из 100 подписей для рассматриваемых алгоритмов получены результаты, приведенные в табл. 1. Для тестирования метода опорных векторов также сформирован набор из подписей злоумышленника. Для формирования данного набора пользователям предлагалось проследить за совершением подписи автором, а затем повторить подпись от лица злоумышленника.

Исследование показало, что наиболее перспективными методами для дальнейшей работы являются алгоритмы на основе нейронной сети и метода опорных векторов, поскольку доля ошибок 1-го и 2-го рода для этих алгоритмов минимальна относительно других. Существует несколько причин возникновения ошибок 1-го рода. Во-первых, некоторые люди не могут приспособиться к подписи на планшете, а подлинные подписи на планшете отличаются от подписей на бумаге. Во-вторых, набор эталонных подписей исходного пользователя не является достаточным для обучения этим методам.

Таблица 1. Результаты тестирования реализованных алгоритмов

Метод	Дискретное преобразование Фурье		Дискретное преобразование Радона		Вейвлет преобразование		Характеристики	
Алгоритм на основе расстояний	19%	17 %	15 %	8 %	13%	4%	11 %	14 %
Алгоритм динамической трансформации	11%	18 %	14 %	10 %	10%	8%	10 %	12 %
Скрытая модель Маркова	10%	17 %	17 %	7 %	14%	17%	8 %	7 %

Нейронная сеть	9 %	12 %	12 %	17 %	13 %	19 %	12 %	7 %
Метод опорных векторов	9 %	9 %	13 %	7 %	9 %	12 %	10%	7%
	Ошибки 1-го рода	Ошибки 2-го рода	Ошибки 1-го рода	Ошибки 2-го рода	Ошибки 1-го рода	Ошибки 2-го рода	Ошибки 1-го рода	Ошибки 2-го рода

Заключение

Рассмотренные алгоритмы верификации подписи имеют достаточно высокие показатели эффективности, однако доля ошибок может быть сокращена в результате усовершенствования метода извлечения признаков подписи в дальнейшем исследовании.

По результатам исследования, приведенным в таблице, можно заметить, что функциональные методы извлечения характеристик дают худший результат в сравнении с локальным методом извлечения. При использовании локальных методов извлечения характеристик подписи значения ошибок первого и второго рода минимальны, а значит точность алгоритма верификации выше. На основе этого можно сделать вывод, что статические и динамические характеристики подписи, извлеченные на каждом интервале, позволяют подробнее описать процесс совершения подписи. В то же время не все характеристики являются информативными, многие из них дублируются либо не являются устойчивыми по времени. Для анализа значимости характеристик в дальнейшем исследовании необходимо провести анализ на основе статистических свойств.

Помимо этого, в дальнейшей работе планируется разработка алгоритма верификации собственноручной подписи на основе алгоритмов машинного обучения, основанного на локальных характеристиках с целью сокращения ошибок первого и второго рода, а также времени обучения и принятия решения.

СПИСОК ЛИТЕРАТУРЫ:

1. Ooi, Shih Yin, Andrew Beng Jin Teoh, Ying-Han Pang and Bee Yan Hiew. “Image-based handwritten signature verification using hybrid methods of discrete Radon transform, principal component analysis and probabilistic neural network.” Appl. Soft Comput. Vol. 40, 2016. P. 274–282. DOI: https://doi.org/10.1016/j.asoc.2015.11.039.
2. Wróbel, Krzysztof & Doroz, Rafal & Porwik, Piotr & Naruniec, Jacek & Kowalski, Marek. (2017). Using a Probabilistic Neural Network for lip-based biometric verification. Engineering Applications of Artificial Intelligence. 64. 112-127. DOI: https://doi.org/10.1016/j.engappai.2017.06.003.
3. Buchegger, P. Hacking Fingerprint Readers Without Making A Mess. Syss. URL:https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Hacking_Fingerprint_Readers_without_Making_a_Mess.pdf (дата обращения: 25.12.2019).
4. Deng, Y. Keystroke Dynamics Advances for Mobile Devices Using Deep Neural Network Y. Deng, Y. Zhong. Recent Advances in User Authentication Using Keystroke Dynamics Biometrics. 2015. Vol. 2. P. 59–70. DOI: https://doi.org/10.15579/gcsr.vol2.ch4.
5. Rosso OA, Ospina R, Frery AC. Classification and Verification of Handwritten Signatures with Time Causal Information Theory Quantifiers // Journal of Computer Aided Design and Computer Graphics. Vol. 19, No. 3. P.243–301. DOI: https://doi.org/10.1371/journal.pone.0166868.
6. L. Lu and Y. Liu, "Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics," in IEEE Transactions on Computational Social Systems, Vol. 2, No. 3. P. 53–64, Sept. 2015. DOI: https://doi.org/10.1109/TCSS.2016.2517648.
7. L. Zhang, L. Zhang and B. Du, "Deep Learning for Remote Sensing Data: A Technical Tutorial on the State of the Art," in IEEE Geoscience and Remote Sensing Magazine, Vol. 4, No. 2. P. 22–40, June 2016. DOI: https://doi.org/10.1109/MGRS.2016.2540798.
8. Al-Ani, Muzhir. (2015). Signature Recognition Using Discrete Fourier Transform. DOI: https://doi.org/10.13140/RG.2.1.5182.6645.
9. Gao ZK, Yang Y-X, Zhai L-S, Ding M-S, Jin N-D. Characterizing slug to churn flow transition by using multivariate pseudo Wigner distribution and multivariate multiscale entropy. Chemical Engineering Journal. Vol. 291, 2016. P. 74–81. DOI: https://doi.org/10.1016/j.cej.2016.01.039.
10. Rosso, Osvaldo & Olivares, Felipe & Plastino, A. (2015). Noise versus chaos in a causal Fisher-Shannon plane. 1852-4249. 7. DOI: https://doi.org/10.4279/PIP.070006.

11. Jain, A., Singh, S.K. & Singh, K.P. Handwritten signature verification using shallow convolutional neural network. Multimed Tools Appl (2020). DOI: https://doi.org/10.1007/s11042-020-08728-6.
12. Yalin Yin and Xiangdong Zhou "End-to-end online handwriting signature verification", Proc. SPIE 11069, Tenth International Conference on Graphics and Image Processing (ICGIP 2018), 1106921 (6 May 2019). DOI: https://doi.org/10.1117/12.2524447.
13. Alona Levy, Ben Nassi, Yuval Elovici, and Erez Shmueli. 2018. Handwritten Signature Verification Using Wrist-Worn Devices. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 3, Article 119 (September 2018). – 26 p. DOI:https://doi.org/10.1145/3264929.
14. Beltramelli, T., & Risi, S. (2015). Deep-Spying: Spying using Smartwatch and Deep Learning. ArXiv, abs/1512.05616.
15. Kumar, R., Phoha, V.V., & Raina, R. (2016). Authenticating users through their arm movement patterns. ArXiv, abs/1603.02211.

REFERENCES:

[1] Ooi, Shih Yin, Andrew Beng Jin Teoh, Ying-Han Pang and Bee Yan Hiew. “Image-based handwritten signature verification using hybrid methods of discrete Radon transform, principal component analysis and probabilistic neural network.” Appl. Soft Comput. Vol. 40, 2016. P. 274–282. DOI: https://doi.org/10.1016/j.asoc.2015.11.039.
[2] Wróbel, Krzysztof & Doroz, Rafal & Porwik, Piotr & Naruniec, Jacek & Kowalski, Marek. (2017). Using a Probabilistic Neural Network for lip-based biometric verification. Engineering Applications of Artificial Intelligence. 64. 112-127. DOI: https://doi.org/10.1016/j.engappai.2017.06.003.
[3] Buchegger, P. Hacking Fingerprint Readers Without Making A Mess. Syss. URL:https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Hacking_Fingerprint_Readers_without_Making_a_Mess.pdf (accessed: 25.12.2019).
[4] Deng, Y. Keystroke Dynamics Advances for Mobile Devices Using Deep Neural Network Y. Deng, Y. Zhong. Recent Advances in User Authentication Using Keystroke Dynamics Biometrics. 2015. Vol. 2. P. 59–70. DOI: https://doi.org/10.15579/gcsr.vol2.ch4.
[5] Rosso OA, Ospina R, Frery AC. Classification and Verification of Handwritten Signatures with Time Causal Information Theory Quantifiers. Journal of Computer Aided Design and Computer Graphics. Vol. 19, No. 3. P.243–301. DOI: https://doi.org/10.1371/journal.pone.0166868.
[6] L. Lu and Y. Liu, "Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics," in IEEE Transactions on Computational Social Systems, Vol. 2, No. 3. P. 53–64, Sept. 2015. DOI: https://doi.org/10.1109/TCSS.2016.2517648.
[7] L. Zhang, L. Zhang and B. Du, "Deep Learning for Remote Sensing Data: A Technical Tutorial on the State of the Art," in IEEE Geoscience and Remote Sensing Magazine, Vol. 4, No. 2. P. 22–40, June 2016. DOI: https://doi.org/10.1109/MGRS.2016.2540798.
[8] Al-Ani, Muzhir. (2015). Signature Recognition Using Discrete Fourier Transform. DOI: https://doi.org/10.13140/RG.2.1.5182.6645.
[9] Gao ZK, Yang Y-X, Zhai L-S, Ding M-S, Jin N-D. Characterizing slug to churn flow transition by using multivariate pseudo Wigner distribution and multivariate multiscale entropy. Chemical Engineering Journal. Vol. 291, 2016. P. 74–81. DOI: https://doi.org/10.1016/j.cej.2016.01.039.
[10] Rosso, Osvaldo & Olivares, Felipe & Plastino, A. (2015). Noise versus chaos in a causal Fisher-Shannon plane. 1852-4249. 7. DOI: https://doi.org/10.4279/PIP.070006.
[11] Jain, A., Singh, S.K. & Singh, K.P. Handwritten signature verification using shallow convolutional neural network. Multimed Tools Appl (2020). DOI: https://doi.org/10.1007/s11042-020-08728-6.
[12] Yalin Yin and Xiangdong Zhou "End-to-end online handwriting signature verification", Proc. SPIE 11069, Tenth International Conference on Graphics and Image Processing (ICGIP 2018), 1106921 (6 May 2019). DOI: https://doi.org/10.1117/12.2524447.
[13] Alona Levy, Ben Nassi, Yuval Elovici, and Erez Shmueli. 2018. Handwritten Signature Verification Using Wrist-Worn Devices. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 3, Article 119 (September 2018). – 26 p. DOI:https://doi.org/10.1145/3264929.
[14] Beltramelli, T., & Risi, S. (2015). Deep-Spying: Spying using Smartwatch and Deep Learning. ArXiv, abs/1512.05616.
[15] Kumar, R., Phoha, V.V., & Raina, R. (2016). Authenticating users through their arm movement patterns. ArXiv, abs/1603.02211.

Поступила в редакцию – 09апреля 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – April 09, 2020. The final version – May 25, 2020.

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

ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ ФУНКЦИЙ

DOI: http://dx.doi.org/10.26583/bit.2020.2.07

Аннотация. Объективная оценка уровня защиты информационной системы (ИС) организации, обеспечиваемой соответствующей системой информационной безопасности (ИБ), как на этапе ее проектирования, так и на этапе эксплуатации, возможна на основе использования оценок текущих и прогнозируемых вероятностей компьютерных атак нарушителей на данную ИС, использующих уязвимости системы ИБ. В статье для оценивания вероятности компьютерной атаки нарушителя предложено использовать функцию ожидаемой полезности, учитывающую ключевые факторы возможности проведения компьютерной атаки (критерии выбора объекта компьютерной атаки нарушителем, этапы и методы реализации атаки, методы получения информации об объекте, навыки нарушителя) и ожидаемую полезность атаки (мотивы нарушителя, состояние нарушителя до компьютерной атаки, в частности, его доход, принципы принятия решения о проведении/продолжении/прекращении компьютерной атаки нарушителем), модернизированную с учетом особенностей данного типа и преступлений в компьютерной сфере. Предложенное решение базируется на теории положений по криминологии, утверждающей, что атака реализуется нарушителем в тех случаях, когда имеется возможность реализации атаки и, одновременно, ожидаемая полезность атаки с точки зрения нарушителя оказывается достаточной. Продемонстрировано, что выбранная функция полезности адекватно описывает связь между вероятностью компьютерной атаки и ключевыми факторами компьютерной атаки. Проведен анализ модернизированной функции полезности, результаты которого показали, что: 1) значение ожидаемой полезности, при прочих равных условиях, для нарушителя, склонного к риску, определяется вероятностью его разоблачения, равной единице минус вероятность проведения незаметной компьютерной атаки, для нарушителя, не склонного к риску, – тяжестью наказания, поэтому необходимо выстраивать дифференцированную систему защиты в зависимости от типа нарушителя; 2) существует возможность значительного сокращения числа потенциальных нарушителей за счет увеличении доходов от легальной деятельности специалистов в области ИБ; 3) существует зависимость количества компьютерных атак за определенный период времени от вероятности проведения незаметной компьютерной атаки, тяжести наказания, наличия и величины альтернативных доходов (выгод).

Ключевые слова: информационная система, информационная безопасность, компьютерная атака, нарушитель, вероятность компьютерной атаки, функция ожидаемой полезности, ключевые факторы компьютерной атаки, теория положений по криминологии.
Для цитирования: МАКАРОВА, Ольга С.; ПОРШНЕВ, Сергей В. ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ ФУНКЦИЙ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 86-96, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1273>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.07.

Olga S. Makarova[1], Sergey V. Porshnev[1,2]
[1]Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B.N. Yeltsin", 19 Mira Str., Ekaterinburg, 620002, Russia
[2]Institute of mathematics and mechanics of the Ural branch of the Russian Academy of Sciences, Sophia Kovalevskaya Str., 16, Ekaterinburg, 620108, Russia

[1]*e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702*
[2]*e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350*

Assessment of probabilities of computer attacks based on function

DOI: http://dx.doi.org /10.26583/bit.2020.2.07

Abstract. An objective assessment of the level of protection of an organization's information system provided by an appropriate information security system (ISS), both at the stage of its design and at the operation stage, is possible based on the use of estimates of current and predicted probabilities of computer attacks of intruder of this IS using vulnerabilities ISS. To assess the probability of a computer attack by an intruder, this study proposes to use the expected utility function that takes into account key attack criteria of the possibility of a computer attack (criteria for choosing an object of a computer attack by an intruder, stages and methods of implementing an attack, methods of obtaining information about an object, skills of an intruder) and the expected usefulness of the attack (motives the offender, the state of the offender before a computer attack, in particular, his income, the principles for deciding on the conduct / continuation / termination of a computer attack intruder), modernized taking into account the characteristics of this type and crimes in the computer sphere. The proposed solution is based on the theory of provisions in criminology, which states that an attack is implemented by an intruder in cases where it is possible to implement an attack and, at the same time, the expected utility of the attack from the point of view of the offender is sufficient. It is demonstrated that the selected utility function adequately describes the relationship between the probability of a computer attack and the key attack criteria of a computer attack. The analysis of the modernized utility function, the results of which showed that: 1) the value of the expected utility, ceteris paribus, for the offender prone to risk, is determined by the probability of exposing it (which is equivalent to the likelihood of an inconspicuous computer attack), for the offender not prone to risk, – the severity of the punishment, therefore it is necessary to build a differentiated protection system depending on the type of intruder; 2) there is the possibility of a significant reduction in the number of potential violators by increasing revenues from the legal activities of security experts; 3) there is a dependence of the number of computer attacks for a certain period of time on the probability of an inconspicuous computer attack, the severity of the punishment, the presence and magnitude of alternative income (benefits).

Keywords: information system, information security, computer attack, intruder, probability of threats, expected utility, computer attack, expected utility function, key attack criteria of computer attack, criminology theory.

For citation: MAKAROVA, Olga S.; PORSHNEV, Sergey V. Assessment of probabilities of computer attacks based on function. IT Security (Russia), [S.l.], v. 27, n. 2, p. 86-96, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1273>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.07.

Введение

Анализ современных методов построения систем информационной безопасности (ИБ) и научных исследований в данной области, в том числе по расчету вероятности угроз [1], выявлению новых и/или существующих уязвимостей, используемых злоумышленниками [2, 3] по оценке прогнозирования уязвимостей ИБ [4], вероятностей угроз и векторов атак [5] позволяют сделать обоснованный вывод об отсутствии единого метода прогнозирования наиболее вероятных векторов атак [4]. Данный вывод, в том числе, подтверждается результатами соревнований по кибербезопасности между командами атакующих, защитников и специалистов в области мониторинга ИБ,

свидетельствующими об отсутствии сегодня системных подходов, обеспечивающих существенное сокращение числа результативных атак на организации[1,2].

Анализ ограничений классических подходов к построению системы ИБ, подробно описан в [5, 6], где также предложена методика динамического оценивания вероятности угроз ИБ с позиции нарушителя, основанная на использовании метода анализа иерархий (МАИ) с динамическими приоритетами и предпочтениями [8]. Выбор данного метода обоснован тем, что он позволяет:

– отказаться от учета ограниченного набора требований к системам ИБ, используемого в классических подходах построения систем ИБ;

– рассматривать вероятность реализации угрозы с точки зрения нарушителя;

– проводить динамическую оценку вероятностей реализации угроз ИБ.

В свою очередь, подходу, предложенному в [8], присущ известный ряд недостатков, обусловленных тем, что выбранный подход базируется на методе экспертных оценок, а также оказывается сложно реализуемым при большом перечне атак, устранить которые, потенциально, возможно за счет использования соответствующей функции, описывающей зависимость вероятности атаки от ключевых факторов, учитываемых при прогнозировании вектора возможных атак на систему ИБ организации.

В статье изложены научные обоснования выбора данной функции и описана методика оценки ее параметров.

1. Обоснование выбора функции, описывающей зависимость вероятности атаки на систему информационной безопасности организации от ключевых факторов атаки

Ключевые факторы, которые должны учитываться при прогнозировании вектора возможных атак на систему ИБ организации, определены в [6, 7]. К ним отнесены факторы, характеризующие нарушителя, в том числе:

– мотивы нарушителя;

– критерии выбора объекта атаки нарушителем;

– этапы и методы реализации атаки;

– методы получения информации об объекте;

– принципы принятие решения о проведении/продолжении/прекращении атаки нарушителем;

– тип, характер и навыки нарушителя;

– а также факторы, характеризующие защищаемую информационную систему;

– перечень компонентов, архитектуру и используемые настройки системы ИБ защищаемой информационной системы;

– компетенции, как рядовых, так и привилегированных сотрудников организации.

Решение задачи выбора функции, описывающей зависимость вероятности атаки от ключевых факторов атаки на систему ИБ организации, существенно осложняет необходимость одновременного учета большого числа разнородных факторов, от которых оцениваемая вероятность зависит. Здесь представляется целесообразным использовать системный подход, рекомендующий в подобных ситуациях проводить анализ структуры факторов и их группировку. Для формализации функциональных зависимостей между

[1]Кибербитва на PHDays, или Как за 30 часов взломать городскую инфраструктуру. phdays.com URL:https://www.phdays.com/ru/press/news/kiberbitva-na-phdays-ili-kak-za-30-chasov-vzlomat-gorodskuyu-infrastrukturu/ (дата обращения: 27.04.2020).

[2]PHDays: точно в девятку. phdays.com URL:https://www.phdays.com/ru/press/news/phdays-tochno-v-devyatku/ (дата обращения: 27.04.2020).

вероятностью атаки на систему ИБ организации и учитываемыми ключевыми факторами мы обратились к опыту, накопленному в экономической и финансовой сферах [9, 10], а также при предупреждении преступлений общей практики [11].

Экономические подходы к анализу мотивов преступников обоснованы Ч. Беккариа и И. Бентама в теории положений по криминологии [11–13] (ТПК). Ее суть состоит в том, что любой человек, потенциально, может стать нарушителем при выполнении следующих условий:

1) наличия возможности совершения преступления;

2) получения в случае совершения преступления достаточной (с точки зрения нарушителя) полезности.

В ТПК условие совершения преступления сформулирована в виде следующего условия: «если ожидаемая полезность от преступления превышает полезность от иной деятельности, на которое были бы затрачены те же силы и время, то нарушитель совершит преступление». Следовательно, в соответствие с ТПК атака реализуется нарушителем в тех случаях, когда, одновременно, имеется возможность реализации атаки и ожидаемая полезность атаки с точки зрения нарушителя оказывается достаточной. Поэтому вероятность реализации атаки, реализуемой нарушителем, является ни чем иным, как условной вероятностью достаточности ожидаемой полезности атаки при наличии возможности атаки как таковой:

$$\rho\left(\frac{EU}{A}\right) = \frac{\rho(EUA)}{\rho(A)}, \quad (1)$$

где $\rho(A)$ – вероятность наличия возможности реализовать атаку А нарушителем,

$\rho\left(\frac{EU}{A}\right)$ – условная вероятность достаточности ожидаемой полезности атаки для нарушителя, при оценивании которой учитывается возможность провести атаку незаметно.

Таким образом, в соответствие с ТПК, выделенные выше ключевые факторы следует сгруппировать в два фактора атаки:

– возможность атаки, включающая в себя критерии выбора объекта атаки нарушителем, этапы и методы реализации атаки, методы получения информации об объекте, навыки нарушителя;

– ожидаемую полезность атаки, включающую в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении атаки нарушителем.

Далее в статье подробно рассматривается второй фактор атаки – ожидаемая полезность. Формирование, обоснование и примеры вычисления количественных значений вероятностей возможности реализации атаки нарушителем являются предметом дальнейших исследований.

2. Способ оценки ожидаемой полезности атаки на систему информационной безопасности организации

Ожидаемая полезность – это ценность выгоды от атаки, зависящая не от конкретной выгоды, а от дополнительной единицы выгоды. Дополнительная единица выгоды – это выгода нарушителя в единицу времени, полученная им в дополнение к ранее

приобретенной выгоде. В соответствии с законом Госсена[3] [14] полезность от каждой дополнительной единицы выгоды сокращается, так как человек приходит к состоянию насыщения. Далее будем использовать это утверждение, учитывая при этом, что нарушитель является среднестатистическим человеком не склонным к риску.

Отметим, что компьютерные преступления, в отличие от правонарушений, являющихся предметом, изучаемым криминологией, требуют от нарушителя наличия специальных знаний, умений и навыков, а также возможности совершить компьютерную атаку. Для связывания факторов, характеризующих нарушителя, друг с другом можно использовать метод анализа иерархий с динамическими приоритетами и предпочтениями [6, 7].

Таким образом, функция ожидаемой полезности, определенная в ТПК [11–13], модернизированная с учетом описанных выше особенностей компьютерных атак и преступлений в информационной сфере, может быть записана в следующем виде:

$$EU = (1-\rho_n)U(W_m + W_i) + \rho_n U(W_m + W_i - F), \quad (2)$$

где $U(\xi)$ – функция полезности,

ρ_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной атаки $\rho_m = 1-\rho_n$),

W_m – выгода нарушителя в случае успешной реализации компьютерной атаки,

W_i – текущий доход нарушителя от легальной деятельности,

F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте).

В качестве функции полезности $U(\xi)$ в ТПК для нарушителя, не склонного к риску, традиционно, используют классическую функцию, предложенную Бернулли [13]:

$$U(\xi) = b\ln\left(\frac{a+\xi}{a}\right), \quad (3)$$

где a, b – константы.

3. Анализ зависимости ожидаемой полезности от параметров функции

Будем считать, что нарушитель системы ИБ, как любой рациональный человек, стремится максимизировать ожидаемую полезность. Следовательно, в предположении о том, что значения всех за исключением одной переменной c в (2) известны, значение

$$c = \arg\max U(C)$$

есть решение уравнения:

$$\frac{\partial EU(c)}{\partial c} = 0. \quad (4)$$

Для анализа зависимости функции (2) от параметров ρ_n, W_m, F используем эластичность функции, представляющую собой предел отношения относительного изменения значения функции к относительному изменению переменной, когда последнее стремится к нулю [15]:

$$\eta_c^{EU} = \lim_{\Delta c \to 0}\left(\frac{\Delta EU}{EU} : \frac{\Delta c}{c}\right) = \frac{c}{EU}\lim_{\Delta c \to 0}\frac{\Delta EU}{\Delta c} = c\frac{\partial EU/\partial c}{EU},$$

[3]Закон убывающей предельной полезности

Выбор данной характеристики обусловлен тем, что по ее значению можно оценивать степень зависимости вероятности принятия нарушителем решения о проведении атаки от вероятности разоблачения нарушителя ρ_n и тяжести наказания *F*.

Подставляя (2) в (5), находим абсолютную величину эластичности ожидаемой полезности от вероятности разоблачения нарушителя ρ_n:

$$\left|\eta_{\rho_n}^{EU}\right| = \left|\rho_n \frac{\partial EU/\partial \rho_n}{EU}\right| = \left|\frac{U\left(W_m + W_i - F\right) - U\left(W_m + W_i\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|\frac{U\left(W_m + W_i - F\right) - U\left(W_m + W_i\right)}{F}\right| \quad (6)$$

и абсолютную величину эластичности ожидаемой полезности от тяжести наказания:

$$\left|\eta_F^{EU}\right| = \left|F \frac{\partial EU/\partial F}{EU}\right| = \left|\frac{U'\left(W_m + W_i - F\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|U'\left(W_m + W_i - F\right)\right|. \quad (7)$$

Из (6), (7) видно, что $\left|\eta_{\rho_n}^{EU}\right|$, $\left|\eta_F^{EU}\right|$ с точностью до множителя $\left|\rho_n F / EU\right|$ равняются, соответственно, тангенсу угла наклона прямой, соединяющей точки $U\left(W_m + W_i - F\right)$ и $U\left(W_m + W_i\right)$, и тангенсу угла наклона касательной к графику функции $U\left(W_m, W_i, F\right)$ в точке $W_m + W_i - F$. Следовательно, $\left|\eta_{\rho_n}^{EU}\right| > \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) > 0$, т.е. функция возрастает ускоренно, и $\left|\eta_{\rho_n}^{EU}\right| < \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) < 0$, т.е. функция возрастает замедленно.

Из (3) так же видно, что в случае нарушителя, не склонного к риску, эластичность ожидаемой полезности от вероятности разоблачения меньше эластичности ожидаемой полезности от тяжести наказания. Это означает, что для нарушителя, не склонного к риску, тяжесть наказания более существенный сдерживающий фактор, в то время как для нарушителя, склонного к риску, при принятии решения об атаке вероятность наказания более существенна. Отметим, что на практике можно реализовать дифференцированный контроль склонности к риску внутренних нарушителей, являющихся сотрудниками данной организации. Для этого можно использовать одну из известных методик, например, HCR-20 («Historical Clinical Risk»), PCL («Psychopathy Checklist»), имеющей несколько различных модификаций, VRAG («Violence Risk Appraisal Guide») или тест RSK Шуберта [16].

Абсолютные величины эластичности ожидаемой полезности от выгоды нарушителя и эластичности ожидаемой полезности от дохода нарушителя от легальной деятельности вычисляются по соответствующим формулам:

$$\left|\eta_{W_m}^{EU}\right| = \left|W_m \frac{dEU/dW_m}{EU}\right| = \left|W_m \frac{(1-p_n)U'\left(W_m + W_i\right) + p_n U'\left(W_m + W_i - F\right)}{EU}\right|, \quad (8)$$

$$\left|\eta_{W_i}^{EU}\right| = \left|W_i \frac{dEU/dW_i}{EU}\right| = \left|W_i \frac{(1-p_n)U'\left(W_m + W_i\right) + p_n U'\left(W_m + W_i - F\right)}{EU}\right|. \quad (9)$$

Из (8) и (9) видно, что ожидаемая полезность компьютерной атаки будет определяться, в первую очередь, выгодой нарушителя в случае успешной реализации компьютерной атаки W_m, если текущей доход нарушителя от легальной деятельности

меньше выгоды нарушителя от реализации компьютерной атаки, т.е. $W_m > W_i$, то и наоборот. Результаты проведенного анализа подтверждаются доступными статистическими данными [17, 18], анализ которых показал:

– большую часть атак осуществляют преступные кибергрупировки, которые работают длительное время [18], в их легальный доход близок к нулю.

– по данным прокуратуры наибольшее число задержанных за компьютерные атаки нарушителей – это люди со средним образованием или студенты, не имеющие постоянного заработка [17, 18].

В том случае, когда доходы от легальной деятельности нарушителя существенно больше выгоды нарушителя в случае успешной реализации компьютерной атаки $(W_i > W_m)$ влияние тяжести наказания на ожидаемую полезность становится больше, чем выгода от компьютерной атаки. Таким образом, вероятность разоблачения нарушителя ρ_n напрямую влияет на ожидаемую полезность от компьютерной атаки, в то время как выгода нарушителя W_m влияет опосредовано.

Из проведенного анализа можно сделать следующие выводы:

– Значение ожидаемой полезности, при прочих равных условиях, определяется, в первую очередь, вероятностью разоблачения нарушителя (вероятность проведения незаметной атаки) для нарушителя, склонного к риску, и тяжестью наказания, для нарушителя, не склонного к риску. Следовательно, нужно строить дифференцированную систему защиты ИБ в зависимости от типа нарушителя.

– Можно ожидать, что увеличение доходов от легальной деятельности специалистов в области ИБ приведет к значительному сокращению числа нарушителей.

– Количество компьютерных атак за определенный период времени зависит от вероятности проведения незаметной компьютерной атаки, тяжести наказания, наличия и величины альтернативных доходов (выгод).

4. Обоснование возможности описания динамики изменения функции полезности

Обоснования необходимости учета динамки изменения вероятности атаки при оценке эффективности системы ИБ приведены в [6, 7]. Для описания изменения значения выгоды от компьютерной атаки во времени в терминах ТПК можно использовать формулу Эрлиха [19]:

$$W(t) = W_0 + W_m(t_m) + W_i(t_i) - F(t_m), \quad (10)$$

где W_0 – благосостояние нарушителя в начале рассматриваемого периода времени *t*,

$W_m(t_m)$ – выгода нарушителя в случае успешной реализации атаки за период времени *t*,

$W_i(t_i)$ – доход нарушителя от легальной деятельности за период времени *t*,

$F(t_m)$ – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте) за период времени *t*,

t_m – время, потраченное в период времени *t* на подготовку и реализацию атаки,

t_i – время, потраченное в период времени *t* на легальную деятельность.

Период времени *t* в этом случае описывается следующим образом:

$$t = t_m + t_i + t_c, \quad (11)$$

где t_c – время, потраченное в период времени t на потребление (досуг, отдых и т.п.).

Так как ожидаемая полезность (2) зависит от дополнительной единицы выгоды, используя в (2) вместо переменной W_m функцию (10), получаем функцию, описывающую зависимость ожидаемой полезности от времени, максимальное значение которой находится из условия $\frac{dEU(t)}{dt} = 0.$

5. Обоснование выбора источников первичной информации для расчета ожидаемой полезности от киберпреступления

Возможность использования статистической информации для оценки вероятности компьютерной атаки нарушителем обоснована в [6, 7]. При расчете вероятности проведения незаметной компьютерной атаки следует учитывать, что предложенная модель строится с точки зрения нарушителя. При «формировании» ожидаемой полезности нарушитель в первую очередь опирается на свои знания, и, следовательно, на открытые источники информации о правонарушениях. В этой связи для расчета вероятности проведения незаметной компьютерной атаки целесообразно использовать результаты анализа статей новостного агрегатора о количестве громких судебных дел [20], а также статистику Генпрокуратуры РФ [18] о количестве зарегистрированных преступлений и данные ФинЦЕРТ [21, 22] о блокировке фишинговых ресурсов и телефонных номеров.

Оценить вероятность проведения незаметной компьютерной атаки можно по следующей формуле:

$$\rho_m = \frac{A_m - A_{mf}}{A_m}, \qquad (12)$$

где A_m – количество выявленных компьютерных атак данного типа, A_{mf} – количество выявленных компьютерных атак, закончившихся арестом (наказанием преступника).

Отметим, что при оценке рисков международные стандарты рекомендуют учитывать ценность активов организации [1]. Однако нарушитель, в отличие от сотрудников организации, не знает реальной ценности активов, поэтому он может оперировать только предполагаемой величиной и потенциальной величиной выгоды, которую может получить (например, выплата за расшифровку данных после компьютерной атаки с помощью шифровальщика). Следовательно, потерянная ценность актива для организации в ходе успешной компьютерной атаки нарушителем не равна выгоде, получаемой нарушителем.

Нарушитель, выбирая методы и объекты компьютерной атаки, планирует получить определенную выгоду, величину которой, как и настоящую ценность активов атакуемой организации, он не может знать предварительно. Следовательно, на практике в качестве оценки W_m может быть использована средняя выручка нарушителя от рассматриваемого типа атак [6, 7]. Для финансового сектора средние значения выручки за 2017–2018 гг. от наиболее распространенных атак были рассчитаны в [6, 7]. Расчеты для других отраслей и типов компьютерных атак можно провести аналогичным образом.

Компьютерные преступления, в отличие от других правонарушений, требуют от нарушителя наличия специальных навыков, знания методов и наличие возможности совершить компьютерную атаку. Следовательно, наибольшую выгоду от законной деятельности нарушитель получит, работая в сфере информационных технологий и информационной безопасности, поэтому W_i может быть рассчитана как средняя зарплата в сфере информационных технологий и ИБ в регионе проживания нарушителя за

рассматриваемый период. В этой связи, чем выше компетентность нарушителя, тем больше у него может быть заработная плата и, соответственно, тем более эффективная компьютерная атака может быть им реализована. Таким образом, при определении функциональной зависимости дохода от времени, можно предположить, что функциональные зависимости $W_m(t_m)$ и $W_i(t_i)$ будут одинаковыми.

В Уголовном кодексе РФ предусмотрены штрафы за совершение компьютерных атак, а также лишение свободы, поэтому при расчете тяжести наказания в денежном эквиваленте следует учитывать как величину штрафа, так и величину потерь за период времени отбывания наказания, а потери, связанные с отбыванием наказания, можно рассчитывать, как потерю легального и не легального заработка за срок заключения.

Заключение

В статье на основе теории принятия решений, общей практики выявления и предупреждения правонарушений, ИТ-подходов к выявлению уязвимостей предложена и математически обоснована функция, описывающая связь между вероятностью компьютерной атаки и ключевыми факторами атаки. Проведен анализ предложенной функции, результаты которого позволят сделать следующие обоснованные выводы:

– осуществление защиты от компьютерных атак возможно за счет изменения восприятия преступником возможностей (в том числе соотношения между выгодой и потерями) совершения преступления;

– необходимо разрабатывать дифференцированные системы ИБ, уменьшающие вероятности компьютерных атак, наиболее опасных для данной ИС, которые будут являться для нарушителей, адекватно оценивающих риски, возникающие вследствие проводимой атаки, и учитывающих тяжесть наказания за совершаемое им деяние, предусмотренное действующим законодательством РФ, сдерживающим фактором;

– нарушитель, безнаказанно совершивший результативную компьютерную атаку, продолжит в будущем предпринимать попытки реализации компьютерных атак;

– количество компьютерных атак за определенный период времени зависит от вероятности того, что компьютерная атака пройдет не заметно, тяжести наказания, наличия и величины альтернативных доходов (выгод) у нарушителя;

– можно ожидать, что увеличение доходов от легальной деятельности специалистов в области ИБ существенно сократит количество нарушителей.

СПИСОК ЛИТЕРАТУРЫ:

1. Международный стандарт ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 с.
2. J. Stuckman, J. Walden and R. Scandariato, "The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models," in IEEE Transactions on Reliability, Vol. 66, No. 1. P. 17–37, March 2017. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
3. Scandariato R., Walden J., Hovsepyan A., Joosen W. Predicting Vulnerable Software Components via Text Mining. IEEE Transactions on Software Engineering. 2014. Vol. 40, No 10. P. 993–1006. DOI: http://dx.doi.org/10.1109/TSE.2014.2340398
4. Yasasin E., Prester J., Wagner G., Schryen G. Forecasting IT security vulnerabilities – An empirical analysis // Computers and Security. 2020. Vol. 88. DOI: http://dx.doi.org/10.1016/j.cose.2019.101610.
5. Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment. Information. Vol. 9, No 11. 2018. – 18 p. DOI: http://dx.doi.org/10.3390/info9110280.
6. Макарова, Ольга С.; Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.], Т. 27, № 1. С. 6–18, mar. 2020. ISSN 2074-7136.

URL: <https://bit.mephi.ru/index.php/bit/article/view/1248> (дата обращения: 27.04.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
7. Makarova O.S., Porshnev S.V. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information // Доклады конференции.2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01
8. А.В. Андрейчиков, О.Н. Андрейчикова Методы и интеллектуальные системы принятия решений для проведения ФОРСАЙТ-исследований // Cloud of science. 2014. №3. URL: https://cyberleninka.ru/article/n/metody-i-intellektualnye-sistemy-prinyatiya-resheniy-dlya-provedeniya-forsayt-issledovaniy (дата обращения: 27.04.2020).
9. Cody T., Adams S., Beling P.A. A utilitarian approach to adversarial learning in credit card fraud detection. Institute of Electrical and Electronics Engineers Inc. Conference paper «Systems and Information Engineering Design Symposium», 2018. P. 237–242. DOI: http://dx.doi.org/10.1109/SIEDS.2018.8374743.
10. Pasquier R., Goulet J., Smith I.F. Measurement system design for civil infrastructure using expected utility. Elsevier Ltd. Advanced Engineering Informatics. 2017. Vol. 32. P. 40–51. DOI: http://dx.doi.org/10.1016/j.aei.2016.12.002.
11. Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, № 11. P. 1701-1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
12. Becker G.S. The economics of crime // Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (дата обращения: 27.04.2020).
13. Бернулли Д. Опыт новой теории измерения жребия. Теория потребительского поведения и спроса // Вехи экономической мысли. СПб.: Экономическая школа, 1999. Т. 1. С. 11–27.
14. Данилов Н.Н. Курс математической экономики // СПб.: Лань.2016. С. 116–118.
15. Ганичева, А.В. Математические модели и методы оценки событий, ситуаций и процессов // СПб.: Лань. 2017. С. 107–110.
16. Dolan M., Doyle M. Violence risk prediction: Clinical and actuarial measures and the role of the Psychopathy Checklist. The British Journal of Psychiatry. 2000. Vol. 177, No 4. P. 303–311. DOI: http://dx.doi.org/10.1192/bjp.177.4.303.
17. Генпрокуратура составила портрет типичного российского хакера. vedomosti.ru URL:https://www.vedomosti.ru/technology/news/2018/12/11/788967-sostavila/ (дата обращения: 27.04.2020).
18. Киберпреступность и киберконфликты // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия/ (дата обращения: 27.04.2020).
19. Ehrlich I. Participation in illegitimate activities: theoretical and empirical investigation //J. of Publ. Econ. 1973. Vol. 81. No 3. C. 521—565.
20. Потери банков от киберпреступности // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/ Статья: Потери_банков_от_киберпреступности / (дата обращения: 27.04.2020).
21. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2017 – 31.08.2018 // CRB.RU/ URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (дата обращения: 27.04.2020).
22. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году // CRB.RU/ URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (дата обращения: 27.04.2020).

REFERENCES:

[1] International Standard ISO/IEC 27001: 2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p. (in Russian).
[2] J. Stuckman, J. Walden and R. Scandariato, "The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models," in IEEE Transactions on Reliability, Vol. 66, No. 1. P. 17–37, March 2017. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
[3] Scandariato R., Walden J., Hovsepyan A., Joosen W. Predicting Vulnerable Software Components via Text Mining. IEEE Transactions on Software Engineering. 2014. Vol. 40, No 10. P. 993–1006. DOI: http://dx.doi.org/10.1109/TSE.2014.2340398.
[4] Yasasin E., Prester J., Wagner G., Schryen G. Forecasting IT security vulnerabilities – An empirical analysis. Computers and Security. 2020. Vol. 88. DOI: http://dx.doi.org/10.1016/j.cose.2019.101610.
[5] Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment. Information. Vol. 9, No 11. 2018. – 18 p. DOI: http://dx.doi.org/10.3390/info9110280.

[6] Makarova, Olga S.; Porshnev, Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.], Vol. 27, No. 1. P. 6–18, mar. 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1248> (accessed: 27.04.2020). DOI:http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[7] Makarova O.S., Porshnev S.V. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information. Conference paper .2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
[8] Andreichikov A.V., Andreichikova O.N. Methods and intelligent decision-making systems for conducting FORSIGHT research. Electronic journal. Cloud of Science. 2014. №3. URL: https://cyberleninka.ru/article/n/metody-i-intellektualnye-sistemy-prinyatiya-resheniy-dlya-provedeniya-forsayt-issledovaniy (accessed: 27.04.2020) (in Russian).
[9] Cody T., Adams S., Beling P.A. A utilitarian approach to adversarial learning in credit card fraud detection. Institute of Electrical and Electronics Engineers Inc. Conference paper «Systems and Information Engineering Design Symposium», 2018. P. 237–242. DOI: http://dx.doi.org/10.1109/SIEDS.2018.8374743.
[10] Pasquier R., Goulet J., Smith I.F. Measurement system design for civil infrastructure using expected utility. Elsevier Ltd. Advanced Engineering Informatics. 2017. Vol. 32. P. 40–51. DOI: http://dx.doi.org/10.1016/j.aei.2016.12.002.
[11] Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, № 11. P. 1701-1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
[12] Becker G.S. The economics of crime. Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (accessed: 27.04.2020).
[13] Bernoulli D. Experience of a new theory of measurement of lots. Theory of consumer behavior and demand. Milestones of economic thought. SPb.: School of Economics. 1999. Vol. 1, P.11–27.
[14] Danilov N.N. The course of mathematical economics. St. Petersburg: Lan. 2016. P. 116–118.
[15] Ganicheva, A.V. Mathematical models and methods for assessing events, situations and processes. St. Petersburg: Lan. 2017. P. 107–110.
[16] Dolan M., Doyle M. Violence risk prediction: Clinical and actuarial measures and the role of the Psychopathy Checklist. The British Journal of Psychiatry. 2000. Vol. 177, No 4. P. 303–311. DOI: http://dx.doi.org/10.1192/bjp.177.4.303.
[17] The Prosecutor General's Office compiled a portrait of a typical Russian hacker vedomosti.ru URL:https://www.vedomosti.ru/technology/news/2018/12/11/788967-sostavila/ (accessed: 27.04.2020) (in Russian).
[18] Cybercrime and cyberconflicts. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Cybercrime_and_kiberconflicts_:_Russia/ (accessed: 27.04.2020) (in Russian).
[19] Ehrlich I. Participation in illegitimate activities: theoretical and empirical investigation. J. of Publ. Econ. 1973. Vol. 81. No 3. P. 521—565.
[20] Losses of banks from cybercrime. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Losses_of_banks_from cybercrime (accessed: 27.04.2020) (in Russian).
[21] Report of the Center for Monitoring and Response to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia 1.09.2017 – 08.31.2018. CRB.RU. URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (accessed: 27.04.2020) (in Russian).
[22] Overview of the main types of computer attacks in the financial sector in 2018. CRB.RU. URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (accessed: 27.04.2020) (in Russian).

Поступила в редакцию – 27 апреля 2020 г. Окончательный вариант – 25 мая 2020 г
Received – April 27, 2020. The final version – May 25, 2020.

Ян А. Сухих[1], Дмитрий И. Правиков[2], Алексей А. Кузичкин[3]
[1]«Ростелеком-Солар»,
Никитский пер. 7, стр. 1, Москва, 125009, Российская Федерация
[2]РГУ нефти и газа (НИУ) имени И.М. Губкина,
Ленинский пр-кт, 65, корп. 1, Москва, 119991, Российская Федерация
«Шнейдер Электрик Центр Инноваций»,
ул. Университетская, 7, Иннополис, 420500, Российская Федерация
[1]e-mail: y.sukhikh@rt-solar.ru, https://orcid.org/0000-0002-0273-023X
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: ansabanyr13@yandex.ru, https://orcid.org/0000-0001-5315-4466

РАЗРАБОТКА ЗАЩИЩЕННЫХ АРХИТЕКТУР АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

DOI: http://dx.doi.org /10.26583/bit.2020.2.08

Аннотация. В настоящее время основным документом, описывающим требования к созданию систем информационной безопасности АСУ ТП промышленных предприятий, является стандарт МЭК 62443. Вместе с тем, опыт его применения выявил ряд аспектов, не описанных или недостаточно подробно описанных в стандарте, но требующих дополнительной детализации для правильного использования, в частности в статье выделяется этап разработки архитектуры защищенной АСУ ТП. В статье рассмотрена обобщенная методика разработки архитектуры, основанная на концепте «зон и связей», детально рассмотрены этапы инвентаризации, определения зон и связей. В статье отмечается, что ключевым элементом, определяющим устойчивость общей системы защиты, является системы противоаварийной защиты, поэтому их интеграции с системами управления уделено особое внимание, в частности рассмотрено несколько способов интеграции, отмечены их преимущества и недостатки. Приведен ряд практических рекомендаций по реализации предложенной методики.

Ключевые слова: АСУ ТП промышленных предприятий, информационная безопасность, кибербезопасность, архитектура системы защиты АСУ ТП, методика проектирования.
Для цитирования. СУХИХ, Ян А.; ПРАВИКОВ, Дмитрий И.; КУЗИЧКИН, Алексей А. РАЗРАБОТКА ЗАЩИЩЕННЫХ АРХИТЕКТУР АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССАМИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 97-117, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1274>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.08.

Yan A. Sukhikh[1], Dmitry I. Pravikov[2], Alexey A. Kuzichkin[3]
[1]"Rostelecom-Solar",
Nikitsky Lane 7,str. 1, Moscow, 125009, Russia
[2]National University of Oil and Gas "Gubkin Universit",
Leninsky av. 65, bd. 1, Moscow, 119991, Russia
[3]"Schneider Electric Innovation Center",
Universitetskaya Str., 7, Innopolis, 420500, Russia
[1]e-mail: y.sukhikh@rt-solar.ru, https://orcid.org/0000-0002-0273-023X
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: ansabanyr13@yandex.ru, https://orcid.org/0000-0001-5315-4466

Development of secure architectures for process control systems

DOI: http://dx.doi.org /10.26583/bit.2020.2.08

Abstract. The IEC 62443 standard is the main document describing the requirements for building secure industrial control systems. However, a number of aspects are not properly described or not sufficiently detailed in the standard, and require additional detail for a proper implementation. In particular, the paper highlights main stages of secure industrial control systems architecture development. Secure architecture

development approach is based on the “zones and conduits” concept and includes detailed description of inventory stage and zones and conduits determination. Considering that emergency shutdown systems (safety systems) are the key element preventing assets from major accidents, special attention is paid to its integration with control systems. Several integration methods are described with its advantages and disadvantages noted. Recommendations for the practical implementation of the proposed methodology are given.
Keywords: ICS/SCADA, information security, cybersecurity, secure ICS/SCADA architecture, design methodology.
For citation: SUKHIKH, Yan A.; PRAVIKOV, Dmitry I.; KUZICHKIN, Alexey A. Development of secure architectures for process control systems. IT Security (Russia), [S.l.], v. 27, n. 2, p. 97-117, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1274>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.08.

Введение

Данная работа посвящена кибербезопасности автоматизированных систем управления технологическим процессом (АСУ ТП). Вопрос защиты промышленных систем управления от киберугроз стал особенно актуальным с началом четвертой промышленной революции (Industry 4.0), когда с целью оптимизации и повышения эффективности производств, промышленные системы управления начали массово подключать к корпоративным информационным системам и глобальной сети Internet.

При построении защищённых промышленных систем управления необходимо учитывать два главных фактора: говорить о кибербезопасности необходимо в контексте комплексной безопасности промышленного предприятия и необходимо выдерживать баланс между безопасностью и удобством использования системы / ее стоимостью. В коммерческом секторе задачи бизнеса всегда имеют высочайший приоритет и важно, чтобы кибербезопасность не стала блокирующим фактором развития бизнеса, она должна стать помощником – помогать бизнесу безопасно внедрять современные цифровые технологии.

Активное внедрение АСУ для управления технологическими процессами в различных отраслях промышленности не только повысило эффективность производства [1], но и породило ряд проблем, в первую очередь связанных с обеспечением информационной безопасности [2]. Указанные проблемы отражены не только в научной литературе, но и в отчетах ведущих компаний, специализирующихся в области информационной безопасности[1]. Показателем значимости угроз кибербезопасности для промышленности является то, что согласно исследованию аналитиков, подготовивших отчет Международного Экономического Форума “The Global Risk Report 2019” by World Economic Forum[2], они вошли в TOP-5 наиболее ожидаемых рисков, с которыми компании могут столкнуться.

Для снижения уровня указанных рисков в промышленно развитых странах активно развиваются как средства обеспечения информационной безопасности АСУ ТП, так и организационно-технические решения. При этом вопросы построения системы защиты и применения указанных средств и решений регламентируются целым рядом нормативных актов, в том числе отраженные в ряде стандартов. Краткий обзор рассматриваемых документов приведен в [3].

[1]Threat landscape for industrial automation systems, H1 2019. URL: https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения: 01.04.2020).
[2]The Global Risks Report 2019. URL: https://www.weforum.org/reports/the-global-risks-report-2019 (дата обращения: 01.04.2020).

В Российской Федерации указанную систему образует Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и целый ряд подзаконных нормативных актов, среди которых необходимо выделить непосредственно ориентированный на реализацию системы защиты информации критической информационной инфраструктуры Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а также Приказ ФСТЭК России от 14.03.2014 №31 «Об утверждении требований 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».

За рубежом, в первую очередь в США и Западной Европе, в качестве общего рамочного документа используется документ американской организации NIST «Framework for Improving Critical Infrastructure Cybersecurity» [4], а также МЭК 62443 [5] (частично гармонизированный в Российской Федерации – ГОСТ Р 56205-2014) и ISA 62443 – серия стандартов, разработанных двумя группами: ISA99 и IEC TC65/WG10.

Проведенный экспертный сравнительный анализ двух систем нормативных актов показывает их подобие друг другу при реализации технических деталей обеспечения информационной безопасности промышленных предприятий[3]. При этом разница заключается в реализации общей концепции защиты на уровне предприятия, национальных отраслей промышленности или в целом национального производства. По мнению отдельных экспертов, международные стандарты в области кибербезопасности, а также стандарты некоторых западных стран опережают по уровню проработки стандарты, действующие в Российской Федерации. Исходя из того, что стандарт МЭК 62443 принят раньше, в отношении практики его применения накоплен более значительный опыт, позволяющий учесть не только положительные стороны, но и выявить аспекты, вызвавшие трудности при его реализации.

Как показывает практика, несмотря на развитую нормативную базу, существующие средства и методы обеспечения информационной безопасности промышленных предприятий, в ряде случаев не обеспечивают надлежащего уровня защищенности. Недостаток знаний, сложность и/или недостаточный уровень детализации стандартов приводит к тому, что организации не могут создать эффективную систему защиты информации. Как следствие, возникает двуединая задача: а) определить, почему в результате применения действующих стандартов (в частности стандарта МЭК 62443) в ряде случаев не обеспечивается приемлемый уровень информационной безопасности промышленных предприятий; б) предложить пути повышения уровня фактической защищенности современных предприятий.

Для решения указанной задачи предлагается:

– провести анализ наиболее известных стандартов в области обеспечения информационной безопасности АСУ ТП и практики их применения;

– сформировать методики по созданию защищенных систем управления;

– предложить решения по повышению уровня защищенности систем, относящихся к критической информационной инфраструктуре.

[3] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/FSTEC-N31-NERK-NIST-ISA-IEC-rus.pdf

1. Общие проблемы обеспечения кибербезопасности АСУ ТП

В соответствии с экспертным мнением, выраженном, в частности, на конференции Indusrial Cybersecurity[4], кибербезопасность систем промышленной автоматизации «в чистом виде» практически не интересует организаторов бизнеса. Более того, как показал опыт расследования киберинцидентов на промышленных предприятиях в первый момент времени очень трудно отличить изменение поведения управляемого оборудования, произошедшего в результате кибератаки, от сбоя, вызванного износом, отказом оборудования или неквалифицированным действием персонала. В результате рассматривают информационную безопасность в совокупности с функциональной безопасностью промышленных систем и операционными рисками, связанными с работой и обслуживанием этих систем и систем управления. Отсюда появилось понятие комплексной безопасности промышленных систем, включающей в себя функциональную безопасность, операционную (промышленную – в терминах российской нормативной базы) безопасность и кибербезопасность [6]. При этом функциональная и операционная безопасность обеспечиваются своими системами контроля, которые тоже должны отвечать требованиям кибербезопасности.

Как следствие, для обеспечения такой комплексной безопасности привлекаются различные группы специалистов, которым приходится преодолевать ряд субъективных проблем, описанных, в частности, в [7]:

1. Традиционно инженеры АСУ ТП не обладают достаточным количеством знаний в области кибербезопасности, а инженеры информационной безопасности (ИБ) или информационных технологий (ИТ) не понимают потребностей и особенностей АСУ ТП. Для создания надежной и безопасной АСУ ТП и/или для должной адаптации стандартов под конкретную систему, персонал должен обладать экспертными знаниями в ИТ, АСУ ТП и кибербезопасности. При этом подходы специалистов АСУ ТП и специалистов ИБ к решению проблем могут иметь противоположную направленность.

В апреле 2020 года был проведён опрос экспертного сообщества с целью определения размеров системы, для которых использование централизованных средств управления информационной безопасностью становится оправданным. 80% аудитории составляли инженеры и эксперты ИБ, 20% - инженеры АСУ ТП и руководители среднего звена. Разброс результатов получился существенным, что свидетельствует об отсутствии единого мнения у представителей экспертного сообщества. По результатам опроса хотелось бы выделить следующие тренды, иллюстрирующие отличия в подходах:

- Инженеры АСУ ТП менее склонны к использованию централизованных средств управления ИБ. По всем вопросам они проголосовали, что сервисы либо не нужны вообще, либо нужны для очень больших систем. Эти результаты свидетельствуют о нежелании представителей АСУ ТП добавлять новые сервисы в классические АСУ.
- Инженеры ИБ более склонны к использованию централизованных средств управления ИБ и считают оправданным их использование даже для маленьких систем. Скорее всего, это связано с тем, что использование централизованных средств управления ИБ способно существенно сократить трудозатраты на конфигурирование и управление системой, разбор инцидентов и т.д.

Другие сведения по результатам проведенного опроса представлены в приложении 1.

2. Сложность систем и стандартов. Так, рассматриваемый в статье стандарт МЭК 62443 имеет достаточно сложную структуру, а в содержании стандарта много требований,

[4] https://ics.kaspersky.ru/conference-2019/

которые могут трактоваться неоднозначно и не всегда интерпретируются пользователями корректно.

3. Ряд существенных аспектов в нормативных документах ФСТЭК России и рассматриваемых стандартах имеет относительно общий уровень требований. Вместе с тем, как показала практика создания конкретных систем защиты, детализация реализации таких требований может оказать существенное влияние на общий уровень безопасности промышленных систем. В отдельных случаях может сложиться ситуация, когда формальное выполнение требований действующих стандартов не обеспечивает фактической защищенности.

Наиболее существенной проблемой, с которой на наш взгляд столкнулись разработчики систем защиты АСУ ТП промышленных предприятий, является разработка архитектуры защищенной промышленной системы управления. Так, например, в [8] приводится описание архитектуры системы защиты АСУ ТП объекта нефтедобычи, при этом какого-либо обоснования предложенного решения не приведено. Аналогично, в [9] вопросы обоснования архитектуры защиты носят описательный характер. Планирование архитектуры защищенной АСУ ТП, ее основных технологий и решений является первым и наиболее ответственным этапом создания системы. Любые ошибки и недоработки на этом этапе впоследствии могут привести к серьезным недостаткам системы в области кибербезопасности и/или к существенным экономическим потерям на исправление ошибок на уже внедренной системе [10]. При этом качественное выполнение работ на данном этапе поможет не только повысить защищенность информационных систем, но и существенно сократить затраты на внедрение и обслуживание системы защиты информации.

2. Методика разработки архитектуры защищенной АСУ ТП

В качестве основы для разработки архитектуры выбран концепт «зоны и связи» или «зоны и тракты», описанный в МЭК 62443. Концепт «зоны и связи» описывает как различные системы взаимодействуют друг с другом, как и в какой форме информация передается между системами, каковы различия в требованиях к безопасности в различных зонах. Этот концепт изначально ориентирован на системы АСУ ТП, как следствие его удобно использовать для разработки архитектур систем защиты. Дополнительно использован «Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2» [11], разработанный комитетом здравоохранения и безопасности Великобритании и ориентированный на практическое использование МЭК 62443.

3. Инвентаризация

Первым шагом при создании защищенных АСУ ТП должна быть инвентаризация, в рамках которой собирается информация об активах:

– информация о технологических установках и схемы материальных потоков;
– планы расположения оборудования и установок;
– информация об информационных системах и АСУ ТП, поддерживающими работу;
– информация о зависимостях между информационными системами, АСУ ТП и технологическими установками;
– общая информация об информационных системах и АСУ ТП, включая данные о производителе, номера версий общесистемного и прикладного программного обеспечения, год внедрения и другие данные;
– информация о сетях (связях) в соответствии с [12];

– информация о взаимодействии с сервисами третьих поставщиков, включая провайдеров облачных сервисов;

– информация о имеющихся средствах защиты информации;

– информация о существующих политиках и процедурах, принятых в компании.

Данная информация необходима для корректного разделения системы на зоны и при анализе рисков.

Наши исследования показали, что менее 5% промышленных компаний в нашей стране имели достаточный уровень осведомлённости о своих производственных подразделениях и процессах до того, как они попали под действие федерального законодательства – Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон обязал компании собирать и анализировать все данные, относящиеся к критическим информационным системам, что значительно повысило осведомлённость компаний и позволяет им двигаться дальше.

4. Как определить зоны и связи?

После того как информация по активам была собрана и проанализирована можно приступать к разделению системы на зоны и связи. Количество зон, то, как активы будут сгруппированы должно определяться индивидуально для каждого конкретного случая на основе следующих факторов:

– тяжесть последствий в результате аварии и/или останова производства/ предоставления услуги;

– размер, функциональное назначение, зависимости от других систем;

– стандарты и требования регуляторов;

– удобство использования и соображения кибербезопасности;

– географическое положение;

– совокупная стоимость системы.

Обычно зоны включают:

– Зона(-ы) систем управления. Эти зоны обычно включают все базовые системы управления технологическими процессами (БСУ ТП, в терминологии МЭК 62443 – basic process control systems). Обычно одна БСУ ТП эквивалентна одной распределенной системе управления (РСУ), или одной функционально законченной системе с архитектурой человеко-машинного интерфейса (ЧМИ) – ЧМИ/SCADA, но такое разделение не является обязательным правилом. В некоторых случаях БСУ ТП могут включать несколько систем.

– Зона(-ы) систем промышленной безопасности. Эти зоны обычно включают системы противоаварийной защиты (ПАЗ) и другие критичные с точки зрения безопасности производства системы.

– Зона(-ы) систем кибербезопасности. В этих зонах обычно располагаются технические и программные средства, обеспечивающие защиту других зон от киберугроз, например, контроллер домена, сетевые системы обнаружения вторжений, сервер сбора и анализа логов и т.д.

– Зона(-ы) систем управления энергоснабжением. Эти зоны включают в себя системы управления и мониторинга энергоснабжением.

– Зона(-ы) систем управления производством. К этим зонам рекомендуется относить системы, работающие на уровне выше, чем SCADA / РСУ, и не имеющие прямого влияния на технологический процесс. Это могут быть системы класса Historian

(или центральный (основный), системы оперативного управления производством (MES), аналитические системы, системы усовершенствованного управления технологическими процессами (СУУ ТП / APC), системы класса Intelligence и другие.

– Демилитаризованная(-ые) зона (ДМЗ). В эти зоны должны быть размещены все сервисы, которые обеспечивают коммуникации между зонами, относящимися к АСУ ТП, и корпоративной сетью или другими «недоверенными» зонами.

– Другие зоны. Сюда могут быть включены все остальные внутренние или внешние зоны (например, комплексные системы управления), или зоны, которыми управляют третьи поставщики (облачные сервисы).

Каждый интерфейс, по которому зоны взаимодействуют между собой, должен быть учтен как «связи», например:

– все коммуникационные интерфейсы между зонами внутри АСУ ТП;

– все коммуникации между внутренними и внешними зонами, а также зонами, обслуживаемыми сторонними поставщиками;

– беспроводные коммуникации;

– переносные (USB устройства, переносные HDD, ноутбуки и др.) и другие не сетевые способы передачи цифровой информации;

– для наиболее ответственных систем дополнительно могут быть учтены способы передачи информации, которые могут использоваться при проведении атак по сторонним каналам: окна, системы видеонаблюдения, кабели питания, сетевые кабели, ЭМИ, микрофоны и т.д.

Как «связи» не должны учитываться стандартные унифицированные электрические сигналы, такие как DI – дискретные входы, DO – дискретные выходы и AI, AO – аналоговые входы и выходы.

Пример практической реализации концепции МЭК 62443 «зоны и связи» показан на рис. 1.

Важно отметить, что состав зон может отличать от представленного, в зависимости от корпоративных стандартов, особенностей предприятия и исторически сложившихся практик. В вопросе разделения по зонам нет, и не может быть, жестких правил, а только рекомендации – слишком многое зависит от уникальных особенностей каждого объекта. Например, сервер Historian может располагаться в зоне систем управления или в зоне систем управления производством; системы оперативного управления производством MES часто размещают в зоне управления производством и в корпоративной сети предприятия; системы класса СУУ ТП (APC) во многих случаях целесообразнее разместить в зоне системы управления, а сервисы обновлений размещать в ДМЗ, как, например, сервис обновлений операционных систем и продуктов Microsoft (WSUS), который не работает оффлайн или без подключения с вышестоящими WSUS серверами.

Несмотря на разнообразие возможных вариантов построения архитектур существует свод базовых рекомендаций единых для всех систем:

– Зона систем промышленной безопасности и, в частности, системы ПАЗ — это последний рубеж защиты активов от серьезных аварий и эти системы/зоны должны быть максимально защищены и изолированы в соответствии с концепцией «защита в глубину» [13].

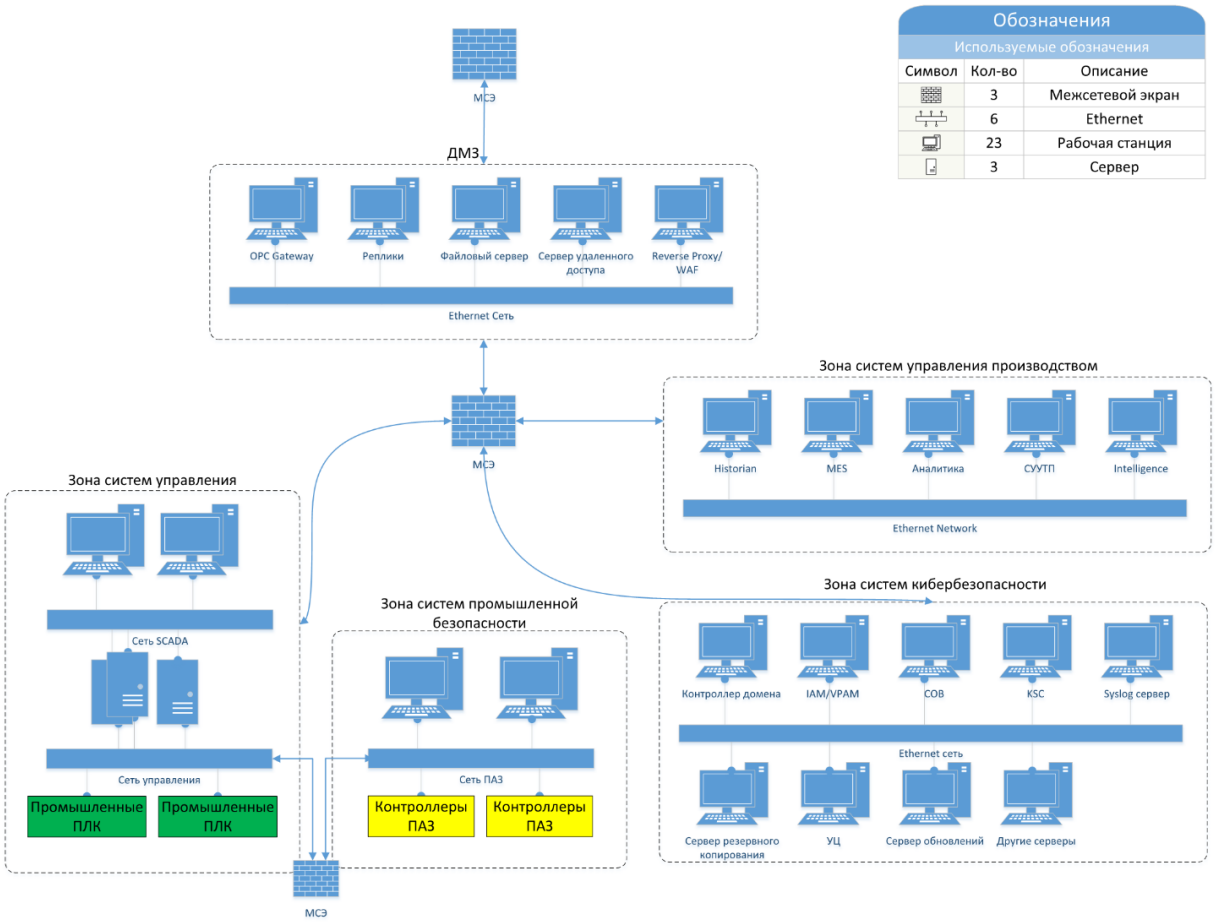


Рис. 1. Пример практической реализации концепции «зоны и связи» стандарта МЭК 62443
(Fig. 1. Example of practical implementation of the IEC 62443 approach, based on «zones and conduits» concept)

– Все системы, которые непосредственно влияют на технологический процесс, но не являются системами ПАЗ, рекомендуется размещать в зоне систем управления.

– Все сервисы, которые поддерживают работу БСУ ТП, но не влияют непосредственно на технологический процесс желательно размещать в зоне систем управления или на вышестоящих уровнях.

– Все коммуникации между зонами должны быть подробно описаны (протоколы, порты, IP-адреса).

– Правила межсетевого экранирования должны быть разработаны с учетом информационных потоков между зонами. По возможности необходимо указывать конкретные хосты и протоколы в правилах и избегать использования подсетей и правил «любой».

– Все коммуникации между зонами, относящимися к БСУ ТП и корпоративной сетью, должны осуществляться через ДМЗ, сквозные коммуникации настоятельно не рекомендуется использовать.

– Разбиение на зоны должно быть выполнено таким образом, что нарушения связи между зонами не должны приводить к немедленному останову технологического

процесса. Технологический процесс должен продолжаться (возможно, в режиме ограниченной функциональности) до восстановления связей между зонами.

– Если возможно, рекомендуется избегать использования зашифрованного трафика между ДМЗ и внутренними доверенными зонами (HTTPS и т. п.). Минимальное использование зашифрованных коммуникаций облегчит задачу по обнаружению злоумышленников, если они уже оказались в промышленной сети.

При определении зон важно учитывать разделение обязанностей сотрудников. При этом необходимо отталкиваться от принципов «необходимо знать» и принципа наименьших привилегий. Например, сотрудник с ролью инженера АСУ ТП, должен обладать правами администратора к средствам АСУ ТП (ПЛК, АРМ, серверы), но этому сотруднику необязательно иметь доступ к средствам кибербезопасности, включая контроллер домена, сервер логов, сетевые системы обнаружения вторжений и т.д. Правило работает и в обратную сторону, сотрудник с ролью инженера/администратора ИБ должен иметь привилегированный доступ к средствами кибербезопасности, но он должен иметь ограниченный доступ к средствам АСУ ТП. Разделение ролей и обязанностей это хорошая возможность повысить общую защищенность системы, но во многих случаях такое разделение подразумевает дополнительные инвестиции в персонал и усложняет процедуры внутри организации. Решение о разделении обязанностей должно приниматься исходя из критичности объекта, организационной структуры компании и компетенций персонала. Пример возможного разделения ролей и прав доступа приведен в табл. 1. При этом один сотрудник может совмещать несколько ролей при наличии достаточных компетенций, таким образом, компания может сэкономить, но одновременно растут угрозы, связанные с возможностями этого сотрудника причинить ущерб компании.

Таблица 1. Пример разделения ролей сотрудников и уровней доступа к зонам

Роль	Доступ к зонам	Права
Инженер АСУ ТП	Зона систем управления, зона систем управления производством, демилитаризованная зона	Полный доступ к компонентам АСУ ТП, ограниченный доступ к общесистемному ПО
Инженер ИБ	Зона систем кибербезопасности, демилитаризованная зона	Уровень доступа администратор с ограничениями к средствам кибербезопасности
Инженер ПАЗ	Зона систем промышленной безопасности	Полный доступ к системам ПАЗ
Администратор ИБ	Зона систем кибербезопасности, демилитаризованная зона	Полный доступ к средствам кибербезопасности
Оператор АСУ ТП	Зона систем управления, зона систем управления производством	Пользовательский уровень доступа

5. Зоны систем промышленной безопасности и их интеграция с системами управления

Как было отмечено выше, программно-технические комплексы, входящие в зону систем промышленной безопасности, являются последним барьером защиты от серьезных аварий на производстве, и интеграция этих систем с системами управления должна осуществляться максимально безопасным способом. Для многих применений лучшим вариантом будет оставить системы ПАЗ изолированными. Независимо от выбранной модели (интегрированная система или изолированная) необходимо соблюдать следующие рекомендации:

– По возможности необходимо избегать объединения в одну сеть независимых систем ПАЗ (или приборных систем безопасности – ПСБ) отвечающих за разные технологические установки. Каждый случай объединения независимых систем ПАЗ должен рассматриваться с учетом рисков комплексной безопасности.

– Если система ПАЗ изолирована, это не означает, что ее не нужно защищать. Переносные медиа устройства, инженерные ноутбуки могут быть источником кибер-угроз. Сотрудники могут (в том числе из лучших побуждений) подключить 3G/4G модемы или использовать персональные Wi-Fi точки для подключения этих систем к сети Интернет (например, чтобы по месту скачать обновление, документацию и т.д.). Если система ПАЗ проектируется как изолированная, должны быть предусмотрены инструменты (желательно автоматизированные), чтобы убедиться, что она остаётся изолированной в любой момент времени.

– При необходимости интеграции ПАЗ с системами управления необходимо выбирать наиболее безопасный способ интеграции, соответствующий корпоративным стандартам и требованиям регуляторов (если таковые имеются).

Существует три основных сценария интеграции ПАЗ с системами управления. Первый сценарий показан на рис. 2 и называется прямая интеграция. В этом случае локальная сеть системы ПАЗ напрямую интегрируется с сетью системы управления по Ethernet. При таком способе интеграции обязательно использование межсетевых экранов (МСЭ) на границе зон. Если использование МСЭ не предусмотрено следует избегать таких сценариев. Правила межсетевого экранирования должны быть сконфигурированы таким образом, чтобы предотвратить любые несанкционированные изменения уставок ПАЗ из системы управления, на случай если последняя была скомпрометирована. В организациях должны быть внедрены должные политики и процедуры позволяющие убедиться, что прошивки межсетевых экранов обновлены, правила настроены, как предписано проектом, и не было попыток несанкционированного изменения конфигурации МСЭ. Плюсом будет наличие у межсетевого экрана способности «понимать» протокол общения между системой ПАЗ и системой управления. В этом случае должен быть настроен функционал глубокого анализа пакетов (deep packet inspection, DPI) с целью блокирования пакетов, имеющих запрещенные команды, например, команды на запись уставок в контроллер ПАЗ.

Некоторые вендоры включают базовый функционал МСЭ в коммуникационные модули контроллеров. Со временем, когда этот функционал будет достаточно развит от использования сторонних МСЭ можно будет отказаться.

Второй сценарий показан на рис. 3 и называется интеграция через промежуточное оборудование. В соответствии с этим сценарием системы ПАЗ подключаются по Ethernet через систему контроллеры системы управления с помощь специальных коммуникационных модулей или выделенных портов.

В большинстве случаев такая архитектура является более безопасной по сравнению с прямой интеграцией, так как чтобы добраться до ПАЗ злоумышленнику нужно получить полный доступ к контроллерам системы управления. Необходимо внимательно изучить технологию работы коммуникационного модуля, в некоторых системах коммуникационные модули работают в прозрачном режиме и предоставляют прямой доступ из сети управления к нижестоящим устройствам. В таком случае использование дополнительных мер защиты (межсетевые экраны) обязательно.

Если коммуникационные модули контроллеров сети управления и/или контроллера системы ПАЗ имеют встроенный развитый функционал межсетевого экранирования, то использование сторонних межсетевых экранов не требуется.

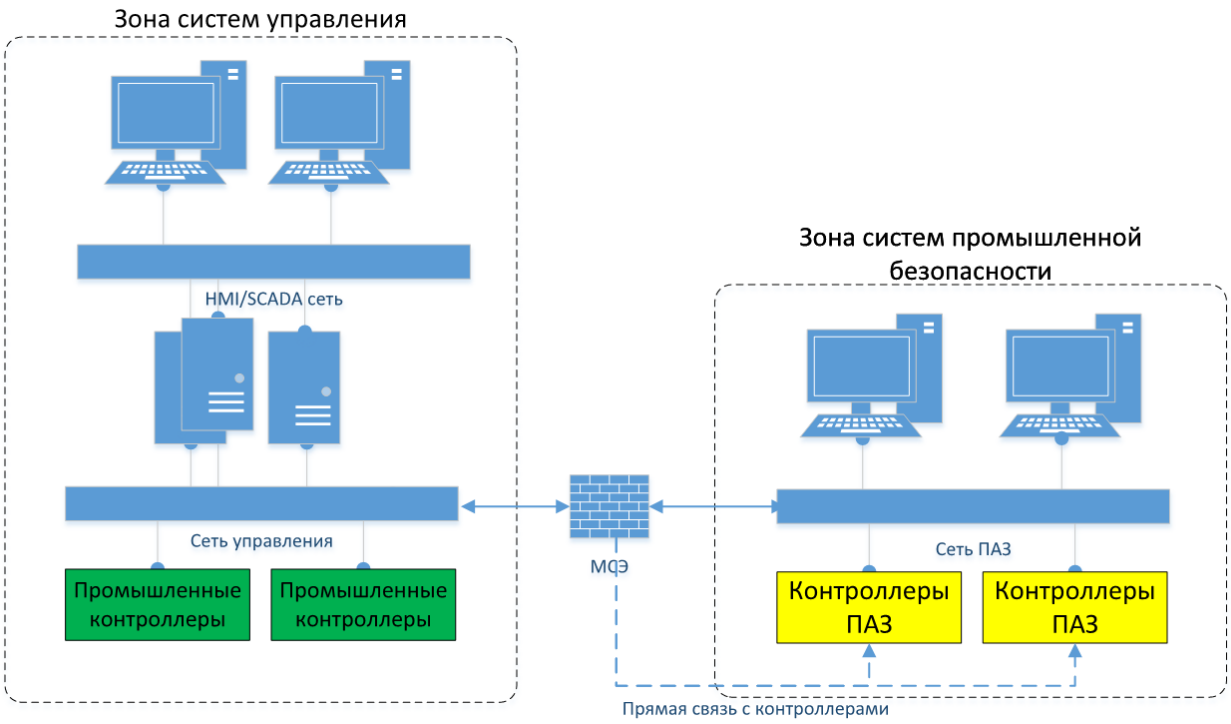


Рис. 2. Пример интеграции системы ПАЗ с системой управления. Прямая интеграция (Fig. 2. Example of integration of an emergency shutdown system with a control system. Direct integration)

Третий сценарий представляет собой наиболее безопасный способ интеграции по сравнению с остальными. В этом сценарии система ПАЗ интегрируется с системой управления по последовательным интерфейсам (чаще всего по RS-485). Пример такого подключения показан на рис. 4.

При использовании такого метода подключения нет необходимости в дополнительных средствах защиты, само по себе использование последовательных интерфейсов значительно снижает риск успешной атаки на систему ПАЗ даже при взломанной системе управления.

Важно отметить, что для обеспечения максимальной защиты контроллеры ПАЗ должны иметь функцию отключения записи уставок ПАЗ через последовательный интерфейс, иначе остается легальная возможность изменения уставок ПАЗ через систему управления, чем могут воспользоваться атакующие. Если все сделано корректно и на контроллере активирована данная функция, то остаются только теоретические шансы на взлом системы ПАЗ по сети. Авторам не удалось найти ни одного упоминания успешных атак, соответствующих описанному сценарию, проведенных в лабораторных или реальных условиях.

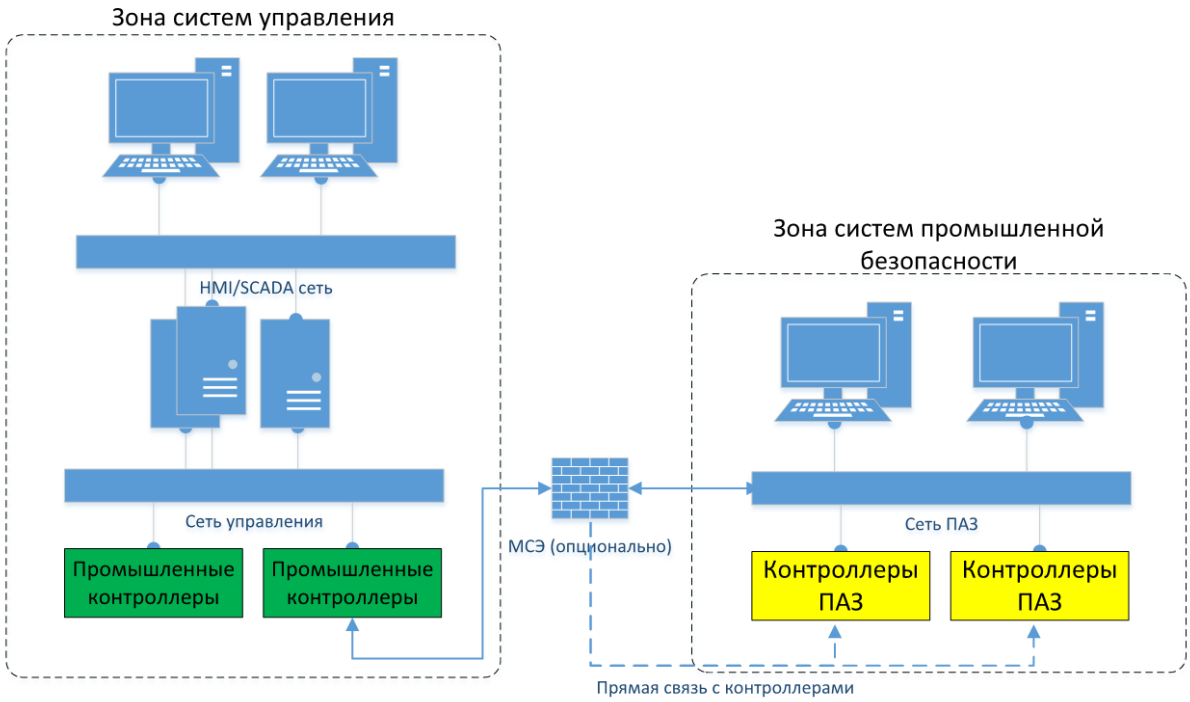


Рис. 3. Пример интеграции системы ПАЗ с системой управления. Интеграция через промежуточное оборудование
(Fig. 3. Example of integration of an emergency shutdown system with a control system. Indirect integration)

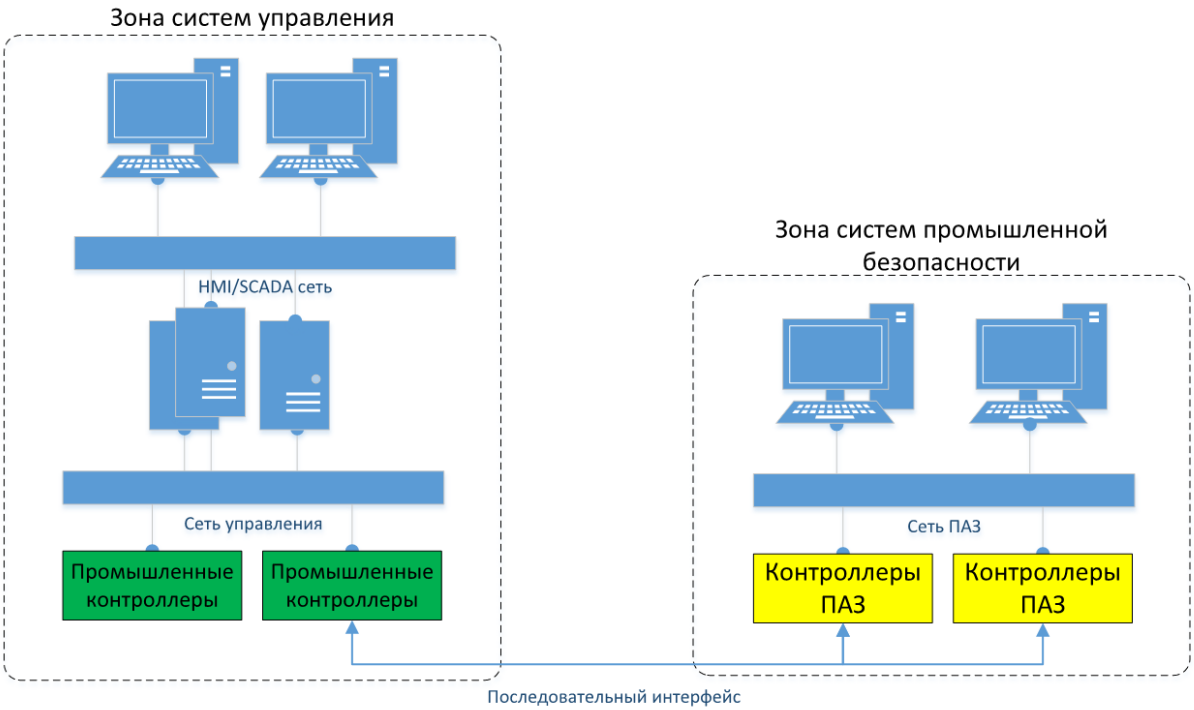


Рис. 4. Пример интеграции системы ПАЗ с системой управления. Интеграция по последовательному интерфейсу
(Fig. 4. Example of integration of an emergency shutdown system with a control system. Integration via serial interfaces)

6. Приоритезация активов и средств защиты

После разработки архитектуры защищенной промышленной системы управления необходимо расставить приоритеты по защите активов и использованию средств защиты информации. Эту процедуру, а также количественную оценку защищенности промышленных систем управления предприятиям, можно выполнить, используя оценку рисков в парадигме комплексной безопасности промышленных систем, которые не рассматриваются в данной статье.

7. Внедрение мер защиты информации

Меры по защите информации в промышленных системах управления обычно включают [14]:

– Построение ДМЗ.
– Безопасная настройка (харденинг) контроллеров и промышленного сетевого оборудования.
– Безопасная настройка рабочих станций и серверов.
– Установка и настройка систем защиты конечных узлов на рабочих станциях и серверах.
– Внедрение средств централизованного управления средствами кибербезопасности.
– Внедрение сетевых систем обнаружения вторжений (сетевые СОВ).
– Установка и настройка межсетевых экранов.

Приведем краткий обзор основных мер по защите информации в промышленных системах управления.

Демилитаризованная зона

Целью создания демилитаризованных зон является обеспечение безопасного способа коммуникации между промышленной системой управления (доверенная зона) и корпоративной сетью и другими зонами, считающимися недоверенными. Это достигается за счет того, что все коммуникации между корпоративной сетью и промышленными системами управления проходят через сервисы, размещенные в ДМЗ [15].

Если ДМЗ построена корректно, то она позволяет скрыть инфраструктуру промышленной сети управления и усложняет задачу злоумышленнику по получению доступа к критичным системам.

Безопасная настройка (харденинг)

Основной задачей безопасной настройки программных и аппаратных средств является уменьшение поверхности атаки. Это означает, что все неиспользуемые службы и сервисы, порты и протоколы, должны быть отключены, сброшены пароли по умолчанию, права и роли учетных записей пользователей настроены в соответствии с их обязанностями по принципу минимальных привилегий. Эти действия уменьшают количество векторов атак и усложняют работу атакующего.

Процесс безопасной настройки зависит от типа промышленной системы управления. Контроллеры, разработанные более 10 лет назад, практически не имеют возможностей по харденингу, в то время как современные средства автоматизации имеют достаточно широкие возможности по обеспечению информационной безопасности. В зависимости от вендора и типа оборудования это могут быть: проверка целостности прошивки, различные уровни доступа к сервисам, возможность отключения неиспользуемых служб и сервисов, белые списки и многое другое. Для повышения уровня защищенности все заложенные разработчиками возможности должны быть правильно использованы при проектировании и пуско-наладке системы автоматизации.

Процесс безопасной настройки распространяется на все оборудование и ПО, входящие в состав промышленной системы управления: активное сетевое оборудование, рабочие станции, серверы, средства ЧМИ, сопутствующие системы и другие. При выполнении работ по безопасной настройке необходимо помнить, что доступность является максимальным приоритетом в промышленных системах управления, поэтому безопасная настройка должна выполняться в соответствии с рекомендациями производителя и/или предварительно тестироваться на стенде.

Защита рабочих станций и серверов

Решения класса защита конечных узлов для рабочих станций и серверов включает:

– Антивирусную защиту (АВЗ).
– Контроль запуска приложений / белые списки.
– Контроль целостности.
– Контроль подключаемых устройств.
– Системы обнаружения вторжений для конечных узлов.
– Другие сервисы (защита от шифровальщиков, контроль Wi-Fi, Bluetooth, и т.д.).

Некоторые вендоры предлагаю эти решения в составе единого продукта, другие – как отдельные сервисы. Выбор конкретных продуктов зависит от имеющихся корпоративных стандартов, рассматриваемых угроз, типа оборудования и общесистемного программного обеспечения, а также рекомендаций вендора.

Централизованные средства управления ИБ

Централизованные средства управления ИБ могут включать в себя:

– Контроллер домена. Используется для централизованного управления учётными данными и политиками Windows.

– Системы централизованного управления антивирусным ПО. Эти сервисы позволяют централизованно управлять системами класс защиты конечных узлов и обновлять базы решающих правил.

– Централизованное средство сбора и хранения логов. Обычно для этих целей используется syslog сервер, который собирает логи со всех устройств в сети.

– Сервер обновлений. Это может быть WSUS или другой сервис, позволяющий централизованно управлять обновлением операционной системы.

– Другие сервисы (сервер резервного копирования, certification authority server и др.).

В небольших системах АСУ ТП управление политиками ОС, конфигурацией систем защиты конечных узлов, учётными данными пользователей и т.д. можно выполнять вручную, что позволяет снизить капитальные затраты на создание защищенной системы.

Для средних и больших АСУ ТП настоятельно рекомендуется использование централизованных средств управления ИБ.

В приложении 1 приведены результаты опроса экспертного сообщества с целью выяснить при каком размере системы использование централизованных средств управления ИБ становится необходимым.

Сетевые системы обнаружения вторжений

Сетевые системы обнаружения вторжений (СОВ) используются для мониторинга трафика в сети с целью выявления вредоносных активностей. Работа сетевых СОВ, как правило, основывается на двух базовых принципах:

– Определение на основе сигнатур.
– Определение на основе аномалий.

Оба метода прекрасно дополняют друг друга. Определение вредоносной активности на основе аномалий хорошо работает при выявлении необычных (нестандартных для этой системы) сетевых взаимодействий (выявление новых устройств, использования новых протоколов или новых коммуникаций между устройствами), которые могут свидетельствовать об атаке на систему. В то же время правила, основанные на сигнатурном методе, могут выявить атаки в легитимном трафике (например, SQL-инъекции, XSS атаки и другие).

Сетевые СОВ с функционалов глубокого сканирования пакетов (DPI) могут обеспечить дополнительный уровень защиты, например, выявлять критические значения параметров (уставок) переданные с АРМ на контроллеры системы управления, неразрешенную команду или другие события, которые могут свидетельствовать о кибер-атаке. Обычно предельные значения уставок/коды команд и другие триггеры, по которым срабатывают СОВ с DPI, устанавливают службы заказчика либо системные интеграторы на основе технологических карт промышленных установок. Этот процесс является крайне трудоемким, поэтому на рынке появились решения, которые могут самостоятельно выявлять отклонения от нормального хода технологического процесса, что существенно сокращает трудозатраты на внедрение систем. Эти системы работают на основе нейронных сетей и/или статистическом анализе данных.

Некоторые сетевые системы обнаружения вторжений могут взаимодействовать с межсетевыми экранами, чтобы «на лету» менять правила межсетевого экранирования при обнаружении атаки с целью ее предотвращения.

Сетевые СОВ важный элемент защиты промышленных систем управления. Они позволяют выявить, а в некоторых случаях и предотвратить, атаки на ранних стадиях, когда эти атаки еще не способны нанести реальный ущерб.

Межсетевые экраны

Межсетевые экраны – это базовый элемент любой архитектуры защищенной АСУ ТП. Весь трафик, который передается между зонами проходит через МСЭ. На уровне межсетевых экранов описываются правила, по которым зоны могут взаимодействовать между собой [16].

Для того что бы правила межсетевого экранирования можно было корректно настроить предварительно должны быть подробно описаны все информационные потоки между зонами. Эту информацию должен предоставить вендор и/или системный интегратор в зависимости от типа системы и того, кто ее внедрял. Как минимум, описание информационных потоков должно содержать:

– Название сервиса и его назначение.

– Протоколы и порты, IP адреса источника и назначения для каждой коммуникации.

– Описание хостов, подсетей, их назначение и адреса.

Эта информация поможет корректно сформировать правила. В дополнение к информации об информационных потоках необходимо следовать лучшим практикам по настройке межсетевых экранов, а именно:

– смена паролей по умолчанию;

– при работе следует избегать использования учетных данных администратора или root пользователя;

– всегда используйте блокирующее по умолчанию правило;

– следует избегать использования опции «любой» в разрешающих правилах. Старайтесь использовать IP адреса конкретных устройств, в крайнем случае адреса подсетей;
– создавайте правила максимально короткими и понятными;
– всегда оставляйте комментарии к правилам и документируйте конфигурацию.

Больше информации о лучших практиках по настройке МСЭ приведено в [17].

Заключение

В статье представлено высокоуровневое описание правил построения защищенных АСУ ТП в соответствии с доступными на текущий момент национальными и международными стандартами (в частности NIST “Framework for Improving Critical infrastructure Cybersecurity”, МЭК 62443, “Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2” by HSE UK, №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», включая подзаконные акты), а также опытом практической реализации подобных систем. В работе описаны основные шаги (этапы) разработки архитектуры защищенной АСУ ТП и описаны основные меры по защите информации, которые наиболее востребованы на реальных объектах.

Информация, представленная в статье, аккумулирует и раскрывает требования национальных и международных стандартов. Представленная методология позволяет осознанно подойти к вопросам разработки архитектур защищенных АСУ ТП и в целом повысить защищенность как создаваемых, так и уже внедренных промышленных систем управления.

В статье рассмотрено понятие комплексной безопасности промышленных объектов. На текущий момент теоретические исследования и опыт практической реализации систем защиты показывает, что кибербезопасность промышленных систем нельзя рассматривать в отрыве от функциональной и операционной безопасности. Как следствие, только рассматривая их в комплексе можно получить объективную картину, поэтому при анализе защищенности и проведении анализа киберрисков необходимо оперировать понятием комплексной безопасности.

Приложение 1

Результаты опроса экспертного сообщества о целесообразности использования централизованных средств управления ИБ в зависимости от размеров АСУ ТП

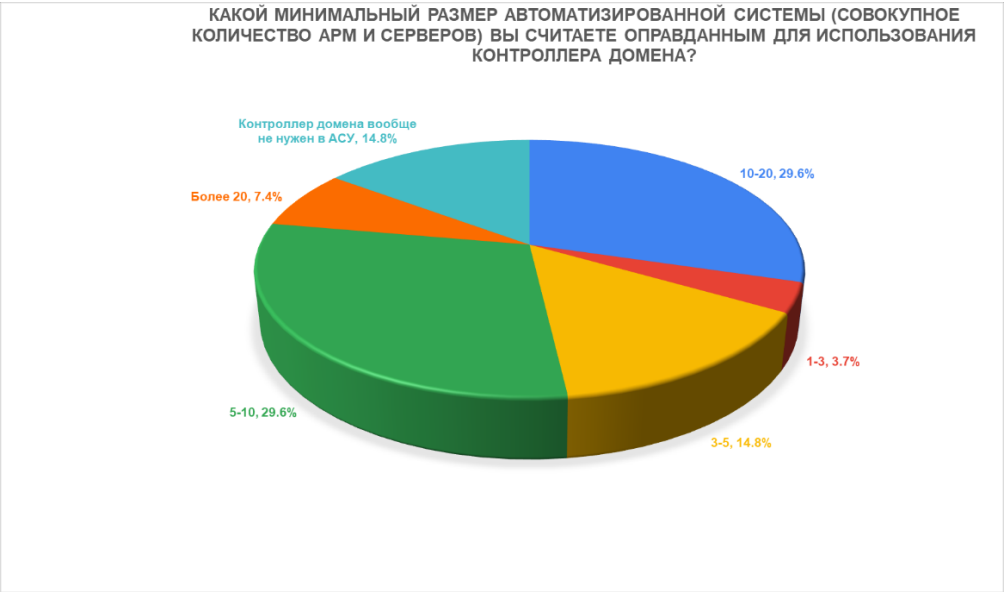


Рис. 1А. Зависимость потребности в контроллере домена от размера системы
(Fig. 1A. A dependency between a control system's size and a need for a domain controller)

Использование контроллера домена одинаковое количество опрощенных считают целесообразным для систем из 5–10 и 10–20 машин (рис. 1А). Учитывая разделение голосов в других группах и наш опыт, предлагаем считать оптимальным для использования контроллера домена системы, в которых количество АРМ и серверов, составляет от 5 до 10 машин.

Рис. 1Б. Зависимость потребности в централизованном управлении АВЗ от размера системы
(Fig. 1B. A dependency between a control system's size and a need for a centralized management of antivirus protection)

Использование централизованного сервера для управления АВЗ большинство считает целесообразным для систем из 5–10 машин (рис. 1Б). Это же количество является медианой. Наша группа разделяет мнение сообщества.

Рис. 1В. Зависимость потребности в выделенном сервере хранения резервных копий от размера системы
(Fig. 1V. A dependency between a control system's size and a need for a dedicated backup storage server)

Использование выделенного сетевого хранилища для резервных копий большинство проголосовавших считает оптимальным для систем из 3–5 и 5–10 машин, при этом большая группа экспертов отдала голоса за 1–3 и 10–20 машин (рис. 1В). Следовательно, использование выделенного хранилища будет целесообразно для систем из 1–5 машин в зависимости от принятых процессов и условий эксплуатации. Медианой и оптимальным выбором для большинства компаний станет использование выделенных сетевых хранилищ для систем из 3–5 машин.

Рис. 1Г. Зависимость потребности в централизованном управлении средствами резервного копирования от размера системы
(Fig. 1G. A dependency between a control system's size and a need for a centralized backup management system)

Необходимость использования централизованного управления средствами резервного копирования большинство проголосовавших признали для систем из 10–20 машин, это же количество является медианой.

Рис. 1Д. Зависимость потребности в централизованном сервере хранения и обработки логов от размера системы
(Fig. 1D. A dependency between a control system's size and a need for a centralized server for storing and processing logs)

Экспертное сообщество разделилось во мнениях по поводу размера систем, для которых следует использовать выделенный сервер Syslog. Медианой являются системы из 10–20 узлов (под узлами подразумеваются не только АРМ и сервера, но и контроллеры, и сетевое оборудование). Наше мнение совпадает с оговоркой, что при использовании Open Source syslog сервера совместно с ОС Linux на виртуальных машинах, использование такого решения экономически целесообразно и для небольших систем из 5–10 узлов.

СПИСОК ЛИТЕРАТУРЫ:

1. Банников Е.В. Использование ПЛК в промышленности. // International scientific review. 2019. URL: https://cyberleninka.ru/article/n/ispolzovanie-plk-v-promyshlennosti (дата обращения: 01.04.2020).
2. Андреев Ю. С., Дергачев А. М., Жаров Ф. А., Садырин Д. С. Информационная безопасность автоматизированных систем управления технологическими процессами. // Известия высших учебных заведений. Приборостроение. 2019. Т. 62, № 4. С. 331–336. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezo-pasnost-avtomatizirovannyh-sistem-upravleniya-tehnologicheskimi-protsessami (дата обращения: 01.04.2020).
3. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции). // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 66–74. URL: http://www.info-secur.ru/is_30/is418_66-74.pdf (дата обращения: 01.04.2020).
4. National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1 April 16, 2018. URL: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (дата обращения: 01.04.2020).
5. Серия стандартов IEC 62443. URL: https://www.isa.org/ (дата обращения: 01.04.2020).
6. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП. // Вопросы кибербезопасности. 2015. № 2 (10). С. 56–59. URL: https://cyberleninka.ru/article/n/missiotsentricheskiy-podhod-k-kiberbezopasnosti-asu-tp (дата обращения: 01.04.2020).

7. Yuri Bobbert, Anderson Domingues Pereira da Silva. Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems. Sci J Research & Rev. 2(3): 2019. SJRR.MS.ID.000536. DOI: https://doi.org/10.33552/SJRR.2019.02.000536.
8. Слинин А.В. Моделирование АСУ ТП объекта нефтедобычи в контексте управления рисками ИБ. // Молодежный Вестник УГАТУ. 2019. № 1 (20). С. 170–173. URL: https://www.elibrary.ru/item.asp?id=41122584 (дата обращения: 01.04.2020).
9. Пакулин М.А. Концепция сетевой безопасности в автоматизированных системах управления технологическим процессом (АСУ ТП) // Сборник трудов X международной научно-практической конференции молодых ученых «Программная инженерия и компьютерная техника (Майоровские чтения)». 2019. С. 103–105. URL: http://micsecs.org/media/MICSECS_RUS_2018.pdf#page=104 (дата обращения: 01.04.2020).
10. Промыслов В.Г., Семенков К.В., Шумов А.С. Синтез архитектуры кибербезопасности для систем управления атомных электростанций. // Пробл. управл., 2019. № 3. С. 61–71 URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pu&paperid=1139&option_lang=rus (дата обращения: 01.04.2020).
11. HSE UK, “Cyber Security for Industrial Automation and Control Systems (IACS)” EDITION 2, URL:https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf (дата обращения: 01.04.2020).
12. National Security Agency, “A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)”, Version 1.1, Systems and network Analysis Center, National Security Agency, August 20, 2010, URL: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/a-framework-for-assessing-and-improving-the-security-posture.cfm (дата обращения: 01.04.2020).
13. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016, URL: https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (дата обращения: 01.04.2020).
14. Charles Kim, Electrical Engineering and Computer Science Howard University, "Cyber-Defensive Architecture for Networked Industrial Control Systems". URL:https://www.researchgate.net/publication/312590499_CyberDefensive_Architecture_for_Networked_Industrial_Control_Systems (дата обращения: 01.04.2020).
15. RE Mahan, JR Burnette, JD Fluckiger, CA Goranson, SL Clements, H Kirkham, C Tews, Pacific Northwest National Laboratory, "Secure Data Transfer Guidance for Industrial Control and SCADA Systems", September 201. DOI: https://doi.org/10.2172/1030885.
16. British Columbia Institute of Technology (BCIT), “Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks (Prepared for National Infrastructure Security Coordination Centre)”, National Infrastructure Security Co-ordination Centre (NISCC), February 2005, URL:https://www.energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf (дата обращения: 01.04.2020).
17. Firewall Best Practices by Kevin Beaver, CISSP. URL: https://www.principlelogic.com/docs/Firewall_Best_Practices.pdf (дата обращения: 01.04.2020).

REFERENCES:

[1] Bannikov E.V. Ispolsovanie programmiruemyh logicheskih kontrollerov v promishlennosty. International scientific review. 2019. URL: https://cyberleninka.ru/article/n/ispolzovanie-plk-v-promyshlennosti (accessed: 01.04.2020).
[2] Andreev U.S., Dergachev A.M., Zharov F.A., Sadyrin D.S. Informacionnaya bezopasnost avtomatizirovannyh system upravleniya tehnologicheslimy processamy. Izvestiya vyshikh uchebnyh zavediniy. Priborostroenie. - 2019. Vol. 62, № 4. P. 331–336. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezo-pasnost-avtomatizirovannyh-sistem-upravleniya-tehnologicheskimi-protsessam (accessed: 01.04.2020) (in Russian).
[3] Vasilyev V.I., Kirillova A.D., Kuharev S.N. Kiberbezopasnost avtomatizirovannyh system upravleniya promyshlennih obiektov (sovremennoe sostoyanie, tendencii). Vestnik UrFO. Bezopasnost v informacionnoy sfere. 2018. № 4(30). P. 66–74. URL: http://www.info-secur.ru/is_30/is418_66-74.pdf (accessed: 01.04.2020) (in Russian).
[4] National Institute of Standards and Technology “Framework for Improving Critical Infrastructure Cybersecurity” Version 1.1 April 16, 2018. URL: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (accessed: 01.04.2020).

[5] IEC 62443. URL: https://www.isa.org/ (accessed: 01.04.2020).
[6] Gordeychuk S.V. Mission-centric approach to ICS/SCADA. Cybersecurity in terms of industrial. Voprosy kiberbezopasnosty. 2015. № 2 (10). P. 56–59. URL: https://cyberleninka.ru/article/n/missiotsentricheskiy-podhod-k-kiberbezopasnosti-asu-tp (accessed: 01.04.2020).
[7] Yuri Bobbert, Anderson Domingues Pereira da Silva. Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems. Sci J Research & Rev. 2(3): 2019. SJRR.MS.ID.000536. DOI: https://doi.org/10.33552/SJRR.2019.02.000536.
[8] Slinin A.V. Modelirovanie ICS/SCADA obiekta neftedobichy v kontekste upravlenia riskamy informacionnoy bezopasnosty. Molodezniy Vestnik UGATU. 2019. № 1 (20). P. 170–173. URL: https://www.elibrary.ru/item.asp?id=41122584 (accessed: 01.04.2020) (in Russian).
[9] Pakulin M.A. Koncepcia setevoy bezopasnosty v avtomatizirovannyh systemah upravlenia tehnologicheskym processom (ICS/SCADA). Sbornik trudov X mezdunarodnoy nauchno-prakticheskoy konferencii molodyh uchenyh “Programmnaya inzeneria i komputernaya tehnika (Mayorovskie chtenia)”. 2019. P. 103–105. URL: http://micsecs.org/media/MICSECS_RUS_2018.pdf#page=104 (accessed: 01.04.2020) (in Russian).
[10] Promyslov V.G., Semenkov K.V., Shumov A.S. Sintez arhitectury kiberbezopasnosty dlya system upravlenia atomnyh electrostancii. Probl. Upravl., 2019. № 3. P. 61–71. DOI: http://doi.org/10.25728/pu.2019.3.7. URL: http://mi.mathnet.ru/pu1139 (accessed: 01.04.2020) (in Russian).
[11] HSE UK, “Cyber Security for Industrial Automation and Control Systems (IACS)” EDITION 2, URL:https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf (accessed: 01.04.2020).
[12] National Security Agency, “A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)”, Version 1.1, Systems and network Analysis Center, National Security Agency, August 20, 2010, URL: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/a-framework-for-assessing-and-improving-the-security-posture.cfm (accessed: 01.04.2020).
[13] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016. URL: https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed: 01.04.2020).
[14] Charles Kim, Electrical Engineering and Computer Science Howard University, "Cyber-Defensive Architecture for Networked Industrial Control Systems" URL:https://www.researchgate.net/publication/312590499_CyberDefensive_Architecture_for_Networked_Industrial_Control_Systems (accessed: 01.04.2020).
[15] RE Mahan, JR Burnette, JD Fluckiger, CA Goranson, SL Clements, H Kirkham, C Tews, Pacific Northwest National Laboratory, "Secure Data Transfer Guidance for Industrial Control and SCADA Systems", September 201. DOI: https://doi.org/10.2172/1030885.
[16] British Columbia Institute of Technology (BCIT), “Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks (Prepared for National Infrastructure Security Coordination Centre)”, National Infrastructure Security Co-ordination Centre (NISCC), February 2005, URL:https://www.energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf (accessed: 01.04.2020).
[17] Firewall Best Practices by Kevin Beaver, CISSP.
URL: https://www.principlelogic.com/docs/Firewall_Best_Practices.pdf (accessed: 01.04.2020).

Поступила в редакцию – 11 апреля 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – April 11, 2020. The final version – May 25, 2020.

Денис О. Стасьев
Московский физико-технический институт
(национальный исследовательский университет),
Институтский пер., 9, Долгопрудный, Московская область, 141701, Россия
e-mail: stasev.do@phystech.edu, https://orcid.org/0000-0002-6972-4635

КОНТРОЛЬ ЦЕЛОСТНОСТИ КОМПОНЕНТОВ ВИРТУАЛЬНЫХ МАШИН, СОЗДАННЫХ НА БАЗЕ ГИПЕРВИЗОРА KVM

DOI: http://dx.doi.org /10.26583/bit.2020.2.09

Аннотация. Сегодня виртуализация широко используется для предоставления масштабируемых ресурсов. Поскольку эта технология означает разделение ресурсов с помощью некоторого абстрактного слоя, то размещение и обработка информации различного уровня доступа в таких системах создаёт угрозу безопасности. Для решения этой проблемы необходимо создавать дополнительные системы контроля целостности виртуальной инфраструктуры. Цель работы: выделить компоненты ВМ, созданных на базе гипервизора KVM, для которых необходим контроль целостности, описать существующие способы обеспечения контроля целостности и выбрать наилучший для применения в централизованных системах. Методы исследования: метод правдоподобного рассуждения, системный анализ, формализация. В работе выделены компоненты виртуальных машин, созданных на базе гипервизора KVM, для которых необходим контроль целостности, описаны существующие способы обеспечения контроля целостности. Определен способ для применения в централизованных системах.

Ключевые слова: виртуализация, гипервизор, KVM, виртуальная машина, целостность, контроль целостности, компоненты виртуальных машин, резидентный компонент безопасности.
Для цитирования: СТАСЬЕВ, Денис О. КОНТРОЛЬ ЦЕЛОСТНОСТИ КОМПОНЕНТОВ ВИРТУАЛЬНЫХ МАШИН, СОЗДАННЫХ НА БАЗЕ ГИПЕРВИЗОРА KVM. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 118-131, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1275>. Дата доступа: 08 june 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.09.

Denis O. Stasyev
Moscow Institute of Physics and Technology (National Research University),
Institutsky Lane, 9, Dolgoprudny, Moscow region, 141701, Russia
e-mail: stasev.do@phystech.edu, https://orcid.org/0000-0002-6972-4635

Integrity monitoring of virtual machines components based on the KVM hypervisor

DOI: http://dx.doi.org /10.26583/bit.2020.2.09

Abstract. Today, virtualization is widely used to provide scalable resources. Since this technology means sharing resources using some abstract layer, the placement and processing of information of various access levels in such systems poses a security risk. To solve this problem, it is necessary to create additional systems for monitoring the integrity of the virtual infrastructure. Objective of the article: to isolate the components of VMs created on the basis of the KVM hypervisor for which integrity monitoring is necessary, describe existing methods for ensuring integrity monitoring and choose the best one for use in centralized systems. Research methods are plausible reasoning method, system analysis, formalization. The article identifies the components of virtual machines created on the basis of the KVM hypervisor for which integrity control is required, and existing methods for ensuring integrity control are described. The result of the article was the determination of the best method for use in centralized systems.

Keywords: virtualization, hypervisor, KVM, virtual machine, integrity, integrity control, components of virtual machines.
For citation: STASYEV, Denis O. Integrity monitoring of virtual machines components based on the KVM hypervisor. IT Security (Russia), [S.l.], v. 27, n. 2, p. 118-131, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1275>. Date accessed: 08 june 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.09.

Введение

Виртуализация – это технология, позволяющая скрыть сложность аппаратного обеспечения с помощью создания абстрактного слоя системных ресурсов для программного обеспечения (ПО) рабочей среды [1]. Виртуализация позволяет использовать полную мощность физического компьютера, распределяя его возможности среди множества пользователей, поэтому часто выделяют ещё одну задачу виртуализации – разделение ресурсов.

Исследования в этой области начались более 50 лет назад. Первые технологии и разработки в области виртуализации были реализованы такими компаниями, как IBM (с 1967 года) и VMware (с 1998 года). В [2] сформулированы требования к виртуализации: эффективность, управление ресурсами (владение монитором) и эквивалентность (физической машине), которые остаются актуальными и в настоящий момент.

В настоящее время виртуализация является основой облачных вычислений. Данная технология широко используется для предоставления масштабируемых ресурсов. Например, разработчики различных проектов в промышленности используют виртуализацию с сервисами облачных вычислений для сокращения неактивных аппаратных ресурсов и достижения эффективной эксплуатации систем.

Виртуальная машина (ВМ, VM) – программная система, эмулирующая аппаратное обеспечение некоторой платформы и исполняющая программы для гостевой операционной системы (ОС) (target-платформа – целевая, заданная платформа) на хостовой ОС (host-платформа – платформа владельца, хозяйская) [3] с помощью технологии виртуализации.

Примером использования технологии виртуализации может быть широко известный сервис “инфраструктура как услуга” (IaaS), который означает предоставление экземпляров ВМ по требованию [4]. Сервис IaaS широко используется для обеспечения необходимых вычислительных ресурсов в средах с общими данными. Например, существуют сервисы Amazon Web Services (AWS), Google Compute Engine, Microsoft Azure, которые предлагают услуги IaaS [5].

Поскольку виртуализация означает разделение ресурсов с помощью некоторого абстрактного слоя системных ресурсов, то возникает ряд особенностей, которые не свойственны обычным хостовым системам. Это проблемы в отношении безопасности, изоляции и производительности гостевых ОС. При разработке систем виртуализации необходимо учитывать угрозы безопасности[1], связанные с нахождением информации различного уровня доступа на различных сегментах виртуальной инфраструктуры (ВИ) [6]. ВИ – это система, поддерживающая виртуализацию серверов (ВМ), сети и хранилищ данных.

В данной работе проводится анализ контроля целостности ВМ. Поскольку попытка обеспечения целостности всех компонентов ВМ может снизить производительность этих ВМ, то требуется отдельно рассмотреть целесообразность и необходимость применения контроля целостности для различных компонентов ВМ. Также следует определить существующие методы обеспечения контроля целостности. Поскольку в будущем планируется создание централизованной системы контроля целостности ВМ, то необходимо сравнить методы с целью дальнейшего применения в централизованных системах контроля целостности ВМ. В работе рассматриваются только ВМ, созданные на базе гипервизора KVM.

[1]Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

Цель работы: выделить компоненты ВМ, созданных на базе гипервизора KVM, для которых необходим контроль целостности, описать существующие способы обеспечения контроля целостности и выбрать наилучший для применения в централизованных системах.

Основные задачи:

1. Изучить устройство и особенности ВМ, созданных на базе гипервизора KVM.
2. Проанализировать нормативную методическую базу в части защиты ВИ и контроля целостности их компонентов.
3. Определить компоненты ВМ, для которых необходим контроль целостности с точки зрения угроз безопасности и нормативной методической базы.
4. Изучить способы контроля целостности компонентов ВМ.
5. Определить наилучший способ контроля целостности компонентов ВМ для применения в централизованных системах.

Методы исследования: метод правдоподобного рассуждения, системный анализ, формализация.

Работа состоит из семи частей: описание серверной виртуализации; устройство гипервизора KVM; описание устройства ВМ, созданных на базе гипервизора KVM; анализ нормативной методической базы; общие сведения о контроле целостности ВИ; описание существующих моделей контроля целостности; способы контроля целостности компонентов ВМ и выбор наилучшего для применения в централизованных системах.

1. Виртуализация серверов

Понятие виртуализации в сфере информационных технологий (ИТ) существует давно, но его сущность с развитием ИТ несколько изменилась. В настоящий момент виртуализация применяется во многих областях ИТ, например, выделяют виртуализацию сети, виртуализацию хранения данных, виртуализацию серверов [7]. Рассмотрим подробнее последнюю, так как создание экземпляров ВМ относится к ней.

Виртуализация серверов (серверная виртуализация) – это маскировка ресурсов сервера от пользователей сервера. Основная цель серверной виртуализации – избавить администратора системы от необходимости понимать и управлять сложной архитектурой серверных ресурсов [7].

Для виртуализации серверов применяется несколько подходов, которые по типу реализации подразделяются на программные и аппаратные [8]. Примерами аппаратных являются технологии Intel VT (VT-x, Intel Virtualization Technology for x86) и AMD-V, их реализуют производители аппаратного обеспечения. Использование таких средств позволяет повысить производительность работы ВИ.

Основной частью программного подхода к виртуализации является гипервизор – основной компонент, обеспечивающий связь между оборудованием и ВМ [5]. Программная виртуализация осуществляется с помощью этого уровня абстракции. Гипервизоры основаны на реализации определённого программного подхода (стратегии), которые делятся на три основные категории: полная виртуализация (full virtualization), паравиртуализация (para-virtualization), виртуализация уровня ОС (OS-level virtualization) [5].

Полная виртуализация – обеспечивает виртуализацию без изменения гостевой (запускаемой) ОС, то есть виртуализация привилегированных инструкций может быть выполнена без поддержки аппаратной или ОС [5]. Паравиртуализация отличается от полной виртуализации тем, что требует изменений в ядре гостевой ОС [5]. Виртуализация уровня ОС (контейнеризация) позволяет запускать в рамках одной ОС на одном ядре несколько ВМ в изолированных разделах. Издержки в этой модели очень ограничены из-за

преимуществ работы в ОС с общим ядром. Гостевая ОС и хостовая должны иметь одну и ту же ОС или ядро [5].

При создании систем виртуализации серверов обычно используется аппаратная виртуализация совместно с гипервизорами, основанными на полной виртуализации. Наличие аппаратной виртуализации обеспечивает высокую производительность, а поддержка полной виртуализации обеспечивает удобство использования, то есть отсутствует необходимость внесения изменений в гостевые ОС.

Гипервизор иначе называют монитором виртуальной машины (MBM, virtual machine monitor, VMM). Эти два термина (гипервизор и MBM) обычно рассматриваются как синонимы, однако имеют существенное отличие. MBM представляет собой программное обеспечение, которое управляет центральным процессором (ЦП), памятью, передачей данных ввода-вывода, прерыванием и набором команд в данной виртуальной среде. Гипервизор может быть частью хостовой ОС со встроенной MBM [5], но это не всегда так.

Как правило, гипервизоры можно разделить на гипервизоры первого и второго типа в зависимости от уровня реализации [4]. Гипервизор первого типа работает непосредственно на физическом оборудовании, то есть связь между оборудованием и ВМ, запускаемой гипервизором, является прямой. ОС хоста не требуется в гипервизоре первого типа, поскольку он работает непосредственно на физическом обеспечении компьютера. По этой причине его иногда называют “аппаратным гипервизором” (“hardware hypervisor”). VMware vSphere/ESXi, Microsoft Windows Server 2012 Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization (RHEV) и система с открытым исходным кодом Kernel-based Virtual Machine (KVM) относятся к этой категории. Гипервизор второго типа находится в ОС [4], позволяя управлять ВМ с поддержкой конфигурации оборудования из ОС. Дополнительный уровень между оборудованием и ВМ в гипервизоре второго типа снижает эффективность по сравнению с гипервизором первого типа. VirtualBox и VMware Workstation можно отнести к этой категории [5].

2. Гипервизор KVM

KVM – полностью открытое программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86, которая поддерживает аппаратную виртуализацию на базе Intel VT либо AMD SVM (Secure VM).

ПО KVM состоит из нескольких компонентов. Основным является модуль ядра. Он состоит из загружаемого основного модуля kvm.ko, предоставляющего базовый сервис виртуализации, и процессорно-специфического загружаемого модуля kvm-amd.ko либо kvm-intel.ko. Для эмуляции аппаратного обеспечения (например, для запуска ОС, предназначенных под одну архитектуру, на другой или для эмуляции устройств ввода-вывода) гипервизор KVM использует программу QEMU [9]. Для управления работой экземпляров ВМ, созданных KVM, используется программа virt-manager [4], предоставляющая доступ из консоли и графический интерфейс (GUI/CLI). Ещё одним из наиболее распространённых методов управления гипервизором KVM, который частично повторяет функционал virt-manager, является доступ с помощью набора свободных инструментов libvirt. Libvirt – это свободная реализация программного интерфейса гипервизора KVM (API), сервис libvirtd (программа, работающая UNIX-подобных ОС в фоновом режиме) (демон) и набор инструментов для управления виртуализацией virsh [10,11], который особенно популярен для управления KVM в режиме командной строки. Ешё одной частью KVM является ядро Linux. Поскольку QEMU работает как обычный процесс [12], планирование соответствующей гостевой ОС выполняется самим ядром Linux.

3. Устройство ВМ, созданных на базе гипервизора KVM

ВМ – это комплексная система, состоящая из различных компонентов. Чтобы понимать принципы работы ВМ, различия между реализациями (типами) таких систем, необходимо определить основные интерфейсы и компоненты (уровни) архитектуры компьютерной системы (Computer system architecture). Интерфейсы связывают различные компоненты, обеспечивая их совместную работу в рамках единой архитектуры компьютерной системы. Определим основные компоненты (уровни) архитектуры компьютерной системы согласно основной иерархии обращений.

На самом низком программным уровне работает исполнитель оборудования (Execution hardware) [13]. Обычно он скрывает преобразование памяти (Memory translation), системную шину (System interconnect (bus)), устройства ввода-вывода и сети (I/O devices and networking), основную память (Main memory) и обеспечивает работоспособность аппаратного обеспечения.

Следующим уровнем архитектуры компьютерной системы является ОС [13], которая взаимодействует с исполнителем оборудования с помощью интерфейса ISA. ISA (Instruction set architecture) – архитектура набора команд, необходимая для запуска ПО на аппаратной платформе, позволяет ОС управлять физическими ресурсами системы.

Выше уровня ОС располагаются библиотеки [13]. Они могут обращаться как к исполнителю оборудования, так и к ОС. Интерфейс ABI (Application binary interface) реализует библиотекам доступ к аппаратным ресурсам (через пользовательскую ISA) и к системным вызовам ОС.

Самым старшим компонентом в иерархии архитектуры компьютерной системы является уровень прикладного программного обеспечения (ППО) [13]. Он взаимодействует с библиотеками через API (Application programming interface) с помощью высокоуровневых (high-level language, HLL) библиотечных вызовов. Компоненты, принадлежащие этому уровню, имеют право доступа к аппаратным ресурсам через пользовательскую ISA.

Существует два основных типа ВМ: ВМ процессов (Process Virtual Machine) и системные ВМ (System Virtual Machine) [13]. ВМ процессов предоставляют виртуальную среду ABI или API для пользовательских приложений. В различных реализациях ВМ процессов предлагают репликацию, эмуляцию и оптимизацию. Примерами таких ВМ могут быть Java Virtual Machine (JVM) и Microsoft Common Language Infrastructure, которая является основой .NET фреймворка (программная платформа, определяющая структуру программной системы, облегчает разработку и объединение различных компонентов программного продукта).

Системная ВМ предоставляет полную среду, в которой могут сосуществовать ОС и множество процессов, возможно принадлежащих нескольким пользователям. Используя системные ВМ, аппаратная платформа с одним хостом поддерживает одновременно несколько изолированных гостевых ОС. Эти возможности напрямую используются в серверной виртуализации, поэтому большинство “серверных” хостовых систем являются системными ВМ. Таким образом, сам гипервизор KVM является системной ВМ и его можно назвать ВМ, однако для разделения терминов будем называть экземпляры (инстансы), которые создаёт KVM (гостевые машины), виртуальными машинами (ВМ), а сам KVM – гипервизором.

При создании ВМ гипервизор создаёт набор определённых файлов на хосте. В отличие от обычной системы с установленной ОС, которая занимает выделенную область диска, гипервизор может динамически менять характеристики каждой отдельно взятой ВМ с помощью изменения конфигурационных файлов. Выделим основные файлы, которые

определяют ВМ. Полученное выделение установит основные компоненты ВМ, созданные на базе гипервизора KVM:

1) Файлы конфигурации описывают пользовательские и другие атрибуты ВМ [14]. Пользовательские атрибуты – это новые графы (поля), которые пользователь может добавить к ВМ и хостам, содержащие специфическую информацию, присущую конкретной организации. Например, если создать новый атрибут «Организация», то в списке ВМ кроме имени ВМ, её состояния, загрузки процессора и использования памяти будет доступна новая графа – «Организация» [15]. Удобство заключается в том, что поскольку информация о принадлежности ВМ к определенной организации является полем, то по нему может осуществляться сортировка. Также к этой категории относятся файлы, содержащие общую информацию о ВМ, то есть: определение сервера, сколько виртуальных процессоров (vCPU) выделено для этой ВМ, сколько оперативной памяти выделено, к каким устройствам ввода-вывода ВМ имеет доступ, сколько сетевых интерфейсных карт (NIC) находятся на виртуальном сервере и другие [14], а также файлы, определяющие параметры, такие как размер и другие, виртуального диска, к которому имеет доступ ВМ [14].

2) При включении или создании ВМ, создаются дополнительные файлы для ведения журнала учёта, подкачки памяти и других функций [14].

3) При копировании отдельных пользовательских файлов, находящихся внутри ВМ, создаётся не только резервная копия этих данных, но и копия всего сервера, включая ОС, приложения и саму конфигурацию оборудования [14]. Файлы, создающиеся при копировании данных, можно выделить в отдельный блок.

4) Файлы, содержащие ППО пользователей.

5) Файлы-образы гостевых ОС.

Таким образом, определено пять основных компонентов ВМ, созданных на базе гипервизора KVM. Компоненты типов (1), (5) существуют всегда, (2)–(4) могут отсутствовать (зависит от настроек системы и пользователя).

4. Анализ нормативной методической базы в части защиты ВИ

Согласно приказам ФСТЭК России[2] набора функций средств виртуализации для настройки ВИ с учетом требований безопасности[1] недостаточно, поэтому для их защиты от несанкционированных изменений необходимо использовать наложенные (внешние) средства защиты информации (СЗИ) [16,17].

Необходимо определить компоненты ВМ, для которых для которых требуется контроль целостности в соответствии с нормативной методической базой, среди определённых ранее компонентов ВМ, созданных на базе гипервизора KVM.

Определим рассматриваемую нормативную методическую базу. Согласно указанным выше приказам ФСТЭК России, основным требованием в области обеспечения контроля целостности ВИ является ЗСВ.7 (Защита среды виртуализации) («Контроль целостности виртуальной инфраструктуры и ее конфигураций»). Поскольку ВМ содержат

[2]Приказ № 17 ФСТЭК России от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Приказ № 31 ФСТЭК России от 14 марта 2014 г. «Об утверждении требований 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».

файлы резервного копирования, то при разработке СЗИ следует учитывать ЗСВ.8 («Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры»). Поскольку ВИ широко используются в финансовых организациях, то включим в рассмотрение рекомендации в области защиты ВИ Банка России [18] для организаций банковской системы Российской Федерации.

Рассмотрим ЗСВ.7. Поскольку темой данной работы является обеспечение контроля целостности только компонентов ВМ, а не ВИ в целом, то будем выделять только аспекты контроля целостности ВМ. Начнём с ОЦЛ.1 (Обеспечение целостности информационной системы и информации), на которую ссылается ЗСВ.7:

1. В информационной системе (ИС) должен осуществляться контроль целостности ПО СЗИ, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам всех компонентов СЗИ, как в процессе загрузки, так и динамически в процессе работы ИС с использованием криптографических методов в соответствии с законодательством Российской Федерации[1].

2. Должен быть реализован контроль целостности компонентов ПО (за исключением СЗИ), по наличию имен (идентификаторов) компонентов ПО и (или) по контрольным суммам, как в процессе загрузки, так и динамически в процессе работы ИС с использованием криптографических методов в соответствии с законодательством Российской Федерации[1].

3. Необходимо проведение тестирования с периодичностью, установленной оператором, функций безопасности СЗИ, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2 (Анализ защищённости информации)[1].

4. В случае если функциональные возможности ИС должны предусматривать применение в составе её ПО средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности ПО после завершения каждого процесса функционирования средств разработки и отладки программ[1].

5. В ИС должна обеспечиваться блокировка запуска ПО и (или) блокировка сегмента (компонента) ИС (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности[1].

Таким образом, согласно пунктам 1–2 необходим контроль целостности не только компонентов ВМ, но и самого СЗИ и его обновлений, как в процессе загрузки, так и в процессе работы ИС. СЗИ должно тестироваться с определённой периодичностью. Для ВМ с ПО средств разработки и отладки программ необходимо выполнять контроль целостности ПО после завершения каждого процесса функционирования средств разработки и отладки программ. В ИС должна обеспечиваться блокировка запуска ПО в случае обнаружения фактов нарушения целостности.

В ЗСВ.7 выделяются аспекты применения СЗИ в ВИ:

1. В ИС должен осуществляться контроль целостности компонентов, критически важных для функционирования хостовой ОС, гипервизора, гостевых ОС и (или) обеспечения безопасности, обрабатываемой в них информации (загрузчика, системных файлов, библиотек ОС и иных компонентов).

2. Должен осуществляться контроль целостности состава и конфигурации виртуального оборудования.

3. Должен осуществляться контроль целостности файлов, содержащих параметры настройки виртуализированного ПО и ВМ.

4. Должен осуществляться контроль целостности файлов-образов виртуализированного ПО и ВМ, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

5. В ИС должен обеспечиваться контроль целостности резервных копий ВМ (контейнеров).

6. В ИС должен обеспечиваться контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры.

7. В ИС должен обеспечиваться контроль целостности программного обеспечения облачных клиентов.

Получаем, что согласно пунктам 1–3 необходимо обеспечивать контроль компонентов типов (1), (3) предыдущего раздела. Пункт 4 соответствует (2), (5), а пункт 7 обязывает обеспечивать контроль файлов типа (4).

По рекомендациям Банка России[3] при создании базовых образов ВМ рекомендуется проводить процедуры, необходимые для выполнения последующего контроля их целостности. Созданный или измененный базовый образ ВМ перед размещением на основном оборудовании, реализующем технологию виртуализации, рекомендуется проверять в тестовом сегменте на соответствие настроек включенных в образ программных компонентов СЗИ требованиям, установленным соответствующей эксплуатационной документацией. Для каждого базового образа ВМ рекомендуется выполнять регламентированные процедуры контроля: соответствия настроек, включенных в образ программных компонентов СЗИ, требованиям, установленным эксплуатационной документацией; целостности ПО, включенного в образ ВМ. Рекомендуется выполнять регламентированные процедуры контроля целостности ПО, выполняемые при загрузке указанного ПО.

Поэтому, в соответствии с рекомендациями Банка России, необходимо обеспечивать контроль целостности ПО ВМ, в том числе выполняемый на этапе загрузки ВМ. Необходимо обеспечивать контроль файлов (1), (2) и (5), участвующих в загрузке ВМ.

Таким образом, несмотря на то, что существуют способы обеспечения контроля целостности файлов пользовательского ППО, содержимого памяти и контекстов центрального процессора в условиях полностью скомпрометированной ОС [4], проведённый анализ нормативной методической базы в части защиты ВИ показал необходимость обеспечения контроля целостности всех файлов ВМ. В частности, необходим контроль целостности конфигурационных файлов, ОС и ПО, установленного внутри экземпляров пользовательских гостевых ВМ.

5. Контроль целостности в серверной виртуализации

Целостность определяется как свойство безопасности информации, при котором отсутствует её несанкционированное изменение (изменение субъектами доступа, не имеющими на него право)[1]. Однако при таком определении целостности информация рассматривается исключительно как неделимый объект в том смысле, что его нельзя разбить на контролируемые и неконтролируемые части [6]. Поэтому под целостностью вычислительной среды (в контексте виртуализации) понимают стабильность в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования [6,19]. Повторим, что контроль целостности

[3]Рекомендации в области стандартизации Банка России – Обеспечение информационной безопасности организаций банковской системы Российской Федерации – Обеспечение информационной безопасности при использовании технологии виртуализации. URL: https://www.cbr.ru/Content/Document/File/46925/rs-28-15.pdf

предполагает сравнение текущего состояния некоторого объекта с набором эталонов, то есть с выделенным состоянием объекта, которое считается корректным и безопасным [20]. Состав, параметры и взаимосвязи и в течение какого периода времени, определяется для каждого конкретного случая отдельно.

Всё множество функций контроля целостности можно сгруппировать в три класса: контроль целостности технических средств ЭВМ, контроль целостности системных областей жестких дисков, контроль целостности отдельных файлов и программных средств. Последний класс отвечает за осуществление контроля целостности ОС и необходимых программных компонентов, в том числе и иных средств защиты и элементов комплексов защиты, работающих после средства доверенного загрузки (СДЗ) в ДВС [19].

Таким образом, для организации тонкой настройки контроля целостности параметров вычислительной среды и повышения эффективности работы процессов, реализующих меры защиты, необходимо обеспечить возможность контроля отдельных элементов: файлов и каталогов, входящих в состав архива и влияющих на загрузку ОС [19].

6. Модели контроля целостности компонентов ВМ

ВИ – динамическая система, некоторые её связи, атрибуты объектов могут быть изменены и при этом состояние системы останется корректным (не нарушающим целостность). Например, для ВМ может быть определён набор хостов-гипервизоров, перемещение между которыми (миграция) разрешено. Если рассматривать эталонную конфигурацию ВИ в традиционном понимании, то есть как некоторый «снимок» конкретного состояния системы, то возникает проблема, связанная с тем, что выбор такого эталона зачастую невозможен – например, одним «снимком» нельзя охватить сразу несколько разрешённых состояний. Необходимо задавать такое представление эталона и текущей конфигурации, такое их сопоставление, которое позволит учитывать множество разрешённых состояний [20]. Поэтому исторически целостность среды оценивалась с использованием моделей целостности [21].

Первые всесторонние модели целостности были предложены в [21], в которых субъектам и объектам назначаются метки целостности на основе их начального состояния целостности, и эти метки располагаются в решётке целостности, где информация может передаваться только от объектов с более высокой целостностью к объектам с более низкой целостностью. Например, субъект может только читать объекты выше (или равные) в решетке целостности и записывать объекты ниже (или равные) в решетке целостности. Должно быть обеспечено начальное состояние целостности системы, которое предоставляет модель целостности Кларка-Вилсона с помощью явного определения процедуры проверки целостности, процесса проверки целостности системы во время инициализации, чтобы гарантировать высокую целостность начальной (отправной) точки [21].

Основная проблема в проверке целостности среды выполнения состоит в том, что системы с высокой степенью целостности могут получать ненадежные входные данные (например, из сети) [21]. Модель целостности Кларка-Вилсона определила эту проблему, в которой программы высокой целостности (называемые процедурами преобразования в модели Кларка-Уилсона) должны быть способны немедленно отбрасывать или обновлять ненадежные входные данные [21]. Однако необходима формальная уверенность в правильности (высокой целостности) этих программ для обоснования такого поведения в модели Кларка-Вилсона. Несмотря на то, что формальная гарантия для программ стала жизнеспособной технологией в 1987 году (то есть, когда была предложена модель Кларка-Вилсона) [21], в настоящее время широко распространено мнение, что формальная гарантия полной правильности нецелесообразна, поэтому в последнее время появились новые идеи

по обеспечению контроля целостности. Они требуют, чтобы программы с высокой степенью целостности были разработаны так, чтобы могли принимать ненадежные входные данные только на интерфейсах, где могут быть приняты решения о целостности.

Одной из реализаций этих идей является атрибутная модель контроля доступа [20]. Важной частью модели являются политики безопасности. Политики безопасности – это совокупность свойств, определяющих эталон ВИ. Обычно их устанавливает администратор безопасности в соответствии с решаемыми задачами. Эти политики передаются на общий сервер проверки. По запросу модуль, работающий на автоматизированном рабочем месте администратора, получает из ВИ данные, определяющие её текущее состояние, и формирует на их основе запросы. После передачи этих запросов на сервер проверки, начинается их оценка на соответствие созданным ранее политикам. Если проверка всех запросов на соответствие политикам прошла успешно, то целостность конфигурации ВИ сохранена. В противном случае имеют место нарушения целостности.

Атрибутная модель контроля доступа может применяться как при решении задачи разграничения доступа, так и при решении задачи обеспечения контроля целостности конфигурации ВИ [20]. Созданы способы упрощения процесса написания политик безопасности для администраторов. Например, использование готовых шаблонов.

При применении атрибутной модели контроля доступа решается основная проблема контроля целостности конфигурации – противоречие с традиционным подходом, при котором разрешённым может быть лишь одно состояние, совпадающее с эталоном [20].

7. Способы контроля целостности компонентов ВМ

В зависимости от расположения СЗИ выделяют несколько способов контроля целостности компонентов ВМ. Рассмотрим основные из них, которые можно использовать с гипервизором KVM. Поскольку KVM является гипервизором первого типа, то СЗИ может либо встраиваться между самим гипервизором и экземплярами ВМ, либо может существовать отдельно, то есть находиться снаружи от системы “гипервизор и экземпляры ВМ”. Выделим основные способы контроля целостности компонентов ВМ, созданных на базе гипервизора KVM:

1) СЗИ может встраиваться между гипервизором и экземплярами ВМ. Это можно реализовать с помощью создания СЗИ, которое будет перехватывать обращения ВМ к гипервизору, обрабатывать эти запросы и пересылать их гипервизору.

2) СЗИ может быть встроенным в гипервизор. Этот способ является развитием первого способа, может быть реализован с помощью изменения исходного кода базового гипервизора, что не всегда допустимо. Также этот способ не позволит полностью реализовать контроль целостности самого гипервизора (поскольку является его частью), которое требуется согласно нормативным методическим актам.

3) СЗИ может быть встроенным в БИОС ВМ. Такой способ может применяться при разработке децентрализованных систем.

4) СЗИ может быть находиться снаружи от системы “гипервизор и экземпляры ВМ”.

Рассмотрение последнего способа невозможно без понятий доверенной вычислительной среды (ДВС) и резидентного компонента безопасности (РКБ). Фрагмент среды электронного взаимодействия, для которого установлена и поддерживается в течение заданного интервала времени целостность объектов и целостность взаимосвязей между ними, называется ДВС [18]. В настоящее время модель ДВС остаётся одной из актуальных и практически применимых субъектно-объектных моделей защиты технологии электронного обмена информации [19]. Появляются предложения по новым реализациям и функциональному составу РКБ, наличие которого требуется для построения ДВС [18,19],

однако контроль целостности элементов среды остаётся одной из основ создания ДВС. Следовательно, одна из основных групп функций, которые должны быть реализованы РКБ, – это функции контроля целостности: контроль целостности технического состава ЭВМ и локальной вычислительной сети (ЛВС), контроль целостности ОС, контроль целостности ППО и данных.

РКБ не может быть встроенным СЗИ, так как в таком случае не может быть полноценно реализована концепция РКБ системы как активного элемента, независящего от защищаемой системы и реализующего заданный набор процедур её контроля, поэтому СЗИ должно быть наложенным. Данная концепция (независящего от защищаемой системы элемента) положена в основу всех программно-аппаратных комплексов компании «ОКБ САПР» для защиты различных инфраструктур виртуализации: «Аккорд-В» для VMware vSphere; «ГиперАккорд» для Microsoft Hyper-V; «Аккорд-KVM» для KVM, – каждый из которых является наложенным СЗИ [17].

Централизованная система контроля целостности компонентов ВМ, созданных на базе гипервизора KVM, должна быть наложенным СЗИ. Это СЗИ должно находиться снаружи от системы “гипервизор и экземпляры ВМ”, то есть должно обладать независимым подключением (прямым соединением) как к ВМ, так и к гипервизору KVM [22] для обеспечения контроля целостности ВМ и гипервизора согласно ЗСВ.7, то есть должно являться РКБ.

Примером успешной реализации подобной схемы с независимыми подключениями является система VIS (Virtualization Introspection System) для обнаружения различных атак [23]. Она обладает независимым подключением к экземплярам ВМ и к гипервизору KVM, поэтому может обнаруживать атаки не только на ВМ, но и на гипервизор [24]. Использование подобной схемы избавляет систему VIS от необходимости постоянно «доверять» гипервизору.

Применение контроля целостности к гипервизору обусловлено не только требованиями нормативной методической базы, но и существованием ряда атак на гипервизор [24], поэтому отказаться от применения к гипервизору контроля целостности, рассматривая задачу контроля целостности компонентов ВМ, нельзя. Полученная система наложенного СЗИ может реализовывать монитор безопасности объектов (МБО) [25].

При рассмотрении способов обеспечения контроля целостности компонентов ВМ следует помнить о том, что возможно разделение ВМ по зонам доверия [26] Возможна и допустима ситуация, когда на одном физическом сервере находятся, например, информация различного уровня доступа. Разработчикам средств контроля целостности компонентов ВИ следует предоставлять администраторам возможность написания соответствующих политик безопасности. Комплексные средства защиты платформ виртуализации таких производителей, как Trend Micro, Reflex Systems, позволяют изолировать машины из разных зон доверия, а также создавать профили и политики безопасности, автоматизирующие применение таких настроек [26]. Более того, при перемещении машины на другой сервер такой профиль может предотвратить ошибочное подключение внутренней системы к внешней сети.

Стоит отметить, что ИС, использующие виртуализацию на базе KVM, могут значительно различаться, но в любом случае необходимой мерой их защиты является обеспечение контроля целостности ВМ [27]. Средствам защиты для таких систем необходимо, но не достаточно решать эту задачу, кроме того, они должны соответствовать всем факторам, характеризующим защищаемую виртуальную инфраструктуру: ОС гипервизоров, способы подключения хранилища, гостевые версии ОС, системы управления и т.д.

Заключение

В работе проведен анализ средств виртуализация серверов, устройство гипервизора KVM и его компоненты: QEMU, virt-manager, libvirt и др.; выделены основные компоненты ВМ: файлы конфигурации, файлы ведения журнала учёта (и подкачки памяти), файлы копирования, файлы, содержащие ППО пользователей, и файлы-образы гостевых ОС.

Проведён анализ нормативной методической базы в части защиты ВИ с целью определения компонентов ВМ, для которых необходим контроль целостности. Определены особенности обеспечения контроля целостности в серверной виртуализации. Описывается возможность использования атрибутной модели для решения задачи обеспечения контроля целостности компонентов ВМ, созданных на базе гипервизора KVM.

Рассмотрены основные способы контроля целостности ВМ, созданных на базе гипервизора KVM. Определяется, что централизованная система контроля целостности компонентов ВМ, созданных на базе гипервизора KVM, должна быть наложенным СЗИ, которое должно находиться снаружи от системы “гипервизор и экземпляры ВМ”, то есть должно независимо подключаться как к ВМ, так и к гипервизору KVM для обеспечения контроля целостности ВМ и гипервизора.

Полученные в данной работе результаты могут быть использованы при разработке централизованной системы контроля целостности компонентов ВМ, созданных на базе гипервизора KVM.

СПИСОК ЛИТЕРАТУРЫ:

1. Durairaj M., Kannan P. A Study On Virtualization Techniques And Challenges In Cloud Computing. International Journal of Scientific & Technology Research. 2014. Vol. 3. P. 147–151. URL: https://www.ijstr.org/final-print/nov2014/A-Study-On-Virtualization-Techniques-And-Challenges-In-Cloud-Computing.pdf (дата обращения: 15.04.2020).
2. Popek G. J., Goldberg R. P. Formal Requirements for Virtualizable Third Generation Architectures. Communications of the ACM. 1974. Vol. 17. P. 412–421. DOI: https://doi.org/10.1145/361011.361073.
3. Дорошенко В. С., Шадрин Д. Б. Использование виртуальных машин в обучении. Новые образовательные технологии в вузе: материалы XII международной научно-методической конференции (НОТВ-2015). 2015. С. 106–108. URL: https://elibrary.ru/item.asp?id=29903669 (дата обращения: 15.04.2020).
4. YamunaDevi, L. & P, Aruna & Dorairaj, Sudha Devi & Priya, Navya. (2011). Security in Virtual Machine Live Migration for KVM. 10.1109/PACC.2011.5979008. DOI: 10.1109/PACC.2011.5979008.
5. Hyungro L. Virtualization Basics: Understanding Techniques and Fundamentals. School of Informatics and Computing, Indiana University. 2014. P. 1–5. URL: http://dsc.soic.indiana.edu/publications/virtualization.pdf (дата обращения: 21.04.2020).
6. Мозолина Н. В. Контроль целостности виртуальной инфраструктуры и её конфигурации. Вопросы защиты информации. 2016. Вып. 3. С. 31–33. URL: https://elibrary.ru/item.asp?id=26992575 (дата обращения: 21.04.2020).
7. Гордиевских В.М. Сущность, структура и классификация современных технологий виртуализации. В лабораторию учёного. 2015. С. 125–133. URL: https://elibrary.ru/item.asp?id=23400691 (дата обращения: 21.04.2020).
8. Елманова Н., Пахомов. С. Виртуальные машины 2007. КомпьютерПресс. 2007. Вып. 9. С. 29–42. URL: https://compress.ru/article.aspx?id=18046 (дата обращения: 21.04.2020).
9. Сайт проекта KVM. Главная страница. URL: https://www.linux-kvm.org/page/Main_Page (дата обращения: 18.10.2019).
10. Сайт проекта KVM. Средства управления. URL: https://www.linux-kvm.org/page/Management_Tools (дата обращения: 19.10.2019).
11. Сайт проекта Libvirt. Часто задаваемые вопросы. URL: https://wiki.libvirt.org/page/FAQ#What_is_libvirt.3F (дата обращения: 22.10.2019).
12. Goto Y. Kernel-based Virtual Machine Technology. FUJITSU Sci. Tech. J. 2011. Vol. 47. P. 362–368. URL: https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol47-3/paper18.pdf (дата обращения: 21.04.2020).
13. J. E. Smith and R. Nair, «The Architecture of Virtual Machines», Computer (IEEE), Vol. 38, No. 5, 2005. P.32–38. DOI:10.1109/MC.2005.173.
URL: https://www.scirp.org/reference/referencespapers.aspx?referenceid=449371 (дата обращения: 21.04.2020).
14. Operating Systems: Internals and Design Principles. Chapter 14. Virtual Machines.
URL: https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH14-OS8e.pdf (дата обращения: 18.11.2019).

15. Использование пользовательских атрибутов в Vcenter Server. URL: http://it-pilot.ru/2013/10/14/atribut/ (дата обращения: 18.11.2019).
16. Рябов А. С., Угаров Д. В., Постоев Д. А. Безопасность виртуальных инфраструктур. Сложности и нюансы выполнения требований регулятора. Комплексная защита информации: материалы XXI научно-практической конференции. 2016. С. 217–220.
URL: https://www.okbsapr.ru/library/publications/ryabov_2015_2/ (дата обращения: 21.04.2020).
17. Лыдин С.С. Средства защиты информации для инфраструктуры виртуализации: встроенные или наложенные? URL: http://www.okbsapr.ru/lydin_kzi2017.html (дата обращения: 01.12.2019).
18. Конявский В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией. Минск: Беллитфонд. 2004. С. 239–245. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf (дата обращения: 21.04.2020).
19. Алтухов А. А. Доверенная загрузка и контроль целостности архивированных данных. Часть и целое. Вопросы защиты информации. 2016. Вып. 2. С. 35–39.
URL: https://www.okbsapr.ru/library/publications/altukhov_2016_1/ (дата обращения: 21.04.2020).
20. Мозолина Н. В. Решение задачи контроля целостности конфигурации, основанное на атрибутной модели контроля доступа // Вопросы защиты информации. 2017. Вып. 3. С. 23–25.
URL: https://www.okbsapr.ru/library/publications/mozolina_2017_2/ (дата обращения: 21.04.2020).
21. Schiffman J., Moyer T., Shal C., Trent J., McDaniel P. Justifying Integrity Using a Virtual Machine // 25th Annual Computer Security Applications Conference (ACSAC), 2009.
URL: http://www.patrickmcdaniel.org/pubs/acsac09c.pdf (дата обращения: 01.12.2019).
22. Liu D. A Research on KVM-Based Virtualization Security. Applied Mechanics and Materials. 2014. Vol. 543-547. P. 3126–3129. DOI: https://doi.org/10.4028/www.scientific.net/AMM.543-547.3126 (дата обращения: 21.04.2020).
23. Lee S., Yu F. Securing KVM-Based Cloud Systems via Virtualization Introspection // 2014 47th Hawaii International Conference on System Sciences. 2014. P. 5028–5037. DOI: 10.1109/HICSS.2014.617.
URL: https://ieeexplore.ieee.org/document/6759220 (дата обращения: 21.04.2020).
24. Авезова Я. Э., Фадин А. А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. Вып. 1. С. 24–30. URL: https://cyberrus.com/wp-content/uploads/2016/02/24-30-114-16_4.-Фадин.pdf (дата обращения: 21.04.2020).
25. Щербаков А. Ю. Современная компьютерная безопасность. М.: Книжный мир. 2009. – 352 с. URL: https://computer-museum.ru/books/computer_safety.pdf (дата обращения: 21.04.2020).
26. Зубарев И. В., Радин П. К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах. Вопросы кибербезопасности. 2014. Вып. 2 (3). С. 40–45. URL: https://cyberrus.com/wp-content/uploads/2014/07/vkb_03_06.pdf (дата обращения: 21.04.2020).
27. Мозолина Н. В. Необходимо и достаточно, или контроль целостности виртуальных машин с помощью Аккорд-KVM. Information Security/Информационная безопасность. 2018. Вып. 5. С. 33
URL: https://www.okbsapr.ru/library/publications/mozolina_2018_1/ (дата обращения: 21.04.2020).

REFERENCES:

[1] Durairaj M., Kannan P. A Study On Virtualization Techniques And Challenges In Cloud Computing. International Journal of Scientific & Technology Research. 2014. Vol. 3. P. 147–151.
URL: https://www.ijstr.org/final-print/nov2014/A-Study-On-Virtualization-Techniques-And-Challenges-In-Cloud-Computing.pdf (accessed: 15.04.2020).
[2] Popek G. J., Goldberg R. P. Formal Requirements for Virtualizable Third Generation Architectures. Communications of the ACM. 1974. Vol. 17. P. 412–421. DOI: https://doi.org/10.1145/361011.361073.
[3] Doroshenko V. S., Shadrin D. B. Ispol'zovanie virtual'nykh mashin v obuchenii. Novye obrazovatel'nye tekhnologii v vuze: materialy XII mezhdunarodnoy nauchno-metodicheskoy konferentsii (NOTV-2015). 2015. C. 106–108. URL: https://elibrary.ru/item.asp?id=29903669 (accessed: 15.04.2020) (in Russian).
[4] YamunaDevi, L. & P, Aruna & Dorairaj, Sudha Devi & Priya, Navya. (2011). Security in Virtual Machine Live Migration for KVM. 10.1109/PACC.2011.5979008. DOI: 10.1109/PACC.2011.5979008.
[5] Hyungro L. Virtualization Basics: Understanding Techniques and Fundamentals. School of Informatics and Computing, Indiana University. 2014. P. 1–5. URL: http://dsc.soic.indiana.edu/publications/virtualization.pdf (accessed: 21.04.2020).
[6] Mozolina N. V. Kontrol' tselostnosti virtual'noy infrastruktury i ee konfiguratsii. Voprosy zashchity informatsii. 2016. Vyp. 3. S. 31–33. URL: https://elibrary.ru/item.asp?id=26992575 (accessed: 21.04.2020) (in Russian).
[7] Gordievskikh V.M. Sushchnost', struktura i klassifikatsiya sovremennykh tekhnologiy virtualizatsii. V laboratoriyu uchenogo. 2015. S. 125–133. URL: https://elibrary.ru/item.asp?id=23400691 (accessed: 21.04.2020) (in Russian).

[8] Elmanova N., Pakhomov. S. Virtual'nye mashiny 2007. Komp'yuterPress. 2007. Vyp. 9. S. 29–42. URL: https://compress.ru/article.aspx?id=18046 (accessed: 21.04.2020) (in Russian).
[9] Sayt proekta KVM. Glavnaya stranitsa. URL: https://www.linux-kvm.org/page/Main_Page (accessed: 18.10.2019). (in Russian).
[10] Sayt proekta KVM. Sredstva upravleniya. URL: https://www.linux-kvm.org/page/Management_Tools (accessed: 19.10.2019).
[11] Sayt proekta Libvirt. Chasto zadavaemye voprosy. URL: https://wiki.libvirt.org/page/FAQ#What_is_libvirt.3F (accessed: 22.10.2019).
[12] Goto Y. Kernel-based Virtual Machine Technology. FUJITSU Sci. Tech. J. 2011. Vol. 47. P. 362–368. URL:https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol47-3/paper18.pdf (accessed: 21.04.2020).
[13] J. E. Smith and R. Nair, “The Architecture of Virtual Machines,” Computer (IEEE), Vol. 38, No. 5, 2005. P.32–38. DOI:10.1109/MC.2005.173. URL: https://www.scirp.org/reference/referencespapers.aspx?-referenceid=449371 (accessed: 21.04.2020).
[14] Operating Systems: Internals and Design Principles. Chapter 14. Virtual Machines. URL: https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH14-OS8e.pdf (accessed: 18.11.2019).
[15] Ispol'zovanie pol'zovatel'skikh atributov v Vcenter Server. URL: http://it-pilot.ru/2013/10/14/atribut/ (accessed: 18.11.2019) (in Russian).
[16] Ryabov A. S., Ugarov D. V., Postoev D. A. Bezopasnost' virtual'nykh infrastruktur. Slozhnosti i nyuansy vypolneniya trebovaniy regulyatora. Kompleksnaya zashchita informatsii: materialy XXI nauchno-prakticheskoy konferentsii. 2016. S. 217–220. URL:https://www.okbsapr.ru/library/publications/ryabov_2015_2/ (accessed: 21.04.2020) (in Russian).
[17] S. Lydin Sredstva zashchity informatsii dlya infrastruktury virtualizatsii: vstroennye ili nalozhennye? URL: http://www.okbsapr.ru/lydin_kzi2017.html (accessed: 01.12.2019) (in Russian).
[18] Konyavskiy V. A., Gadasin V. A. Osnovy ponimaniya fenomena elektronnogo obmena informatsiey. Minsk: Bellitfond. 2004. S. 239–245. URL: https://www.okbsapr.ru/upload/iblock/016/osnovi_ponim_el_obmen_inf.pdf (accessed: 21.04.2020) (in Russian).
[19] Altukhov A. A. Doverennaya zagruzka i kontrol' tselostnosti arkhivirovannykh dannykh. Chast' i tseloe. Voprosy zashchity informatsii. 2016. Vyp. 2. S. 35–39. URL: https://www.okbsapr.ru/library/publications/altukhov_2016_1/ (accessed: 21.04.2020) (in Russian).
[20] Mozolina N. V. Reshenie zadachi kontrolya tselostnosti konfiguratsii, osnovannoe na atributnoy modeli kontrolya dostupa. Voprosy zashchity informatsii. 2017. Vyp. 3. S. 23–25. URL: https://www.okbsapr.ru/library/publications/mozolina_2017_2/ (accessed: 21.04.2020) (in Russian).
[21] Schiffman J., Moyer T., Shal C., Trent J., McDaniel P. Justifying Integrity Using a Virtual Machine. 25th Annual Computer Security Applications Conference (ACSAC), 2009. URL: http://www.patrickmcdaniel.org/pubs/acsac09c.pdf (accessed: 01.12.2019).
[22] Liu D. A Research on KVM-Based Virtualization Security. Applied Mechanics and Materials. 2014. Vol. 543–547. P. 3126–3129. DOI: https://doi.org/10.4028/www.scientific.net/AMM.543-547.3126 (accessed: 21.04.2020).
[23] Lee S., Yu F. Securing KVM-Based Cloud Systems via Virtualization Introspection. 2014 47th Hawaii International Conference on System Sciences. 2014. P. 5028–5037. DOI: 10.1109/HICSS.2014.617. URL: https://ieeexplore.ieee.org/document/6759220 (accessed: 21.04.2020).
[24] Avezova Ya. E., Fadin A. A. Voprosy obespecheniya doverennoy zagruzki v fizicheskikh i virtual'nykh sredakh. Voprosy kiberbezopasnosti. 2016. Vyp. 1. S. 24–30. URL: https://cyberrus.com/wp-content/uploads/2016/02/24-30-114-16_4.-Фадин.pdf (accessed: 21.04.2020) (in Russian).
[25] Shcherbakov A. Yu. Sovremennaya komp'yuternaya bezopasnost'. M.: Knizhnyy mir. 2009. – 352 s. URL: https://computer-museum.ru/books/computer_safety.pdf (accessed: 21.04.2020) (in Russian).
[26] Zubarev I. V., Radin P. K. Osnovnye ugrozy bezopasnosti informatsii v virtual'nykh sredakh i oblachnykh platformakh. Voprosy kiberbezopasnosti. 2014. Vyp. 2 (3). S. 40–45. URL: https://cyberrus.com/wp-content/uploads/2014/07/vkb_03_06.pdf (accessed: 21.04.2020) (in Russian).
[27] Mozolina N. V. Neobkhodimo i dostatochno, ili kontrol' tselostnosti virtual'nykh mashin s pomoshch'yu Akkord-KVM. Information Security/Informatsionnaya bezopasnost'. 2018. Vyp. 5. S. 33. URL: https://www.okbsapr.ru/library/publications/mozolina_2018_1/ (accessed: 21.04.2020) (in Russian).

Поступила в редакцию – 09 мая 2020 г. Окончательный вариант – 06 июня 2020 г.
Received – May 09, 2020. The final version – June 6, 2020.

ПРАВИЛА ДЛЯ АВТОРОВ

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

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

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

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы с почтовым адресом, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, ПРОПИСНЫМИ буквами), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив); аннотация (200 – 250 слов, по ширине, строчными буквами – см. **правила 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 10.06.2020. Формат 60x84 1/8
Печ. л. 17. Уч.-изд. л. 17. 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