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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

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

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

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

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

Основные тематические направления журнала:

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

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

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

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

Papers in Russian and English are equally welcome.

Focus topics:

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

СОДЕРЖАНИЕ

CONTENT

Роман В. Наталичев[1], Виктор С. Горбатов[2], Григорий П. Гавдан[3], Анатолий П. Дураковский[4]
Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail*: *r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144*
[2]*e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
[3]*e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076*
[4]*e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735*

ЭВОЛЮЦИЯ И ПАРАДОКСЫ НОРМАТИВНОЙ БАЗЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2021.3.01

Аннотация. В настоящее время в России проводится активная работа по реализации относительно нового механизма государственного регулирования в области информационной безопасности, законодательно определяемого как обеспечение безопасности значимых объектов критической информационной инфраструктуры (КИИ). Субъектами данного законодательства выполнен достаточно большой объем организационных мероприятий, поддержанных научными исследованиями отечественных и зарубежных специалистов. Настоящая работа посвящена исследованию вопросов обеспечения безопасности значимых объектов КИИ на основе проведения критического системного анализа нормативной базы с указанием неоднозначности толкования и возможных вариантов практического выполнения требований применительно к конкретной сфере деятельности. Высокий уровень напряженности дискуссий по данному направлению на различных форумах показывает, что формирование новой системы на местах, на уровне отдельных субъектов, вызывает много сложностей и даже порой неприятие по некоторым аспектам нормативных требований. Как правило, это происходит всегда на начальных этапах становления любой новой системы в силу неоднозначности формулировок и наличия существенных внутренних противоречий в отдельных нормативных актах различных регуляторов. Одной из существенных проблем является определенное недопонимание на местах, особенно в реальном секторе экономики, необходимости введения и роли нового механизма обеспечения безопасности в общем комплексе мер обеспечения информационной безопасности, уже реализуемых в России более четверти века. Проведение системного анализа такой проблемной ситуации особенно актуален для образовательного сообщества, уже приступившего к реализации новых программ обучения различного уровня подготовки, переподготовки и повышения квалификации специалистов в области информационной безопасности. На основе описания эволюции отечественного законодательства в области информационной безопасности дано обоснование необходимости нового механизма государственного регулирования. Приводятся примеры неоднозначности и внутренних противоречий (парадоксов) некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывающие насущную необходимость их совершенствования и дополнительных усилий по толкованию основных положений, исходя из принципа креативного подхода по разъяснению сложных вопросов.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, значимый объект, значимые последствия, показатель значимости, нормативные правовые акты системный анализ, угрозы безопасности, подготовка специалистов.

Для цитирования: НАТАЛИЧЕВ, Роман В. и др. ЭВОЛЮЦИЯ И ПАРАДОКСЫ НОРМАТИВНОЙ БАЗЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.]. Т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1359. DOI: http://dx.doi.org/10.26583/bit.2021.3.01.

Roman V. Natalichev[1], Viktor S. Gorbatov[2], Grigory P. Gavdan[3]
Anatoly P. Durakovskiy[4]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144
[2]e-mail: VSGorbatov@mephi.ru, https://orcid.org/ /0000-0001-9998-9733
[3]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[4]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735

Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities

DOI: http://dx.doi.org/10.26583/bit.2021.3.01

Abstract. Today in Russia the active work is going on the implementation of a relatively new mechanism of state regulation in the field of information security, which is legally defined as ensuring the security of significant objects of critical information infrastructure (CII). The subjects of this legislation have carried out a fairly large amount of organizational measures supported by scientific research of domestic and foreign specialists. The paper is devoted to the study of the issues of ensuring the safety of significant CII objects based on a critical system analysis of the regulatory framework and indicating the ambiguity of interpretation and possible options for the practical implementation of the requirements related to a specific field. The high level of tension of discussions in this area at various forums demonstrates that the formation of a new system at the level of individual subjects causes many difficulties and even sometimes leads to rejection of some aspects of regulatory requirements. As a rule, this always happens at the initial stages of the formation of any new system due to ambiguity of the wordings and the presence of significant internal contradictions in certain regulatory acts. One of the significant problems, in our opinion, is a certain misunderstanding, especially in the real sector of the economy, of the need to introduce and the role of a new security mechanism within the overall set of information security measures that have already been implemented in Russia for more than a quarter of a century. Conducting a system analysis of such a problematic situation is especially relevant for the educational community that has already started implementing new training programs of various levels of training, retraining and advanced training of specialists in the field of information security. Based on the description of the evolution of domestic legislation in the field of information security, for the need for a new mechanism of state regulation is justified. Examples of ambiguity and internal contradictions (paradoxes) of some provisions of regulatory legal acts on the safety of CII facilities are given, showing the urgent need for their improvement as well as for additional efforts to interpret the main provisions, based on the principle of a creative approach to explaining complex issues.

Keywords: information security, critical information infrastructure, significant object, significant consequences, significance indicator, regulatory legal acts, system analysis, threats to security, training of specialists.

For citation: NATALICHEV, Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 28, n. 3, p. 6–27, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1359. DOI: http://dx.doi.org/10.26583/bit.2021.3.01.

Введение

Прошло уже несколько лет от вступления в действие относительно нового механизма государственного регулирования в области информационной безопасности, законодательно[1] определяемого как обеспечение безопасности объектов критической информационной инфраструктуры (КИИ). За это время данное направление нормативно

[1]Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

поддержано на законодательном уровне путем внесения поправок в Уголовный Кодекс[2] (УК РФ) и Кодекс об административных правонарушениях[3], соответствующими Федеральными законами[4,5], и имеет достаточно обширную нормативно-методическую базу основных регуляторов в области информационной безопасности – ФСТЭК России и ФСБ России[6].

В период подготовки настоящей статьи вышел в свет новый вариант Стратегии национальной безопасности[7], в которой в пункте 51 в качестве одной из существенных угроз безопасности указано стремление и отработка действий иностранных государств по выведению из строя объектов КИИ Российской Федерации. В пункте 57 (подпункт 3) дается директива по реализации противодействия такой угрозе в рамках государственной политики по обеспечению информационной безопасности России.

Государственными и бизнес-структурами, законодательно определенными как субъекты этого направления нормативного регулирования, проведен достаточно обширный перечень организационных и методико-просветительных мероприятий по его практической реализации. Среди них разработка и реализация новых образовательных программ подготовки, переподготовки и повышению квалификации работников соответствующих сил обеспечения [1, 2].

Активно проводятся научно-технические исследования по данной тематике как отечественных [3, 4], так и зарубежных специалистов, по разработке, в частности, комплексных инструментов определения важнейших услуг информационной инфраструктуры [5]; оценок каскадированного воздействия на системы КИИ [6]; методов выявления взаимозависимостей отказов инфраструктурных служб организаций [7]; комплексных подходов по оценке устойчивости критически важных элементов инфраструктуры [8].

В то же время формирование новой системы на местах, на уровне отдельных субъектов, вызывает много сложностей и даже порой неприятие по некоторым аспектам нормативных требований. Об этом свидетельствуют достаточно напряженные дискуссии в ходе профильных конференций, совещаний и семинаров[8]. Это происходит, как правило, всегда на начальных этапах становления любой новой системы в силу неоднозначности формулировок и наличия существенных внутренних противоречий в отдельных нормативных актах различных регуляторов. Но, в данном случае, одним из существенных,

[2]«Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ.

[3]«Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ.

[4]Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

[5]Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 194-ФЗ.

[6]Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования», Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ», Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам», Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ».

[7]Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

[8]ТБ Форум, конференции: Защита информации в АСУ ТП. Безопасность критической информационной инфраструктуры (16.07.2020, 09.02.2021, 08.04.2021, 15.07.2021), Защита критической инфраструктуры в государственных и бизнес-структурах (29.10.2020). URL: https://www.tbforum.ru/program (дата обращения: 16.03.2021).

на наш взгляд, факторов является определенное недопонимание на местах, особенно в реальном секторе экономики, необходимости введения, а главное, роли нового механизма в общем комплексе уже существующих мер обеспечения информационной безопасности. Тем более, что нововведение принято в декларируемых условиях «регуляторной гильотины»[9] с целью развития бизнеса за счет повышения эффективности государственного управления.

На наш взгляд, многие субъекты реального сектора экономики, особенно крупные корпорации [9, 10], а также банковская система[10], объективно мотивированные необходимостью обеспечивать устойчивость своих бизнес-процессов, уже имеют необходимые силы обеспечения противодействия кибератакам. По данным исследователей [11] 95% отечественных компаний, подвергшихся атакам, построены с учетом прежних и действующих в настоящее время, нормативно-правовых требований и/или на основе гармонизированных с лучшими мировыми практиками стандартов открытых систем, использующих риск-ориентированные подходы по оценке их безопасности.

Очевидно, что для выполнение новых государственных требований необходимо выделение дополнительных ресурсов, как правило, в условиях их недостаточности. Поэтому очевидна и скептическая позиция субъектов реальных секторов экономики, которые в лучшем случае выполняют формальные организационные процедуры, а в худшем занимают выжидательную позицию, что само по себе можно расценивать как своеобразную угрозу национальной безопасности.

Ссылки на реальную возможность практической реализации угроз безопасности КИИ[11], а также, например, на результаты кибератаки по блокированию нефтяного трубопровода в США 6 мая 2021 г. с целью получения выкупа[12], явно не могут поколебать эту скептическую позицию, особенно субъектов, использующих в своей деятельности риск-ориентированные подходы.

Возникает необходимость проведения системного анализа указанной проблемной ситуации, что особенно актуально для образовательного сообщества. В целом образовательные учреждения не являются субъектами рассматриваемого законодательства, хотя по разъяснению регулятора в их число должны быть включены крупные вузы с большой научной составляющей своей деятельности [12]. Но, главное, как упомянуто выше, данное сообщество уже приступило к практической реализации новых образовательных программ. Поэтому в силу своего целевого предназначения и необходимости реализации креативного подхода по подготовке специалистов высокой квалификации оно не может занимать ни выжидательную, ни тем более формальную позицию. То есть при изучении нормативной базы как основы становления всей практической деятельности специалиста, необходимо, с одной стороны, доказательно обосновать объективную необходимость того или иного вида государственного регулирования. В то же время даже простое изложение основных положений действующих нормативных актов при нынешнем их объеме выходит за рамки нормативно заданных объемов учебного времени, включая самостоятельные

[9]Реформа контрольно-надзорной деятельности, нацеленная на повышение уровня безопасности и устранение избыточной административной нагрузки на субъекты предпринимательской деятельности. Определена Федеральным законом от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_358670/ (дата обращения: 16.03.2021).

[10]«Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399)

[11]Аналитики заявили о росте кибератак на критическую инфраструктуру на 150%. URL: https://www.rbc.ru/technology_and_media/12/07/2021/60eb7ca69a7947b2f91f6a8d?from=newsfeed (дата обращения: 16.03.2021).

[12]Байден заявил о предложении Путину защитить 16 секторов от кибератак. URL: https://www.rbc.ru/politics/16/06/2021/60ca35199a7947191c7a646d (дата обращения: 16.03.2021).

занятия. Необходим критический системный анализ нормативной базы с указанием возможности неоднозначного толкования, наличия внутренних противоречий и вариантов практического выполнения применительно к конкретной сфере деятельности.

Исследованию этих вопросов для сферы обеспечения безопасности КИИ и посвящена настоящая работа, ориентированная, прежде всего, на образовательное сообщество по обучению специалистов в области информационной безопасности, но может быть полезной и для специалистов реального сектора экономики при принятии соответствующих управленческих решений.

Первый вопрос, а именно обоснование объективной необходимости новых подходов государственного регулирования, рассмотрен в сжатом историческом обзоре развития нормативно-правовой базы со ссылками на научные публикации по комплексу обеспечения информационной безопасности. Данный обзор не претендует на полноту исследования и изложения всех возможных нюансов, но, на наш взгляд, достаточно доказательно, без ссылок на директивные акты, показывает актуальность рассматриваемых вопросов и их роль в общем комплексе обеспечения информационной безопасности.

В качестве примеров неоднозначности и внутренних противоречий (парадоксов) проводится критический анализ некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывающий насущную необходимость их совершенствования и дополнительных усилий по толкованию основных положений, исходя из принципа креативного подхода по разъяснению сложных вопросов: «не как и что надо делать, а почему это надо».

1. Эволюция законодательной базы КИИ

1.1. Традиционные элементы правовой базы информационной безопасности

Условной точкой отсчета начала формирования российской нормативно-правовой базы в области информационной безопасности, не считая традиционной, очень устойчивой части по защите государственной тайны, можно считать 1995 г., с момента принятия, так называемого в кругах узких специалистов, «трехглавого» федерального закона[13].

Системный анализ его основных положений позволяет выделить несколько ключевых элементов, в той или иной степени послуживших импульсом к дальнейшему формированию действующей нормативной базы на уровнях иных правовых актов и нормативно-методических документов уполномоченных федеральных органов государственной исполнительной власти, для краткости далее называемых регуляторами. Как будет показано ниже, этот процесс формирования активно продолжается и в настоящее время с учетом новых достижений *социально-технологической революции* [13].

Первый и основной момент анализируемого закона – разделение общей государственной системы защиты информации с ограниченным доступом на две подсистемы, во многом похожих по методологическим подходам их организации, но законодательно разделенными по совокупности отдельных нормативных требований. Наряду с государственной тайной, выделенной в отдельный объект правового регулирования, введен правовой режим защиты, так называемой, конфиденциальной информации, в частности, многочисленных профессиональных тайн [14]. Это заложило основу формирования устойчивого отечественного рынка технических средств и оказания услуг в области информационной безопасности, регулируемого достаточно прозрачной и/или непротиворечивой нормативной базой.

[13]Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации».

Второй элемент – выделение в особую категорию конфиденциальной, то есть требующей защиты, информации так называемых персональных данных. Период становления этого направления государственного регулирования в силу чрезвычайной сложности проблемы растянулся до условного срока завершения в 2011 г. после принятия основополагающих поправок в специальное законодательство[14]. В настоящее время это направление фактически стало самостоятельным, так как получило новый законодательный импульс[15] для дальнейшего развития в части определения механизмов государственного регулирования процессов распространения так называемых общедоступных персональных данных.

Таким образом, эти первые два элемента, претерпевая за прошедшее время значительные изменения, как на законодательном, так и на нормативном уровнях, заложили правовую основу обоснования актуальности государственных требований для такого наиболее традиционного показателя безопасности информации (по общепринятой методологии информационной безопасности) как *конфиденциальность*. Справедливости ради отметим, что в настоящих реалиях это утверждение для персональных данных не совсем верно, о чем и свидетельствует упомянутая выше тенденция развития этого законодательства, но это предмет отдельного обсуждения.

Третий элемент – законодательная «путевка в жизнь» для электронного документооборота на основе электронно-цифровой подписи (ЭЦП), уже активно используемой в реальном секторе экономики, в частности, в платежных банковских системах. Актуальность этого направления нормативного регулирования и в настоящее время определяется необходимостью выполнения такого показателя безопасности передаваемых сведений как *целостность* и ее производных: достоверности, доверия, юридической значимости. Так как все технологии электронной подписи требуют выполнения условий конфиденциальности и «привязаны» к определенному физическому лицу, то можно утверждать о взаимосвязи и, соответственно, системности всех трех рассмотренных элементов. Становление нормативно-правовой базы регулирования электронного документооборота также заняло немалый период времени и условно завершилось в 2011 г. с выходом специального закона[16]. Стоит отметить, что в обозримом будущем и этот элемент будет существенно трансформирован в аспекте государственного регулирования в связи с бурным внедрением в финансовую сферу[17], а также сферу государственного управления и в реальный сектор экономики, систем обеспечения бизнес-процессов на основе технологии блокчейн [15, 16].

Вывод. Очевидно, что все рассмотренные выше элементы, даже с терминологической точки зрения, не могут быть положены в основу анонсированного выше обоснования для выделения рассматриваемой проблемы безопасности КИИ. Они либо достаточно устойчивы на текущий момент, либо тенденции их дальнейшего существенного развития определяются необходимостью их совершенствования с учетом новых современных вызовов в деле обеспечения информационной безопасности. Но, без

[14]Федеральный закон «О внесении изменений в Федеральный закон "О персональных данных» от 25 июля 2011 г. № 261-ФЗ.

[15]Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» от 30.12.2020 № 519-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_372682/ (дата обращения: 16.03.2021).

[16]Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 16.03.2021).

[17]Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 16.03.2021).

понимания этой структуры сложно определить роль и место нового механизма госрегулирования в общем комплексе обеспечения информационной безопасности.

1.2. Предыстория законодательного регулирования безопасности КИИ

Анализ публикаций периода подготовки «трехглавого закона» показывает, что уже тогда у специалистов по защите информации было понимание того, что указанных выше устойчивых до настоящего времени основных элементов недостаточно для полноты общей системы (комплекса) информационной безопасности. Так, например, банковская сфера, как и другие сектора реальной экономики, мотивированные на обеспечение непрерывности и устойчивости своего бизнеса, развивали свои системы безопасности на основе риск-ориентированных подходов, не предполагающих существенного государственного регулирования, но и, не выходя за его рамки. Но, к сожалению, в литературе применительно к теме нашего исследования можно указать лишь одну монографию [17] с научным обоснованием этого вопроса и оставшейся незамеченной профильными специалистами, возможно из-за ее названия, терминологически не связанного с проблемой защиты информации. В этой работе автором показана взаимосвязь общепринятых основных показателей безопасности информации: *доступности, целостности и конфиденциальности* с очевидным понятием качества *информационных ресурсов*, необходимых согласно законам *кибернетики* наряду с другими ресурсами для эффективного функционирования любой системы управления. Именно эта системная взаимосвязь может быть логическим обоснованием для часто используемых в СМИ и научно-популярной литературе терминов «кибербезопасность», «кибератаки», киберфизические системы и т.д. Но в действующей нормативно-правовой базе они практически нигде не используются, что иногда затрудняет ее толкование с точки зрения методологических основ информационной безопасности.

Такое киберпредставление, правда, своеобразным образом, нашло свое отражение в описанном выше «трехглавом» законе при легальном определении «первой головы» – информации как объекта права. Это своеобразие заключалось в том, что, нарушая, с точки зрения правоведов, каноны вещного права на отдельно выделенную категорию информации под названием информационные ресурсы, независимо от категории доступа, было распространено классическое право собственности, то есть защита законом в рамках гражданских правоотношений как элемента состава имущества. Эта норма была поддержана Гражданским Кодексом путем включения информации в объекты гражданских прав, нормой о возможности информации быть товаром и т.д. Взаимосвязь указанных норм с киберпредставлением работы Герасименко В.А. [17] становится очевидной не просто в силу чисто терминологического совпадения, а потому, что в терминах «трехглавого» закона информационные ресурсы – это документированная информация, то есть документы или массивы документов, которые и обращаются в любой системе управления. Таким образом, логически начинает проявляться необходимый четвертый элемент системы нормативного регулирования.

В общепринятых методологических терминах информационной безопасности его можно трактовать как требование обеспечения доступности, так как остальные показатели безопасности в аспекте госрегулирования заданы описанными выше элементами.

В то же время собственники (в терминах нынешнего законодательства обладатели) информации – это по определению санкционированные пользователи, иначе декларированное право собственности оказывается ничтожным, обладающие правовой возможностью защиты своих ресурсов даже при отсутствии у них свойства конфиденциальности. Самый главный вывод из приведенного анализа состоит в том, что таким, хотя и «экзотическим», образом определялась системность критериев и взглядов на

проблему правовой защиты информации, исходя из всех трех основных показателей информационной безопасности. И, на наш взгляд, четвертый элемент «трехглавого» закона можно рассматривать как предтечу рассматриваемого нового механизма госрегулирования. Но, в силу наличия существенных внутренних противоречий с позиций вещного права, обсуждение которых выходит за рамки настоящей работы, такое «киберпредставление» не получило сколь-нибудь существенного развития в нормативной базе, включая стандарты открытых систем. Более того, эти противоречия в совокупности с другими факторами привели к принятию в 2006 г. нового закона[18], анализ которого применительно к данному исследованию, в том числе по отношению к показателю доступности, будет дан далее.

Дальнейшая предыстория появления законодательства о безопасности КИИ связана уже с феноменом все возрастающего влияния современных информационно-коммуникационных технологий. Переход на рубеже XX–XXI века к глобальному постиндустриальному (именуемого иногда информационным) сообществу развитых стран зафиксировано впервые Окинавской Хартией. В то же время по мере развития информационных технологий актуализировались проблемы обеспечения их безопасности [18]. Адекватным отечественным ответом на новые вызовы стало утверждение в этот период информационной безопасности как одного из приоритетного направления в рамках Стратегии национальной безопасности и государственной политики по ее реализации.

В 2000 г. принимается первый обширный вариант Доктрины информационной безопасности, который по своей структуре и содержанию являлся директивой прямого действия [19]. Так одним из важных положений Доктрины стал достаточно короткий обобщенный перечень угроз национальной безопасности в информационной сфере, не потерявшим актуальности и в настоящее время в силу фундаментальности предложенных формулировок.

Среди них, имеющие прямое отношение к предмету данного исследования, хотя и с отсутствием прямой терминологической связи с понятием «информационная инфраструктура»:

– нарушения технологии обработки информации;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации.

Доктрина стала мощным стимулом для развития научных исследований и формирования отечественной целостной системы обеспечения информационной безопасности, включая системную структуру и распределение полномочий органов государственной власти.

В 2004 г. в ходе административной реформы Гостехкомиссия России, выполнявшая функции одного из регуляторов в сфере защиты информации с ограниченным доступом, была преобразована в Федеральную службу по техническому и экспортному контролю

[18]Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 16.03.2021).

(ФСТЭК России)[19]. При этом наряду с традиционными полномочиями Гостехкомиссии служба также получила статус уполномоченного органа по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры (ОБИ КСИИ). Этот момент можно условно считать исходной точкой начального периода становления анализируемого нового направления госрегулирования, которое и на настоящий момент еще далеко от своего завершения.

Исходя из общепринятой иерархии, верхним уровнем любой нормативной базы госрегулирования является базовый специальный закон либо, Указ Президента Российской Федерации.

Как показывает опыт формирования законодательства по электронному документообороту и персональным данным, период от исходной точки до принятия такого закона занимает от пяти, а то и более десяти лет с возможной вариацией базовых терминов. Такая же ситуация произошла и в сфере безопасности информационной инфраструктуры, хотя можно указать довольно существенную фундаментальную проработку правовых аспектов этой проблемы в рамках научных исследований.

В [20] научно обоснована необходимость выделения в качестве отдельного направления правового противодействия угрозам безопасности информационной инфраструктуре. Оно направлено «на нормативное регулирование отношений в области обеспечения сохранности объектов и сооружений связи, работоспособности средств связи, рационального использования радиочастотного ресурса, обслуживания абонентов сети связи, устойчивого функционирования сетей связи, информационных и компьютерных систем, глобальных информационных сетей и иных организационно-технических систем, предназначенных для повышения эффективности деятельности субъектов информационной сферы, а также производства и распространения продукции систем массовой информации и книгоиздания. Это противодействие основывается на нормах конституционного, административного, информационного и уголовного права».

Научное обоснование актуальности таких вопросов с позиций субъекта реального сектора экономики, например, Российские железные дороги (РЖД), представлено в [21]. В ней авторы ввели понятие *«функциональной безопасности»* как способности сложной системы устойчиво (штатно) функционировать в условиях наличия дестабилизирующих факторов. В свою очередь, такая устойчивость определяется *надежностью* ее аппаратно-технологических элементов и элементов обеспечения *информационной безопасности,* представление которой базировалось на перечне угроз, данном в Доктрине информационной безопасности.

Тем не менее, специальный законодательный акт отсутствовал, так как основные усилия законодателей и регуляторов в этот период были сосредоточены на совершенствовании базового «трехглавого» закона и нормативной базы трех основных его элементов. Показателен в этом смысле новый закон[18], принятый в 2006 г. вместо «трехглавого» закона. В аспекте данного исследования этот закон положение не исправил, а в некотором смысле даже усугубил, так как:

– информация в связи с отменой права собственности на информационные ресурсы юридически перестала быть объектом права, что было далее закреплено в Гражданском Кодексе;

– раздел о защите информации структурно и содержательно остался практически тем же, за исключением некоторых норм, понимание которых невозможно без дополнительных комментариев с указанием серьезных внутренних противоречий. В

[19]Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

частности, введена норма о возможности технологической защиты общедоступной информации, об актуальности этого отмечено выше. Но, сформулированные в законе условия такой возможности полностью разрушают всю логическую системную структуру самого раздела о защите информации, что является предметом отдельного анализа;

– замена «информатизации» как объекта правового регулирования на «информационные технологии» привело к тому, что в дальнейшем этот закон развивался в направлении правового регулирования вопросов создания и функционирования, прежде всего, глобальной сети Интернет. Поэтому закон фактически перестал быть базовым для области обеспечения информационной безопасности.

Несмотря на отсутствие специального закона, продолжалась работа по развитию директивной базы анализируемого направления, особенно после 2011 г., отмеченного выше как условный срок завершения формирования законодательной базы основных элементов правового обеспечения информационной безопасности. Так, можно еще рассмотреть директивный документ[20], в котором в пункте 3 (подпункт в) появилось определение *критической информационной инфраструктуры* Российской Федерации как *совокупности автоматизированных систем* ***управления критически важными объектами*** *и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий*.

В новом варианте Доктрины информационной безопасности в пункте 8 (подпункт б) (Указ Президента Российской Федерации от 5 декабря 2016 г. № 646) данное направление обозначено как одно из приоритетных в аспекте национальных интересов в информационной сфере. Следует также указать на интересную работу [22] общепризнанного специалиста в области информационной безопасности, в которой автор системно анализирует данную проблему в терминах «промышленной кибербезопасности», имеющей отличительные особенности от традиционной безопасности офисной информационной инфраструктуры. Но, как уже упомянуто выше такие «кибер» представления практически не используются в отечественной законодательной, а соответственно, и в нормативной базе.

Не будем выдвигать конспирологические причины еще почти пятилетнего срока до принятия базового закона[1], просто отметив 2017 г. как начало практического формирования действующей нормативной базы в сфере безопасности КИИ.

Вывод. описание эволюции законодательной и директивной базы, итогом которой стало приведенное выше легальное определение КИИ, методически увязанное с киберпредставлением безопасности информации, данным в работе Герасименко В.А. [17], на наш взгляд, полностью отвечает цели постановки в данном исследовании первой задачи по обоснованию понимания необходимости разработки новой нормативной базы государственного регулирования наряду с традиционно используемыми элементами.

2. Парадоксы нормативной базы безопасности объектов КИИ

2.1. Субъекты и предмет государственного регулирования безопасности КИИ

[20]«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803.

Субъекты и предмет нового направления государственного регулирования по букве Федерального закона № 187-ФЗ[1] во многом отличны, не всегда в лучшую сторону, от вышеприведенного определения критической информационной инфраструктуры[20].

Критерий ***субъектности*** не привязан к понятию «критически важный объект» (КВО), а задается по факту принадлежности к одной из 13 сфер деятельности, охватывающих значительный объем предприятий и организаций, как реального сектора экономики, так и социальной сферы. Они по умолчанию объявляются критическими в связи с предполагаемым наличием потенциально опасных процессов, показателем опасности которых, естественно, задан возможный ущерб нарушения штатного (устойчивого) функционирования. Очевидно, что анализируемое направление сближается с широко применяемым в бизнесе риск-ориентированным подходом. Но, отличие состоит в том, что в рассматриваемом случае неприемлемый уровень риска в интересах государства заранее задан в виде некоторых показателей значимости.

Предметом регулирования является безопасность объектов КИИ, к которым отнесены не только АСУ, но и ИС, а также ИТКС, принадлежащие субъектам «на праве собственности, аренды или ином законном основании».

Дополнительно к вышеупомянутым субъектам и объектам КИИ, естественно, добавляются владельцы и их сети электросвязи, используемые для организации ***взаимодействия*** указанных выше объектов. То есть, формально по «букве закона», если сетевая структура используется только для ***обеспечения*** функционирования конкретно заданной ИС или АСУ (что, как правило, и происходит на практике), то она не задает ни субъектность, ни объектность данного законодательства. Этот пример одной из неточностей нормативной базы, так как задать критерий по выделению процессов взаимодействия из простого обеспечения довольно затруднительно. Хотя заметим, что эта неточность не является большим препятствием на практике, так как обеспечение устойчивости функционирования сетей, относится скорее к проблеме надежности технических средств, чем к информационной безопасности. И, как следствие, эта проблема всегда имела адекватное решение, в том числе на уровне отраслевого нормативно-правового регулирования, начиная с принятия в 2003 г. первоначального варианта Закона «О связи»[21]. Но, формальное толкование этого положения создает, как будет показано ниже, определенные сложности при разработке нормативных актов отраслевого уровня для операторов связи.

Основная сложность практической реализации нормативных требований для субъектов, в нашем случае, возникает на этапе инвентаризации своих информационных объектов, объективно необходимого для дальнейшего категорирования и обеспечения безопасности. Особенно актуальна такая ситуация для крупных субъектов реального сектора экономики. Напомним, что их функциональная безопасность во многом определяется и адекватно обеспечивается надежностью производственных и технологических процессов [21]. В то же время выделить свою КИИ в виде отдельных, достигающих десятки и сотни ИС, АСУ и ИТКС крайне сложно. Какая-либо обоснованная методика инвентаризации, использующая непротиворечивые критерии отсутствует. Организация и определение процедур этого объективно необходимого этапа отдана на «откуп» самим субъектам. Поэтому очевидной становится возможная экономическая мотивация выжидательной позиции большой части субъектов, особенно реального сектора экономики.

[21]Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 16.03.2021).

Не помогает, а наоборот усложняет процедуру инвентаризации, привязка отдельных объектов КИИ к критическим процессам, которые они обеспечивают. (подпункты «а», «б» пункта 5 Постановления Правительства 127[22]. Нормативный перечень таких процессов охватывает практически все возможные виды, а именно – «управленческие, технологические, производственные, финансово-экономические и другие процессы в рамках выполнения функций (полномочий) или осуществления деятельности субъектов КИИ».

Такой парадокс продемонстрируем на примере, приведенном в методическом пособии АРСИБ[23], когда АС «Бухгалтерия 1С» металлургического предприятия (субъекта КИИ), обеспечивающая финансово-экономический процесс (*критический*, по указанным выше формальным критериям), должна быть отнесена к объектам КИИ. По мнению авторов пособия, в силу того, что эта АС не осуществляет управление, контроль или мониторинг (заметим, что последние являются обязательными элементами любой системы управления) потенциально опасных производственных процессов данного субъекта, она включается в инвентаризационный перечень (табл. 1), но не подлежит категорированию. В то же время в соответствии с нормативно установленной процедурой категорирования такому объекту присваивается четвертая категория как незначимого. И далее можно сделать парадоксальный вывод о ненужности защиты такого объекта.

Таблица 1. Пример заполнения инвентаризационной таблицы в методическом документе АРСИБ

№	Наименование ИС (АСУ, ИТКС)	ОКВЭД 2	Относимость к КИИ
1	Бухгалтерия 1С	69.20.2	-
2	АСУ металлургического цеха	24.10.1	+
3	ИС конструкторского отдела	72.19.2	+
п/п...	ИС склада	52.10.9	-

Вывод. Разрешение различных противоречий на текущий момент находится на уровне субъекта наряду с его ответственностью, что, очевидно, снижает адекватность нового механизма государственного регулирования. Поэтому, на наш взгляд, существующая нормативно-методическая база должна быть дополнена унифицированной методикой проведения инвентаризационного этапа так же, как и этапа категорирования. Методологической базой такой методики должно стать научно обоснованное киберпредставление [17] безопасности информационных ресурсов и понятие функциональной безопасности [21] критических процессов. При этом для мотивации субъектов по упомянутому выше критерию экономической целесообразности (снижению затрат на инвентаризацию) достаточно ограничиться объектами КИИ, встроенными в систему управления потенциально опасными процессами. А их дальнейшее нормативное категорирование и обеспечение безопасности в соответствии с государственными показателями значимости позволит формализовать (и в определенной степени

[22]Постановление Правительства Российской Федерации № 127 от 08.02.2018 «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» (с изменениями от 13 апреля 2019 г.).

[23]Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 2.0). Подготовлены Ассоциацией руководителей служб информационной безопасности (АРСИБ) The Association of Heads of Information Services security (AHISS) URL: http://aciso.ru/files/docs/metodichka_2.0.pdf (дата обращения: 16.03.2021).

унифицировать) требования ко всему комплексу обеспечения информационной безопасности субъекта.

2.2. Парадокс категорирования объектов КИИ

Далее покажем на отдельном примере категорирования объекта из сферы топливно-энергетического комплекса, что отдельные объекты КИИ, определенные по формальным признакам, могут и не являться таковыми.

Основные элементы приведенного примера установленной процедуры категорирования (рис. 1).

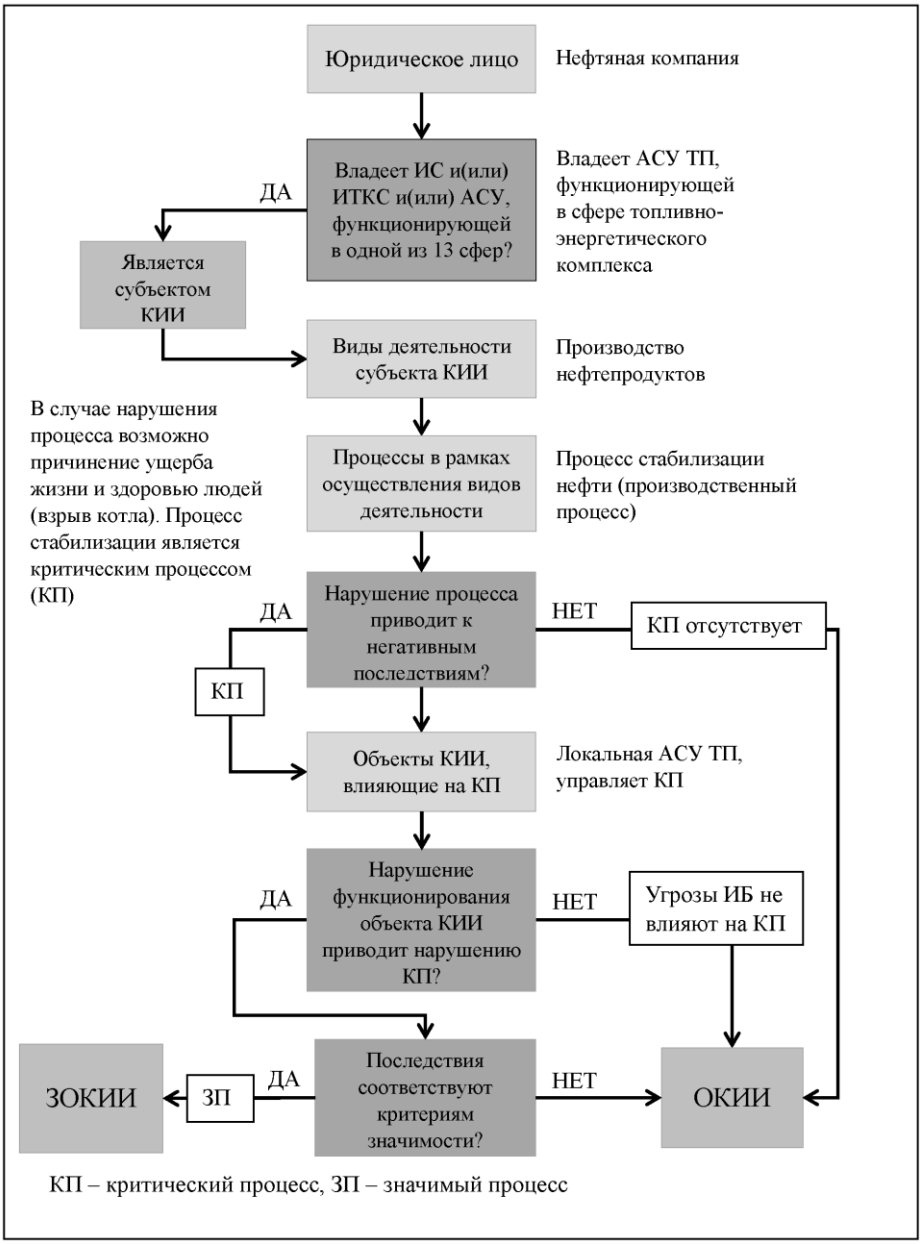


Рис. 1. Пример категорирования объекта КИИ
Fig. 1. Example of object categorization

1) ***Субъект КИИ*****:** нефтяная компания – российское юридическое лицо, которому на праве собственности принадлежит АСУ ТП, функционирующая в сфере топливно-энергетического комплекса согласно статье 2 пункт 8 закона 187-ФЗ[1]);

2) ***Вид деятельности как критерий субъектности КИИ*****:** производство нефтепродуктов в соответствии с пунктом 5 «а» Постановления Правительства 127[22]);

3) ***Критический процесс*****:** стабилизация нефти в ходе ее переработки, когда в случае нештатной ситуации, например, несанкционированного перекрытия технологической заслонки, может произойти взрыв и потенциальное причинение ущерба жизни и здоровью людей (п. 5 «б» Постановления Правительства 127[22]);

4) ***Объект КИИ*****:** локальная АСУ ТП стабилизации нефти, осуществляющая обеспечение указанного критического процессом (п. 5 «в» Постановления 127[22]) и подлежащая включению в перечень объектов КИИ и, соответственно, категорированию (п. 5 «г» Постановления Правительства 127[22]).

5) ***Этап оценки соответствию показателям критериев значимости*** масштаба возможных последствий в случае возникновения компьютерных инцидентов

В соответствии с 187-ФЗ[1] компьютерным инцидентом является факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки (т.е. причины нарушения могут быть любые). Предположим, что обеспечение противодействия указанному выше условию критичности, а именно, перекрытие технологической заслонки возможно лишь механическим способом по специальному регламенту. Как правило, так и происходит в большинстве случаев в реальном секторе экономики, когда нарушение и (или) прекращение функционирования АСУ ТП не может привести к последствиям, масштаб которых соответствует установленным показателям значимых последствий. Тогда, соответственно, должна быть присвоена 4-ая категория, как критерий незначимости.

В итоге рассмотренная локальная АСУ ТП, относящаяся к объектам КИИ по формальным признакам, таковой не является в силу того, что выполнение условий безопасности заложены непосредственно в регламент технологического процесса, а не в систему автоматизированного управления, что является типовой реализацией риск-ориентированного подхода субъектов реального сектора.

Разрешение такого парадокса требует уточнения самого понятия КИИ, определяющего область действия нового законодательства. Выше было показано[20], что информационная инфраструктура директивно определяется как ***совокупность*** объектов, хотя и без указания какой либо их взаимосвязи. А в анализируемой нормативной базе отсутствует даже термин совокупность, что, видимо, должно приниматься по умолчанию. Такой подход противоречит методологии разработки нормативной базы, не допускающей неясность и неоднозначное толкование основных положений.

Одно из возможных общепринятых определений инфраструктуры формулируется как комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования системы[10]. Если увязать это определение с киберпредставлением [17], то такой основой для КИИ любого субъекта выступает структурно определенная совокупность элементов (в нашем случае объектов КИИ) управления критическими процессами. Их устойчивость обеспечивается необходимым уровнем качества (безопасности) используемых информационных ресурсов.

Иными словами между объектами инфраструктуры должна существовать какая-либо взаимосвязь – физическая, информационная, функциональная и т.п., и именно она

определяет сущность самого понятия инфраструктуры. То есть, локальная АСУ ТП, не имеющая взаимосвязи с другими критическими объектами, не включается в КИИ по определению. Принимая во внимание ее функциональное предназначение с позиций представления, данного в [21], методологически она может быть отнесена к инфраструктуре топливно-энергетического комплекса, к производственной (промышленной) инфраструктуре в целом, но никак не к рассматриваемой нами проблеме.

В связи с важностью вопроса о легальном, прозрачном определении понятия КИИ целесообразно привести мировой опыт развитых стран.

1) В США основой методологии разрешения анализируемой проблемы является фундаментальное понятие «*Критическая инфраструктура* (КИ)»[24].

Во избежание лингвистических неточностей приведем оригинальное определение: «Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters».

В переводе с комментариями КИ США – это системы и активы, будь то физические (аналог отечественных КВО и/или значимых объектов КИИ) или виртуальные (в нашем понимании информационные ресурсы), настолько жизненно важные для Соединенных Штатов, что неспособность или разрушение таких систем и *активов* (в частности, в нашем понимании информационных ресурсов) окажет ослабляющее воздействие на *кибербезопасность*, национальную экономическую безопасность, национальное общественное здравоохранение или безопасность или любую комбинацию этих вопросов. То есть, основополагающим в такой формулировке является государственный интерес, выраженный в масштабе последствий нарушения их устойчивого функционирования. При этом не важно, в какой сфере они функционируют и являются-ли они «физическими» либо «виртуальными». В практической плоскости в США имеются естественные приоритетные ограничения, которые по сообщениям СМИ оцениваются в 16 наименований объектов.

2) Аналогичный подход использует и Европейский Союз, в частности, его политико-экономический лидер Германия. Ее к*ритически важная инфраструктура* представлена как организации или объекты, имеющие важное значение для государства, отказ или нарушение работы которых может привести к долгосрочным перебоям в поставках, значительным сбоям в общественной безопасности или другим серьёзным нарушениям. То есть основу КИ составляют «важные» объекты, совокупность которых далее [23] подразделяется на базовую техническую инфраструктуру (энергетика, информационные и коммуникационные технологии, транспорт и движение, водоснабжение и водоотведение) и инфраструктуру социально-экономических услуг (здравоохранение, «питание», аварийно-спасательные службы, борьба с бедствиями, парламент, правительство, государственное управление, судебные учреждения, финансы и страхование, СМИ и культурные ценности). Безопасность объектов КИ Германии выражается в терминах обеспечения их *кибербезопасности, то есть безопасности систем управления*.

Вывод. Проведенный выше анализ настоятельно подчеркивает актуальность совершенствования анализируемой нормативной базы в аспекте более четкого и однозначного толкования базового понятия КИИ. При этом необходимо выстроить логическую цепочку взаимосвязи действующих процессов в КВО (физических объектах)

[24]NIST Special Publication 800-30 Revision 1 - Специальная публикация Национального института Стандартов и Технологий США.

с «виртуальными» (в нашем понимании, информационными) объектами КИ. Тем более, что в ближайшее время в состав КИ России должны войти так называемые киберфизические системы управления[25], анализ свойств которых как объектов КИИ выходит за рамки данной работы.

2.3. Взаимопересечение различных объектов КИИ

Как было показано выше предметом нового механизма госрегулирования является безопасность законодательно заданных видов объектов, а именно ИС, АСУ, ИТКС и сетей их взаимодействия. Несмотря на кажущуюся по умолчанию простоту определения объектов регулирования, на практике при проведении организационных процедур по реализации нормативных требований могут возникнуть определенные сложности по их выделению из общей информационной инфраструктуры.

Так в соответствии с ГОСТ Р 50922-2006[26] ИС как некий объект проектирования представляет собой **совокупность** содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Без специального разъяснения формально такая дефиниция может быть распространена и на бумажное делопроизводство, часто осуществляемое в настоящее время с использованием компьютеров. Поэтому, на наш взгляд целесообразнее было бы использование понятия автоматизированной системы обработки информации (АСОИ). Тем более, что термин автоматизированная система (АС) достаточно часто использован в традиционной нормативной базе ФСТЭК России.

Понятие АСУ как объекта, обеспечивающего устойчивость критического процесса и, соответственно, обоснованно включенного в КИИ, уже было рассмотрено ранее, поэтому останавливаться на нем специально не имеет смысла.

В нашем случае отметим тот факт, что многие ИС (АС) и АСУ на практике как объекты КИИ являются распределенными системами, поэтому отделить их от ИТКС практически невозможно (рис. 2). Именно ИТКС по определению (ГОСТ Р 52653-2006[27]) соединяет все компоненты (объекты) в единую информационную инфраструктуру.

Конечно, данную «размытость» границ законодательно заданных объектов КИИ можно попытаться разрешить на уровне локальных нормативных актов отдельных отраслей деятельности субъектов КИИ. Уже изданы различные методические рекомендации по категорированию, в которых разъясняются отдельные неоднозначные моменты: в сфере связи, в сфере здравоохранения, в области топливно-энергетического комплекса и т.д. Но, жесткая привязка этих актов к вышестоящим законодательным нормам дает прямо противоположные результаты.

В соответствии с методическими рекомендациями в сфере связи[28] выделенная сеть передачи данных для ***управления и мониторинга*** сетей электросвязи является ИТКС,

[25]Национальная программа «Цифровая экономика Российской Федерации». Утверждена протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

[26]ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации «Защита информации. Основные термины и определения», разработан ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (далее – ГОСТ Р 50922-2006).

[27]ГОСТ Р 52653-2006 Национальный стандарт Российской Федерации «Информационно-коммуникационные технологии в образовании. Термины и определения», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 419-ст (далее – ГОСТ Р 52653-2006).

[28]Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих. субъектам критической информационной инфраструктуры, функционирующим в сфере связи. Введены в действие для опытного использования в тестовом режиме

хотя по функционалу, как видно из названия, она должна входить в состав автоматизированной системы управления и мониторинга сетей электросвязи, являясь частью АСУ.

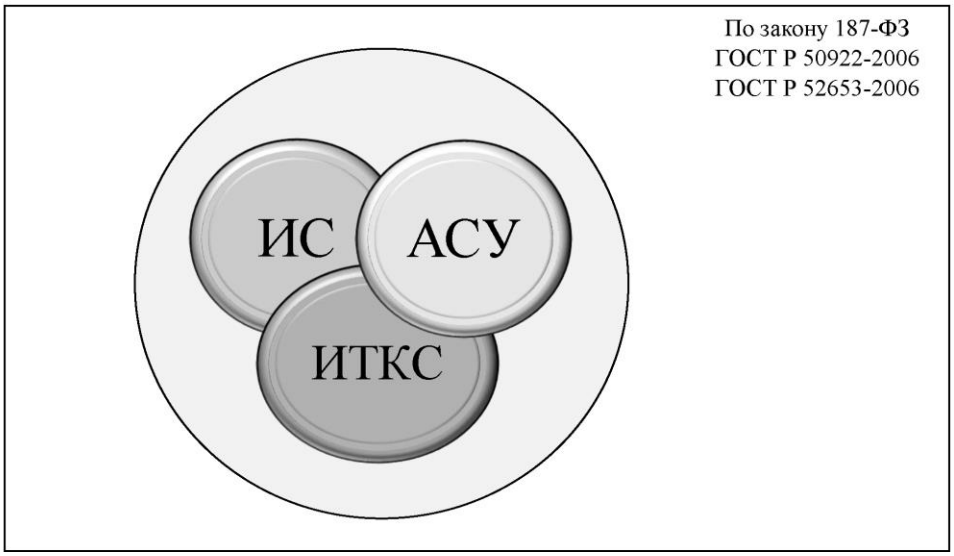


Рис. 2. Терминологическое пересечение понятий ИС, АСУ и ИТКС
Fig. 2. Terminological intersection of the concepts of Information Systems, Automated Control Systems and Information and Telecommunications Systems

Помимо вышеуказанного пересечения ИС и АСУ с ИТКС, сами ИС и АСУ также имеют терминологическое взаимопересечение. Например (в соответствии с теми же рекомендациями в сфере связи), система самообслуживания абонентов является ИС. Хотя по своему функционалу она обеспечивает автоматизацию управления (подключения/отключения) услуг связи (то есть управление критическим процессом) и должна являться АСУ. На данном примере видно, что АСУ является той же самой ИС (и наоборот), разница лишь в том, что в АСУ обрабатывается исключительно служебная информация, и целью этой обработки является управление определенным процессом, т.е. сама обработка информации не является целью функционирования АСУ.

Примером положительного выхода из указанной понятийной размытости может служить нормативно-методический акт[29] основного регулятора в рассматриваемой сфере – ФСТЭК России. В п. 1.3. данной методики, не привязанной к Постановлению Правительства 127, значительно расширена как субъектность, так и объектность применения данного акта на государственные и муниципальные ИС, системы персональных данных (ИСПДн), ИС управления производством, используемым организациями оборонно-промышленного комплекса, АСУ П и АСУ ТП на критически важных объектах (потенциально опасных), представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Это подтверждает тот факт, что подход к обеспечению защиты иных «критических» информационных структур по своей сути должен быть такой же, как и к объектам КИИ.

решением Исполкома Общественно-государственного объединения «Ассоциация документальной электросвязи» от 26 июня 2019 г. Согласовано: 8 Центр ФСБ России и ФСТЭК России. URL: https://www.rans.ru/images/metrecKII.pdf (дата обращения: 16.03.2021).

[29] Методика оценки угроз безопасности информации, утверждена ФСТЭК России 5 февраля 2021 г. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения: 16.03.2021).

Помимо этого, в новую методику было добавлено понятие «информационно-телекоммуникационная инфраструктура, на базе которой функционируют объекты КИИ», а также прописана возможность разработки модели угроз для «совокупности взаимодействующих систем и сетей оператора».

Не останавливаясь подробно на анализе основных положений методики, что является предметом отдельного анализа, заметим, что они дают возможность исключения необходимости определения угроз безопасности (и соответственно установления мер защиты) строго для отдельного объекта КИИ, границы которого, как уже отметили ранее, могут быть достаточно размыты.

Так как задание модели угроз безопасности с методологической точки зрения – это определяющий этап создания и совершенствования любой системы информационной безопасности, то принятие указанного нормативно-методического документа, безусловно, положительный факт. В то же время многие его положения расходятся с нормами анализируемого законодательства по безопасности КИИ. Достаточно указать только, что расширяя перечень объектов, методика ограничивает сферу применения для субъектов только в виде государственных и муниципальных образований. Другие субъекты, частности, реального сектора экономики, в силу ограничений механизмов госрегулирования на основе общего законодательства, выведены из сферы действия данного нормативного акта. Следовательно, их действия, по-прежнему, остаются на уровне принятия самостоятельных реальных решений вопросов обеспечения безопасности своих критических процессов.

Вывод. Терминологическая размытость границ объектов защиты вследствие неоднозначности толкования законодательно заданных понятий приводит к трудностям в их выявлении с целью дальнейшего категорирования. В итоге это может оказать влияние и на обоснованность предполагаемых мероприятий по обеспечению их безопасности (устойчивости) – «проблематично» защищать то, что однозначно не определено.

3. Нормативное регулирование и ответственность субъектов КИИ

Основой системы государственного регулирования является задание и реализация мер юридической ответственности за невыполнение субъектами правоотношений нормативных требований. В этом аспекте проблемой по обеспечению безопасности КИИ, на наш взгляд, будет являться то, что основой для определения субъектности, а, следовательно, и ответственности служит принадлежность к одной из 13 сфер деятельности.

В то же время очевидно, что в данном случае такой основой, как принято в методологии правоведения, должны быть последствия или ущерб национальным интересам, к которым может привести невыполнение нормативных требований. Именно такой подход был заложен в рассмотренном выше определении[20] понятия «критическая информационная инфраструктура». В данной формулировке присутствует понятие «совокупность», причем все объекты, входящие в совокупность, объединены в некую систему своим предназначением, а, главное, масштабом последствий их устойчивого функционирования.

Если сравнить указанное определение с нормами нового законодательства, то не трудно заметить, часть сфер деятельности «образца» 2012 г. законодательно «выпали» из состава КИИ, хотя сама область расширилась путем включения наряду с АСУ также ИС и ИТКС.

Усугубляет проблему и формулировка определения значимого объекта КИИ[1], в которой нет указанной выше причинно-следственной связи, а значение имеют не свойства

объекта регулирования, а наличие его записи в соответствующем государственном реестре.

И опять на передний план для субъектов реального сектора экономики выходит мотивация их выжидательной позиции, исходя из экономической целесообразности включения их объектов в состав государственного реестра. Тем более, что функциональная безопасность этих субъектов во многом и так обеспечивается выполнением требований технологической устойчивости. В этой ситуации применение новых норм *административной ответственности,* на наш взгляд, вряд ли будет адекватным в аспекте существенного развития анализируемого направления государственного регулирования. Это может лишь способствовать к переходу субъектами от выжидательной позиции к формальному выполнению установленных процедур, что как уже указывалось не меньшая угроза национальной безопасности.

Нестыковки и неточности директивной и нормативно-правовой базы вряд ли дадут возможность адекватного применения соответствующих расширенных норм об уголовной ответственности в соответствии с п. 3 статьи 274.1 УК РФ[2]. Должностные лица субъектов КИИ можно привлечь к уголовной ответственности за нарушение «***правил эксплуатации*** средств хранения, обработки или передачи *охраняемой компьютерной информации*, содержащейся в *критической информационной инфраструктуре* Российской Федерации, или ***информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре*** Российской Федерации ... если оно **повлекло причинение вреда критической информационной инфраструктуре** Российской Федерации».

Учитывая вышеуказанные проблемы, в данной формулировке нормы уголовной ответственности либо не будут работать вообще, так как принципиально невозможно причинить вред сразу всем объектам КИИ (в том числе никак не взаимосвязанным), либо нарушения на одном объекте КИИ априори будут приравнены к причинению вреда всей КИИ, что, будет не совсем логично, учитывая «некритичность» отдельных объектов КИИ.

Кроме того, в данном случае вред рассматривается не в отношении государства и его граждан, который оценивается по установленным критериям значимости[22], а в отношении такого правового объекта как КИИ, нынешнее нормативное определение которой, как показано выше, достаточно спорно и неоднозначно.

Вывод. Хотя новая система госрегулирования безопасности КИИ на текущий момент и поддержана нормами административной и уголовной ответственности, но в силу размытости, нестыковок и неоднозначности нормативной базы возможность их практического применения в условиях «регуляторной гильотины» является очень дискуссионной.

Заключение

Анализ предыстории развития и действующей нормативно-правовой базы по обеспечению безопасности объектов КИИ показал необходимость применения нового механизма государственного регулирования, а также его место в общем комплексе информационной безопасности страны.

Тем не менее, приведенные в работе примеры неоднозначности и внутренних противоречий (парадоксов) некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывают существующий общественный запрос по их совершенствованию. Необходимы дополнительные усилия, как со стороны научных специалистов, так и регуляторов по толкованию основных положений нормативно-

правовой базы. Основная цель этих усилий – снижение излишних затрат субъектов за счет более четкого нормативного определения самого понятия КИИ, ее структуры, объектов защиты и их взаимосвязей, исходя из общих принципов системного подхода к анализу сложных систем.

Изложенные в работе результаты могут быть полезны всем субъектам анализируемого законодательства, а также образовательным организациям, приступившим к практической реализации новых образовательных программ подготовки, переподготовки и повышения квалификации работников сил обеспечения, ответственных за реальный уровень безопасности отечественной КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбатов В.С., Дураковский А.П., Лобанов М.И. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 54–68. 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.04.
2. Каннер Т.М. Особенности повышения квалификации специалистов по обеспечению безопасности значимых объектов критической информационной инфраструктуры. безопасность информационных технологий. Безопасность информационных технологий, [S.l.]. Т. 26, № 3. С. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02.
3. Грачков И.А., Малюк А.А. Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты). Безопасность информационных технологий, [S.l.]. Т. 26, №. 1. С. 56–63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06.
4. Грачков И.А Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты. Безопасность информационных технологий, [S.l.]. Т. 25, №. 1. С. 90–98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09.
5. Herrera Luis-Carlos & Maennel Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. Vol. 25. P. 50–61. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
6. 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.
7. 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.
8. 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.
9. В РЖД заявили о небольшом ущербе от атаки вируса WannaCry // Interfax.ru//. URL: https://www.interfax.ru/russia/563900/ (дата обращения: 16.03.2021).
10. Трунина А., Рождественский И., Фадеева А., Вовнякова А. «Роснефть» сообщила о мощной хакерской атаке на свои серверы // URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c/ (дата обращения: 16.03.2021).
11. Макарова О.С., Поршнев С.В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
12. Вавичкие А.Н., Горбатов В.С., Дураковский А.П., Чжен Д.А. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений. Безопасность информационных технологий, [S.l.]. Т. 26, № 2. С. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
13. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности // Стратегические приоритеты. 2017. № 2 (14). С. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (дата обращения: 16.03.2021).

14. Фатьянов А.А. Тайна и право (основные системы ограничений на доступ к информации в российском праве) / М.: МИФИ. 1999. – 288 с. URL: https://elibrary.ru/item.asp?id=29067845& (дата обращения: 16.03.2021).
15. Будзко В.И., Мельников Д.А. Информационная безопасность и блокчейн // Системы высокой доступности. 2018. Т. 14. № 3. С. 5–11. DOI: http://dx.doi.org/10.18127/j20729472-201803-02.
16. Запечников, Сергей В. Системы распределенного реестра как инструмент обеспечения доверия между участниками бизнес-процессов. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 37–53, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.03.
17. Герасименко В.А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. – 320 с.
18. Тарасов, Анатолий М. Окинавская хартия и конгрессы ООН: Вопросы противодействия киберпреступности. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 120–131, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09.
19. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические - и методологические основы. /Под редакцией В.А. Садовничего, В.П. Шерстюка. (Монография). М.: МЦНМО – МГУ им. М.В Ломоносова, 2002. – 351 с. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf (дата обращения: 16.03.2021).
20. Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России : Дис. д-ра юрид. наук : 05.13.19 : Москва, 2004. – 371 с. РГБ ОД, 71:05-12/1. URL: https://static.freereferats.ru/_avtoreferats/01002635074.pdf (дата обращения: 16.03.2021).
21. Шубинский И.Б., Тарасов А.А. Современная парадигма безопасности критически важных систем информационной инфраструктуры. Безопасность информационных технологий. 2005, № 3. С. 7–13.
22. Касперский Е.В. В заложниках у автоматики: как защитить промышленность от кибератак. Безопасность информационных технологий, [S.l.]. Т. 23, № 3. С. 7–10, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (дата обращения: 16.03.2021).
23. Котов А. Развитие критических инфраструктур в Германии: выход из тени // Научно-аналитический вестник ИЕ РАН, 2021, №1. С. 96–102. DOI: http://dx.doi.org/10.15211/vestnikieran1202196102.

REFERENCES

[1] Gorbatov Viktor S., Durakovskiy Anatoly P., Lobanov Maxim I. On professional standards for personnel training on safety of critical information infrastructure objects. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 54–68, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.04 (in Russian).
[2] Kanner Tatiana M. Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure. IT Security (Russia), [S.l.]. Vol. 26, no. 3. P. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (in Russian).
[3] GRACHKOV, Ignaty A.; MALYUK, Anatoly A. Development problems of trusted software applied at critical information infrastructure objects (organizational and methodological aspects). IT Security (Russia), [S.l.]. Vol. 26, no. 1. P. 56–63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06 (in Russian).
[4] Grachkov Ignatiy A. Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.]. Vol. 25, no. 1. P. 90–98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09 (in Russian).
[5] Herrera Luis-Carlos & Maennel Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. Vol. 25. P. 50–61. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
[6] 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.
[7] 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.
[8] 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.
[9] Russian Railways announced a small damage from the attack of the WannaCry virus. Interfax.ru. URL: https://www.interfax.ru/russia/563900 (accessed: 16.03.2021) (in Russian).
[10] Trunina A., Rozhdestvensky I., Fadeeva A., Vovnyakova A. Rosneft reported a powerful hacker attack on its servers. URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c (accessed: 16.03.2021) (in Russian).

[11] Makarova Olga S., Porshnev Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.]. Vol. 27, no. 1. P. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[12] Vavichkin Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.]. Vol. 26, no. 2. P. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03 (in Russian).
[13] Akhromeeva T.S., Malinetskiy G.G., Posashkov S.A. Strategies And Risks Of Digital Reality. Strategic Priorities. 2017. No 2 (14). P. 88–102. URI: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (accessed: 16.03.2021) (in Russian).
[14] Fatyanov A.A. Secrecy and law (the main systems of restrictions on access to information in Russian law). M.: MEPHI. 1999. – 288 p. URL: https://elibrary.ru/item.asp?id=29067845& (accessed: 16.03.2021) (in Russian).
[15] Budzko V.I., Melnikov D.A. Information security and blockchain. Highly available systems. 2018. Vol. 14. No. 3. P. 5–11. DOI: http://dx.doi.org/10.18127/j20729472-201803-02 (in Russian).
[16] Zapechnikov, Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 37–53, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.03 (in Russian).
[17] Gerasimenko V.A. Fundamentals of information literacy. M.: Energoatomizdat, 1996. – 320 p.
[18] Tarasov, Anatoly M. The Okinawa Charter and the Congress of the United Nations: cybercrime countering issues. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 120–131, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09 (in Russian).
[19] Streltsov A.A. Ensuring information security of Russia. Theoretical - and methodological foundations. Edited by V. A. Sadovnichy, V. P. Sherstyuk. (Monograph). Lomonosov Moscow State University, 2002. – 351 p. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf (accessed: 16.03.2021) (in Russian).
[20] Streltsov A. A. Theoretical and methodological foundations of legal support of information security in Russia: Dis. Dr. yurid. sciences': 05.13.19: Moscow, 2004. – 371 p. URL: https://static.freereferats.ru/_avtoreferats/01002635074.pdf (accessed: 16.03.2021) (in Russian).
[21] Shubinsky I. B., Tarasov A. A. Modern security paradigm of critical information infrastructure systems. IT Security (Russia). 2005, no. 3. P. 7–13 (in Russian).
[22] Kaspersky E.V. Automation hostage: how to protect the industry againts cyber attacks. IT Security (Russia), [S.l.]. Vol. 23, no. 3. P. 7–10, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (accessed: 16.03.2021) (in Russian).
[23] Kotov A. Development of Critical Infrastructures in Germany: Out of the Shadow. Scientific and Analytical Bulletin of the IE RAS, 2021, no. 1. P. 96–102. DOI: http://dx.doi.org/10.15211/vestnikieran1202196102 (in Russian).

Поступила в редакцию – 02 апреля 2021 г. Окончательный вариант – 17 августа 2021 г.
Received – April 02, 2021. The final version – August 17, 2021.

Ирина Г. Дровникова[1], Елена С. Овчинникова[2]
[1,2]Воронежский институт министерства внутренних дел Российской Федерации,
пр-кт Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524

ОБОСНОВАНИЕ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПРОВЕДЕНИЯ НАТУРНОГО ЭКСПЕРИМЕНТА

DOI: http://dx.doi.org/10.26583/bit.2021.3.02

Аннотация. Целью статьи является обоснование законов распределения времени на различных этапах реализации сетевых атак в защищенных автоматизированных системах органов внутренних дел. Для достижения поставленной цели применен метод натурного эксперимента по исследованию динамики протекания информационного конфликта «Сетевая атака – система защиты» с учетом различий изначальных и потенциальных возможностей конфликтующих сторон на основе разработанной обобщенной графовой модели. Результаты натурного эксперимента представлены в виде количественных значений времен запуска и реализации типовой сетевой атаки, воздействующей на информационные ресурсы и элементы защищенной автоматизированной системы органов внутренних дел, времен загрузки и функционирования системы защиты информации от несанкционированного доступа. Рассчитано количество итераций экспериментов, проводимых над сетевой атакой и системой защиты, достаточное для адекватного обоснования законов распределения времени на различных этапах конфликтного взаимодействия. Для обоснования нормального закона распределения времени на начальном этапе протекания информационного конфликта использован χ^2-критерий К. Пирсона, а для обоснования экспоненциального закона на последующем его этапе – λ-критерий А.Н. Колмогорова. Результаты эмпирического распределения значений времен реализации сетевой атаки и функционирования системы защиты представлены в табличной форме и наглядно отображены графически. Знание законов распределения позволит разработать аналитическую модель информационного конфликта «Сетевая атака – система защиты» на основе графовой модели динамики реализации типовой сетевой атаки и обобщенной графовой модели динамики протекания конфликта. Перспективы использования разработанной аналитической модели связаны с расчетом вероятностно-временных характеристик и проведением точной количественной оценки опасности реализации сетевых атак в автоматизированных системах, эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел.

Ключевые слова: сетевая атака, система защиты информации от несанкционированного доступа, информационный конфликт, натурный эксперимент, закон распределения времени.
Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С. ОБОСНОВАНИЕ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПРОВЕДЕНИЯ НАТУРНОГО ЭКСПЕРИМЕНТА. Безопасность информационных технологий, [S.l.], т. 28, №. 3, с. 28–43, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1360. DOI: http://dx.doi.org/10.26583/bit.2021.3.02.

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2]
[1,2]Voronezh Institute of the Ministry of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524

Justification of network attacks time distribution in automated systems of internal affairs bodies based on a full-scale experiment

DOI: http://dx.doi.org/10.26583/bit.2021.3.02

Abstract. The goal of the paper is to substantiate the laws of time distribution at various stages of the implementation of network attacks in protected automated systems of internal affairs bodies. To achieve this goal, a full-scale experiment to study the dynamics of the "Network attack-protection system" information conflict was carried on taking into account the differences in the initial and potential capabilities of the conflicting parties on the basis of the developed generalized graph model. The results of the full-scale experiment are presented in the form of quantitative values of the start and implementation times of typical network attack affecting information resources and elements of a protected automated system of internal affairs bodies, the times of loading and functioning of the information protection system. The number of iterations of experiments with a network attack and security system sufficient for an adequate justification of the laws of time distribution at various stages of conflict interaction is calculated. To justify the normal law of time distribution at the initial stage of the information conflict, the χ^2-criterion of K. Pearson was used, while to justify the exponential law at its subsequent stage the λ-criterion of A.N. Kolmogorov was used. The results of the empirical distribution of the values of the time of the implementation of a network attack and the functioning of the protection system are presented in tabular form and graphically displayed. Knowledge of the distribution laws will allow us to develop an analytical model of the"Network attack-protection system" information conflict based on a graph of the dynamics of the implementation of a typical network attack and a generalized graph of the dynamics of the conflict. The prospects of using the developed analytical model are associated with the calculation of probabilistic-temporal characteristics and an accurate quantitative assessment of the danger of implementing network attacks in automated systems operated in a protected version at the informatization objects in internal affairs bodies.

Keywords: network attack, information protection system against unauthorized access, information conflict, full-scale experiment, law of time distribution.

For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA, Elena S. Justification of network attacks time distribution in automated systems of internal affairs bodies based on a full-scale experiment. IT Security (Russia), [S.l.], v. 28, n. 3, p. 28–43, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1360. DOI: http://dx.doi.org/10.26583/bit.2021.3.02.

Введение

Получение точных количественных оценок опасности угроз удаленного несанкционированного доступа (НСД), реализуемых посредством сетевых атак в автоматизированных системах (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), в соответствии с требованиями международных и отраслевых стандартов Российской Федерации[1,2,3], нормативных и методических документов ФСТЭК России[4,5,6] и руководящих документов МВД России, посвященных вопросам информационной безопасности АС[7], приводит к необходимости разработки аналитической модели оценки вероятности реализации сетевых атак в защищенных АС ОВД. Построение такой модели подразумевает обоснование закона распределения времени реализации сетевых атак.

Проведенный анализ открытых литературных источников, посвященных данной

[1]ISO/IEC 15408-2012. Common Criteria for Information Technology Security Evaluation.
[2]ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.
[3]ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.
[4]ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
[5]ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
[6]ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации. (утв. ФСТЭК России 5 февраля 2021 г.).
[7]Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169.

проблеме, позволяет констатировать, что при разработке аналитической модели закон распределения времени реализации сетевых атак в АС традиционно полагается экспоненциальным [1–4]. При этом процесс реализации атаки рассматривается либо независимо от функционирования системы защиты информации (СЗИ) от НСД в АС [1, 2], либо принимается допущение, что в конфликтном взаимодействии изначальные возможности сторон равны и конфликтные действия начинаются ими одновременно [3, 4], что в реальной практике эксплуатации защищенных АС ОВД выполняется крайне редко [5–7].

В данной статье представлено обоснование различных законов распределения времени в процессе поэтапной реализации типовых сетевых атак в защищенных АС ОВД, основанное на проведении экспериментального исследования динамики их конфликтного взаимодействия с СЗИ от НСД с учетом различий изначальных и потенциальных возможностей конфликтующих субъектов.

1. Постановка задачи

Процесс обоснования распределения времени реализации типовых сетевых атак на основе проведения экспериментального исследования динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, включает следующие этапы:

1. Построение обобщенной графовой модели динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД с выделением основных этапов конфликтного взаимодействия.
2. Проведение натурного эксперимента и представление его результатов в табличной форме в виде количественных значений времен запуска и реализации сетевой атаки, времен загрузки и функционирования СЗИ от НСД на основе разработанной модели.
3. Расчет достаточного количества итераций экспериментов, проводимых над сетевой атакой и СЗИ от НСД на различных этапах их конфликтного взаимодействия в АС ОВД.
4. Обоснование законов распределения времени реализации сетевой атаки и функционирования СЗИ от НСД на различных этапах их конфликтного взаимодействия на основе χ^2-критерия К. Пирсона и λ-критерия А.Н. Колмогорова с достаточностью 0,05.
5. Графическое представление количества реализаций сетевой атаки и функционирований СЗИ от НСД в защищенной АС ОВД в зависимости от времени для основных этапов обобщенной графовой модели динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД».

2. Метод исследования

Методом исследования является натурный эксперимент, описывающий динамику протекания информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД. Для его проведения был развернут лабораторный стенд, состоящий из сервера и трех автоматизированных рабочих мест (АРМ) со следующими характеристиками: процессор Intel Core i3-2100 с тактовой частотой 3.1 ГГц, оперативная память (ОЗУ) 4 Гб, дисковая память (HDD) 500 Гб, функционирующими под управлением 32-разрядной операционной системы (ОС) Windows 7. Вне локальной сети на отдельном персональном компьютере (ПК) установлена ОС Kali Linux с целью реализации деструктивных воздействий в виде сетевых атак.

Практическая составляющая поэтапного удаленного НСД к информационным

ресурсам и элементам защищенной АС ОВД реализовалась в виде скриптов, написанных на языке Bash. Запуск данных скриптов проводился с ПК, функционирующего под управлением ОС Kali Linux, посредством разработанного для каждого типа атаки программного кода.

Инсталляция и настройка СЗИ от НСД в АС ОВД основывались на рекомендациях разработчика. При этом была развернута полная версия СЗИ от НСД на трех АРМ и совместно с нею установлено прикладное программное обеспечение в виде пакета Microsoft Office 13 и антивируса «Kaspersky». В качестве СЗИ от НСД использована широко применяемая в АС ОВД СЗИ от НСД «Dallas Lock 8.0-С»[8], являющаяся сертифицированным программным комплексом средств защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну, в локальных и сетевых АРМ под управлением ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

3. Модель и результаты исследования

Для обеспечения успешности реализации сетевой атаки или защиты информационных ресурсов и элементов АС ОВД необходимо оценить возможности обеих сторон в информационном конфликте «Сетевая атака – СЗИ от НСД». На рис. 1 приведена предложенная в [8] обобщенная графовая модель динамики протекания указанного конфликта в виде ориентированного графа состояний и переходов моделирующего его конечного полумарковского процесса (КПМП) с выделением основных этапов взаимодействия конфликтующих субъектов.

В качестве изначальных возможностей конфликтующих сторон, по которым осуществляется их сравнение в представленной графовой модели для определения начальных условий конфликта, рассматриваются производительности и объемы памяти сетевой атаки и СЗИ от НСД, определяемые в ходе проведения натурного эксперимента.

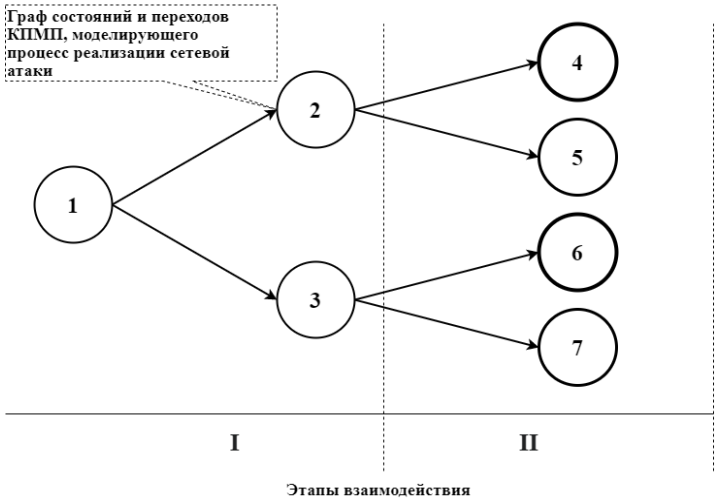
В [9–12] определены и проанализированы восемь наиболее опасных и часто реализуемых в настоящее время (типовых) сетевых атак, воздействующих на информационные ресурсы и элементы защищенных АС ОВД. Для каждой из указанных атак осуществлено обоснование распределения времени ее реализации в АС ОВД на основе эмпирических данных натурного эксперимента. Полученные результаты представлены на примере одной из типовых атак – парольной атаки.

Для расчета достаточного количества итераций N экспериментов, проводимых над сетевой атакой и СЗИ от НСД, с целью адекватного обоснования законов распределения времени на различных этапах их конфликтного взаимодействия в АС ОВД использована формула [13, 14]:

$$N = \frac{t_\varphi{}^2 \sigma^2}{\varepsilon^2}, \quad (1)$$

где: t_φ – квантиль нормального распределения вероятностей порядка $\varphi = \frac{1+Q}{2}$ (находится в таблицах Лапласа); Q – достоверность оценки; $\sigma = \sqrt{D}$ – среднеквадратическое отклонение исследуемых времен; $D = \sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2$ – дисперсия; $n = 10$ – объем первоначальной выборки; ε – заданная точность (достаточность) решения.

[8]Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации. URL: https://dallaslock.ru/upload/medialibrary/cp/documents/C%20ИК5%202017/RU.48957919. 501410-02%2092%20Руководство%20по%20 эксплуатации.pdf. Яз. рус. (дата обращения: 11.04.2021).



1 – производительности и объемы памяти сетевой атаки и СЗИ от НСД заданы;
2 – сетевая атака изначально имеет преимущество;
3 – СЗИ от НСД изначально имеет преимущество;
4, 6 – финальные состояния: победа сетевой атаки;
5, 7 – финальные состояния: победа СЗИ от НСД.

I этап – определение начальных условий конфликта;
II этап – процесс конфликтного взаимодействия сетевой атаки и СЗИ от НСД.

Рис. 1. Обобщенная графовая модель динамики протекания информационного конфликта «Сетевая атака – СЗИ от НСД»
Fig. 1. Generalized graph model of the dynamics of the information conflict "Network attack – SPI from NSD"

Результаты расчета достаточного количества итераций экспериментов, проводимых над сетевой атакой на первом этапе конфликтного взаимодействия ($\varepsilon = 0{,}05$) приведены в табл. 1, где x_i – эмпирические значения времен запуска сетевой атаки (получены в результате проведения натурного эксперимента).

Таблица 1. Результаты расчета достаточного количества итераций экспериментов над сетевой атакой на первом этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	$\overline{x_i}$, с	D	σ	N
15,016	15,0094	0,013505	0,116211	≈ 21
15,02				
15,015				
15				
14,699				
15,171				
15,039				
15,015				
15,003				
15,116				

Адекватные результаты эксперимента, проведенного 21 раз, представлены в табл. 2. Приведенные в табл. 2 характеристики позволили определить и обосновать закон распределения времени реализации сетевой атаки на первом этапе конфликтного взаимодействия (x_i – количественные значения случайных времен реализации атаки на

первом этапе, n_i – количественные значения соответствующих частот их появления).

Предполагая, что распределение времени реализации сетевой атаки на первом этапе соответствует нормальному закону, проведено доказательство согласования полученного эмпирического распределения с законом нормального распределения. Нормальное распределение имеет место в случае, когда формирование времен реализации сетевой атаки подвержено влиянию бесконечного числа случайных факторов.

Таблица 2. Расчетная таблица нахождения критерия $x^2_{\text{набл}}$ для процесса реализации сетевой атаки на первом этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	n_i	n'_i	$n_i - n'_i$	$(n_i - n'_i)^2$	$(n_i - n'_i)^2/n_i$
14,8	1	0,763640583	0,236359417	0,055865774	0,073157157
14,9	3	2,738242592	0,261757408	0,068516941	0,025022232
15	5	5,508436673	-0,508436673	0,25850785	0,04692944
15,1	6	6,128295556	-0,128295556	0,01645975	0,002685861
15,2	4	3,94281372	0,05718628	0,003270271	0,000829426
15,3	2	1,402670359	0,597329641	0,3568027	0,254373879
					$x^2_{\text{набл}} = 0{,}402997994$

В рассматриваемом информационном конфликте такими факторами являются производительности и объемы памяти сетевой атаки и СЗИ от НСД, влияние которых отчетливо прослеживается на начальном этапе протекания конфликта, когда время конфликтного взаимодействия напрямую зависит от входных параметров обеих сторон. С учетом вышеизложенного для первого этапа необходимо проверить нулевую гипотезу H_0: генеральная совокупность распределена по нормальному закону.

Проверка гипотезы о предполагаемом нормальном распределении проводилась с использованием критерия согласия: x^2 («хи квадрат») К. Пирсона (то есть при помощи специально подобранной случайной величины) [15]. Для этого сравнивались эмпирические значения частот n_i (наблюдаемые в ходе проведения эксперимента) и их теоретические значения n'_i (вычисляемые в предположении нормального распределения). x^2-критерий Пирсона не доказывает справедливость гипотезы, а устанавливает согласие или несогласие с данными наблюдений на принятом уровне значимости.

Критерий проверки нулевой гипотезы, определяемый случайной величиной, имеет вид:

$$x^2_{\text{набл}} = \sum (n_i - n'_i)^2 / n'_i. \quad (2)$$

Чем меньше различия эмпирических и теоретических частот, тем меньше полученная величина критерия. Доказано, что при $n \to \infty$ закон распределения случайной величины независимо от того, какому закону распределения подчинена генеральная совокупность, стремится к закону распределения x^2 с k степенями свободы, где: $k = s - 1 - r$; s – число групп выборки; r – число параметров выборки.

Односторонний критерий с большей вероятностью, чем двусторонний отклоняет нулевую гипотезу, поэтому исходя из требования вероятности P попадания критерия в исследуемую область с уровнем значимости ε строилась правосторонняя критическая область:

$$P\left[x^2_{\text{набл}} > x^2_{\text{кр}}(\varepsilon;\ k)\right] = \varepsilon, \quad (3)$$

где: $x^2_{\text{набл}}$ – значение критерия, вычисляемое по данным наблюдений.

Таким образом, для того чтобы при заданном уровне значимости проверить нулевую гипотезу H_0: генеральная совокупность распределена нормально, необходимо

сначала вычислить теоретические частоты, затем – наблюдаемое значение критерия $x^2_{\text{набл}}$ по формуле (2) и далее по таблице критических точек распределения x^2 для заданного уровня значимости ε и числа степеней свободы k найти критическую точку $x^2_{\text{кр}}(\varepsilon; k)$.

При $x^2_{\text{набл}} < x^2_{\text{кр}}$ нулевая гипотеза подтверждается (n_i и n'_i различаются незначимо – случайно), в противном случае – отвергается (n_i и n'_i различаются значимо).

Для процесса реализации сетевой атаки на первом этапе ее конфликтного взаимодействия с системой защиты алгоритм расчетов по полученным эмпирическим данным, представленным в табл. 2, имеет вид [15]:

1) методом произведений вычисляются выборочная средняя ($\overline{x_{\text{в}}} = 15{,}07142857$) и выборочное среднее квадратичное отклонение ($\sigma_{\text{в}} = 0{,}131449274$);

2) рассчитываются теоретические значения частот n'_i по формуле:

$$n'_i = \frac{nh}{\sigma_{\text{в}}} \cdot \varphi(u_i),$$

где $n = \sum n_i$ – объем выборки ($n = 21$), h – шаг ($h = 0{,}1$), $u_i = \frac{x_i - \overline{x_{\text{в}}}}{\sigma_{\text{в}}}$, $\varphi(u_i) = \frac{1}{\sqrt{2\pi}} e^{-u_i^2/2}$;

3) с помощью x^2-критерия Пирсона сравниваются эмпирические и теоретические значения частот:

– составляется расчетная табл. 2 для вычисления наблюдаемого значения критерия $x^2_{\text{набл}}$;

– по таблице критических точек распределения x^2 [15] для уровня значимости $\varepsilon = 0{,}05$ и числа степеней свободы $k = 6 - 1 - 2 = 3$ обозначается критическая точка правосторонней критической области $x^2_{\text{кр}}(0{,}05; 3) = 7{,}8$ (в рассматриваемом случае $s = 6$ и для предполагаемого нормального распределения $r = 2$, поскольку оцениваются два параметра – математическое ожидание и среднее квадратичное отклонение).

Выполнение неравенства $x^2_{\text{набл}} < x^2_{\text{кр}}$ подтверждает нулевую гипотезу H_0 о предполагаемом нормальном законе распределения времени реализации сетевой атаки на первом этапе конфликтного взаимодействия.

График распределения количества реализаций рассматриваемой сетевой атаки в зависимости от времени на первом этапе конфликтного взаимодействия с системой защиты представлен на рис. 2.

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над СЗИ от НСД с целью адекватного обоснования закона распределения времени на первом этапе конфликтного взаимодействия с сетевой атакой в АС ОВД ($\varepsilon = 0{,}05$) [13, 14], представлены в табл. 3, где x_i – эмпирические значения времен загрузки системы защиты (получены в результате проведения натурного эксперимента).

Адекватные результаты эксперимента, проведенного 17 раз, представлены в табл. 4. Приведенные в табл. 4 характеристики позволили определить и обосновать закон распределения времени функционирования системы защиты на первом этапе конфликтного взаимодействия (x_i – количественные значения случайных времен функционирования СЗИ от НСД на первом этапе, n_i – количественные значения соответствующих частот их появления).

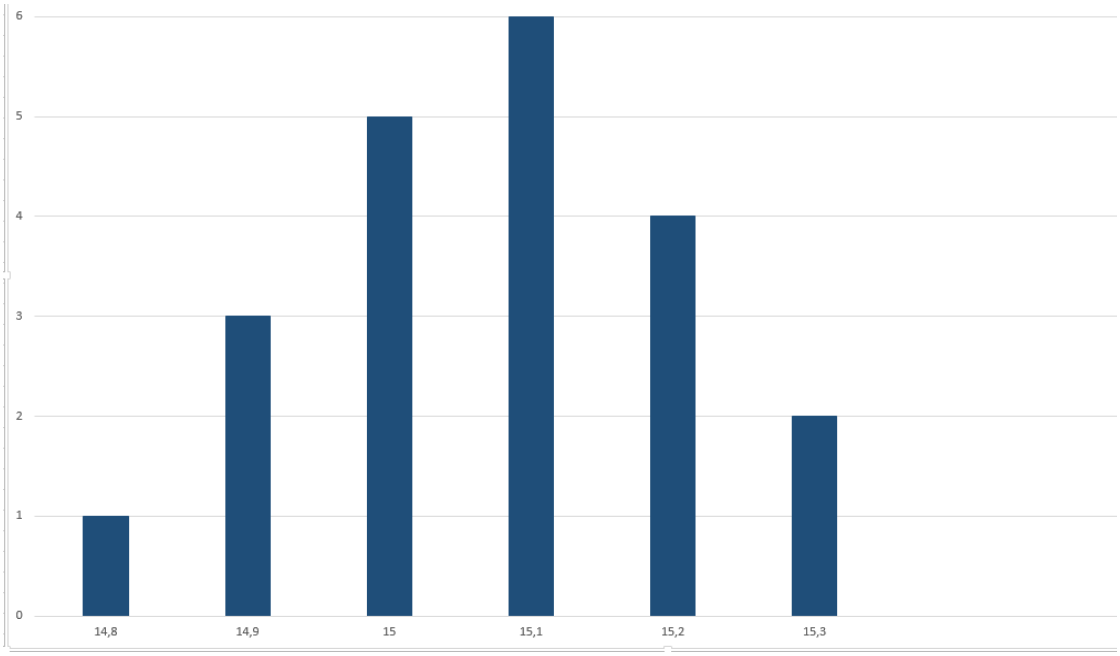


Рис. 2. График распределения количества реализаций сетевой атаки в зависимости от времени на первом этапе конфликтного взаимодействия с СЗИ от НСД
Fig. 2. Time distribution of the number of network attack implementations at the first stage of conflict interaction with the SPI from the NSD

Таблица 3. Результаты расчета достаточного количества итераций экспериментов над СЗИ от НСД на первом этапе конфликтного взаимодействия с сетевой атакой

x_i, с	$\overline{x_i}$, с	D	σ	N
1,71	1,732	0,010836	0,104096109	≈ 17
1,7				
1,89				
1,7				
1,61				
1,9				
1,83				
1,63				
1,6				
1,75				

Предполагая, что распределение времени функционирования СЗИ от НСД на первом этапе соответствует нормальному закону, проведено доказательство согласования полученного эмпирического распределения с законом нормального распределения с использованием критерия К. Пирсона аналогично первому этапу конфликтного взаимодействия при реализации сетевой атаки [15]. Результаты расчетов, проведенных по указанному выше алгоритму для $n = 17$, представлены в табл. 4.

По табл. 4 критических точек распределения x^2 [14] для уровня значимости ε = 0,05 и числа степеней свободы $k = 7 - 1 - 2 = 4$ обозначается критическая точка правосторонней критической области $x^2_{\text{кр}}(0{,}05;\ 4) = 9{,}5$ (в рассматриваемом случае $s = 7$, $r = 2$).

Таблица 4. Расчетная таблица нахождения критерия $x^2_{\text{набл}}$ для процесса функционирования СЗИ от НСД на первом этапе конфликтного взаимодействия с сетевой атакой

x_i	n_i	n'_i	$n_i - n'_i$	$(n_i - n'_i)^2$	$(n_i - n'_i)^2/n_i$
1,5	1	0,50209144	0,49790856	0,247912934	0,493760528
1,6	2	1,547841802	0,452158198	0,204447036	0,132085227
1,7	2	3,194132906	-1,194132906	1,425953397	0,446428949
1,8	3	4,315361066	-1,315361066	1,730174735	0,400933945
1,9	6	3,870151445	2,129848555	4,536254865	1,172113011
2	2	2,304807545	-0,304807545	0,09290764	0,040310368
2,1	1	0,894794766	0,105205234	0,011068141	0,012369475
					$x^2_{\text{набл}} = 2{,}698001503$

Выполнение неравенства $x^2_{\text{набл}} < x^2_{\text{кр}}$ подтверждает нулевую гипотезу H_0 о предполагаемом нормальном законе распределения времени функционирования СЗИ от НСД на первом этапе конфликтного взаимодействия.

График распределения количества функционирований СЗИ от НСД в зависимости от времени на первом этапе конфликтного взаимодействия с сетевой атакой представлен на рис. 3.

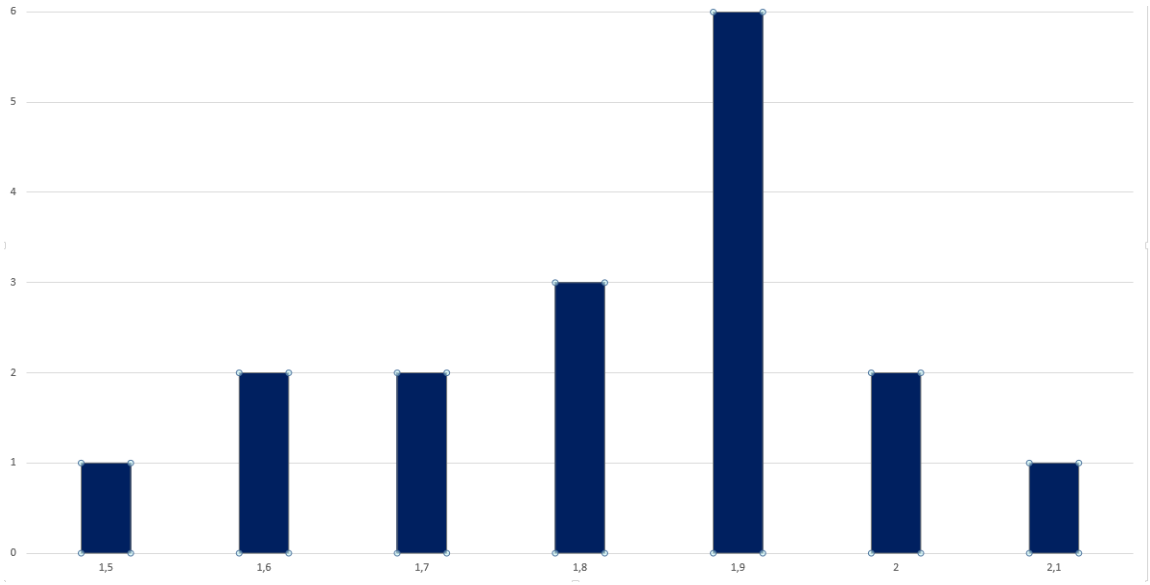


Рис. 3. График распределения количества функционирований СЗИ от НСД в зависимости от времени на первом этапе конфликтного взаимодействия с сетевой атакой
Fig. 3. Time distribution of the number of SPI from the NSD implementations at the first stage of conflict interaction with the network attack

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над сетевой атакой с целью адекватного обоснования закона распределения времени ее реализации на втором этапе конфликтного взаимодействия с системой защиты ($\varepsilon = 0{,}05$) [13, 14], приведены в табл. 5, где x_i – эмпирические значения времен реализации сетевой атаки (получены в результате проведения натурного эксперимента).

Адекватные результаты эксперимента, проведенного 25 раз, представлены в табл. 6. Приведенные в табл. 6 характеристики позволили определить и обосновать закон распределения времени реализации сетевой атаки на втором этапе конфликтного взаимодействия.

Таблица 5. Результаты расчета достаточного количества итераций экспериментов над сетевой атакой на втором этапе конфликтного взаимодействия с СЗИ от НСД

x_i, с	$\overline{x_i}$, с	D	σ	N
756,04	755,979	0,016009	0,126526677	≈ 25
756,08				
756,02				
755,64				
756,03				
756,01				
755,89				
755,95				
756,1				
756,03				

Таблица 6. Расчетная таблица нахождения критерия $\lambda_{\text{набл}}$ для процесса реализации сетевой атаки на втором этапе конфликтного взаимодействия с СЗИ от НСД

x_i	x_{i+1}	n_i	x_i^*	$x_i^* n_i$	$F^*(x_i^*)$	$F(x_i^*)$	$\lvert F^*(x_i^*) - F(x_i^*)\rvert$
755,7	755,8	10	755,75	7557,5	0,4	0,632052417	0,232052417
755,8	755,9	7	755,85	5290,95	0,28	0,632101091	0,352101091
755,9	756	2	755,95	1511,9	0,08	0,632149759	0,552149759
756	756,1	2	756,05	1512,1	0,08	0,63219842	0,55219842
756,1	756,2	2	756,15	1512,3	0,08	0,632247075	0,552247075
756,2	756,3	2	756,25	1512,5	0,08	0,632295723	0,552295723
				$\overline{x_в} = 755{,}89$			$\lambda_{\text{набл}} = 1{,}352842709$

Поскольку времена реализации сетевой атаки на данном этапе можно рассмотреть как непрерывную случайную величину, то их распределение может быть задано в виде последовательности конечных интервалов $x_i - x_{i+1}$ и соответствующих им частот n_i, что позволяет использовать λ-критерий А.Н. Колмогорова для подтверждения нулевой гипотезы H_0 о законе распределения времени.

В основе использования λ-критерия А.Н. Колмогорова лежит сравнение эмпирической $F^*(x)$ и гипотетической $F(x)$ функций распределения (для χ^2-критерия К. Пирсона – эмпирической и теоретической). Вместе с этим в λ-критерии теоретические значения гипотетического закона распределения известны (для χ^2-критерия – рассчитываются по результатам выборки). Указанные ограничения могут оказывать влияние на качество проводимого подтверждения гипотезы H_0. Несмотря на это λ-критерий А.Н. Колмогорова широко применяется на практике, кроме того для случая, когда параметры гипотетического закона распределения оцениваются по результатам выборки (как в данном случае) λ-критерий показывает лучшее согласие с эмпирическим законом распределения, чем χ^2-критерий [16].

Для проверки нулевой гипотезы о предполагаемом распределении с использованием λ-критерия А.Н. Колмогорова необходимо сначала расположить полученные результаты наблюдений в возрастающем порядке либо в виде интервального ряда, затем – рассчитать значения эмпирической функции распределения по формуле:

$$F^*(x) = \frac{n_i}{n}. \quad (4)$$

Далее, пользуясь гипотетической функцией распределения, следует определить значения теоретической функции распределения $F(x)$ (в рамках проведенного натурного эксперимента данные значения находятся по результатам выборки). Для каждого значения x_i необходимо вычислить модуль разности полученных значений эмпирической

и теоретической функций распределения:

$$|F^*(x) - F(x)|. \quad (5)$$

По результатам рассчитанных модулей разности определяется наблюдаемое значение λ выборочной статистики А.Н. Колмогорова:

$$\lambda = \max_x |F^*(x) - F(x)| \cdot \sqrt{n}. \quad (6)$$

В случае верности нулевой гипотезы выборочная статистика при $\lambda \to \infty$ имеет функцию распределения $K(\lambda)$ вида:

$$K(\lambda) = \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2\lambda_\varepsilon^2}. \quad (7)$$

Задав уровень значимости ε, находятся квантили распределения А.Н. Колмогорова из соотношения:

$$P(\lambda \geq \lambda_\varepsilon) = 1 - \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2\lambda^2} = \varepsilon. \quad (8)$$

Сравнивая $\lambda_{\text{набл}}$ с λ_ε, определяемом по таблице критических значений распределения А.Н. Колмогорова, делается вывод о согласовании выдвинутой нулевой гипотезы с полученными эмпирическими данными. При $\lambda_{\text{набл}} < \lambda_\varepsilon$ нулевая гипотеза подтверждается, в противном случае ($\lambda_{\text{набл}} \geq \lambda_\epsilon$) – отвергается.

Предполагая, что закон распределения времени реализации сетевой атаки на втором этапе является экспоненциальным (показательным) [9], осуществлялось обоснование данной гипотезы согласно методике, изложенной в [17].

Для процесса реализации сетевой атаки на втором этапе ее конфликтного взаимодействия с системой защиты алгоритм расчетов по полученным эмпирическим данным имеет вид:

1) рассчитывается выборочная средняя эмпирического распределения $\overline{x_в} = \frac{\sum_{i=1}^{s} x_i^* n_i}{n} = 755{,}89$ где $s = 6$ – количество интервалов. Для этого в качестве «представителя» i-го интервала принимается его середина $x_i^* = (x_i + x_{i+1})/2$ и составляется последовательность равностоящих вариант и соответствующих им частот [18];

2) определяется величина оценки показателя экспоненциального распределения $\lambda = \frac{1}{\overline{x_в}} = 0{,}001322944$;

3) по формуле (4) для объема выборки $n = 25$ вычисляются значения эмпирической функции распределения $F^*(x_i^*)$;

4) рассчитываются значения теоретической функции распределения по формуле $F(x_i^*) = 1 - e^{-\lambda x_i^*}$;

5) проводится сравнение по модулю значений эмпирической и теоретической функций распределения для определения максимальной величины их разницы по формуле (5);

6) по формуле (6) находится наблюдаемое значение выборочной статистики $\lambda_{\text{набл}} = 1{,}352842709$.

Полученные результаты представлены в табл. 6.

По таблице квантилей распределения А.Н. Колмогорова [17] для уровня значимости $\varepsilon = 0{,}05$ обозначается критическая точка $\lambda_\varepsilon(0{,}05) = 1{,}358$.

Выполнение неравенства $\lambda_{\text{набл}} < \lambda_\varepsilon$ подтверждает нулевую гипотезу H_0 о предполагаемом экспоненциальном законе распределения времени реализации сетевой атаки на втором этапе конфликтного взаимодействия.

График распределения количества реализаций рассматриваемой сетевой атаки в зависимости от времени на втором этапе конфликтного взаимодействия с СЗИ от НСД представлен на рис. 4.

Результаты расчета по формуле (1) достаточного количества итераций экспериментов, проводимых над СЗИ от НСД с целью адекватного обоснования закона распределения времени на втором этапе конфликтного взаимодействия с сетевой атакой ($\varepsilon = 0{,}05$) [13, 14], приведены в табл. 7, где x_i – эмпирические значения времен функционирования системы защиты (получены в результате проведения натурного эксперимента).

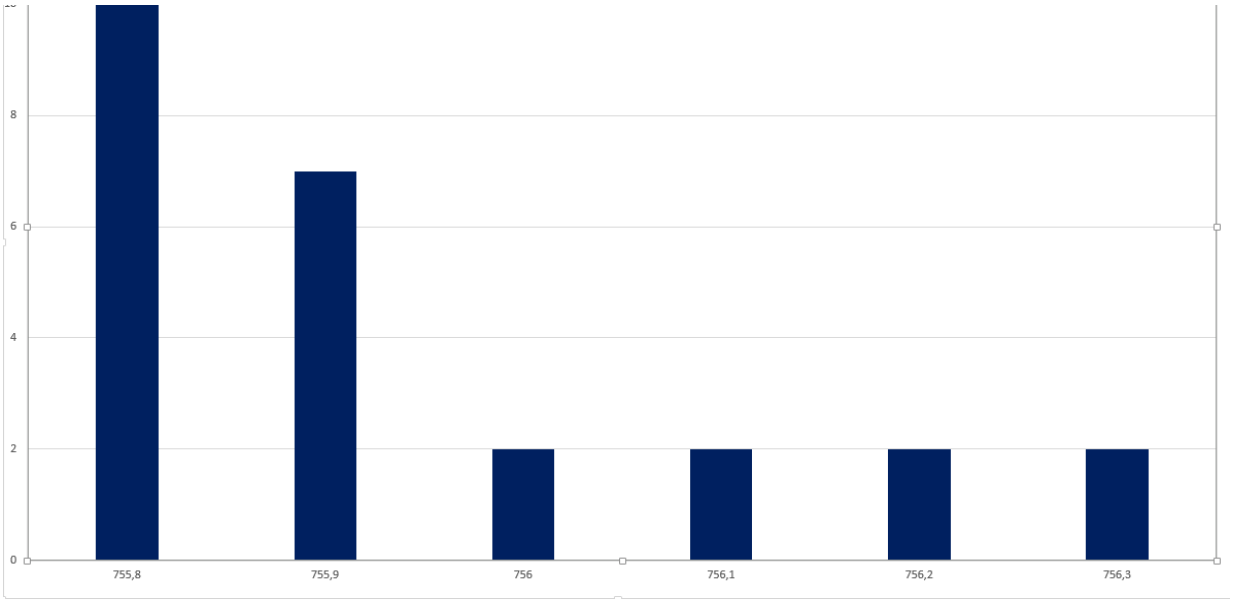


Рис. 4. График распределения количества реализаций сетевой атаки в зависимости от времени на втором этапе конфликтного взаимодействия с СЗИ от НСД
Fig. 4. Time distribution of the number of network attack implementations at the second stage of conflict interaction with the SPI from the NSD

Предполагая, что распределение времени функционирования СЗИ от НСД на втором этапе соответствует экспоненциальному закону, проведено доказательство согласования полученного эмпирического распределения с законом экспоненциального распределения с использованием критерия А.Н. Колмогорова аналогично второму этапу конфликтного взаимодействия при реализации сетевой атаки [17, 18]. Результаты расчетов, проведенных по указанному выше алгоритму для $s = 7$ и $n = 30$, представлены в табл. 8.

По таблице квантилей распределения Колмогорова [17] для уровня значимости $\varepsilon = 0{,}05$ обозначается критическая точка $\lambda_\varepsilon(0{,}05) = 1{,}358$.

Выполнение неравенства $\lambda_{\text{набл}} < \lambda_\alpha$ подтверждает нулевую гипотезу H_0 о предполагаемом экспоненциальном законе распределения времени функционирования системы защиты на втором этапе конфликтного взаимодействия.

Таблица 7. Результаты расчета достаточного количества итераций экспериментов над СЗИ от НСД на втором этапе конфликтного взаимодействия с сетевой атакой

x_i, с	$\overline{x_i}$, с	D	σ	N
912,96	912,963	0,019261	0,138784005	≈ 30
913,04				
912,93				
913,11				
913				
912,86				
913,02				
913,2				
912,81				
912,7				

Таблица 8. Расчетная таблица нахождения критерия $\lambda_{\text{набл}}$ для процесса функционирования СЗИ от НСД на втором этапе конфликтного взаимодействия с сетевой атакой

x_i	x_{i+1}	n_i	x_i^*	$x_i^* n_i$	$F^*(x_i^*)$	$F(x_i^*)$	$\lvert F^*(x_i^*) - F(x_i^*)\rvert$
912,7	912,8	5	912,75	4563,75	0,166666667	0,63200638	0,465339714
912,8	912,9	5	912,85	4564,25	0,166666667	0,632046683	0,465380016
912,9	913	4	912,95	3651,8	0,133333333	0,632086981	0,498753647
913	913,1	4	913,05	3652,2	0,133333333	0,632127274	0,498793941
913,1	913,2	4	913,15	3652,6	0,133333333	0,632167563	0,49883423
913,2	913,3	4	913,25	3653	0,133333333	0,632207848	0,498874514
913,3	913,4	4	913,35	3653,4	0,133333333	0,632248128	0,498914795
				$\overline{x_{\text{в}}} =$ 913,0333333			$\lambda_{\text{набл}} =$ 1,320004472

График распределения количества функционирований СЗИ от НСД в зависимости от времени на втором этапе конфликтного взаимодействия с сетевой атакой представлен на рис. 5.

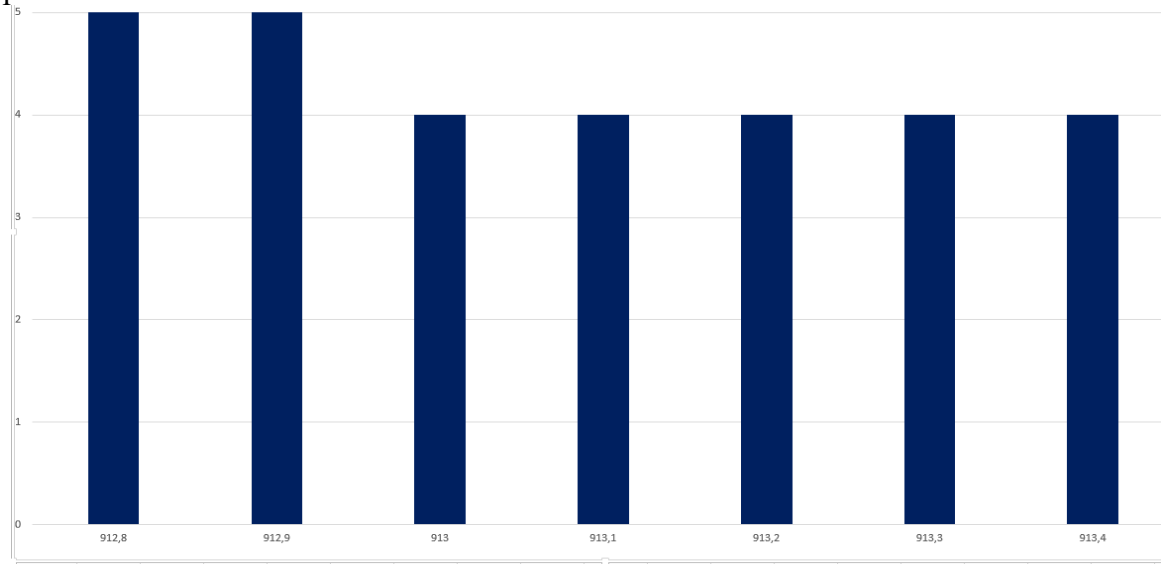


Рис. 5. График распределения количества функционирований СЗИ от НСД в зависимости от времени на втором этапе конфликтного взаимодействия с сетевой атакой
Fig. 5. Time distribution of the number of SPI from the NSD implementations at the second stage of conflict interaction with the network attack

Заключение

На основе построения обобщенной графовой модели, описывающей механизм информационного конфликта «Сетевая атака – СЗИ от НСД» в защищенной АС ОВД, и проведения натурного эксперимента обоснованы законы распределения времени реализации типовой сетевой атаки и функционирования СЗИ от НСД на различных этапах их конфликтного взаимодействия. на различных этапах

На основе использования χ^2-критерия К. Пирсона и -критерия А.Н. Колмогорова с достаточностью 0,05 представлено математическое подтверждение нормального (на первом этапе конфликтного взаимодействия) и экспоненциального (на втором этапе) законов распределения, а также их графическое отображение.

Полученные результаты позволят разработать аналитическую модель динамики реализации сетевой атаки в конфликтном взаимодействии с СЗИ от НСД, рассчитать вероятностно-временные характеристики и провести точную количественную оценку опасности реализации сетевых атак на этапах всего жизненного цикла функционирования, защищенных АС ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. – 232 с. URL: https://bookree.org/reader?file=1213197 (дата обращения: 15.04.2021).
2. Радько Н.М., Язов Ю.К., Корнеева Н.Н. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа. Воронеж: Воронеж. госуд. технич. ун-т, 2013. – 265 с.
3. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография. Воронеж: Кварта, 2018. – 588 с.
4. Язов Ю.К., Анищенко А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография. Воронеж: Кварта, 2020. – 173 с.
5. Concept for increasing security of national information technology infrastructure and private clouds / D.A. Melnikov, A.P. Durakovsky, S.V. Dvoryankin, V.S. Gorbatov // Proceedings-2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud 2017: 5, Prague, August 21-23, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
6. Stages and procedures for forming a method to assess reliability of the information security systems in automated systems and main areas of its implementation in the normative-technical documentation / O.I. Bokova, A.S. Etepnev, E.A. Rogozin, O.M. Bulgakov // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, November 11-13, 2019. Voronezh: Institute of Physics Publishing, 2020. – P. 012022. DOI: https://doi.org/10.1088/1742-6596/1479/1/012022.
7. Михайлов Р.Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238–251. DOI: https://doi.org/10.24411/2410-9916-2020-10309.
8. Дровникова И.Г., Овчинникова Е.С., Рогозин Е.А., Калач А.В. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри-Маркова. Вестник Воронежского института ФСИН России. 2020. № 4. С. 37–44. URL: https://vi.fsin.gov.ru/upload/territory/Vi/nauchnaja_dejatelnost/v_fsin_2020_4.pdf (дата обращения: 01.04.2021).
9. Дровникова И.Г., Овчинникова Е.С. К вопросу моделирования процесса функционирования системы защиты информации в условиях реализации сетевых атак на объектах информатизации органов внутренних дел // Общественная безопасность, законность и правопорядок в III тысячелетии. 2020. № 6-2. С. 218–225. URL: https://www.elibrary.ru/download/elibrary_44250423_88392617.pdf (дата обращения: 01.04.2021).
10. Дровникова И.Г., Овчинникова Е.С., Конобеевских В.В. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47 (1): С. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85.
11. Bokova O.I. et al. Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources. 2020 J. Phys.: Conf. Ser. 1691 012063.

DOI: https://doi.org/10.1088/1742-6596/1691/1/012063.
12. Бацких Анна В. и др. Анализ и классификация основных угроз информационной безопасности автоматизированных систем на объектах информатизации органов внутренних дел. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 40–50, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1250 (дата обращения: 10.02.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.04.
13. Советов Б.Я., Яковлев С.А. Моделирование систем. – 3-е изд., перераб. и доп. М.: Высшая школа, 2001. – 343 с.
14. Советов Б.Я., Яковлев С.А. Моделирование систем. Практикум. – 4-е изд., перераб. и доп. М.: Юрайт, 2014. – 295 с.
15. Гмурман В.Е. Теория вероятностей и математическая статистика // 9-е изд., стер. М.:Высшая школа, 2003. – 479 с. URL: https://bookree.org/reader?file=567344&pg=4 (дата обращения: 01.04.2021).
16. Nazarenko S.V., Grebenev V.N. Self-similar formation of the Kolmogorov spectrum in the Leith model of turbulence // Journal of Physics A: Mathematical and Theoretical. 2017. Vol. 50. No 3. P. 035501. DOI: https://doi.org/10.1088/1751-8121/50/3/035501.
17. Герасимович А.И., Матвеева Я.И. Математическая статистика. Минск: Вышэйшая школа, 1978. – 200 с. URL: https://booksee.org/book/637093 (дата обращения: 01.04.2021).
18. Kozera R., Noakes L., Szmielew P. (2013) Trajectory estimation for exponential parametrization and various samples. Saeed K., Chaki R., Cortes A., Wierzchoń S. (eds) Computer Information Systems and industrial management. SIM 2013. Lecture notes on Computer Science, vol. 8104. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-40925-7_40.

REFERENCES:

[1] Radko N.M., Skobelev I.O. Risk models of information and telecommunication systems in the implementation of threats of remote and direct access. M.: Radiosoft, 2010. – 232 p. URL: https://bookree.org/reader?file=1213197 (accessed: 15.04.2021) (in Russian).
[2] Radko N.M., Yazov Yu.K., Korneeva N.N. Penetration into the computer operating environment: models of malicious remote access. Voronezh: Voronezh state technical University, 2013. – 265 p. (in Russian).
[3] Yazov Yu K., Solovyov S.V. Organization of information protection in information systems from unauthorized access: monograph. Voronezh: Kvart, 2018. – 588 p. (in Russian).
[4] Yazov Yu.K., Anishchenko A.V. Petri-Markov networks and their application for modeling the processes of implementing information security threats in information systems: monograph. Voronezh: Kvart, 2020. – 173 p. (in Russian).
[5] Concept for increasing security of national information technology infrastructure and private clouds. D.A. Melnikov, A.P. Durakovsky, S.V. Dvoryankin, V.S. Gorbatov. Proceedings-2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud 2017: 5, Prague, August 21-23, 2017. – Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
[6] Stages and procedures for forming a method to assess reliability of the information security systems in automated systems and main areas of its implementation in the normative-technical documentation. O.I. Bokova, A.S. Etepnev, E.A. Rogozin, O.M. Bulgakov. Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, November 11-13, 2019. Voronezh: Institute of Physics Publishing, 2020. P. 012022. DOI: https://doi.org/10.1088/1742-6596/1479/1/012022.
[7] Mikhailov R.L. Dynamic model of information conflict of special purpose information and telecommunications systems. Control, communication and security systems. 2020. No. 3. P. 238–251. DOI: https://doi.org/10.24411/2410-9916-2020-10309 (in Russian).
[8] Drovnikova I.G., Ovchinnikova E.S., Rogozin E.A., Kalach A.V. Modeling of the dynamics of information conflict in protected automated systems of internal affairs bodies based on the Petri-Markov network. Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2020. No. 4. P. 37–44. URL: https://vi.fsin.gov.ru/upload/territory/Vi/nauchnaja_dejatelnost/v_fsin_2020_4.pdf (accessed: 01.04.2021) (in Russian).
[9] Drovnikova I. G., Ovchinnikova E. S. On the issue of modeling the process of functioning of the information protection system in the conditions of network attacks on the objects of informatization of internal affairs bodies. Public security, legality and law and order in the III millennium. 2020. No. 6-2. P. 218–225. URL: https://www.elibrary.ru/download/elibrary_44250423_88392617.pdf (accessed: 01.04.2021) (in Russian).
[10] Drovnikova I.G., Ovchinnikova E.S., Konobeevskikh V.V. Analysis of typical network attacks on automated systems of internal affairs bodies. Bulletin of the Dagestan State Technical University. Technical sciences. 2020; 47 (1): P. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85 (in Russian).
[11] Bokova O.I. et al. Innovative technology in the research of implementation dynamics of network attacks on the

digital educational resources. 2020 J. Phys.: Conf. Ser. 1691 012063. DOI: https://doi.org/10.1088/1742-6596/1691/1/012063.

[12] Batskikh Anna V. et al. Analysis and classification of the main threats to the information security of automated systems at the objects of informatization of internal affairs bodies. IT Security (Russia), [S. l.]. Vol. 27, no. 1. P. 40–50, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1250 (accessed: 10.02. 2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.04 (in Russian).

[13] Sovetov B.Ya., Yakovlev S.A. Modeling of systems. – 3rd ed., reprint. and add. M.: Higher School, 2001. – 343 p. (in Russian).

[14] Sovetov B.Ya., Yakovlev S.A. Modeling of systems. Practicum. – 4th ed., reprint. and add. M.: Yurayt, 2014. – 295 p. (in Russian).

[15] Gmurman V.E. Probability theory and mathematical statistics. 9th ed., ster. Moscow: Higher School, 2003. – 479 p. URL: https://bookree.org/reader?file=567344&pg=4 (accessed: 01.04.2021) (in Russian).

[16] Nazarenko S.V. Self-similar formation of the Kolmogorov spectrum in the Leith model of turbulence S.V. Nazarenko, V.N. Grebenev. Journal of Physics A: Mathematical and Theoretical. 2017. Vol. 50. No 3. P. 035501. DOI: https://doi.org/10.1088/1751-8121/50/3/035501 (in Russian).

[17] Gerasimovich A.I., Matveeva Ya.I. Mathematical statistics. Minsk: Higher School, 1978. – 200 p. URL: https://booksee.org/book/637093 (accessed: 01.04.2021) (in Russian).

[18] Kozera R., Noakes L., Szmielew P. (2013) Trajectory estimation for exponential parametrization and various samples. Saeed K., Chaki R., Cortes A., Wierzchoń S. (eds) Computer Information Systems and industrial management. SIM 2013. Lecture notes on Computer Science, vol. 8104. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-40925-7_40.

Поступила в редакцию – 25 апреля 2021 г. Окончательный вариант – 17 августа 2021 г.
Received – April 25,2021. The final version – August 17, 2021.

Валентина В. Дмитриева[1], Николай Н. Тупицын[2], Евгений В. Поляков[3], Елена М. Носова[4], Александра Д. Палладина[5], Вячеслав И. Цыпляк[6], Кирилл А. Либерис[7]

[1,3,6,7]Национальный исследовательский ядерный университет «МИФИ», Каширское ш, 31, Москва, 115409, Россия

[2,5]Национальный медицинский исследовательский центр онкологии им.Н.Н.Блохина», Каширское ш, 24, Москва, 115478, Россия

[4]Московский государственный технический университет гражданской авиации, Кронштадский б-р, 20, Москва, 125993, Россия

[1]e-mail: dmitrievq@yandex.ru, https://orcid.org/0000-0002-9202-6691

[2]e-mail: nntca@yahoo.com, https://orcid.org/0000-0003-3966-128X

[3]e-mail: voterstreit@inbox.ru, https://orcid.org/0000-0002-5346-6504

[4]e-mail: emnosova@mail.ru, https://orcid.org/0000-0002-8443-9357

[5]e-mail: alexandra.93@mail.ru, https://orcid.org/0000-0002-9400-7347

[6]e-mail: slavca.ru@yandex.ru, https://orcid.org/0000-0002-0930-3951

[7]e-mail: liberiska@gmail.com, https://orcid.org/0000-0002-4059-4320

МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА С ПРИМЕНЕНИЕМ WEB-ТЕХНОЛОГИЙ ДЛЯ ДИАГНОСТИКИ ОСТРЫХ ЛИМФОБЛАСТНЫХ ЛЕЙКОЗОВ И МИНИМАЛЬНОЙ ОСТАТОЧНОЙ БОЛЕЗНИ

DOI: http://dx.doi.org/10.26583/bit.2021.3.03

Аннотация. В работе раскрыта реализация прототипа медицинской информационной системы (МИС) для диагностики острых лейкозов и минимальной остаточной болезни. В качестве основной рассмотрена задача интеграции систем интеллектуальной компьютерной микроскопии и лазерной проточной цитофлуориметрии – интегрированный метод диагностики гемобластозов с применением технологий искусственного интеллекта. Предлагаемый информационный веб-сайт предоставляет удаленный доступ к тематическому контенту диагностики острых лимфобластных лейкозов и контроля минимальной остаточной болезни через специализированное кроссплатформенное веб-приложение, моделирующее работу различных подсистем при проведении исследований. Одной из проблем при разработке и создании МИС является обеспечение информационной безопасности как в отношении персональных данных о здоровье пациентов и ходе лечебно-диагностического процесса, так и информации, характеризующий реализуемый функционал МИС: компьютерное и сетевое оборудование, программные модули и базы данных. Особенностью медицинской информации является ее конфиденциальность. Безопасность данных в рассматриваемой системе обеспечивается посредствам аутентификации пользователей. Защита информационных ресурсов от внешних и внутренних угроз обеспечивается путем разделения и контроля привилегий доступа для пользователей различного уровня, а также посредствам администрирования веб-сервера.

Ключевые слова: медицинская информационная система, веб-приложение, диагностика острых лейкозов, классификация клеток костного мозга и крови, минимальная остаточная болезнь.

Для цитирования: ДМИТРИЕВА, Валентина В. и др. МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА С ПРИМЕНЕНИЕМ WEB-ТЕХНОЛОГИЙ ДЛЯ ДИАГНОСТИКИ ОСТРЫХ ЛИМФОБЛАСТНЫХ ЛЕЙКОЗОВ И МИНИМАЛЬНОЙ ОСТАТОЧНОЙ БОЛЕЗНИ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 44–55, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1361. DOI: http://dx.doi.org/10.26583/bit.2021.3.03.

Благодарности. Работа выполнена при поддержке РФФИ по проекту №18-29-09115.

Valentina V. Dmitrieva[1], Nikolai N. Tupitsyn[2], Evgeniy V. Polyakov[3], Elena M. Nosova[4],
Alexandera D. Palladin[5], Vyacheslav I. Tsyplyak[6], Kirill A. Liberis[7]
[1,3,6,7]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse 31, Moscow, 115409, Russia
[2,5]N.N. Blokhin National Medical Research Center of Oncology,
Kashirskoe shosse 24, Moscow, 115478, Russia
[4]Moscow State Technical University of Civil Aviation (MSTUCA),
Kronshtadtskiy bulvar, 20, Moscow, 125993, Russia
[1]e-mail: dmitrievq@yandex.ru, https://orcid.org/0000-0002-9202-6691
[2]e-mail: nntca@yahoo.com, https://orcid.org/0000-0003-3966-128X
[3]e-mail: voterstreit@inbox.ru, https://orcid.org/ 0000-0002-5346-6504
[4]e-mail: emnosova@mail.ru, https://orcid.org/0000-0002-8443-9357
[5]e-mail: alexandra.93@mail.ru, https://orcid.org/0000-0002-9400-7347
[6]e-mail: slavca.ru@yandex.ru, https://orcid.org/0000-0002-0930-3951
[7]e-mail: liberiska@gmail.com, https://orcid.org/0000-0002-4059-4320

Medical information system based web technologies for the diagnosis of acute lymphoblastic leukemia and minimal residual disease

DOI: http://dx.doi.org/10.26583/bit.2021.3.03

Abstract. The paper considers the implementation of a medical information system (MIS) prototype for the diagnosis of acute leukemia (OL) and minimal residual disease (MRD). The main goal is the integration of intelli-gent computer microscopy and laser flow cytofluorimetry systems – an integrated method for the diagnosis of hemoblastosis using artificial intelligence technologies. The proposed information website provides re-mote access to thematic content for the diagnosis of acute lymphoblastic leukemia (ALL) and the control of minimal residual disease through a specialized cross-platform web application that simulates the opera-tion of various subsystems during research. One of the problems in the development of MIS is to ensure information security both in relation to personal data about the health of patients and the course of the medical and diagnostic process, and information that characterizes the implemented MIS functionality: computer and network equipment, software modules and databases. A special feature of medical infor-mation is its confidentiality. Data security is ensured by user authentication. Protection of information resources from unauthorized access is provided by separation and verification of access privileges for the administrator, doctors and patients. The level of security against external threats is provided via the admin-istration of the web server.

Keywords: medical information system, Web application, diagnosis of acute leukemia, classification of bone marrow and blood cells, minimal residual disease.

For citation: DMITRIEVA, Valentina V. et al. Medical information system based web technologies for the diagnosis of acute lymphoblastic leukemia and minimal residual disease. IT Security (Russia), [S.l.], v. 28, n. 3, p. 44–55, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1361. DOI: http://dx.doi.org/10.26583/bit.2021.3.03.

Acknowledgement. The reported study was funded by RFBR according to the research project № 18-29-09115.

Введение

Высокие темпы развития современных информационных технологий расширяют функциональные возможности разработки информационных систем, повышая их производительность благодаря непрерывному совершенствованию программных и аппаратных средств. При этом ранее разработанное программное обеспечение быстро устаревает и требует постоянной модернизации и адаптации под всё новые и новые программно-аппаратные платформы. Выход из этой, довольно непростой, ситуации

заключается в переходе к созданию универсальных кроссплатформенных веб-приложений.

Одной из наиболее важных и актуальных задач развития современных информационных технологий в медицине является разработка специализированных информационных ресурсов для решения научных и образовательных задач с учетом специфики и особенностей предметных областей. Процесс разработки медицинской информационной системы (МИС) представлен в [1]. Классификация данных систем, а также анализ факторов, влияющих на постановку корректного диагноза, рассмотрены в [2]. Быстрый, эффективный сбор и анализ больших объемов данных, гибкая оперативная мобильность обновления данных, синергетическое открытое сотрудничество интеллектуальных агентов с информационными платформами и аналитическими системами позволят ускорить цифровую трансформацию высокотехнологичной отрасли и социальной сферы, отмечается в [3]. Вопросы телемедицины, на решения которых авторы опирались при рассмотрении раскрываемой задачи, представлены в [4]. Специфика конкретной предметной области требует серьезной адаптации стандартных компьютерных технологий общего назначения, обычно используемых в научных и образовательных целях, к специфике задач и к конкретным условиям эксплуатации информационных систем. В частности, это актуально для разработки компьютерной системы интегрирующей возможности компьютерной микроскопии и проточной цитометрии при диагностике минимальной остаточной болезни [5], что значительно сокращает время принятия решений и повышает точность диагностики системы за счёт аккумулирования клинических морфологических данных и данных проточной цитометрии путем внедрения технологий искусственного интеллекта. Разработка новых методов направлена, в частности, на улучшение обнаружения лейкозных клеток посредством снижения размерности используемых маркеров [6]. Применение альтернативных технологий является привлекательным для выявления и прогнозирования заболевания по сравнению с существующими сложными методами визуализации. Однако золотой стандарт диагностики и мониторинга заболеваний по-прежнему включает инвазивные методы – биопсия тканей или костного мозга, т. к. многие технологии находятся еще в стадии разработки [7] В настоящее время ощущается острая нехватка систем, обеспечивающих интеграцию данных. Применяют системы без использования лазерного проточного цитометра [8]. В то же время, точная классификация острых лимфобластных лейкозов (ОЛЛ) имеет решающее значение для адекватного лечения [9].

Рассматриваемая МИС предоставляет врачам возможность работать непосредственно с информацией о пациентах из интерфейса системы при постановке диагноза. Также в системе предусмотрена возможность сравнения полученных изображений от новых пациентов с изображениями, уже загруженными в системе. Помимо ведения электронной истории болезни в системе предусмотрена опция по формированию диагностического заключения по результатам выполненных исследований.

Цель работы: разработка новых принципов и методов построения медицинской информационной системы и создание программного нейросетевого комплекса, обеспечивающих информационную безопасность данных в обучении и проведении исследований при диагностике острых лимфобластных лейкозов и контроле минимальной остаточной болезни

1. Концепция системы

В качестве развития систем диагностики ОЛЛ и контроля минимальной остаточной болезни (МОБ) может быть предложен прототип метода интеграции систем интеллектуальной компьютерной микроскопии и лазерной проточной цитофлуориметрии – интегрированный метод диагностики гемобластозов, где распознавание изображений выполняется на основе сформированной референсной базы знаний и экспертного нейросетевого анализатора. В рамках данного проекта решается задача по созданию подсистем единой МИС, в стуктуру которой вкючен интеллектуальный модуль, помогающий врачу в принятии решения при диагностике заболевания.

В настоящее время всё большую популярность приобретают веб-решения, что вызвано их понятностью и легкой доступностью для конечного пользователя [10]. Так как поставленная в работе задача предполагает активное взаимодействие пользователей с сайтом, то за основу было выбрано именно веб-приложение, которое как раз имплементирует данные функции, а не сайт, который в основном хранит статическую информацию (рис. 1).

Рис. 1. Общая схема веб-приложения
Fig. 1. The general scheme of a web application

Веб-приложения обладают следующими преимуществами:

- доступ осуществляется с любого устройства, подключенного к Интернету. С веб-приложением можно работать в любой точке мира с компьютера, планшета или смартфона;
- экономия. Веб-приложения работают на всех платформах и исключают необходимость разработки приложения отдельно для Android и iOS;
- адаптивность. Если нативные приложения оптимизированы под конкретные операционные системы (ОС,) то для работы с веб-приложением подходят любая ОС (Windows, MAC, Linux и т.д.) и любой браузер (InternetExplorer, Opera, FireFox, GoogleChrome и т.д.);
- отсутствие клиентского программного обеспечения (ПО). Данный факт приводит к более дешевым и простым установке, обслуживанию и модернизации клиентского интерфейса. При этом обновление до последней версии происходит при очередной загрузке страницы;
- сетевая безопасность. Веб-система имеет единую точку входа, защитить и настроить безопасность которой можно централизованно;

- масштабируемость. С ростом нагрузки на систему нет необходимости наращивания мощности клиентских мест. Веб-приложение позволяет обрабатывать большее количество данных, как правило, только силами аппаратных ресурсов, без переписывания кода и смены архитектуры;
- защита от потери данных. Данные пользователей хранятся в «облаке», за целостность которого отвечают хостинг-провайдеры, и защищены от потери при повреждении жесткого диска компьютера.

В то же время, веб-приложения обладают рядом существенных недостатков, к которым можно отнести:

- зависимость от интернет-соединения. При отсутствии соединения теряется доступ к сервису, что может иногда существенно увеличить критически необходимое время для анализа и диагностики cito;
- сложная или невозможная реализация комплексных ПО. В настоящее время системы, часто обеспечивающие хорошую визуализацию, например, 3D-моделирование, достаточно сложно реализовать на практике в связи с необходимостью значительных затрат системных ресурсов в веб-приложении.

2. Архитектура и реализация МИС

При проектировании концепции МИС была осуществлена разработка прототипа интегрированного метода диагностики гемобластозов путем объединения систем интеллектуальной компьютерной микроскопии и лазерной проточной цитофлуориметрии, а распознавание изображений выполняется на основе сформированной референсной базы знаний [11] с использованием экспертных оценок [12].

Функциональная модель МИС обладает следующими основными комплексными характеристиками (рис. 2):

- централизованная база данных с предоставлением удаленного защищенного доступа для пользователей, база знаний изображений препаратов костного мозга, в частности база лейкоцитов. Работа пользователей в системе осуществляется в режиме тонкого клиента через Web-браузер, функционирующего в различных операционных средах – Microsoft Windows, Mac OS, Unix (Linux);
- организация системы проводится по принципу трехзвенной архитектуры: Webбраузер, Web-сервер и сервер базы знаний и базы данных;
- встроенные механизмы расширения функционала системы позволяют, при внедрении готового продукта, провести дополнительные настройки.

Разработанный прототип МИС базируется на следующих архитектурных и технологических решениях, позволяющих решить следующие задачи:

- разграниченные права доступа (врач/администратор ЛПУ, инженер по знаниям);
- электронное сопровождения процесса оказания медицинских услуг на всех этапах, включая дистанционную запись к врачу;
- ведение электронных медицинских карт;
- контроль исполнения назначений;
- система поддержки принятия решений при диагностике острых лейкозов;
- формирование статистической и аналитической отчетности.

Данные хранятся в базе PostgreSQL (рис. 3), извлекаются бэкендом через сериализатор (конвертор области памяти в представляемое изображение). Затем эти данные передаются от бэкенд компонента фронтенду, который производит над ними манипуляции необходимые для визуального представления конечному пользователю.

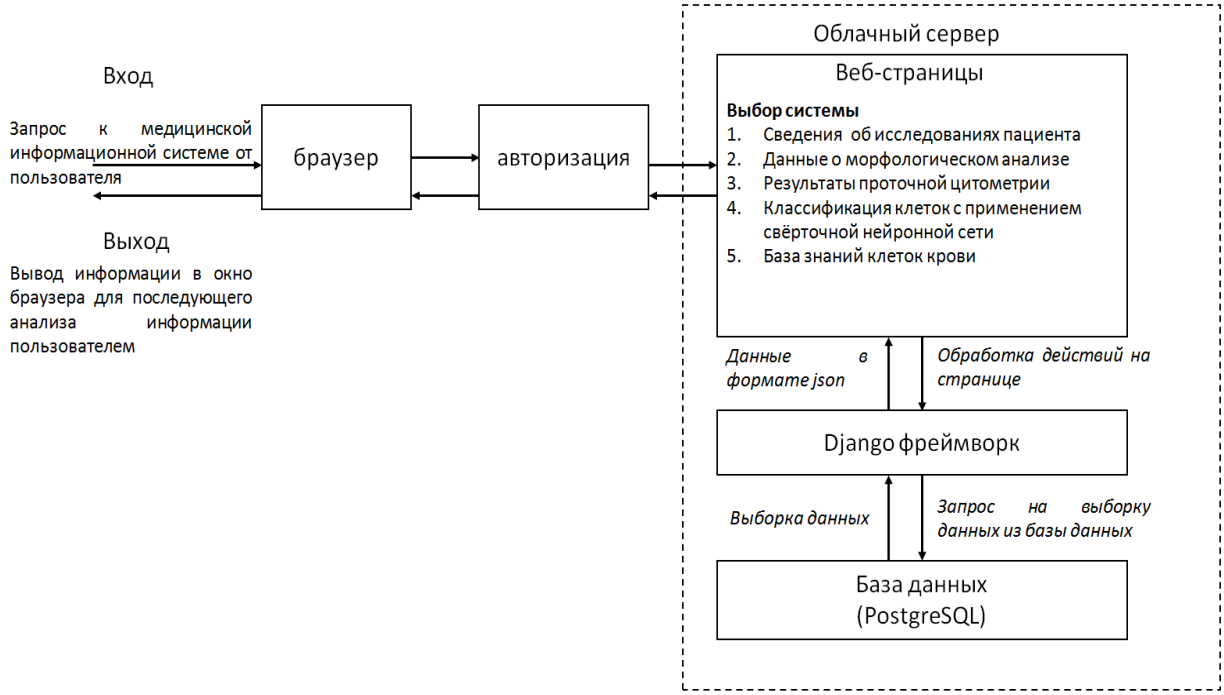


Рис. 2. Функциональная модель МИС
Fig. 2. MIS Functional model

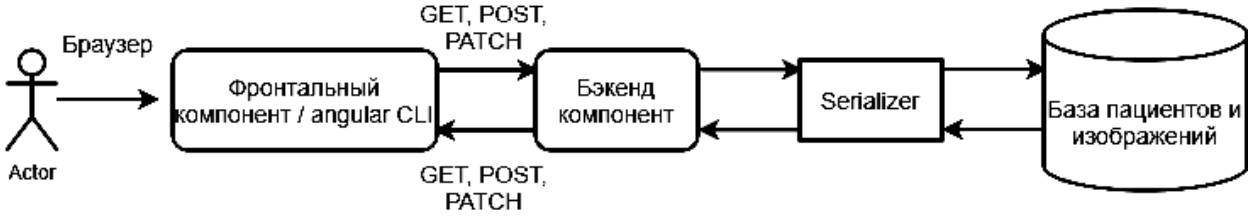


Рис. 3. Структура взаимодействия подсистем МИС
Fig. 3. The structure of MIS subsystems

В МИС применяются следующие технологии:

1. PostgreSQL (База данных);
2. Angular CLI (Frontend);
3. DjangoRestFramework (Backend).

Разработка системы поддержки принятия решений при диагностике острого лейкоза велась на локальном компьютере с характеристиками:

- ОС Windows 10 64-bit;
- Процессор Intel Core i5-6500 3.3GHz;
- 16 Гб оперативной памяти.

В рамках веб-приложения с «тонким» клиентом взаимодействие пользователя с приложением реализуется в существенной степени через сервер, что требует отправки данных на сервер, получения ответа от сервера и перезагрузки страницы на стороне клиента. В дальнейшем, для увеличения быстродействия веб-приложения, целесообразно применение Ajax-технологии, позволяющей обращаться к серверу без полной перезагрузки страницы и реализующей динамическую подгрузку только содержимого обновляемых компонентов.

3. Интерфейс МИС

Архитектура и опциональность МИС реализуют добавление/удаление/изменение персональных данных, анализов и приемов пациентов. Функционал, ориентированный на работу с пациентами, достаточно обширен и включает в себя следующее:

1. добавление и редактирование информации о пациенте;
2. создание первичного приема и открытие медицинской карты;
3. использование модуля предсказание при создании миелограммы;
4. назначение на иммунофенотипирование на вторичном приеме;
5. создание отчёта по результатам иммунофенотипического анализа.

Система Window имеет в своем составе встроенную возможность работы в режиме «клиент-сервер». Однако она базируется на открытых протоколах передачи данных и, следовательно, существует возможность перехвата данных передаваемых в графической сессии пользователя. Для ее исключения графические терминалы соединяются с сервером приложений через подсистему шифрования.

Для подключения к системе с графического терминала используется программа – login менеджер. Она может подключаться по протоколу к серверу приложений и запускать на нем графическую сессию.

Процесс работы системы выглядит следующим образом:

1. включается графический терминал;
2. после его загрузки запускает login менеджер, который по сети загружает список доступных серверов приложений и запрашивает у пользователя учетные данные для входа;
3. происходит подключение к выбранному серверу приложений;
4. после окончания работы вновь запускается login менеджер.

Авторизовавшемуся через учетную запись врача предоставляется доступ в раздел с клиникой «Clinic». Далее предлагается выбрать опцию «Patients» и выбрать пациента, внесенного в базу данных пациентов, либо нажать «Addnewpatient» для добавления нового пациента (для демонстрации будем работать с вымышленным пациентом, но данные предоставляются из реально существующих анализов пациентов). После чего открывается меню, в котором реализована навигация по разделу пациентов/

Опция «Medicalfile» открывает медицинскую карту пациента (рис. 4), а опция «Addnewmedicalrecord» позволяет добавить первичный прием пациента. Особое внимание стоит обратить на необходимость выбора времени и даты приема, а ниже можно либо позволить системе автоматически сгенерировать номер истории болезни (это опция по дефолту), либо можно ввести номер болезни самостоятельно. Это сделано для удобства переноса уже существующих в бумажном виде историй болезни в информационную систему, что позволит связать клинические случаи.

После заполнения всех форм можно сразу же добавить направление на исследование через пункт меню «Orderanalyzeforthepatient». Затем выбирается тип анализа, назначается время анализа и выбирается форма «Клиника», в которой будет проводиться исследование анализа. Активация «Addmedicalrecord» позволяет увидеть в медицинской карте пациента запись о первичном приеме и просмотреть информацию о проведенном приеме.

«Showmedicalhistory» дает возможность просмотреть историю болезни пациента, а также редактировать информацию о ней. По кнопке «Closemedhistory» происходит закрытие истории болезни при выздоровлении пациента.

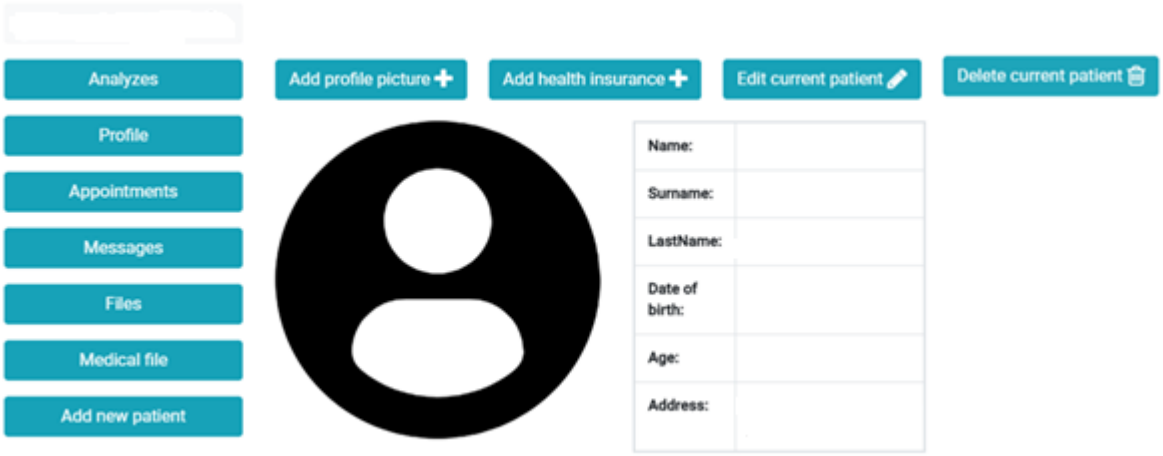


Рис. 4. Навигация по разделу пациентов
Fig. 4. Navigate through the patient section

Для добавления анализа необходимо войти в систему через пользователя с правами врача-диагноста. Для подсчета клеток костного мозга при добавлении анализа миелограммы врач может воспользоваться системой поддержки принятия решений (СППР). Для этого осуществляется переход через меню или через домашнюю страницу в соответствующий раздел путем активации опции «CDSS». Далее выбирается тип изображений клеток костного мозга для работы. При выборе «BloodCell» будут подгружаться изображения препаратов клеток костного мозга из референсной базы знаний эталонов, что позволит врачу сравнивать клетки из пунктата костного мозга с эталоном для идентификации принадлежности к классам. Выбираем интересные для исследования клетки, например лимфоциты и лимфобласты. По выбору подгружаются изображения препаратов клеток костного мозга из эталонной базы с информацией о них. Навигация осуществляется через кнопки и через карусель изображений, указанные на интерфейсе. Для каждого изображения клетки есть указание на увеличение, тип окраски и непосредственно класс, к которому относится клетка.

По кнопке «Uploadfiletoworkwith» можно загрузить изображение препарата костного мозга для сравнения. Таким образом, можно использовать эталонную базу изображений препаратов костного мозга для помощи врачу в распознавании клеток крови, находящиеся в препарате (рис.5).

В системе распознавания задействован модуль предсказаний. Данный модуль позволяет определять класс клетки. Для определения используется сверточная нейронная сеть, построенная на базе «Tensorflow». Указанный модуль получает на вход изображение клетки, которое должно быть предварительно очищенно от цитоплазмы (клетка на белом фоне). В дальнейшем система проводит сравнения и выдает результат о принадлежности клетки к одному из десяти классов (миелоцит, сегментоядерный нейтрофил, нормобласт, палочкоядерный нейтрофил, бласт, лимфоцит, моноцит, метамиелоцит, эозинофил).

Также в системе предусмотрена возможность проведения классификации клеток на изображениях с препаратов костного мозга (КМ) на основе методов классификации без применения нейронной сети. Распознавание проводится на основе анализа морфологических [13], текстурных [14] и вейвлет- характеристик [15].

Навигация и загрузка сравниваемого изображения с препарата клеток КМ осуществляется точно также, как и на клетках периферической крови. В клинических

случаях на конкретном слайде можно выбрать определенные клетки, что позволит также использовать уже существующие клинические случаи для принятия решений.

Во время работы с СППР в новой вкладке можно открыть секцию с пациентами и заполнять миелограмму параллельно. Выберем пациента и перейдем в опцию «Analyzes». Нажимаем вкладку «Addnewanalyze», выбираем тип исследования – в данном случае, подсчет миелограммы (рис. 6), также выберем направление на исследование для данного пациента, которое назначали ранее под учетной записью другого врача.

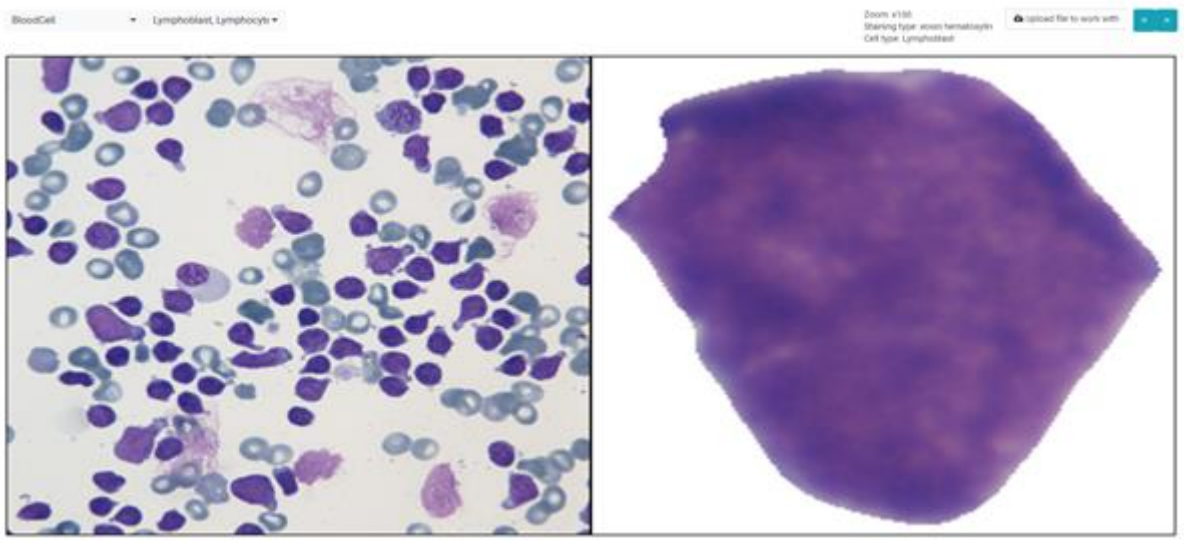
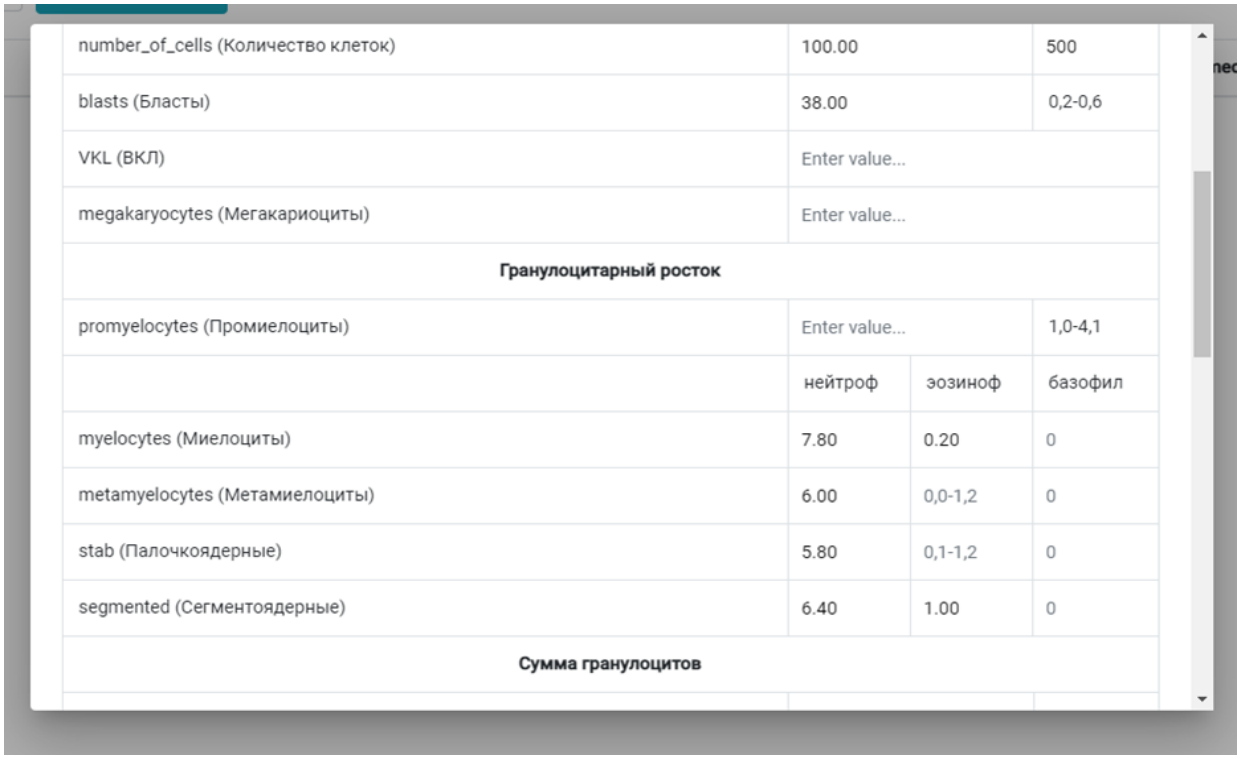


Рис. 5. Форма – Загрузка препарата для сравнения с базой знаний
Fig. 5. Form – Upload cytology sample for comparison with the knowledge base



number_of_cells (Количество клеток)	100.00		500
blasts (Бласты)	38.00		0,2-0,6
VKL (ВКЛ)	Enter value...		
megakaryocytes (Мегакариоциты)	Enter value...		
Гранулоцитарный росток			
promyelocytes (Промиелоциты)	Enter value...		1,0-4,1
	нейтроф	эозиноф	базофил
myelocytes (Миелоциты)	7.80	0.20	0
metamyelocytes (Метамиелоциты)	6.00	0,0-1,2	0
stab (Палочкоядерные)	5.80	0,1-1,2	0
segmented (Сегментоядерные)	6.40	1.00	0
Сумма гранулоцитов			

Рис. 6. Форма - Пример заполнения миелограммы
Fig. 6. Example of filling out a myelogram

В итоге заполняется форма «Заключение» и добавляется результат проведенного исследования.

Актуальность защиты информации достаточно очевидна, однако основные проблемы и последствия ее несоблюдения значительно различаются и зависят от требований, предъявляемых конкретными приложениями. Вопрос защиты информационных систем истем – это обеспечение сохранности и целостности быстро изменяющихся информационных ресурсов, ее защищенность от случайных или преднамеренных вмешательств в нормальный процесс ее функционирования, выражающийся в хищении или изменении информации, а также в нарушении ее работоспособности из-за отказов. Защита информационных ресурсов в МИС от внешних и внутренних угроз обеспечивается путем разделения и контроля привилегий доступа для пользователей различного уровня, а также посредствам администрирования веб-сервера.

Заключение

В результате выполненной работы был предложен и разработан прототип МИС с применением веб-технологий для диагностики ОЛЛ и МОБ на основе интегрированного метода компьютерной микроскопии и лазерной проточной цитофлуориметрии, что является вкладом в разработку принципиально новой концептуальной основы в разработке и применении МИС при комплексных диагностических исследованиях пациента, а также позволяет принимать решение о тактике проведения дальнейшего лечения.

Получены математические модели СППР при диагностике острых лейкозов и МОБ, выполнена программно-аппаратная реализация интегрированной системы диагностики ОЛЛ и МОБ на основе СППР при диагностике острых лейкозов. Проведено экспериментальное исследование, связанное с тестированием созданного программного продукта.

Разработанный информационный веб-сайт предоставляет удаленный доступ к тематическому контенту диагностики ОЛЛ и контроля МОБ через специализированное кроссплатформенное веб-приложение, моделирующее работу различных подсистем при проведении диагностических исследований. Защита информационных ресурсов от несанкционированного доступа обеспечивается через разделение и контроль привилегий доступа для администратора, врачей и пациентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Primova H.A., Sakiyev T.R., Nabiyeva S.S. Development of medical information systems //Journal of Physics: Conference Series. IOP Publishing, 2020. Vol. 1441. No. 1. P. 012160. DOI: http://dx.doi.org/10.1088/1742-6596/1441/1/012160.
2. Bryndin E. Development of Artificial Intelligence by Ensembles of Virtual Agents with Mobile Interaction //Automation, Control and Intelligent Systems. 2020. Vol. 8. P. 1–8. DOI: http://dx.doi.org/10.11648/j.acis.20200801.11.
3. Shabaniyan T. et al. An artificial intelligence-based clinical decision support system for large kidney stone treatment //Australasian physical & engineering sciences in medicine. 2019. Vol. 42. No. 3. P. 771–779. DOI: http://dx.doi.org/10.1007/s13246-019-00780-3
4. Kindle R. D. et al. Intensive care unit telemedicine in the era of big data, artificial intelligence, and computer clinical decision support systems //Critical care clinics. 2019. Vol. 35. No. 3. P. 483–495. DOI: http://dx.doi.org/10.1016/j.ccc.2019.02.005.
5. Rathe M. et al. Minimal residual disease monitoring cannot fully replace bone marrow morphology in assessing disease status in pediatric acute lymphoblastic leukemia //Apmis. 2020. Vol. 128. No. 5. P. 414–419. DOI: http://dx.doi.org/10.1111/apm.13037.
6. Dix C. et al. Measurable residual disease in acute myeloid leukemia using flow cytometry: a review of where we are and where we are going //Journal of Clinical Medicine. 2020. Vol. 9. No. 6. P. 1714. DOI: http://dx.doi.org/10.3390/jcm9061714.

7. Fu Y., Zhang Y., Khoo B. L. Liquid biopsy technologies for hematological diseases //Medicinal Research Reviews. DOI: http://dx.doi.org/10.1002/med.21731.
8. Doan M. et al. Label-free leukemia monitoring by computer vision //Cytometry Part A. 2020. Vol. 97. No. 4. P. 407–414. DOI: http://dx.doi.org/10.1002/cyto.a.23987.
9. Lhermitte L. et al. Automated identification of leukocyte subsets improves standardization of database-guided expert-supervised diagnostic orientation in acute leukemia: a EuroFlow study //Modern Pathology. 2020. P. 1–11. DOI: http://dx.doi.org/10.1038/s41379-020-00677-7.
10. Bibi N. et al. IoMT-based automated detection and classification of leukemia using deep learning //Journal of Healthcare Engineering. 2020. T. 2020. DOI: http://dx.doi.org/10.1155/2020/6648574.
11. Никитаев В.Г., Тупицын Н.Н., Проничев А.Н., Поляков Е.В., Дмитриева В.В., Чернышева О.А., Серебрякова И.Н., Палладина А.Д. Технологии искусственного интеллекта в диагностике острых лимфобластных лейкозов и минимальной остаточной болезни // Медицинская техника. 2020. №5. С. 42–44. DOI: http://dx.doi.org/10.1007/s10527-021-10038-6.
12. Nikitaev V.G., Pronichev A.N., Polyakov E.V., Dmitrieva V. Approach to building knowledge bases in information-measuring systems diagnostics of acute leukemias // Journal of Physics: Conference Series. 2018. No. 945. P. 012007. DOI: http://dx.doi.org/10.1088/1742-6596/945/1/012007.
13. Никитаев В.Г., Проничев А.Н., Поляков Е.В. и др. Модель описания лейкоцитов периферической крови на основе оптических особенностей структуры ядер // Измерительная техника. 2014. № 5. С. 56–58. DOI: http://dx.doi.org/10.1007/s11018-014-0497-x.
14. Chaki J., Dey N. Texture feature extraction techniques for image recognition. – Springer Singapore, 2020. DOI: https://doi.org/10.1007/978-981-15-0853-0.
15. Поляков Е.В. Анализ эффективности методов и моделей обработки изображений препаратов крови и костного мозга для автоматизированной диагностики острых лейкозов // Системный анализ и управление в биомедицинских системах. 2019. Т. 18, № 2. С. 133–144. DOI: http://dx.doi.org/10.25987/VSTU.2019.18.2.021.

REFERENCES:

[1] Primova H.A., Sakiyev T.R., Nabiyeva S.S. Development of medical information systems. Journal of Physics: Conference Series. IOP Publishing, 2020. Vol. 1441. No. 1. P. 012160. DOI: http://dx.doi.org/10.1088/1742-6596/1441/1/012160.
[2] Bryndin E. Development of Artificial Intelligence by Ensembles of Virtual Agents with Mobile Interaction. Automation, Control and Intelligent Systems. 2020. Vol. 8. P. 1–8. DOI: http://dx.doi.org/10.11648/j.acis.20200801.11.
[3] Shabaniyan T. et al. An artificial intelligence-based clinical decision support system for large kidney stone treatment. Australasian physical & engineering sciences in medicine. 2019. Vol. 42. No. 3. P. 771–779. DOI: http://dx.doi.org/10.1007/s13246-019-00780-3.
[4] Kindle R.D. et al. Intensive care unit telemedicine in the era of big data, artificial intelligence, and computer clinical decision support systems. Critical care clinics. 2019. Vol. 35. No. 3. P. 483–495. DOI: http://dx.doi.org/10.1016/j.ccc.2019.02.005.
[5] Rathe M. et al. Minimal residual disease monitoring cannot fully replace bone marrow morphology in assessing disease status in pediatric acute lymphoblastic leukemia. Apmis. 2020. Vol. 128. No. 5. P. 414–419. DOI: http://dx.doi.org/10.1016/j.ccc.2019.02.005.
[6] Dix C. et al. Measurable residual disease in acute myeloid leukemia using flow cytometry: a review of where we are and where we are going. Journal of Clinical Medicine. 2020. Vol. 9. No. 6. P. 1714. DOI: http://dx.doi.org/10.3390/jcm9061714.
[7] Fu Y., Zhang Y., Khoo B.L. Liquid biopsy technologies for hematological diseases. Medicinal Research Reviews. DOI: http://dx.doi.org/10.1002/med.21731.
[8] Doan M. et al. Label-free leukemia monitoring by computer vision. Cytometry Part A. 2020. Vol. 97. No. 4. P. 407–414. DOI: http://dx.doi.org/10.1038/s41379-020-00677-7.
[9] Lhermitte L. et al. Automated identification of leukocyte subsets improves standardization of database-guided expert-supervised diagnostic orientation in acute leukemia: a EuroFlow study. Modern Pathology. 2020. P. 1–11. DOI: http://dx.doi.org/10.1038/s41379-020-00677-7.
[10] Bibi N. et al. IoMT-based automated detection and classification of leukemia using deep learning. Journal of Healthcare Engineering. 2020. T. 2020. DOI: http://dx.doi.org/10.1155/2020/6648574.
[11] Nikitaev V.G. et al. Artificial Intelligence Technologies in the Diagnosis of Acute Lymphoblastic Leukemia and Minimal Residual Disease. Biomedical Engineering. 2021. Vol. 54. No. 5. P. 354–356. DOI: http://dx.doi.org/10.1007/s10527-021-10038-6 (in Russian).

[12] Nikitaev V.G., Pronichev A.N., Polyakov E.V., Dmitrieva V. Approach to building knowledge bases in information-measuring systems diagnostics of acute leukemias. Journal of Physics: Conference Series. 2018. No. 945. P. 012007. DOI: http://dx.doi.org/10.1088/1742-6596/945/1/012007.

[13] Nikitaev V.G., Nagornov O.V., Pronichev A.N., Polyakov E.V., Sel'chuk V.Y., Chistov K.S., Blindar' V.N., Dmitrieva V.V., Gordeev V.V. Model of description of leukocytes of peripheral blood based on the optical features of the structure of nuclei. Measurement Techniques. 2014. Vol. 57. No. 5. P. 560–563. DOI: http://dx.doi.org/10.1007/s11018-014-0497-x (in Russian).

[14] Chaki J., Dey N. Texture feature extraction techniques for image recognition. Springer Singapore, 2020. DOI: https://doi.org/10.1007/978-981-15-0853-0.

[15] Polyakov Ye.V. Analysis of the effectiveness of methods and models of image processing of blood and bone marrow preparations for automated diagnosis of acute leukemia, Sistemnyy analiz i upravleniye v biomeditsinskikh sistemakh. 2019. Vol. 18. No. 2. P. 133–144. DOI: http://dx.doi.org/10.25987/VSTU.2019.18.2.021 (in Russian).

Поступила в редакцию – 16 апреля 2021 г. Окончательный вариант – 18 августа 2021 г.
Received – April 16, 2021. The final version – August 18, 2021.

Константин Г. Когос[1], Михаил А. Финошин[2], Сергей В. Айрапетян[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
[1]*e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X*
[2]*e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645*
[3]*e-mail: sergey.hayrapetyan@mail.ru, https://orcid.org/0000-0002-3415-8530*

МЕТОД ИДЕНТИФИКАЦИИ СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.3.04

Аннотация. Целью статьи является описание разработанного метода идентификации сетевых скрытых каналов. Традиционно схему противодействия утечке информации по скрытым каналам разделяют на несколько этапов. Первым этапом является идентификация скрытых каналов – выявление потенциально возможных скрытых каналов в системе. Для идентификации скрытых каналов используются методы, основанные на матрице разделяемых ресурсов, дереве скрытых информационных потоков и графе скрытых информационных потоков. При этом возникает необходимость конкретизировать формальное описание этапов вышеуказанных методов идентификации в случае сетевых скрытых каналов. В статье приведено описание разработанного метода идентификации сетевых скрытых каналов по памяти, а также результаты тестирования программной реализации данного метода, для скрытого канала, основанного на изменении поля TTL заголовка IP-пакета. Результаты могут быть расширены и для других сетевых скрытых каналов по памяти в IP сетях, основанных на изменении полей заголовков пакетов.
Ключевые слова: скрытый канал, метод идентификации, общий ресурс, атрибут, информационный поток.
Для цитирования: КОГОС, Константин Г.; ФИНОШИН, Михаил А.; АЙРАПЕТЯН, Сергей В. МЕТОД ИДЕНТИФИКАЦИИ СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 56–64, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1362. DOI: http://dx.doi.org/10.26583/bit.2021.3.04.

Konstantin G. Kogos[1], Mihail A. Finoshin[2], Sergey V. Airapetyan[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe highway, 31, Moscow, 115409, Russia
[1]*e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X*
[2]*e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645*
[3]*e-mail: sergey.hayrapetyan@mail.ru, https://orcid.org/0000-0002-3415-8530*

Method for identifying network covert channels

DOI: http://dx.doi.org/10.26583/bit.2021.3.04

Abstract. The aim of this paper is to describe the created method for identifying network covert channels. Traditionally, the scheme for countering information leakage through covert channels is divided into several stages. The first stage is the covert channels identification, that is, the identification of potentially possible covert channels in the system. To identify covert channels, methods based on a shared resources matrix, a tree of covert information flows and a graph of covert information flows are used. Thus, it becomes necessary to concretize the formal description of the stages of the above identification methods in the case of network covert channels. The article describes the created method for identifying network storage covert channels, as well as the results of testing the software implementation of this method for covert channel based on changing the TTL field of the IP packet header. The results can be extended for other network storage covert channels in IP networks, based on the packet header fields changes.
Keywords: covert channel, identification method, shared resource, attribute, information flow.
For citation: KOGOS, Konstantin G.; FINOSHIN, Mihail A.; AIRAPETYAN, Sergey V. Method for identifying

network covert channels. IT Security (Russia), [S.l.], v. 28, n. 3, p. 56-64, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1362. DOI: http://dx.doi.org/10.26583/bit.2021.3.04.

Введение

Понятие скрытого канала впервые было введено Лэмпсоном в [1]. Лэмпсон определил скрытый канал как коммуникационный канал, который изначально не был предназначен для передачи информации. Были предложены и другие подходы к определению скрытого канала. В отечественном стандарте[1] скрытый канал определен как не предусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. Под политикой безопасности информации в этом случае понимают совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. В [2] скрытый канал определен через понятие информационных потоков. Здесь все информационные потоки в системе делятся на два непересекающихся подмножества (разрешенные и неразрешенные), и в силу того, что политика безопасности также определяется через понятие информационных потоков, система защиты должна обеспечивать поддержку разрешенных потоков и препятствовать запрещенным потокам. Тогда скрытый канал – неразрешенный информационный поток, не выявляемый системой защиты.

Таким образом, скрытый канал может использоваться для несанкционированного доступа к информации ограниченного доступа, а передача информации по скрытому каналу осуществляется способом, не предполагаемым разработчиками данной автоматизированной системы как способ передачи информации. В связи с этим встает задача противодействия утечке информации по скрытым каналам. Авторы в [3] предложили методику противодействия утечке информации по скрытым каналам, включающую в себя следующие этапы: идентификация, анализ, устранение, ограничение пропускной способности, аудит и обнаружение. На этапе идентификации рассматриваются всевозможные потенциальные скрытые каналы, которые могут реализовываться в системе.

Из-за широкого распространения протокола IP в области передачи информации актуальной задачей является задача противодействия утечке информации по скрытым каналам, функционирующих в рамках IP-сетей [4–10]. Для реализации первого этапа упомянутой выше методики [3] были предложены различные методы идентификации скрытых каналов [11–13]. Стоит отметить необходимость уточнения этапов работы методов идентификации в случае сетевых скрытых каналов, так как в данном случае существует ограниченный набор возможностей как для построения системы защиты, так и для реализации скрытого канала. В связи с этим целью настоящей работы является разработка метода идентификации сетевых скрытых каналов для повышения защищенности сетей пакетной передачи данных.

1. Методы идентификации скрытых каналов

В [11] предложен метод, основанный на матрице разделяемых ресурсов, и набор условий, необходимых для существования скрытых каналов. Для существования скрытого канала по памяти должны выполняться следующие необходимые условия:

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

– процессы отправки и получения информации должны иметь доступ к одному и тому же атрибуту общего ресурса;

– должны быть средства, с помощью которых процесс отправки может заставить общий атрибут измениться;

– должны быть средства, с помощью которых принимающий процесс может обнаружить изменение атрибута;

– должен существовать механизм для инициирования связи между процессами отправки и получения информации.

Необходимые условия для существования скрытого канала по времени:

– процессы отправки и получения информации должны иметь доступ к одному и тому же атрибуту общего ресурса;

– процессы отправки и получения должны иметь доступ к временной привязке, например, к часам реального времени;

– отправитель должен быть способен модулировать время отклика получателя для обнаружения изменения в общем атрибуте;

– должен существовать механизм для инициирования связи между процессами отправки и получения информации.

В [12] предложен другой метод идентификации скрытых каналов, основанный на построении дерева скрытых информационных потоков. Информация, необходимая для построения дерева скрытых информационных потоков, по существу является той же самой информацией, необходимой для построения базовой матрицы разделяемых ресурсов. Каждая операция характеризуется в терминах списка ссылок, списка изменений и списка возврата.

В [13] предложен метод идентификации скрытых каналов, основанный на построении графа скрытых информационных потоков. Граф скрытых информационных потоков – структура данных, моделирующая поток информации от одного атрибута общего ресурса к другому с целью идентификации последовательности операций, которые поддерживают потенциальные каналы связи, используемые двумя пользователями.

2. Предложенный метод идентификации скрытых каналов по памяти

Постановка задачи, которую необходимо решить в рамках исследования: дана сеть, состоящая из N узлов, и необходимо описать метод, выявляющий все возможные сетевые скрытые каналы в данной сети. В рамках исследования рассматриваются только сетевые скрытые каналы по памяти.

В рассмотренных выше методах идентификации скрытых каналов используются различные структуры данных, однако информация, необходимая для построения всех структур, по существу является одной и той же. Данная информация включает в себя все атрибуты общих ресурсов в системе, а также все операции в системе, которые определяются на первом этапе методов [11–13]. В случае двух узлов, один из которых является получателем, а другой отправителем, общим ресурсом будет являться передаваемый пакет. Так как в рамках данного исследования рассматриваются только скрытые каналы по памяти, то атрибутами общего ресурса (передаваемого пакета) будут являться поля заголовка пакета и его длина. Согласно методам идентификации [11–13], после определения атрибутов необходимо определить элементарные операции во всей системе. Для реализации скрытого сетевого канала операции должны иметь возможность модифицировать атрибуты. Пусть некоторая операция модифицирует атрибут A общего

ресурса. Для реализации скрытого канала изменения атрибута *A* недостаточно, так как после изменения пакет все еще находится у отправителя, и получатель не имеет доступ к атрибуту *A*. Таким образом, вместе с выполнением операции (или последовательности операций), в результате которого атрибут *A* будет модифицирован, должна выполняться передача атрибута *A* получателю. Если в качестве примера рассматривать операционную систему Linux [14], то для реализации сетевого скрытого канала необходимо, чтобы в системе функционировал сетевой сервис, который вызывает функции для модификации атрибутов пакета и обеспечивает отправку пакета получателю. Однако и этого может быть недостаточно. Из-за сложной структуры стека протоколов TCP/IP может случиться, что после получения пакета с модифицированным атрибутом *A* у получателя не будет доступа к атрибуту *A*. Следовательно, для реализации сетевого скрытого канала необходимо, чтобы в системе приемника функционировал сетевой сервис, который обеспечивает получение пакета и вызывает функции для распознавания значения атрибута *A*. Таким образом, для выявления скрытых каналов в сети необходимо провести анализ каждого узла на наличие сервисов, удовлетворяющих вышеперечисленным требованиям.

На основе анализа узлов сети строится граф скрытых информационных потоков в IP-сетях, вершинами которого являются узлы сети и существует дуга из вершины *i* в вершину *j*, если существует возможность построения скрытого канала, где отправителем является узел *i*, а получателем – узел *j*. При этом каждой дуге ставится в соответствие множество атрибутов, по которым возможна реализация скрытого канала.

На следующем этапе определяются скрытые информационные потоки во всей сети. После выбора атрибутов, в рамках которых будет рассматриваться наличие скрытых каналов в сети, рассматриваются множества, соответствующие дугам графа. Если во множестве нет выбранных атрибутов, в рамках которого будет проведено выявление скрытых каналов, то дуга, соответствующая данному множеству, удаляется из графа. После удаления дуг строится транзитивное замыкание графа, которое и выявляет все скрытые информационные потоки в сети, в рамках выбранных атрибутов.

Таким образом, метод идентификации скрытых каналов по памяти в IP-сетях включает следующие этапы:

– определение всех атрибутов общих ресурсов в сети, которые могут быть использованы для построения скрытых каналов по памяти;
– анализ каждого узла сети, включающий:
  - выделение портов, подлежащих анализу, и связанных с ними сокетов;
  - определение процессов, использующих данный сокет;
  - выявление сервисов, запустивших эти процессы;
  - анализ сервисов, включающий в себя выявление системных вызовов, изменяющих и считывающих определенные на первом этапе атрибуты.
– построение графа скрытых информационных потоков в IP-сетях на основе анализа узлов сети;
– выбор атрибутов, в рамках которых будет рассматриваться наличие скрытого канала в сети и выделение подграфа;
– нахождение транзитивного замыкания подграфа.

3. Реализация предложенного метода идентификации

Первым этапом метода идентификации является определение всех атрибутов общих ресурсов в сети. Как было отмечено выше, общим ресурсом в данном случае является передаваемый пакет и связанные с ним характеристики. В рамках данной работы рассматриваются только атрибуты, связанные с протоколом IPv4. На рис. 1 представлен

формат заголовка IPv4 [15]. Как правило, поля «Version», «Source IP address» и «Destination IP address», содержащие версию протокола IP, адрес отправителя и адрес получателя соответственно, не изменяемы и не могут служить атрибутом для передачи информации по скрытому каналу.

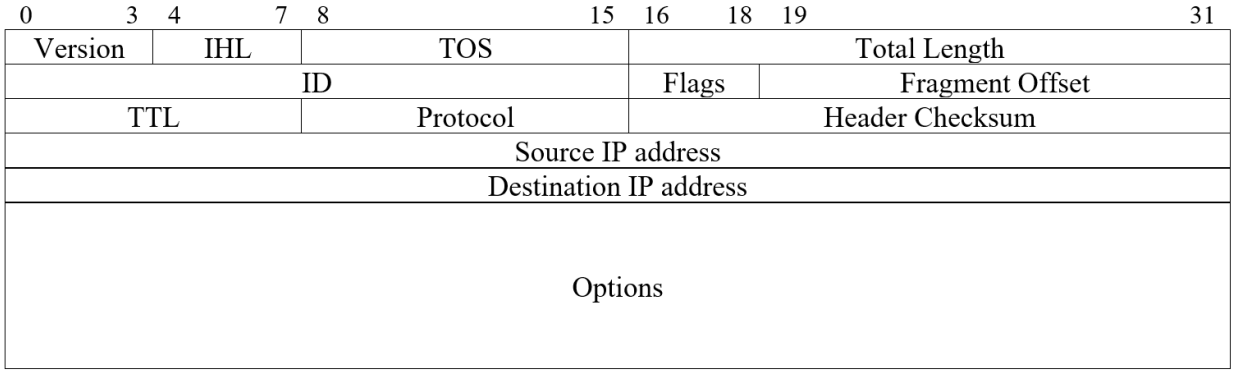


Рис. 1. Формат заголовка IPv4
Fig. 1. IPv4 header format

Поля «Total Length» и «Header Checksum», содержащие длину пакета и контрольную сумму заголовка соответственно, устанавливаются ядром операционной системы и не могут быть изменены напрямую. Однако можно использовать расширения полей заголовка (поле «Options») и заполнить их таким образом, чтобы получить требуемое значение в поля «Header Checksum» [15]. Это дает возможность рассматривать поле «Header Checksum» как атрибут при передаче информации по скрытому каналу. По такому же принципу в качестве атрибута можно рассматривать поле «IHL», в котором содержится размер заголовка IP-пакета. В случае поля «Total Length» требуемое значение поля можно получить, изменяя полезную нагрузку IP-пакета. Известны скрытые каналы, основанные на модификации поля «TTL» заголовка IP-пакета, один из которых описан в [4]. Поле «Protocol» содержит идентификатор протокола транспортного уровня в передаваемом пакете и не может изменяться при использовании в сети транспортного уровня. Согласно [5], существует возможность создания скрытого канала путем модификации поля «ID». При отсутствии фрагментации поле «Fragment offset» также может использоваться при создании скрытого канала [6]. Первый бит поля «Flags» зарезервирован и не используется при передаче пакета, что дает возможность рассматривать его в качестве атрибута. Наконец, поле «TOS», отвечающее за тип обслуживания в сети, также может рассматриваться в качестве атрибута при создании скрытого канала.

На втором этапе разработанного метода идентификации скрытых каналов проводится анализ каждого узла сети. Анализ каждого узла сети подразумевает выполнение четырех шагов. На первом шаге выделяются порты, подлежащие анализу, и связанные с ними сокеты. В зависимости от сети и узла, выбор портов для дальнейшего анализа может быть различным. Существуют различные утилиты для идентификации портов и связанных с ними сокетов в операционной системе Linux. Одним из примеров такой утилиты является *ss* [16], которая была использована при разработке программного средства идентификации сетевых скрытых каналов. Утилита *ss* предоставляет подробную информацию о сокете, в том числе информацию о процессе, который использует данный сокет, а также информацию о сервисе, запустившем этот процесс, что является вторым и третьим шагом при анализе узла. На четвертом шаге проводится анализ сервиса,

выделенного на третьем шаге, и идентифицируются все те системные вызовы, которые изменяют и считывают атрибуты, определенные на первом этапе.

В [17] представлено программное средство идентификации сетевых скрытых каналов, разработанное авторами статьи. На вход программному средству подается порт, который необходимо проанализировать. Программное средство идентифицирует процесс, связанный с данным портом, и сервис, запустивший этот процесс. После этого программное средство идентифицирует все системные вызовы, относящиеся к данному сервису, и выделяет те, которые предоставляют доступ к атрибутам. Затем проводится анализ аргументов данных системных вызовов и на основе анализа принимается решение о возможном существовании скрытого канала.

Данное программное средство идентифицирует скрытые каналы, основанные на изменении поля «TTL» заголовка IP-пакета путем сравнения значения поля «TTL», устанавливаемого ядром ОС, и значения, передаваемого системному вызову в качестве аргумента. Стоит отметить, что приведенный подход может быть применен и для идентификации других видов скрытых каналов.

Например, при отсутствии фрагментации пакетов ядро устанавливает значение поля «Fragment offset», равное нулю. Таким образом, можно идентифицировать скрытый канал, основанный на использовании атрибута «Fragment Offset», путем выявления передачи системным вызовам значения поля «Fragment offset», отличного от нуля.

Реализована одноранговая сеть со встроенными скрытыми каналами [17] для тестирования разработанного программного средства идентификации скрытых каналов. На рис. 2 представлен процесс идентификации скрытых каналов в одноранговой сети при применении разработанного метода идентификации сетевых скрытых каналов.

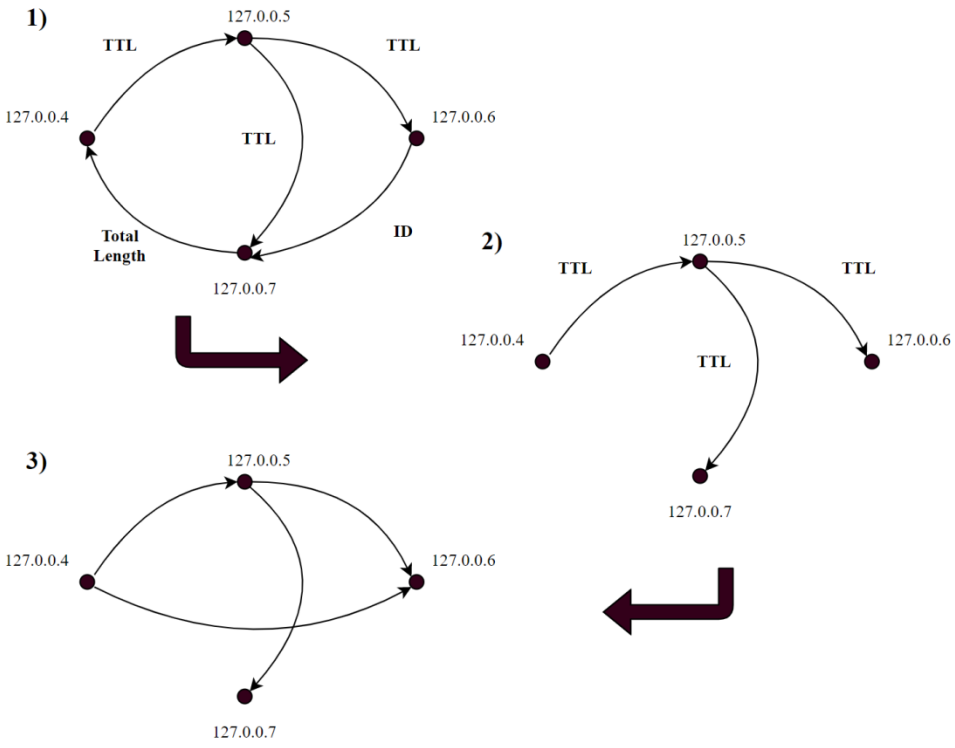


Рис. 2. Процесс идентификации скрытых каналов в одноранговой сети при использовании разработанного метода идентификации сетевых скрытых каналов

Fig. 2. The process of identifying hidden channels in a peer-to-peer network when using the developed method of identifying network hidden channels

Первый граф описывает скрытые информационные потоки построенной одноранговой сети, где метками дуг являются те атрибуты, которые используются для создания скрытого канала. Второй граф показывает скрытые информационные потоки в рамках третьего этапа метода идентификации, которые получены в результате применения разработанного программного средства. На четвертом этапе проводится выбор атрибутов, в рамках которых будет рассматриваться наличие скрытого канала в сети и выделяется подграф. В данной работе выбран атрибут «TTL», а так как программное средство идентификации разработано для скрытых каналов, основанных на изменении атрибута «TTL», то выделенный подграф совпадает с графом скрытых информационных потоков одноранговой сети, построенным при использовании разработанного программного средства (ни одна дуга не удалена).

На пятом этапе строится транзитивное замыкание подграфа, выделенного на предыдущем этапе. В данном случае транзитивным замыканием является третий граф на рис. 2, представляющий собой все скрытые информационные потоки в сети, определенные разработанным методом.

При сравнении результата применения разработанного метода идентификации (третий граф) с графом скрытых информационных потоков созданной сети (первый граф) можно убедиться, что третий граф является транзитивным замыканием первого графа в рамках атрибута «TTL». Следовательно, применение разработанного метода позволило идентифицировать все скрытые информационные потоки в рамках атрибута «TTL».

В данной работе представлено тестирование разработанного метода идентификации для скрытых каналов, основанных на изменении атрибута «TTL». Однако разработанный метод может быть применен и для идентификации других видов сетевых скрытых каналов по памяти.

Заключение

В работе приведено описание разработанного метода идентификации сетевых скрытых каналов. Преимущество данного метода перед известными в том, что он может быть легко автоматизирован для практических задач идентификации скрытых каналов в IP-сетях на основе изменения полей заголовков пакетов.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
2. Тимонина Е.Е. Скрытые каналы (обзор). Jet info. 2002. Т. 14. №. 114. С. 3–11. URL: https://www.jetinfo.ru/Sites/portal/Uploads/2002_11.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf (дата обращения: 20.04.21).
3. Kogos K., Sokolov A. Methods of IPD normalization to counteract IP timing covert channels. CEUR Workshop Proceedings. 2017. P. 118–126. URL: http://ceur-ws.org/Vol-1901/paper20.pdf (дата обращения: 20.04.21).
4. Zander S., Armitage G., Branch P. An empirical evaluation of IP Time To Live covert channels. 2007 15th IEEE International Conference on Networks. IEEE, 2007. P. 42–47. DOI: http://dx.doi.org/10.1109/ICON.2007.4444059.
5. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 2007. Vol. 9, no. 3. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
6. Rowland C.H. Covert channels in the TCP/IP protocol suite. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/download/528/449?inline=1 (дата обращения: 20.04.21).

7. Ahsan K., Kundur D. Practical data hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia. 2002. Vol. 2, no. 7. P. 1–8. URL: https://www.comm.toronto.edu/~dkundur/pub_pdfs/AhsKunMMSec02.pdf (дата обращения: 20.04.21).
8. Yao Q., Zhang P. Coverting channel based on packet length. Computer engineering. 2008. Vol. 34, no. 3. P. 183–185. URL: https://en.cnki.com.cn/Article_en/CJFDTotal-JSJC200803064.htm (дата обращения: 20.04.21).
9. Ji L., Jiang W., Dai B. and Niu X. A novel covert channel based on length of messages. 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE, 2009. P. 551–554. DOI: http://dx.doi.org/10.1109/IEEC.2009.122.
10. Ji L., Liang H., Song Y. and Niu X. A normal-traffic network covert channel. 2009 International Conference on Computational Intelligence and Security. IEEE, 2009. P. 499–503. DOI: http://dx.doi.org/10.1109/CIS.2009.156.
11. Kemmerer R.A. Shared resource matrix methodology: An approach to identifying storage and timing channels. ACM Transactions on Computer Systems (TOCS). 1983. Vol. 1, no. 3. P. 256–277. DOI: https://doi.org/10.1145/357369.357374.
12. Porras P.A. and Kemmerer R.A. Covert flow trees: a technique for identifying and analyzing covert storage channels, Proceedings. IEEE Computer Society Symposium on Research in Security and Privacy, 1991. P. 36–51. DOI: https://doi.org/10.1109/RISP.1991.130770.
13. Song X.M., Ju S.G. Covert Flow Graph Approach to Identifying Covert Channels. Journal of Networks. 2011. Vol. 6, no. 12. P. 1740–1746. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.658.385&rep=rep1&type=pdf#page=88 (дата обращения: 20.04.21).
14. Socket: Linux Programmer's Manual. URL: https://www.man7.org/linux/man-pages/man2/socket.2.html (дата обращения: 12.05.2020).
15. RFC 791: Internet Protocol – Data Internet Program – Protocol Specification. 1981. URL: https://datatracker.ietf.org/doc/html/rfc791 (дата обращения: 20.04.21).
16. Ss: Linux man page. URL: https://linux.die.net/man/8/ss (дата обращения: 19.03.2021).
17. Software for identifying network covert channels page. URL: https://github.com/HayrapetyanSV/network_cc_identification/blob/master/program.py (дата обращения: 20.04.21).

REFERENCES:

[1] Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
[2] Timonina E.E. Skrytye kanaly (obzor). Jet info. 2002. T. 14, no. 114. S. 3–11. URL: https://www.jetinfo.ru/Sites/portal/Uploads/2002_11.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf (accessed: 20.04.21) (in Russian).
[3] Kogos K., Sokolov A. Methods of IPD normalization to counteract IP timing covert channels. CEUR Workshop Proceedings. 2017. P. 118–126. URL: http://ceur-ws.org/Vol-1901/paper20.pdf (accessed: 20.04.21).
[4] Zander S., Armitage G., Branch P. An empirical evaluation of IP Time To Live covert channels //2007 15th IEEE International Conference on Networks. IEEE, 2007. P. 42–47. DOI: http://dx.doi.org/10.1109/ICON.2007.4444059.
[5] Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 2007. Vol. 9, no. 3. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
[6] Rowland C. H. Covert channels in the TCP/IP protocol suite. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/download/528/449?inline=1 (accessed: 20.04.21).
[7] Ahsan K., Kundur D. Practical data hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia. 2002. Vol. 2, no. 7. P. 1–8. URL: https://www.comm.toronto.edu/~dkundur/pub_pdfs/AhsKunMMSec02.pdf (accessed: 20.04.21).
[8] Yao Q., Zhang P. Coverting channel based on packet length. Computer engineering. 2008. Vol. 34, no. 3. P. 183–185. URL: https://en.cnki.com.cn/Article_en/CJFDTotal-JSJC200803064.htm (accessed: 20.04.21).

[9] Ji L., Jiang W., Dai B. and Niu X. A novel covert channel based on length of messages. 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE, 2009. P. 551–554. DOI: http://dx.doi.org/10.1109/IEEC.2009.122.

[10] Ji L., Liang H., Song Y. and Niu X. A normal-traffic network covert channel. 2009 International Conference on Computational Intelligence and Security. IEEE, 2009. P. 499–503. DOI: http://dx.doi.org/10.1109/CIS.2009.156.

[11] Kemmerer R.A. Shared resource matrix methodology: An approach to identifying storage and timing channels. ACM Transactions on Computer Systems (TOCS). 1983. Vol. 1, no. 3. P. 256–277. DOI: https://doi.org/10.1145/357369.357374.

[12] Porras P.A. and Kemmerer R.A. Covert flow trees: a technique for identifying and analyzing covert storage channels, Proceedings. IEEE Computer Society Symposium on Research in Security and Privacy, 1991. P. 36–51. DOI: https://doi.org/10.1109/RISP.1991.130770.

[13] Song X.M., Ju S.G. Covert Flow Graph Approach to Identifying Covert Channels. Journal of Networks. 2011. – Vol. 6, no. 12. P. 1740–1746. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.658.385&rep=rep1&type=pdf#page=88 (accessed: 20.04.21).

[14] Socket: Linux Programmer's Manual. URL: https://www.man7.org/linux/man-pages/man2/socket.2.html (accessed: 12.05.2020).

[15] RFC 791: Internet Protocol – Data Internet Program – Protocol Specification. 1981. URL: https://datatracker.ietf.org/doc/html/rfc791 (accessed: 20.04.21).

[16] Ss: Linux man page. URL: https://linux.die.net/man/8/ss (accessed: 19.03.2021).

[17] Software for identifying network covert channels page. URL: https://github.com/HayrapetyanSV/network_cc_identification/blob/master/program.py (accessed: 20.04.21).

Поступила в редакцию – 20 апреля 2021 г. Окончательный вариант – 19 августа 2021г.
Received – April 20, 2021. The final version – August 19, 2021.

Андрей И. Терентьев
Московский государственный технический университет гражданской авиации,
Кронштадтский б–р, 20, Москва, 125993, Россия
e-mail: terentyev-doc@yandex.ru, http://orcid.org/0000-0002-0493-3161

КОНЦЕПТУАЛЬНАЯ СХЕМА (ПАРАДИГМА) ТЕХНОЛОГИИ СВЯЗНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.3.05

Аннотация. В статье предложена концептуальная схема (парадигма) практических взглядов и подходов в отношении технологии связных математическим, криптографическим и иным способом данных, рассматриваемых с позиции математики как некоторое множество *M*, элементами которого могут являться множества, а также конструктивные, гибридные и иные объекты, включающие, в том числе, информационную и служебную составляющие. Вводятся понятия связного множества, размерности его структуры и силы установленной связи. Утверждается, что потенциал практического применения различных систем связных данных, особенно нетрадиционно организованных структур многомерно связных данных, гораздо выше, чем это представляется в настоящее время. В качестве примера предложены двумерная структура множества *M* в виде цилиндрической трубы (линейно-кольцевая структура) и трехмерная структура в ортогональном базисе в виде куба (параллелепипеда), которые могут иметь перспективы практического использования в различных проектах цифровой экономики, где данные используются одновременно в нескольких процессах.

Ключевые слова: технологии связных данных, технологии блокчейна, связное множество, структура связного множества, размерность структуры связного множества, сила связи элементов связного множества.

Для цитирования: ТЕРЕНТЬЕВ, Андрей И. КОНЦЕПТУАЛЬНАЯ СХЕМА (ПАРАДИГМА) ТЕХНОЛОГИИ СВЯЗНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 65–72, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1363. DOI: http://dx.doi.org/10.26583/bit.2021.3.05.

Andrey I. Terentyev
The Moscow State Technical University of Civil Aviation (MSTUCA),
Kronshtadtskiy bulvar, 20, Moscow, 125993, Russia
e-mail: terentyev-doc@yandex.ru, http://orcid.org/0000-0002-0493-3161

Conceptual scheme (paradigm) of connected data technologies

DOI: http://dx.doi.org/10.26583/bit.2021.3.05

Abstract. The paper proposes to consider blockchain technology as one of the possible technologies aimed at ensuring the integrity, availability and reliability of various data sets. In order to streamline the directions of research of such technologies, the paper proposes an initial conceptual scheme (paradigm) of practical views and approaches in relation to the technology of mathematically, cryptographically and otherwise connected data, considered from the standpoint of mathematics as a set M, the elements of which can be sets, as well as constructive, hybrid and other objects, including, inter alia, information and service components. The concepts of a connected set, the dimensions of its structure and the strength of the established connection are introduced. It is argued that the potential for practical application of various systems of connected data, especially unconventionally organized structures of multidimensionally connected data, is much higher than it seems at present. As an example, a two-dimensional structure of the set M in the form of a cylindrical pipe (linear-ring structure) is proposed, as well as a three-dimensional structure in an orthogonal basis in the form of a cube (parallelepiped), which may have prospects for practical applications in various projects of digital economy where data is used simultaneously in several processes.

Keywords: connected data technologies, blockchain technology, connected set, structure of a connected set, dimension of the structure of a connected set, strength of connection of elements of a connected set.
For citation: TERENTYEV, Andrey I. Conceptual scheme (paradigm) of connected data technologies. IT Security (Russia), [S.l.], v. 28, n. 3, p. 65–72, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1363. DOI: http://dx.doi.org/10.26583/bit.2021.3.05.

Введение

В настоящее время научным и профессиональным сообществом достаточно широко и в ряде случаев эмоционально обсуждаются проблемы эффективности, потенциальных возможностей и границ применимости популярной технологии блокчейн (blockchain), поскольку с каждым годом становится все более очевидным, что она во многом не оправдывает возлагаемых на нее обществом завышенных ожиданий, несмотря на отдельные примеры ее успешного использования. При этом суть самой технологии не нова. Можно привести исторические примеры более двухтысячелетнего использования идеи передачи наследуемых признаков или свойств вновь создаваемым объектам или сущностям для обеспечения их аутентичности, которые применяются по сей день.

Широкий спектр мнений о рыночных и социальных перспективах распространения и внедрения технологии блокчейн изложен в [1–3]. Конкретные вопросы его практического применения и стандартизации рассмотрены в [4] и приведены основные первоисточники и наиболее часто цитируемые определения технологии блокчейн, из которых следует, что в настоящее время понятие технологии блокчейн устойчиво связано с одновременным использованием технологии распределенного реестра и специальной криптографической процедуры, основанной на свойствах функции хэширования и древовидном способе хэширования данных, посредством которой обеспечивается связь блоков данных, входящих в формируемую и постоянно удлиняющуюся рекуррентную последовательность (цепь). Кроме этого, в [4] аргументированно отмечается, что остается еще много нерешенных вопросов в области унификации и реализации технологии блокчейн. Характерные примеры критического отношения к завышенным ожиданиям, связанным с этой технологией приведены в [5–6]. К этому следует добавить, что на практике часто происходит смешение или отождествление технологии блокчейн с другими сопоставимыми методиками, процессами и технологиями, которые также направлены на обеспечение целостности, доступности и достоверности различных массивов данных, но основаны на иных принципах обеспечения их связанности. При этом все подобные технологии призваны способствовать формированию высокого уровня доверия у потенциальных пользователей к использующим их прикладным системам, что в условиях тотальной цифровизации и сопутствующего ей взрывного роста количества киберпреступлений очень востребовано обществом. Это в свою очередь побуждает разработчиков-практиков предлагать различные пути решения этой проблемы. Однако в области теории какого-либо единого базиса для описания и исследования технологий связных данных не существует.

1. Исходная концептуальная схема (парадигма) технологии связных данных

Учитывая изложенное, автор предпринял попытку сформировать некую исходную концептуальную схему практических взглядов и подходов в отношении технологии связных[1] тем или иным способом данных, которая могла бы дать повод для дальнейшей

[1]Термин «связный» применяется в отношении совокупности элементов (множества) и употребляется в значении, которое используется в математике и основывается, в том числе на его толковании в русском языке следующим образом: хорошо и последовательно организованный, логически стройный. Его не следует путать со словом «связанный», которое имеет другие значение. При этом, рассматривая

научно-практической дискуссии. Приводимые далее утверждения достаточно очевидны и не требуют доказательства. При необходимости они могут быть доказаны, однако это выходит за рамки настоящей статьи. К используемым в статье элементам дискретной математики можно обратиться, в том числе, в классических работах [7–9] и более современных источниках, например, [10]. Предлагаемые ниже постулаты и суждения упорядочены согласно авторскому представлению об их логической взаимосвязи и последовательности:

1. Любые данные или наборы данных (далее – данные) могут быть тем или иным способом представлены и идентифицированы. При этом для конкретной практической задачи всегда существует способ их идентификации, при котором идентификаторы не будут совпадать (повторяться).

2. Любые данные, в том числе идентифицированные, могут быть тем или иным способом представлены как элементы некоторого множества M, которое может быть задано посредством перечисления всех его элементов: $M = \{m_1, m_2, ..., m_k\}$, или посредством указания порождающей процедуры (алгоритма) или свойства, на основании которого они принадлежат этому множеству: $M = \{m|P(m)\}$. При этом следует учитывать, что элементами множества могут являться множества, а также конструктивные, гибридные и иные сложно структурированные объекты, включающие, в том числе, информационную и служебную составляющие.

3. Множество M будем считать связным, если на нем установлено бинарное или иное отношение R, обладающее свойством связности (на других свойствах, в том числе рефлективности, симметричности и транзитивности, пока останавливаться не будем). Соответственно данные, которые представляются элементами такого множества, будут являться в той или иной степени связанными между собой.

4. Свойство (порождающая процедура, функция, алгоритм), посредством которого устанавливается взаимосвязь между элементами множества и обеспечивается его связность, может быть любой природы, в зависимости от решаемой научной или практической задачи. Например, природа свойства (порождающей процедуры, функции, алгоритма), обеспечивающего связность, может быть:

- математической (числовой, логической, аналитической и т.п.);
- криптографической;
- семантической;
- визуально-смысловой;
- лексикографической;
- табличной;
- комбинированной и иной[2].

5. На связном множестве M может быть установлено отношение порядка, при котором нумерация (индексирование) его элементов будет не случайной (будет носить регулярный характер).

Таким образом возможно последовательное порождение всех элементов множества M, которое будет являться перечислимым и разрешимым. Это позволяет, в том числе, проверить для любого элемента такого множества актуальность свойства связности, т.е.

особенности и взаимосвязь отдельных, например, двух конкретных элементов множества, находящихся в каком-либо отношении, можно использовать термины «связь», «связаны» и т.п.

[2]В технологии блокчейн использована криптографическая порождающая процедура на базе хэш-функции. В качестве одной из основ для математической порождающей процедуры могут, по мнению автора, эффективно использоваться числовые линейные блоковые корректирующие коды над кольцом конечных десятичных дробей [11].

выполнение порождающей процедуры (функции, алгоритма) и наличие установленной ею связи с любым другим элементом этого множества. Если результат проверки отрицательный, то считается, что рассматриваемый элемент множеству M не принадлежит.

6. Установление связности элементов множества, а также отношение порядка, задаваемое на множестве, должны иметь здравый смысл и конкретную цель, обусловленные решаемой научной или практической задачей. При этом основная цель обеспечения связности – это существенное затруднение или исключение возможности бесконтрольного или нештатного изменения (модификации) таких структур и их элементов. Иные задачи, в том числе, направленные на обеспечение приватности, анонимности, репликации, децентрализации, производительности, масштабируемости и т.п., решаются посредством применения других методов и технологий.

7. Установление связности элементов и отношения порядка на множестве (совокупности множеств) может быть линейным или нелинейным, односвязным или многосвязным, а также n-мерным (многомерным), что определяет структуру множества M. В случае многомерности ($n \geq 2$) такое множество уместно называть системой связных множеств (подмножеств). Примером одномерной ($n = 1$) структуры может являться последовательность или кольцо, двумерной ($n = 2$) – таблица или матрица (в ортогональном базисе), а также труба или объекты спирально-винтового типа. Простейшим примером трехмерной ($n = 3$) структуры множества M является куб или параллелепипед (в ортогональном базисе).

8. Результирующая сила S установленной связи (т.е. условная стойкость к ее изменению или нарушению) зависит от сложности T порождающей процедуры, p – глубины рекурсии, n-мерности структуры множества M и мощности множества M:

$$S = \partial\,(T, p, n, |M|),$$

где ∂ – функция соответствующих аргументов.

Интуитивно понятно, чем алгоритмически сложнее порождающая процедура и глубже рекурсия, тем больше элементов множества M будут вовлечены в установление такой связи и тем больше результирующая сила связи между элементами связного множества, полученного в результате этой процедуры. Соответственно, чем больше n, тем больше у каждого элемента множества M соседних (т.е. окружающих его) элементов, которые могут быть задействованы в установление связи. При больших значениях p, n и $|M|$ (где $|M|$ – мощность множества M) изменение установленного ранее порядка или замена (модификация) элемента, с сохранением связности множества M, может является трудновыполнимой задачей, а при $n > \mu$ эта задача может быть теоретически не выполнимой (где μ – некоторое пороговое значение, сложным образом зависящее от мощности множества M, алгоритмической сложности T порождающей процедуры и глубины рекурсии p).

В общем случае, когда элемент m_i множества M не является первым или последним, минимальное количество связей h_{min} элемента m_i определяется количеством соседних с ним элементов и зависит от размерности n множества M следующим образом: $h_{min} = 2n$. Например, в случае одномерной структуры множества M (т.е. при $n = 1$) соседними элементами с m_i являются m_{i-1} и m_{i+1}, а $h_{min} = 2$.

Максимально возможное количество связей h_{max} элемента m_i множества M с другими элементами этого множества зависит не только от размерности n множества M, но и от используемой порождающей такое связное множество процедуры, в том числе глубины рекурсии. Предельное значение h_{max} определяется следующим образом: $h_{max} = |M|–1$.

9. Отношение порядка может устанавливаться тем или иным способом, в том числе рекуррентным.

Если отношение порядка установлено рекуррентным способом, то при $n = 1$ множество M можно рассматривать как рекуррентную последовательность, в которой для любой пары элементов будет выполняться отношение строго порядка $m_i R m_j$, а для каждой пары соседних элементов (m_{i-1}, m_i) или (m_i, m_{i+1}) рекуррентной последовательности будет выполняться отношение доминирования $m_{i-1} R m_i$ и $m_i R m_{i+1}$. Абстрактное графическое представление такой последовательности в ортогональном базисе приведено на рис. 1.

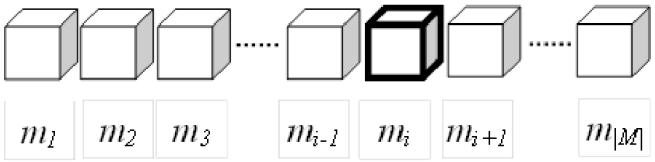


Рис. 1. Абстрактное графическое представление рекуррентной последовательности (n=1)
Fig. 1. Abstract graphical representation of a recurrent sequence (n=1)

Формулу общего члена рекуррентной последовательности можно представить следующим образом:

$$m_i = f(i, m_{i-1}, m_{i-2}, \ldots, m_{i-p}),$$

где f – порождающая процедура, функция или алгоритм формирования членов последовательности; m_i – i-ый или общий член последовательности, а i – порядковый номер (индекс), $i \in N$ (N – множество натуральных чисел); p – ранг рекуррентной последовательности (количество предыдущих членов последовательности, участвующих в формировании текущего члена последовательности).

По принципу образования элементов это рекуррентная последовательность, а, по сути, полученная таким образом вся совокупность элементов – это связное перечислимое разрешимое и упорядоченное множество, допускающее, при необходимости, дополнение его новыми элементами.

10. Любые данные могут быть тем или иным способом представлены в виде наборов чисел или одного числа. Если средством обработки таких данных является электронное техническое устройство (электронная вычислительная машина), то соответствующие числа или число будут являться элементами кольца конечных десятичных дробей D.

2. Примеры нетрадиционно организованных структур связных данных

Абстрактное графическое представление двухмерной структуры ($n = 2$) связного множества M в виде таблицы или матрицы достаточно тривиально. Характерной особенностью такой прямоугольной структуры является то, что составляющие ее линейные подмножества, ориентированные по строкам и столбцам, могут являться постоянно растущими последовательностями (цепями). Существенно больший интерес для исследования вызывают нетрадиционно организованные структуры связных данных. В связи с этим автором предлагается к рассмотрению двумерная структура в виде цилиндрической трубы (линейно-кольцевая структура), которая приведена на рис. 2. Преимущества и перспективы практического использования такой структуры в большей степени связаны с процессами, которые носят цикличный характер. Например, в часе

60 минут, в сутках 24 часа, в году 12 месяцев. В связи с этим кольцевая структура органично подходит для создания связного множества цифровых данных, отражающих события (факты, соглашения, транзакции), произошедшие, например, за текущие сутки, а линейная связь одноименных (имеющих одинаковые индексы) элементов из каждого кольца в постоянно растущую последовательность (цепь) позволяет сформировать защищенное от модификации множество цифровых данных, отражающих события в конкретным момент времени суток, но произошедшие в течение какого-либо более продолжительного временного периода, например, недели, месяца или года. При этом линейный рост соответствующих последовательностей (цепей) не ограничен, а новые кольца по мере их формирования «нанизываются» на трубу.

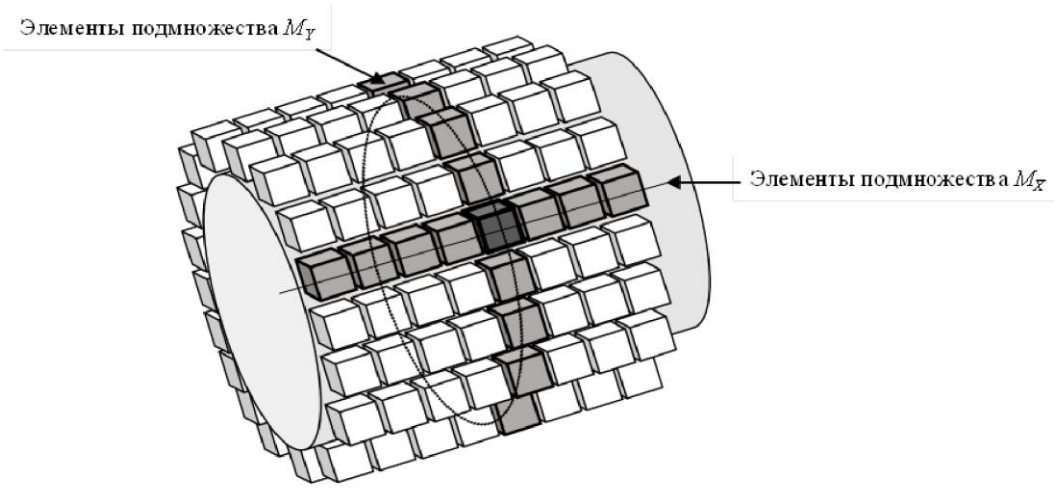


Рис. 2. Абстрактное графическое представление двухмерной структуры (n = 2) связного множества M в виде цилиндрической трубы
Fig. 2. Abstract graphical representation of a two-dimensional structure (n = 2) of a connected set M in the form of a cylindrical tube

Следует отметить, что порождающая процедура (функция, алгоритм), посредством которой будет устанавливаться взаимосвязь между элементами кольцевого и линейного подмножеств с целью обеспечения их связности, может быть любой природы, что зависит от решаемой практической задачи. Если за основу взята технология блокчейн, то порождающая процедура, обеспечивающая связность каждого из подмножеств, в силу использования функции хэширования, будет являться (согласно предложенной в п. 4 классификации) криптографической. В случае использования иных принципов обеспечения взаимосвязи между элементами подмножеств, например, посредством их кодирования числовым линейным блоковым корректирующим кодом [11], порождающая процедура (по предложенной в п. 4 классификации) будет математической. Также может использоваться комбинированная порождающая процедура, сочетающая в себе различные принципы обеспечения связности подмножеств.

Абстрактное графическое представление трехмерной структуры ($n = 3$) множества M в ортогональном базисе в виде куба приведено на рис. 3. Поскольку каждый элемент таким образом организованного связного множества одновременно входит в каждое из составляющих его связных подмножеств M_x, M_y и M_z, то результирующая сила установленной связи S, а следовательно и стойкость связного множества к модификации, будет (при прочих равных условиях) выше, чем в любой двумерной структуре.

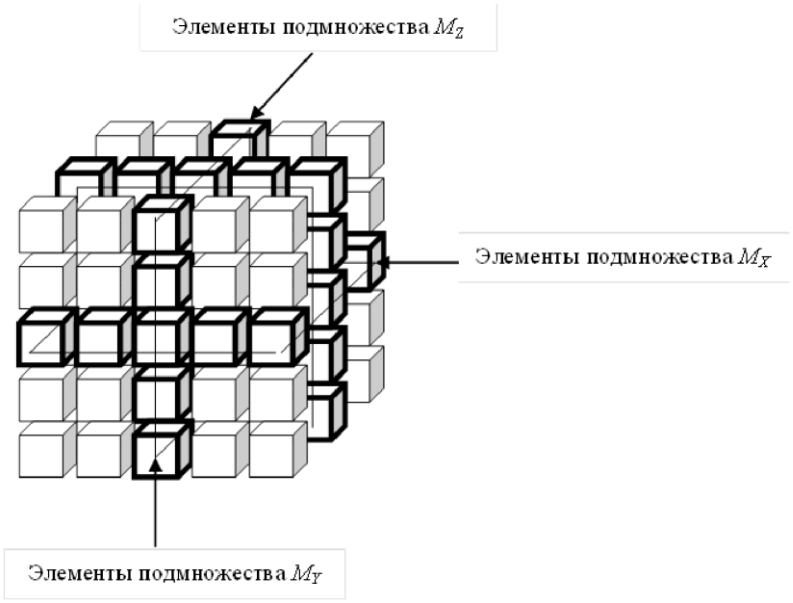


Рис. 3. Абстрактное графическое представление трехмерной структуры (n = 3) связного множества M в виде куба
Fig. 3. Abstract graphical representation of the three-dimensional structure (n = 3) of a connected set M in the form of a cube

Заключение

С потребительской точки зрения организованные подобным образом связные множества являются источниками той или иной информации, необходимой пользователю в конкретный момент времени, т.е. информационными системами, базами или массивами данных. Основное требование, которое к ним предъявляется пользователем – соответствие заявленным характеристикам, в том числе связанным с их целостностью и достоверностью.

Общественная и научная дискуссии в отношении специфики использования связных данных ведутся, в основном, применительно к системам, основанным на технологии блокчейн (функции хэширования) и имеющим одномерную структуру. Однако потенциал применения различных систем связных данных может быть выше в случае построения многомерных структур, а также использования отличных от технологии блокчейн (альтернативных) порождающих процедур, например, основанных на числовом помехоустойчивом кодировании блоков данных. В ближайшем будущем они могут быть востребованы в различных областях и проектах цифровой экономики, особенно в тех, где данные используются одновременно в нескольких процессах. Однако это требует дополнительных исследований, которые в настоящее время ведутся автором.

СПИСОК ЛИТЕРАТУРЫ:

1. Генкин А., Михеев А. Блокчейн: Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. – 592 с.
2. Дон Тапскотт, Алекс Тапскотт. Технология блокчейн: то, что движет финансовой революцией сегодня / [пер. с англ. К. Шашковой, Е. Ряхиной]. М.: Эксмо, 2018. – 443 с.
3. Шваб, Клаус. Технологии Четвертой промышленной революции: [перевод с английского]. М.: Эксмо, 2018. – 320 с.
4. Будзко, Владимир И.; Милославская, Наталья Г. Вопросы практического применения технологии блокчейна. Безопасность информационных технологий, [S.l]. Т. 26, № 1. С. 36–45, 2019. ISSN 2074-

7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1178 (дата обращения: 19.02.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.04.
5. Колодзей А. Ключ к паутине. Перспективы использования блокчейн-технологий в цифровом государстве // BIS JOURNAL. 2019, № 1. С. 106–111. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (дата обращения: 19.04.2021).
6. Катанкина А. Аргументы против фактов. Удачный маркетинговый ход или экономически успешная стратегия? // BIS JOURNAL. 2019, № 1. С. 112–113. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (дата обращения: 19.04.2021).
7. Б.Л. ван дер Варден. Алгебра: Пер. с нем. М.: Наука, 1979. – 624 с.
8. Кузнецов О.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. – 2-е изд., перераб. и доп. М.: Энергоатомиздат, 1988. – 480 с.
9. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика. М.: Наука. Физматлит, 1999. – 544 с.
10. Андерсон, Джеймс А. Дискретная математика и комбинаторика: Пер. с англ. М.: Издательский дом «Вильямс», 2003. – 960 с.
11. Терентьев А.И. Элементы теории и практики числовых линейных блоковых корректирующих кодов. М.: Альтекс, 2000. – 204 с.

REFERENCES:

[1] Genkin A., Mikheev A. Blockchain: How it works and what awaits us tomorrow. M.: Alpina Publisher, 2018. – 592 p. (in Russian).
[2] Don Tapscott, Alex Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. M.: Eksmo, 2018. – 443 p. (in Russian).
[3] Klaus Schwab. Shaping the Fourth Industrial Revolution. M.: Eksmo, 2018. –320 p. (in Russian).
[4] Budzko, Vladimir I.; Miloslavskaya, Natalia G. Issues of Practical Application of Blockchain Technology. IT Security (Russia), [S.l]. Vol. 26. No. 1. P. 36–45, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1178 (accessed: 19.02.2021). DOI: http://dx.doi.org/10.26583/bit.2019.1.04 (in Russian).
[5] Colodzey A. The key to the web. Prospects for the use of blockchain technologies in the digital state. BIS JOURNAL. 2019. No. 1. P. 106–111. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (accessed: 19.04.2021) (in Russian).
[6] Catankina A. Arguments against facts. Marketing Success or Economically Successful Strategy? BIS JOURNAL. 2019. No. 1. P. 112–113. URL: https://ib-bank.ru/bisjournal/number_pdf/61 (accessed: 19.04.2021) (in Russian).
[7] B.L. Van Der Waerden. Algebra. Springer-Verlag. Berlin. Heidelberg. New York. 1971 (in Russian).
[8] Kuznetsov O.P., Adelson-Velsky G.M. Discrete math for an engineer. – 2nd ed. M.: Energoatomizdat, 1988. – 480 p. (in Russian).
[9] Gorbatov V.A. Fundamentals of discrete mathematics. Information mathematics. M.: Science. Fizmatliit, 1999. – 544 p. (in Russian).
[10] James A. Anderson. Discrete Mathematics with Combinatorics. M.: Publishing house «Williams», 2003. – 960 p. (in Russian).
[11] Terentyev A.I. Elements of the theory and practice of numeric linear block error-correcting codes. M.: Alteks, 2000. – 204 p. (in Russian).

Поступила в редакцию – 20 апреля 2021 г. Окончательный вариант – 20 августа 2021г.
Received – April 20, 2021. The final version – August 20, 2021.

Алексей В. Плугатарев[1], Анатолий Л. Марухленко[2], Михаил А. Бугорский[3],
Андрей С. Булгаков[4], Михаил А. Марченко[5]
[1,2]Юго-Западный государственный университет,
ул. 50 лет октября, 94, Курск, 305040, Россия
[3]в/ч 33310, п. Шайковка, Кировский р-н, Калужская обл, 249455, Россия
[4,5]Национальный исследовательский университет «Московский институт электронной техники»,
площадь Шокина, 1, Зеленоград, Москва, 124498, Россия
[1]e-mail: aplugatarev@bk.ru, https://orcid.org/0000-0002-8549-4382
[2]e-mail: proxy33@mail.ru, https://orcid.org/0000-0002-3575-924X
[3]e-mail: bygorbtc2013@gmail.com, https://orcid.org/0000-0003-1788-0211
[4]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[5]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.3.06

Аннотация. Для минимизации ущерба от кибератак, организации используют системы мониторинга своей сетевой инфраструктуры. Такие инфраструктуры собирают огромное количество информации из журналов систем безопасности и систем управления событиями. Структурируя эти данные и анализируя при помощи нейронных сетей, данное исследование ставит цель – разработка алгоритма автономного обнаружения вредоносных хостов в сети. Автоматизация этого процесса, позволит более точно, и оперативно, чем это делают эксперты вычислять вредоносные компьютеры-хосты, что увеличит отказоустойчивость информационной системы предприятия. Для моделирования системы принятия решений используется ограниченная машина Больцмана, в данном исследовании – модель стохастической нейронной сети, определяющей распределение вероятности на входных образцах данных. Эффективность предложенной модели исследуется при помощи показателя AUC – численной характеристики кривой ошибок, которая является площадью, ограниченной ROC-кривой и осью. Даная ось отделяет долю ложных положительных результатов – вероятностей, которые классификатор верно отнёс к безопасным хостам. Представленная модель с применением нейронных сетей, обеспечивает мониторинг и обнаружение вредоносных компьютеров-хостов в информационных системах в реальном времени, позволяет принимать решение о событиях информационной безопасности без участия экспертов, на основе анализа данных различных внутренних систем и служб.

Ключевые слова: система машинного обучения; обнаружение вредоносного хоста; системы информационной безопасности.

Для цитирования: ПЛУГАТАРЕВ, Алексей В. и др. ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 73–80, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1364. DOI: http://dx.doi.org/10.26583/bit.2021.3.06

Alexey V. Plugatarev[1], Anatoly L. Maruhlenko[2], Mikhail A. Bugorskij[3],
Andrey S. Bulgakov[4], Mikhail A. Marchenko[5]
[1,2]South-West State University,
50 Let Oktyabrya str., 94, Kursk, 305040, Russia
[3]Military unit No. 33310, item Shaikovka, Kirovsky district, Kaluga region, 249455, Russia
[4,5]National Research University of Electronic Technology,
Shokin Square, 1, Zelenograd, Moscow, 124498, Russia
[1]e-mail: aplugatarev@bk.ru, https://orcid.org/0000-0002-8549-4382
[2]e-mail: proxy33@mail.ru, https://orcid.org/0000-0002-3575-924X
[3]e-mail: bygorbtc2013@gmail.com, https://orcid.org/0000-0003-1788-0211
[4]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[5]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

The neural networks application for information security systems

DOI: http://dx.doi.org/10.26583/bit.2021.3.06

Abstract. In order to minimize the damage caused by cyberattacks, most organizations are using the network monitoring systems for its infrastructures. Such infrastructures collect a huge amount of information from security system logs event management systems. By structuring this data and analyzing it with the help of neural networks, the current study sets autonomous detection of malware hosts in a network as a goal. Automatization of this process will allow to detect malware computer hosts more precisely and promptly than experts do. It increases fault tolerance of the information system of a department. In order to design a decision-making system a restricted Boltzmann machine is used, while in the present study a stochastic neural network model determining probability distribution at the input data samples was used. Efficiency of the proposed model is investigated with the help of AUC indicator. This is a numeric characteristic of the error curve, which is an area, limited by a ROC-curve and the axis. The axis defines a share of false positive results which are the probabilities correctly defined by the classifier as safe hosts.The proposed model with the usage of neural networks provides monitoring and detection of malware computer hosts in information systems in real-time. This architecture significantly increases analysis efficiency and improves risk detection in an information environment with the help of data analysis or various internal systems and services. Development of this concept allows for involving a bigger amount of data from corporate networks and adding extra functions for improvement of vulnerabilities detection accuracy and reduction of the number of false alarms.

Keywords: machine learning system; detection of a malicious host; information security systems
For citation: PLUGATAREV, Alexey V. et al. The neural networks application for information security systems. IT Security (Russia), [S.l.], v. 28, n. 3, p. 73–80, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1364. DOI: http://dx.doi.org/10.26583/bit.2021.3.06.

Введение

В эпоху развитых сетевых технологий для обеспечения информационной защиты предприятиям, как правило, приходится выстраивать систему информационной безопасности, которая занимается оценкой рисков и анализов данных всей сетевой инфраструктуры [1]. Данное исследование посвящено обнаружению опасных компьютеров-хостов внутри сетевой инфраструктуры, на основе анализа данных с помощью нейронных сетей. Аналитики в центре безопасности исследуют предупреждения, чтобы решить, являются ли связанные хосты злонамеренными или нет. Однако, количество предупреждений и событий, как правило, огромно, и превышает возможности аналитиков по обработке информации, а ложное срабатывание может повлечь за собой потраченные впустую ресурсы. Следовательно, существует потребность в максимальном уменьшении количества ложных срабатываний. Данное исследование сосредоточено на обнаружении взломанных хостов в информационных системах интеллектуальной системой с использованием глубокого машинного обучения [2].

Основополагающий принцип классических систем управления событиями безопасности состоит в том, что данные о безопасности информационной системы собираются из разных источников, и результат их обработки предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что помогает изучать характерные особенности, которые соответствуют инцидентам информационной безопасности [3]. Построение таких систем опирается на анализ существующих данных, стараясь улучшить долгосрочную эффективность системы и оптимизировать хранение информационных данных, а также делается акцент на выгрузке из имеющихся данных определенного объема информации, с помощью которого могут быть немедленно выявлены уязвимости [4].

Система, спроектированная по предлагаемому алгоритму, способна самостоятельно анализировать информационные оповещения, журналы безопасности и информацию

аналитиков; готова к интеграции с реальной корпоративной средой для определения хостов с высокой вероятностью компрометации в реальном времени.

1. Материалы и методы

Основное преимущество глубокого машинного обучения перед другими моделями машинного обучения состоит в том, что для анализа используются, как правило, очень сложные линии поведения или особенности компьютера-хоста [5]. Например, хост может посещать разные вредоносные веб-сайты, скачивать/закачивать файлы или иметь различные поражения вредоносным программным обеспечением одновременно. Фактически, создаются сотни функций в день для описания состояния безопасности хоста [6, 7]. Таким образом, главное преимущество глубокого машинного обучения – это способность его послойной стратегии обучения, в которой функции более высокого уровня извлечены из предыдущих, то есть высокоуровневые функции лучше извлекают информацию из входных данных [8, 9].

Ограниченная машина Больцмана – двухслойная стохастическая модель, которая включает скрытый слой и видимый слой. Видимый слой состоит из видимых состояний $V = (v_1, \ldots, v_m)$, а скрытый слой имеет состояния $H = (h_1, \ldots, h_n)$, которые нельзя измерить напрямую. Между двумя уровнями состояния полностью связные. Однако нет никакой связи между состояниями в одном слое, что означает, что состояния в одном слое взаимно независимы.

В рамках данной структуры рассмотрим обучающий набор двоичных векторов, которые будем считать двоичными изображениями для аутентификации хостов. Совместная конфигурация в данной модели состоит из видимых и скрытых единиц (v, h), которые обладают энергией, определяемой:

$$E(v,h) = -\sum_i a_i v_i - \sum_j b_j h_j - \sum_i \sum_j v_i w_{i,j} h_j, \quad (1)$$

где v_i, h_j – двоичные состояния видимой единицы i и скрытой единицы j; a_i, b_j – их смещения, а $w_{i,j}$ – вес между ними. Сеть присваивает вероятность каждой возможной паре видимого и скрытого векторов через энергетическую функцию:

$$P(v,h) = \frac{1}{Z} e^{-E(v,h)}, \quad (2)$$

где «статистическая сумма» Z определяется суммированием всех возможных пар видимых и скрытых векторов:

$$Z = \sum_{v,h} e^{-E(v,h)}. \quad (3)$$

Вероятность того, что сеть присваивает доверительное значение видимому вектору v, определяется суммированием всех возможных скрытых векторов:

$$p(v) = \frac{1}{Z} \sum_{v,h} e^{-E(v,h)}, \quad (4)$$

где Z – константа нормализации, которая гарантирует, что сумма всех вероятностей равна единице.

Предложенная сеть глубокого обучения – это вероятностная генеративная модель. Как показано на рис. 1, сеть глубокого обучения в первую очередь построена путем интегрирования ограниченных машин Больцмана и классификатора (верхний слой).

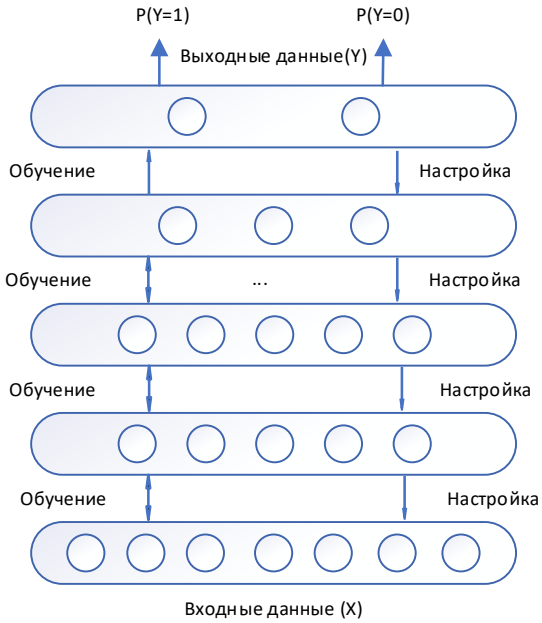


Рис. 1. Структура глубокого машинного обучения
Fig. 1. Structure of Deep Belief Network

Структура обучения имеет две части: объединённые ограниченные машины Больцмана и классификатор (верхний слой). Тренировочный процесс для данной сети включает предварительное обучение и настройку соответственно.

Необработанные данные собираются из журналов служб внутренней безопасности. Данные состоят из предупреждений от систем интеллектуальной защиты, заметок аналитики и журналов из разных источников, включая межсетевой экран, систему обнаружения/предотвращения вторжений, HTTP/FTP/DNS–трафики, DHCP, сканирование уязвимостей, событий безопасности Windows, VPN и т.д. В журналах появляются терабайты данных каждый день. В табл. 1 перечислены данные оповещений ключевых элементов системы интеллектуальной защиты:

Таблица 1. Пример входных данных

ID хоста	Результаты 1 категории	Индикатор 2 категории	Показатель 3 категории	Показатель 4 категории	Метка
Хост1	13	1	0,65	5,17	1 (рискованный)
Хост2	25	0	2,74	9,34	1 (рискованный)
Хост3	4	0	1,33	3,52	0 (нормальный)

Аналитические функции создаются на уровне отдельного хоста, так как основная цель – спрогнозировать риск хоста [10]. Характеристики, которые в данном исследовании выделены для анализа, можно классифицировать в следующие четыре категории:

1) Сводные характеристики: эти функции могут быть сгенерированы из статистических сводок. Например, число событий «Вредоносное ПО: не исправлено» за последние 24 часа, или количество событий высокой важности (с определённой степенью серьёзности) за последние 7 дней.

2) Характеристики индикатора: эти функции представлены в двоичном формате (0 – событие ложно, 1 – событие верно), например, «Вредоносное ПО: не исправлено – ложно»; «событие происходит в выходные дни – верно».

3) Временные особенности: эти события включают временную информацию, например, частота появления оповещения системы безопасности, которая учитывает временной интервал между двумя последовательными событиями.

4) Реляционные функции: эти функции получены из анализа событий, рассчитанные по графу хост-событие, где узлы – это хосты или события. Отношение между хостом и его событиями представлен ребром графа, а вес ребра – это количество определенных событий на хосте. На рис. 2. приведен пример подграфа на один конкретный хост с его событиями безопасности и некоторые взвешенные значения, полученные из более крупных графов с большим количеством хостов и событий. Более высокий показатель подразумевает более подозрительное поведение компьютера-хоста.

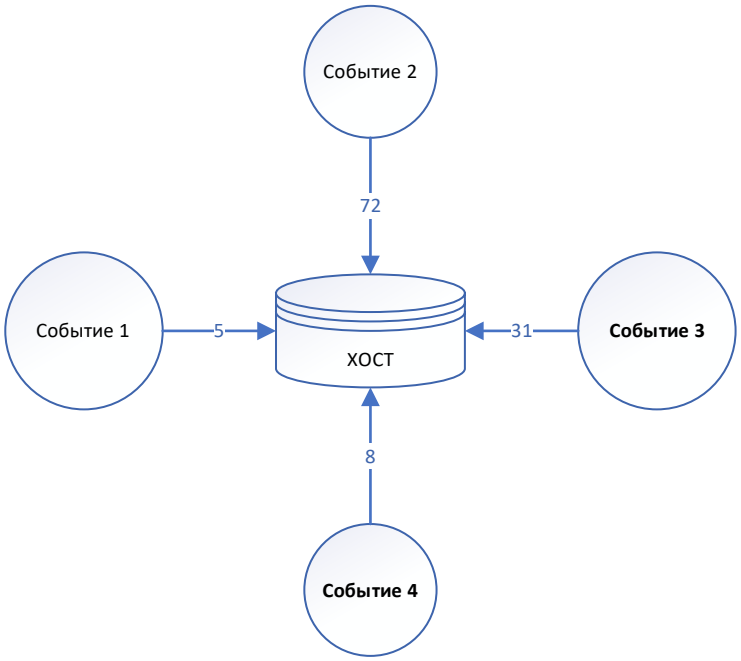


Рис. 2. Пример функции взвешенного рейтинга событий хоста
Fig. 2. Example of a weighted host event rating function

2. Результаты и их обсуждение

В рамках исследований было проведено математическое моделирование для поиска вредоносных хостов [11, 12]. В данных тестированиях были смоделированы 5100 хостов с данными, из которых 60 будем считать потенциально опасными. В данном исследовании будем тестировать разные модели машинного обучения, чтобы определить, могут ли они работать лучше, чем действующая система, основанная на правилах. Как правило, необходимо случайным образом разделить на данные с хостов (75% образцов для мониторинга) и тестовые (оставшиеся 25%). Были опробованы разные соотношения между целевыми выборками и тестами – 50% / 50%, 60% / 40% и 75% / 25%. При моделировании было получено, что коэффициенты разделения мало повлияли на классификацию полученных результатов [13].

Меры оценки определены в уравнениях (5) – (7).

Модель AUC – численная характеристика кривой ошибок – площадь, ограниченная ROC-кривой и осью, которая отделяет долю ложных положительных результатов – вероятностей, которые классификатор верно отнёс к безопасным хостам:

$$\approx \sum_i \frac{y_{i+1}+y_i}{2} \times (x_{i+1} - x_i), \quad (5)$$

где x – вероятность i-го успешного определения хоста к вредоносным или безопасным, а y – классификатор хостов, принимающий значения 0 – если хост был определён к вредоносным и 1 если к безопасным.

Модель оценки эффективности обнаружения вредоносных хостов, определяется как отношение прогнозируемых опасных хостов, к общему количеству опасных хостов в сети:

$$\frac{\text{Прогнозируемое количество опасных хостов}}{\text{Общее количество опасных хостов}} \times 100\%. \quad (6)$$

Мера производительности алгоритма рассчитывается как отношение доли прогнозируемых опасных хостов в сети к общей доле опасных хостов в сети:

$$\frac{\text{Доля прогнозируемых опаных хостов}}{\text{Общая доля опасных хостов}} \times 100\%. \quad (7)$$

На рис. 3 приведены результаты моделирования от количества скрытых нейронов N, при следующих параметрах: количество эпох для точной настройки – 100; четыре слоя с одним входным слоем, двумя скрытыми слоями и один выходной слой; в каждом слое 100, 20, 10, 2 нейрона соответственно.

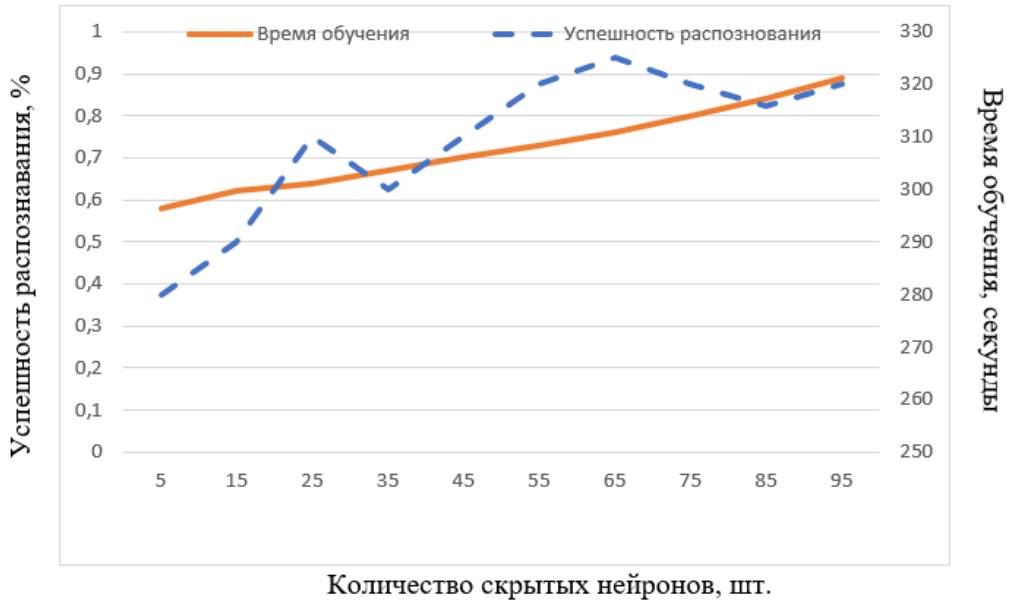


Рис. 3. Время обучения относительно количества скрытых нейронов
Fig. 3. Training time as function of the number of hidden neurons

Из рис. 3 видно, что время обучения модели увеличивается почти линейно с N, что означает, что модель имеет хорошую масштабируемость с большим количеством скрытых нейронов. С другой стороны, показатель AUC на тестовых данных увеличивается, когда $N<25$, и начинается уменьшаться после этого, затем наблюдаются тенденции к росту, однако тенденции нестабильны, что может означать, что обобщаемость нейронной сети снижается из-за слишком большого количества скрытых нейронов. В рамках исследования были проведены исследования с более сложной структурой и с большим количеством нейронов и слоев, но нет очевидного повышения производительности – время обучения продолжает расти линейно, а успешность распознавания колеблется 0,85 – 0,95 (тенденции к этому видны в диапазоне $N>85$). Поэтому, на графике представлен диапазон до 100 скрытых нейронов, который и представляет наибольший интерес. Оптимальным можно

назвать диапазон $60<N<70$, который даёт лучшее соотношение времени обучения и успешности распознавания.

Заключение

Описанный в статье подход, основан на нейросети с глубоким машинным обучением, которая использует данные журналов безопасности различных устройств в информационной системе, предупреждающую информацию и аналитические сведения для идентификации рискованных компьютеров-хостов. Разработанный алгоритм предназначен для работы с информацией из необработанных и неструктурированных массивов данных, чем и отличается от традиционных моделей систем управления событиями безопасности. Алгоритм реализован, таким образом, что готов для программной или аппаратной реализации и последующей интеграции в информационную инфраструктуру, также имеет возможность выявлять опасные хосты в режиме реального времени, обновляя данные, получая их из журналов систем безопасности. Программная реализация алгоритма позволит полностью автоматизировать процесс: от сбора данных, до обновления оценки в реальном времени, что значительно улучшает эффективность аналитики и повышает эффективность обнаружения рисков в информационной среде.

СПИСОК ЛИТЕРАТУРЫ:

1. Marukhlenko A.L., Plugatarev A.V., Bobyntsev D.O. Complex evaluation of information security of an object with the application of a mathematical model for calculation of risk indicators. Lecture Notes in Electrical Engineering. 2020. Vol. 641 LNEE. P. 771–778. DOI: https://doi.org/10.1007/978-3-030-39225-3_84.
2. A.L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications urveys & Tutorials. Vol. 18, no. 2. P. 1153–1176. DOI: https://doi.org/10.1109/COMST.2015.2494502.
3. M. Bhuyan, D. Bhattacharyya and J. Kalita. Network anomaly detection: Methods systems and tools. IEEE Commun. Surv. Tuts., vol. 16, no. 1. P. 303–336, 2014. DOI: http://dx.doi.org/10.1109/SURV.2013.052213.00046.
4. T.T.T. Nguyen and G. Armitage. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tuts., vol. 10, no. 4. P. 56–76, 2008 DOI: https://doi.org/10.1109/SURV.2008.080406.
5. D.Y. Yeung and Y. Ding. Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition. Vol. 36, Issua 1, 2003. P. 229–243. DOI: https://doi.org/10.1016/S0031-3203(02)00026-2.
6. B. Li, M.H. Gunes, G. Bebis and J. Springer. A supervised machine learning approach to classify host roles on line using sflow, Proceedings of the first edition workshop on High performance and programmable networking. Association for Computing Machinery, New York, NY, USA, 2013. P. 53–60. DOI: https://doi.org/10.1145/2465839.2465847.
7. Kuleshova E., Marukhlenko A., Dobritsa V., Tanygin M. Formation of Unique Characteristics of Hiding and Encoding of Data Blocks Based on the Fragmented Identifier of Information Processed by Cellular Automata. Computers 9(2), 51 (2020). DOI: https://doi.org/10.3390/computers9020051.
8. Марухленко А.Л., Плугатарев А.В., Таныгин М.О. Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации и др. Известия Юго-Западного государственного университета. 2020. Т. 24. № 2. С. 108–121. DOI: https://doi.org/10.21869/2223-1560-2020-24-2-108-121.
9. A. Fischer and C. Igel. Training restricted Boltzmann machines: An introduction, Pattern Recognition. 2014. Vol. 47, Issue 1. P. 25–39. DOI: https://doi.org/10.1016/j.patcog.2013.05.025.
10. M. Kang and J. Kang. A novel intrusion detection method using deep neural network for in-vehicle network security, 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). P. 1–5. DOI: https://doi.org/10.1109/VTCSpring.2016.7504089.
11. Center for Strategic and International Studies (CSIS) and McAfee. Economic Impact of Cybercrime Slowing Down Report. URL: https://www.csis.org/analysis/economic-impact-cybercrime (дата обращения: 02.04.2021).
12. Deep Learning 0.1 documentation: Deep Belief Networks. URL: https://deep-learning-tensorflow.readthedocs.io/en/latest/ (дата обращения: 03.04.2021).

13. A. Fischer and C. Igel. Training restricted Boltzmann machines: An introduction, Pattern Recognition. 2014. Vol. 47, Issue 1. P. 25–39. DOI: https://doi.org/10.1016/j.patcog.2013.05.025.

REFERENCES:

[1] Marukhlenko A.L., Plugatarev A.V., Bobyntsev D.O. Complex evaluation of information security of an object with the application of a mathematical model for calculation of risk indicators. Lecture Notes in Electrical Engineering. 2020. Vol. 641 LNEE. P. 771–778. DOI: https://doi.org/10.1007/978-3-030-39225-3_84.
[2] A.L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications urveys & Tutorials. Vol. 18, no. 2. P. 1153–1176. DOI: https://doi.org/10.1109/COMST.2015.2494502.
[3] M. Bhuyan, D. Bhattacharyya and J. Kalita. Network anomaly detection: Methods systems and tools. IEEE Commun. Surv. Tuts., vol. 16, no. 1. P. 303–336, 2014. DOI: http://dx.doi.org/10.1109/SURV.2013.052213.00046.
[4] T.T.T. Nguyen and G. Armitage. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tuts., vol. 10, no. 4. P. 56–76, 2008. DOI: https://doi.org/10.1109/SURV.2008.080406.
[5] D.Y. Yeung and Y. Ding. Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition. Vol. 36, Issua 1, 2003. P. 229–243. DOI: https://doi.org/10.1016/S0031-3203(02)00026-2.
[6] B. Li, M.H. Gunes, G. Bebis and J. Springer. A supervised machine learning approach to classify host roles on line using sflow, Proceedings of the first edition workshop on High performance and programmable networking. Association for Computing Machinery, New York, NY, USA, 2013. P. 53–60. DOI: https://doi.org/10.1145/2465839.2465847.
[7] Kuleshova E., Marukhlenko A., Dobritsa V., Tanygin M. Formation of Unique Characteristics of Hiding and Encoding of Data Blocks Based on the Fragmented Identifier of Information Processed by Cellular Automata. Computers 9(2), 51 (2020). DOI: https://doi.org/10.3390/computers9020051.
[8] Marukhlenko A.L., Plugatarev A.V., Tanygin M.O., Marukhlenko L.O., Shashkov M.Yu. Option of Control of Access to Information Resources Based on Implicit Authentication. Proceedings of the Southwest State University. 2020.Vol. 24. No. 2. P. 108–121. DOI: https://doi.org/10.21869/2223-1560-2020-24-2-108-121 (in Russian).
[9] A. Fischer and C. Igel. Training restricted Boltzmann machines: An introduction, Pattern Recognition. 2014. Vol. 47, Issue 1. P. 25–39. DOI: https://doi.org/10.1016/j.patcog.2013.05.025.
[10] M. Kang and J. Kang. A novel intrusion detection method using deep neural network for in-vehicle network security, 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). P. 1–5. DOI: https://doi.org/10.1109/VTCSpring.2016.7504089.
[11] Center for Strategic and International Studies (CSIS) and McAfee. Economic Impact of Cybercrime – No Slowing Down Report. URL: https://www.csis.org/analysis/economic-impact-cybercrime (accessed: 02.04.2021).
[12] Deep Learning 0.1 documentation: Deep Belief Networks. URL: https://deep-learning-tensorflow.readthedocs.io/en/latest/ (accessed: 03.04.2021).
[13] A. Fischer and C. Igel. Training restricted Boltzmann machines: An introduction, Pattern Recognition. 2014. Vol. 47, Issue 1. P. 25–39. DOI: https://doi.org/10.1016/j.patcog.2013.05.025.

Поступила в редакцию – 28 апреля 2021 г. Окончательный вариант – 20 августа 2021 г.
Received – April 28, 2021. The final version –August 20, 2021.

Александр П. Мартынов[1], Дмитрий Б. Николаев[2], Кирилл Д. Ермаков[3]
СарФТИ Национального исследовательского ядерного университета «МИФИ»,
ул. Духова, 6, Саров, Нижегородская обл., 607184, Россия
[1]e-mail: dim010307@yandex.ru, http://orcid.org/0000-0002-8985-615X
[2]e-mail: dim010307@yandex.ru, http://orcid.org/0000-0003-4618-1022
[3]e-mail: ermakov-kir@mail.ru, http://orcid.org/0000-0002-3723-7111

РЕАЛИЗАЦИЯ НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ПОДСТАНОВКИ В ВИДЕ ЭЛЕМЕНТОВ СИСТЕМЫ СЧИСЛЕНИЯ РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

DOI: http://dx.doi.org/10.26583/bit.2021.3.07

Аннотация. В работе исследуется нелинейное преобразование подстановки, представленное как элемент системы счисления факториальных множеств. Данное представление учитывает характерные особенности подстановок и позволяет минимизировать объем памяти для их хранения. На основе подхода однозначной нумерации подстановок рассмотрено три способа их хранения в памяти: в виде вектора, в виде значений циклических сдвигов элементов тождественной подстановки и в виде десятичного номера подстановки. Приведены результаты анализа объема данных, необходимого для хранения нелинейного преобразования подстановки для криптографических примитивов и определена трудоемкость перевода преобразованных подстановок в стандартный вид хранения вектором. Полученные результаты могут быть применены в программных решениях для обеспечения информационной безопасности с использованием криптографических примитивов, содержащих нелинейное преобразование подстановки. Предложенный подход к записи в виде преобразования подстановок рекомендуется для реализации в комплексах с ограниченным объемом памяти.

Ключевые слова: криптографические примитивы, нелинейное преобразование подстановки, система счисления ряда факториальных множеств.

Для цитирования: МАРТЫНОВ, Александр П.; НИКОЛАЕВ, Дмитрий Б.; ЕРМАКОВ, Кирилл Д. РЕАЛИЗАЦИЯ НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ПОДСТАНОВКИ В ВИДЕ ЭЛЕМЕНТОВ СИСТЕМЫ СЧИСЛЕНИЯ РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 81–91, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1365. DOI: http://dx.doi.org/10.26583/bit.2021.3.07.

Alexander P. Martynov[1], Dmitry B. Nikolaev[2], Kirill D. Ermakov[3]
SarFTI of National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Dukhova Str., 6, Sarov, Nizhny Novgorod Region, 607184, Russia
[1]e-mail: dim010307@yandex.ru, http://orcid.org/0000-0002-8985-615X
[2]e-mail: dim010307@yandex.ru, http://orcid.org/0000-0003-4618-1022
[3]e-mail: ermakov-kir@mail.ru, http://orcid.org/0000-0002-3723-7111

Implementation of a nonlinear transformation of a substitution in the form of elements of a numbering system of a number of factorial sets

DOI: http://dx.doi.org/10.26583/bit.2021.3.07

Abstract. The paper investigates a nonlinear substitution transformation, presented as an element of the number system of factorial sets. This approach takes into account the characteristic features of substitutions and al-lows you to minimize the amount of memory for storing. Based on the unambiguous numbering approach for substitutions, three methods of storing in memory are considered: in the form of a vector, in the form of values of cyclic shifts of elements of an identical substitution, and in the form of a decimal substitution number. The results of the analysis of the amount of data required for storing the nonlinear substitution transformation for cryptographic primitives are presented. The complexity of translating the transformed substitutions into the standard form of storage by a vector is determined. The obtained results can be ap-plied in software solutions for ensuring information security using cryptographic primitives

containing a nonlinear substitution transformation. The proposed approach to writing in the form of substitution trans-formations is recommended for implementation in complexes with a limited amount of memory.

Keywords: cryptographic primitives, nonlinear substitution transformation, number system of a number of factorial sets.

For citation: MARTYNOV, Alexander P.; NIKOLAEV, Dmitry B.; ERMAKOV, Kirill D. Implementation of a nonlinear transformation of a substitution in the form of elements of a numbering system of a number of factorial sets. IT Security (Russia), [S.l.], v. 28, n. 3, p. 81–91, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1365. DOI: http://dx.doi.org/10.26583/bit.2021.3.07.

Введение

В настоящее время актуальной и важной проблемой является обеспечение информационной безопасности данных. Одним из решений данной проблемы является использование криптографических протоколов и примитивов. В качестве одного из таких примитивов можно выделить блочные алгоритмы шифрования с секретным ключом, которые широко применяются для обеспечения конфиденциальности данных.

Алгоритмы блочного шифрования могут строиться при помощи различных структур, таких как SP-сети, сети Фейстеля, схемы Лая-Мэсси и др., однако все данные подходы состоят из различных преобразований, часто схожих друг с другом [1–3]. Все данные преобразования можно рассматривать как линейные и нелинейные преобразования. Стоит отметить, что при криптоанализе алгоритмов шифрования, стойкость алгоритму обеспечивает в основном использование нелинейных преобразований (если бы алгоритм шифрования состоял только из линейных преобразований, он бы тривиально взламывался противником) [4–6].

Одним из самых популярных видов нелинейных преобразований, используемых в алгоритмах, являются блоки подстановок (S-блоки). Блок подстановки является преобразованием, которое принимает на вход двоичный набор некоторой длины и преобразует его в другой двоичный набор. При исследовании данного преобразования анализируются не только его свойства [7–9], но и применимость в алгоритмах [10, 11]. При программной реализации такого преобразования в памяти обычно хранят вектор, где под индексом входного набора в векторе хранится значение выходного набора. При этом функциональная гибкость устройства преобразования будет зависеть от возможности вариативного изменения значений выходного набора [12, 13]. Следует отметить, что количество перестановок определяется факториалом, и при возрастании размерности выходного вектора количество возможных комбинаций существенно увеличивается [14] и это при условии статичности применяемых S-блоков. В случае применения управляемых блоков [15] объем хранимой информации является ключевым параметром при аппаратной или программной реализации алгоритма, а процесс оценки и, при необходимости, оптимизации данной информации при хранении носит, несомненно, актуальный характер. Ключевым аспектом работы является переход от традиционных подходов представления данных к представлению через формы [16, 17], учитывающие особенности множеств, формируемых из используемых выходных наборов – представление в факториальной системе счисления.

В [18] дано понятие факториального множества, введена система счисления факториальных множеств, а также предложен способ перевода чисел из десятичной системы счисления в систему счисления факториальных множеств и обратно. Кроме того приведен способ однозначной нумерации подстановок, который позволяет представить подстановки при помощи десятичного числа или элемента системы счисления факториальных множеств.

Однако при описании данных подходов не была проведена оценка объемов памяти для хранения параметров нелинейных преобразований в существующих криптографических алгоритмах.

1. Факториальное множество

Для понятия системы счисления ряда факториальных множеств рассмотрим основополагающие понятия.

Факториал $n!$ – это произведение натуральных чисел от 1 до числа n. Множество натуральных чисел $\{1, 2, 3, \dots, n\}$ называется множеством образующих элементов функции факториала.

Факториальное множество Φ_n – множество перестановок из n чисел, мощность которого $P(\Phi_n)$ равняется значению факториала образующих элементов множества $(n!)$. Ряд факториальных множеств представлен на рис. 1.

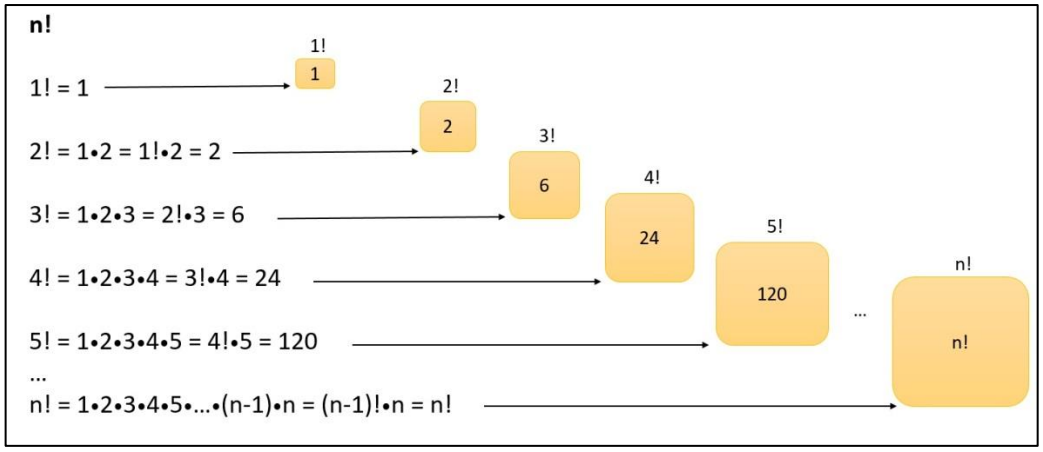


Рис. 1. Представление ряда факториальных множеств
Fig. 1. Representation of a number of factorial sets

Элементом факториального множества Φ_n является перестановка его образующих элементов $\{1, 2, 3, \dots, n\}$. Так как элементы множества Φ_n мощностью $P(\Phi_n) = n!$ можно переставить $n!$ способами, любое преобразование подстановки можно удобно представить как элемент множества Φ_n.

Авторы в [19] представили упорядоченную систему счисления, установив однозначное соответствие между конкретной перестановкой n элементов и ее эквивалентом в системе счисления факториальных множеств.

Как показано на рис. 1, каждое факториальное множество Φ_n содержит в себе n подмножеств Φ_{n-1} меньшей на единицу мощности. На данном факте строится идея формирования позиционной системы счисления ряда факториальных множеств. Этапы формирования позиционной системы счисления [18, 19] описываются следующим образом:

1. Факториальные множества Φ_n раскладываются на подмножества, количество которых равно числу образующих элементов или же номеру факториального множества.

2. Данные подмножества также циклически раскладываются на меньшие по мощности множества, вплоть до множества подстановок, состоящего из одного элемента (Φ_1).

3. Полученные составляющие элементы ряда факториальных множеств записываются в общем виде в соответствии с их позициями.

4. Позиционным коэффициентам $a_1, \dots, a_n$ системы счисления факториальных множеств обозначают соответствующие им множества.

Нулем в данной системе счисления обозначается тот факт, что перестановки образующих элементов множества нет. Этапы формирования системы счисления ряда факториальных множеств на примере первых пяти множеств представлены на рис. 2.

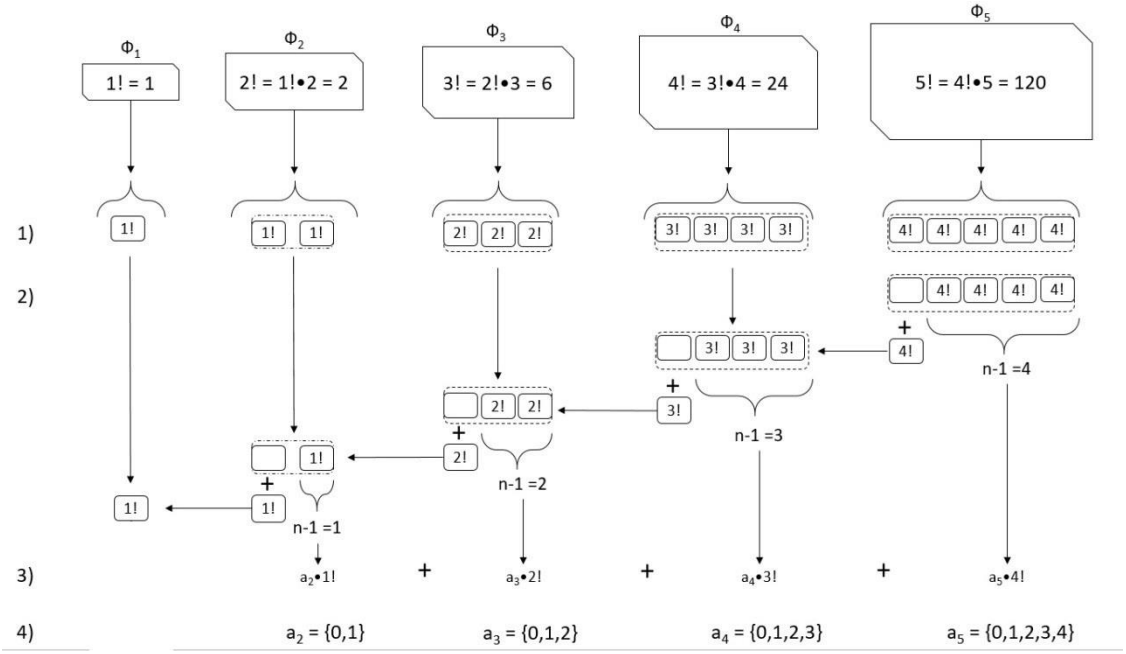


Рис. 2. Формирование системы счисления ряда факториальных множеств
Fig. 2. Formation of the number system of a number of factorial sets

Полученную систему счисления можно представить выражением:

$$X = a_{(n-1)}(n-1)! + \cdots + a_3 2! + a_2 1!,$$

где a_i – позиционные коэффициенты. Значение данных коэффициентов зависит от конкретно взятого факториального множества. В данной системе счисления вместо традиционного основания системы счисления q в степени $\{1, \dots, n-1\}$ используются мощности $P(\Phi_i)$ последовательно следующих факториальных множеств.

2. Преобразование чисел из десятичной системы счисления в систему счисления ряда факториальных множеств и наоборот

В [19] представлен алгоритм перевода чисел из различных систем счисления по отношению к системе счисления ряда факториальных множеств. Стоит отметить, что данный способ перевода чисел является оригинальным и разработан авторами статьи. Далее будет представлен метод перевода чисел в данных системах счисления.

Как известно, любой элемент, входящий в факториальное множество, можно представить в виде количества целых частей предыдущего множества и некоего остатка от деления:

$$\frac{X}{(n-1)} = \mathrm{c} + b,$$

где X – делимое, c – целая часть от деления, b – остаток.

Для перевода элементов множеств из системы с основанием 10 в систему счисления факториальных множеств используется описанный выше метод деления, в котором происходит последовательное деление на значение мощности предыдущих факториальных множеств. Любое десятичное число от 0 до $n! - 1$ можно представить элементом факториального множества Φ_n.

Пример. Допустим необходимо перевести десятичное число 100 в систему счисления факториальных множеств. Данное число является элементом Φ_5, так как в нем содержится менее $5! = 120$ подстановок. Первым делением является деление на мощность $P(\Phi_{n-1})$ предыдущего факториального множества Φ_4, равную 24. Далее полученные остатки b от деления делятся на последующие меньшие значения мощностей вплоть до множества Φ_2:

$$100 = 24 \cdot 4 + 4;$$
$$4 = 6 \cdot 0 + 4;$$
$$4 = 2 \cdot 2 + 0.$$

Таким образом, после перевода десятичное число в системе факториальных множеств будет представлено в виде целых частей от деления и последнего остатка, и иметь следующий вид:

$$100 \to 4\ 0\ 2\ 0$$

Перевод чисел из системы счисления факториальных множеств в десятичную систему счисления происходит при помощи суммирования произведений позиционных коэффициентов элемента множества на мощности факториальных подмножеств. Ниже приведены примеры перевода в десятичную систему счисления:

$$1111 = 1 \cdot 24 + 1 \cdot 6 + 1 \cdot 2 + 1 \cdot 1 = 33_{10};$$
$$4321 = 4 \cdot 24 + 3 \cdot 6 + 2 \cdot 2 + 1 \cdot 1 = 119_{10};$$
$$2210 = 2 \cdot 24 + 2 \cdot 6 + 1 \cdot 2 + 0 \cdot 1 = 62_{10};$$
$$301 = 3 \cdot 6 + 0 \cdot 2 + 1 \cdot 1 = 19_{10};$$
$$34321 = 3 \cdot 120 + 4 \cdot 24 + 3 \cdot 6 + 2 \cdot 2 + 1 \cdot 1 = 479_{10}.$$

3. Использование подстановок как элементов системы счисления факториальных множеств

Подстановка – однозначное отображение элементов некоторого множества на себя. Так как любая подстановка может быть получена при помощи некоторого числа сдвигов элементов тождественной подстановки, в [19] предложено рассмотреть подстановку как элемент системы счисления факториальных множеств. Однако в данном подходе операция сдвига отдельных элементов заменена операцией сдвига всех элементов конкретного факториального множества.

Каждой подстановке определяется ее образ, который соответствует числу сдвигов для каждого факториального множества. То есть, в данном подходе значение позиционных коэффициентов элемента множества обозначает конкретное значение циклического сдвига вправо элементов подстановки. Последовательность циклических сдвигов для множества Φ_n равна

$$\Phi_n \to \Phi_{n-1} \to \cdots \to \Phi_2.$$

Это значит, что сначала циклически сдвигаются на некоторое значение все n элементов подстановки, затем первые $n - 1$ элементов подстановки, вплоть до первых двух элементов подстановки (сдвиг одного элемента смысла не имеет).

Рассмотрим пример. Возьмем элемент факториального множества Φ_5, данный элемент соответствует подстановке на множестве {1, 2, 3, 4, 5}. Пусть элемент множества

может быть представлен как $\Phi_5 = 4, \Phi_4 = 0, \Phi_3 = 2, \Phi_2 = 1$. Тогда данные значения сдвигов воздействуют на подстановку следующим образом:

$$12345 \to 23451 \to 23451 \to 34251 \to 43251.$$

Имея переход элементов счисления факториального множества в конкретные подстановки при помощи операции циклического сдвига частей тождественной подстановки, можно осуществлять перевод чисел из десятичной системы счисления в подстановки и наоборот. Для того, чтобы перевести число от 0 до $n! - 1$ при некотором фиксированном n, операции циклического сдвига будут осуществляться на подстановках с числом элементов, равном n. Графически перевод десятичного числа на примере числа 78 в подстановку и получение значений циклических сдвигов представлено на рис. 3.

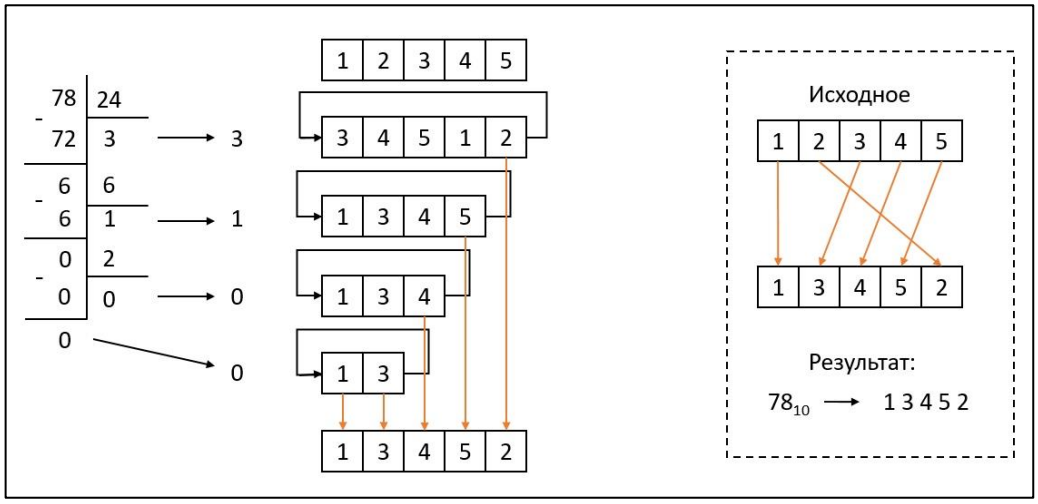


Рис. 3. Перевод десятичного числа 78 в подстановку
Fig. 3. Converting Decimal number 78 to Substitution

Как видно из рис. 3, пять элементов подстановки циклически сдвигаются вправо на 3 (частное от деления на 24), затем первые четыре элемента циклически сдвигаются на 1, далее первые три элемента сдвигаются на 0 и два элемента сдвигаются на 0. Циклический сдвиг одного элемента смысла не имеет.

Таким образом, можно сделать вывод, что описанные выше методы и подходы к представлению подстановок могут быть применены как в уже существующих, так и в разрабатываемых криптографических алгоритмах, так как нелинейное преобразование подстановки используется почти во всех криптографических примитивах с секретным ключом. Однако для использования такого вида записи необходимо оценить, эффективна ли запись подстановок в таком виде при программной реализации алгоритмов.

4. Оценка емкости памяти для хранения подстановки стандартным способом

При программной реализации криптографических примитивов нелинейное преобразование биективной подстановки размером $n \times n$ бит обычно реализуется при помощи хранения вектора данных. Данный вектор занимает объем данных, равный

$$n \cdot 2^n \text{ бит},$$

так как в векторе содержится 2^n элементов, каждый из которых занимает n бит В табл. 1 приведены объемы памяти, требуемые для хранения подстановок размерности n в виде вектора.

5. Оценка емкости памяти для хранения подстановки в системе счисления ряда факториальных множеств

При использовании подхода, основанного на системе счисления ряда факториальных множеств, каждую подстановку из 2^n элементов можно однозначно представить в виде десятичного числа от 0 до $2^n! - 1$ (так как у множества из 2^n элементов может существовать $2^n!$ биективных отображений на себя). При хранении в памяти номера подстановки, вместо ее самой, необходимо выделение такого числа бит, которое способно представлять число до $2^n!$. В табл. 1 приведено количество бит необходимое для хранения номера подстановки. Как видно из табл. 1, хранение номера подстановки, вместо ее самой, дает существенное уменьшение требуемой памяти. Например, при хранении подстановки из 16 элементов экономится примерно 30% занимаемой памяти.

Также существует еще один способ уменьшения объема памяти требуемой для хранения подстановки. Так как при переводе номера подстановки в саму подстановку при помощи операции деления вычисляются значения сдвигов, которые впоследствии последовательно воздействуют на тождественную подстановку, в памяти можно хранить не номер подстановки, а значения используемых в ее генерации сдвигов. В данном случае экономится меньший объем памяти, однако операция деления для получения сдвигов будет совершаться заранее, тем самым вычисление подстановки менее трудозатратно при выполнении алгоритма криптографического примитива.

Для подстановки, состоящей из 2^n элементов, при помощи операции деления генерируется $2^n - 1$ значений сдвигов, причем диапазон значений отличается для каждого сдвига. Например, для хранения подстановки из 16 элементов необходимо 15 сдвигов, где первый принимает значения от 0 до 15, второй от 0 до 14 и так далее. Для данного способа объем памяти, необходимый для хранения значений циклических сдвигов для n разрядной подстановки, можно определить так:

$$\sum_{i=1}^{n} i \cdot 2^{i-1} \text{ бит.}$$

В табл. 1 приведено количество бит необходимое для хранения подстановок при помощи значений циклических сдвигов.

Таблица 1. Объем памяти для хранения подстановки

Размерность подстановки, n бит	Объем памяти, бит		
	Стандартный подход	Номер подстановки	Циклический сдвиг
2	8	5	5
3	24	16	17
4	64	45	49
5	160	117	129
6	384	298	321
7	896	716	769
8	2048	1684	1793
9	4608	3876	4097
10	10240	8770	9217

Как видно из табл. 1, способ хранения значений циклических сдвигов требует большего объема памяти, например, для 4-х битной подстановки необходимо на 6% больше памяти. Однако данный способ дает существенный прирост в производительности, так как вычисление значений сдвигов будет осуществляться до начала работы алгоритма,

использующего подстановку. Зависимости требуемого объема памяти для трех способов задания нумерации подстановок приведены на рис. 4. Как видно из рис. 4 объем памяти растет экспоненциально при увеличении размерности n подстановки. При этом хранение номера подстановки требует меньшего объема памяти. Стоит отметить, что так как рост функции факториала происходит быстрее степенной функции, то при больших значениях n хранение подстановок в виде элементов факториальной системы счисления будет менее эффективным, чем стандартный подход. Однако так как на данный момент основными используемыми подстановками являются преобразования размерностями 4 и 8 бит, предложенный метод хранения может использоваться в существующих алгоритмах.

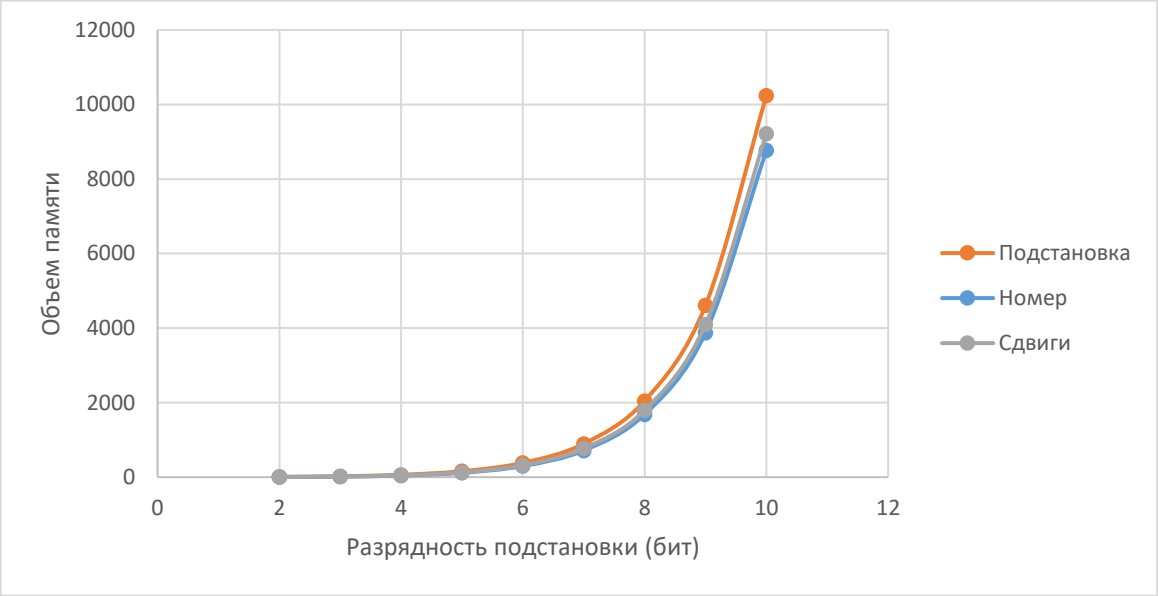


Рис. 4. Зависимость объема памяти от разрядности подстановки
Fig. 4. Dependence of the amount of memory on the substitution digit capacity

При хранении номера подстановки трудоемкость ее развертывания в подстановку заключается в нахождении значений циклических сдвигов тождественной подстановки при помощи последовательного деления ее номера на значения факториалов. Число операций деления для n битной подстановки равно $2^n - 1$. После получения значений сдвигов они циклически воздействуют на тождественную подстановку. Трудоемкость получения подстановки при помощи сдвигов для n битной размерности можно определить так:

$$2^n \cdot \sum_{i=2}^{n} i \quad \text{битовых операций.}$$

Заключение

В данной статье преобразование подстановки рассмотрено как элемент системы счисления ряда факториальных множеств. Проведен анализ трех способов хранения нумерации подстановок в памяти: в виде вектора (стандартный метод), в виде значений циклических сдвигов элементов тождественной подстановки и в виде десятичного номера подстановки. Проведена оценка объема памяти, требуемого для хранения подстановки каждым способом. При больших значениях размерности подстановки, хранение стандартным подходом будет более эффективным.

Использование предлагаемых способов дает возможность затрачивать меньший объем памяти для хранения подстановок малой размерности, однако требует использования дополнительных вычислительных ресурсов для определения номера подстановки или значений циклических сдвигов. Благодаря введению в криптопримитивы дополнительных операций по вычислению подстановки, сложность алгоритма будет возрастать, что приведет к замедлению к скорости работы примитива. Это может показаться отрицательным фактором, однако такой подход можно использовать для замедления таких примитивов как криптографические хеш-функции для улучшения стойкости к словарным атакам и другим атакам, основанным на большом переборе входных значений.

Данные подходы к хранению подстановок целесообразно использовать в малоресурсных программно-аппаратных комплексах, ограниченных в объемах используемой памяти.

Предложенные способы нумерации подстановок могут быть применены в криптографических блочных алгоритмах шифрования, в которых частью секретного ключа являются подстановки, использующиеся на каждом раунде. Применение данных способов позволит увеличить длину секретной информации, а также увеличит стойкость алгоритма к дифференциальным и линейным методам криптоанализа, так как алгоритм основывается на незнании противником используемых в конкретном шифровании подстановок, увеличив тем самым область возможного перебора.

СПИСОК ЛИТЕРАТУРЫ:

1. Гнуда В.Д. Структурный анализ преобразования типа «подстановка» / В.Д. Гнуда, В.Т. Карасев, Р.Ж. Тополян // СПбНТОРЭС: труды ежегодной НТК. 2019. № 1 (74). С. 102–103. URL: https://www.elibrary.ru/item.asp?id=39133391 (дата обращения: 01.02.2021).
2. Буров Д.А., Погорелов Б.А. Рассеивающие свойства линейных преобразований с точки зрения теории групп подстановок // Математические вопросы криптографии. 2018. Т. 9. № 2. С. 47–58. DOI: https://doi.org/10.4213/mvk252.
3. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Современные методы обеспечения безопасности информации в атомной энергетике: Монография / Под ред. А.И. Асайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014. – 636 с. DOI: http://dx.doi.org/10.53403/9785951502650.
4. Борисенко Н.П. Построение «лёгких» шифров с использованием подстановок с тривиальной группой инерции по отношению к аффинным преобразованиям // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции. В 4 т., Санкт-Петербург, 27–28 февраля 2019 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019. С. 154–159. URL: https://www.elibrary.ru/item.asp?id=41383511 (дата обращения: 01.02.2021).
5. Мартынов А.П., Фомченко В.Н. Криптография и электроника / Под редакцией А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2006. – 452 с.
6. Пичкур А.Б. Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек // Математические вопросы криптографии. 2012. Т. 3. № 2. С. 79–95. URL: https://www.elibrary.ru/item.asp?id=18024011(дата обращения: 01.02.2021).
7. Мартынова И.А., Сплюхин Д.В. Анализ основных характеристических свойств элементов рядов факториальных множеств в процессе защиты информационных систем // Наука. Мысль. 2017. № 5. С. 13–16. URL: https://www.elibrary.ru/item.asp?id=30742615 (дата обращения: 01.02.2021).
8. Sudoplatov S.V. Distributions of Countable Models of Disjoint Unions of Ehrenfeucht Theories. Lobachevskii J Math 42. 2021. P. 195–205. DOI: https://doi.org/10.1134/S1995080221010248.
9. Мартынова И.А., Мартынов А.П., Николаев Д.Б. Криптографические системы и метод факториального сжатия // Известия института инженерной физики. 2016, № 4 (42). С. 54–57. URL: https://www.elibrary.ru/item.asp?id=27697857 (дата обращения: 01.02.2021).
10. Lanini, M. Twisted quadratic foldings of root systems / M. Lanini, K.V. Zainoulline // Algebra and Analysis. 2021. Vol. 33. No. 1. P. 93–118. URL: https://arxiv.org/abs/1806.08962 (дата обращения: 01.02.2021).

11. Бабанов Н.Ю., Мартынов А.П., Николаев Д.Б., Фомченко В.Н., Новиков А.В. Виртуальная интерактивная система формирования и отработки управляющей информации. Вестник НГИЭИ. 2016. № 4 (59). С. 15–29. URL: https://www.elibrary.ru/item.asp?id=26083908 (дата обращения: 01.02.2021).
12. Зубей Е.В. О перестановочности силовских подгрупп с коммутантами *B*-подгрупп. Журнал Белорусского государственного университета. Математика. Информатика. 2019. № 1. С. 12–17. DOI: https://doi.org/10.33581/2520-6508-2019-1-12-17.
13. Dimitrov R.D., Harizanov V.S, Morozov A.S. Turing Degrees and Automorphism Groups of Substructure Lattices. Algebra Logic 59. P. 18–32 (2020). DOI: https://doi.org/10.1007/s10469-020-09576-x.
14. Аборнев А.В. Построение подстановок с использованием разрядно-подстановочных преобразований модуля над кольцом Галуа характеристики // Прикладная дискретная математика. 2014. № 1 (23). С. 9–19. URL: https://www.elibrary.ru/item.asp?id=21403880 (дата обращения: 01.02.2021).
15. Молдовян А.А. и др. Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002. – 496 с.
16. Мартынов А.П., Мартынова И.А. Функции перестановки в системе счисления ряда факториальных наборов // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2016, № 3. С. 21–22. URL: https://www.elibrary.ru/item.asp?id=27296781 (дата обращения: 01.02.2021).
17. Пчелинцев С.В. О тождествах первичных альтернативных алгебр. Алгебра и логика. 2020. Т. 59. № 2. С. 215–238. DOI: https://doi.org/10.33048/alglog.2020.59.204.
18. Мартынова И.А., Машин И.Г., Фомченко В.Н. Теория поля и защита информации: Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017. – 209 с.
19. Мартынов А.П., Мартынова И.А., Фомченко В.Н. Аксиоматические основы функции подстановки в системе счисления ряда факториальных множеств и их характеристики. Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2019. – 209 с.

REFERENCES:

[1] Gnuda V.D. Structural analysis of the transformation of the «substitution» type. V.D. Gnuda, V.T. Karasev, R. Zh. Topolyan. SPbNTORES: Proceedings of the Annual Scientific and Technical Conference. 2019. No. 1 (74). P. 102–103. URL: https://www.elibrary.ru/item.asp?id=39133391 (accessed: 01.02.2021) (in Russian).
[2] Burov D.A., Pogorelov B.A. The permutation group insight on the diffusion property of linear mappings. Mathematical problems of cryptography. 9:2 (2018). P. 47–58. DOI: https://doi.org/10.4213/mvk252 (in Russian).
[3] Gribunin V.G., Kostyukov V.E., Martynov A.P., Nikolaev D.B., Fomchenko V.N. Modern methods of ensuring the safety of information in nuclear power: Monograph. Ed. A.I. Asaykin. Sarov: FSUE RFNC-VNIIEF, 2014. – 636 p. DOI: http://dx.doi.org/10.53403/9785951502650 (in Russian).
[4] Borisenko N.P. Construction of "light" ciphers using substitutions with a trivial group of inertia in relation to affine transformations / N. P. Borisenko // Actual problems of information telecommunications in science and education (APINO 2019): collection of scientific articles of the VIII International scientific-technical and scientific-methodical conference: in 4 volumes, St. Petersburg, February 27-28, 2019. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2019. P. 154–159. URL: https://www.elibrary.ru/item.asp?id=41383511 (accessed: 01.02.2021) (in Russian).
[5] Martynov A.P., Fomchenko V.N. Cryptography and Electronics. Edited by A.I. Astaykin. Sarov: FSUE RFNC-VNIIEF, 2006. – 452 p. (in Russian).
[6] Pichkur, A.B. Description of the class of substitutions representable as a product of two substitutions with a fixed number of mobile points. Mathematical problems of cryptography. 2012. Vol. 3. No. 2. P. 79–95. URL: https://www.elibrary.ru/item.asp?id=18024011 (accessed: 01.02.2021) (in Russian).
[7] Martynova I.A., Splyukhin D.V. Analysis of the main characteristic properties of the elements of the series of factorial sets in the process of protecting information systems. Nauka. Think. 2017. No. 5. P. 13–16. URL: https://www.elibrary.ru/item.asp?id=30742615 (accessed: 01.02.2021) (in Russian).
[8] Sudoplatov S.V. Distributions of Countable Models of Disjoint Unions of Ehrenfeucht Theories. Lobachevskii J Math 42. 2021. P. 195–205. DOI: https://doi.org/10.1134/S1995080221010248.
[9] Martynova I.A., Martynov A.P., Nikolaev D.B. Cryptographic systems and the factorial compression method. Bulletin of the Institute of Engineering Physics. 2016, no. 4 (42). P. 54–57. URL: https://www.elibrary.ru/item.asp?id=27697857 (accessed: 01.02.2021) (in Russian).
[10] Lanini, M. Twisted quadratic foldings of root systems. M. Lanini, K.V. Zainoulline. Algebra and Analysis. 2021. Vol. 33. No 1. P. 93–118. URL: https://arxiv.org/abs/1806.08962 (accessed: 01.02.2021).
[11] Babanov N.Yu., Martynov A.P., Nikolaev D.B., Fomchenko V.N., Novikov A.V. Virtual interactive system for generating and processing control information Vestnik NGIEI. 2016. No. 4 (59). P. 15–29. URL: https://www.elibrary.ru/item.asp?id=26083908 (accessed: 01.02.2021) (in Russian).

[12] Zubei E.V. On the permutability of Sylow subgroups with commutators of B-subgroups. Journal of the Belarusian State University. Mathematics and Informatics.2019. No. 1. P. 12–17. DOI: https://doi.org/10.33581/2520-6508-2019-1-12-17 (in Russian).
[13] Dimitrov R.D., Harizanov V.S, Morozov A.S. Turing Degrees and Automorphism Groups of Substructure Lattices. Algebra Logic 59. P. 18–32 (2020). DOI: https://doi.org/10.1007/s10469-020-09576-x.
[14] Abornev A.V. Construction of substitutions using bit-substitution transformations of a module over a Galois ring of characteristic. Applied discrete mathematics. 2014. No. 1 (23). P. 9–19. URL: https://www.elibrary.ru/item.asp?id=21403880 (accessed: 01.02.2021) (in Russian).
[15] Moldovyan A.A. and other Cryptography: high-speed ciphers. SPb.: BHV-Petersburg, 2002. – 496 p. (in Russian).
[16] Martynov A.P., Martynova I.A. Permutation functions in the number system of a number of factorial sets. Vestnik VSU. Series: System Analysis and Information Technology. 2016. No. 3. P. 21–22. URL: https://www.elibrary.ru/item.asp?id=26083908 (accessed: 01.02.2021) (in Russian).
[17] Pchelintsev S.V. Identities of Prime Alternative Algebras. Algebra Logic. Vol. 59. P. 147–164 (2020). DOI: https://doi.org/10.1007/s10469-020-09587-8.
[18] Martynova I.A., Mashin I.G., Fomchenko V.N. Field theory and information protection: Monograph. Sarov: FSUE RFNC-VNIIEF, 2017. – 209 p. (in Russian).
[19] Martynov A.P., Martynova I.A., Fomchenko V.N. Axiomatic foundations of the substitution function in the number system of a number of factorial sets and their characteristics. Monograph. Sarov: FSUE RFNC-VNIIEF, 2019. – 209 p. (in Russian).

Поступила в редакцию – 11 февраля 2021 г. Окончательный вариант – 20 августа 2021 г.
Received – February 11, 2021. The final version – August 20, 2021.

Владимир Л. Евсеев[1], Руфия Ш. Садекова[2]
[1]Российский государственный университет нефти и газа
(национальный исследовательский университет) им. И.М. Губкина
Ленинский пр-кт, 65, корпус 1, Москва, 119991, Россия
[2]Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский пр–кт, 49, Москва, 125993, Россия
[1]e-mail: Evll@list.ru, https://orcid.org/0000-0003-3283-3106
[2]e-mail: sadekova.rufiya@gmail.com, https://orcid.org/0000-0001-6223-7730

ПРОТИВОДЕЙСТВИЕ КИБЕРБУЛЛИНГУ В СОЦИАЛЬНЫХ СЕТЯХ

DOI: http://dx.doi.org/10.26583/bit.2021.3.08

Аннотация. Статья посвящена разработке программы определения тональности текста. В статье обосновывается актуальность защиты социума от кибербуллинга. Анализируются методы противодействия кибербуллингу. Введен показатель негативности информации сайта. Подробно рассмотрена работа блокировщика сайтов. Обосновано использование сентимент-анализа, в основе которого лежит использование нейронных сетей. Для сентимент-анализа информационных потоков разработана программа на высокоуровневом языке программирования Python с внедрением в нее готовых обученных нейронных сетей. Используется словарь по стемам. Информационные потоки разбиты на токены, представленные в виде векторов. Приведены примеры нейронных сетей для определения тональности текста. Проведено сравнение результатов выполнения кодов анализа текста по вероятности получения правильного уровня негативности текста. Обосновывается целесообразность использования блокировщиков сайтов, как методов для защиты от кибербуллинга, и использование датасетов для обучения нейронных сетей.

Ключевые слова: кибербуллинг, блокировщик сайтов, межсетевой экран, негативная информация, анализ тональности текста, сентимент-анализ, нейронные сети, стемы.

Для цитирования: ЕВСЕЕВ, Владимир Л.; САДЕКОВА, Руфия Ш. ПРОТИВОДЕЙСТВИЕ КИБЕРБУЛЛИНГУ В СОЦИАЛЬНЫХ СЕТЯХ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 92–102, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1366. DOI: http://dx.doi.org/10.26583/bit.2021.3.08.

Vladimir L. Evseev[1], Rufiya Sh. Sadekova[2]
[1]National University of Oil and Gas «Gubkin University» (Gubkin University),
Leninsky Prospekt, 65, building 1, Moscow, 119991, Russia
[2]Financial University under the Government of the Russian Federation (Financial University),
Leningradsky Prospekt, 49, Moscow, 125993, Russia
[1]e-mail: Evll@list.ru, https://orcid.org/0000–0003-3283-3106
[2]e-mail: sadekova.rufiya@gmail.com, https://orcid.org/0000-0001-6223-7730

Countering cyberbullying in social networks

DOI: http://dx.doi.org/10.26583/bit.2021.3.08

Abstract. The study is devoted to the development of a program for determining the text tonality. The paper substantiates the relevance of protecting society from cyberbullying. The methods of cyberbullying countering are analyzed. An indicator of the negativity of the site's information was introduced. The work of the site blocker is considered in detail. The use of sentiment analysis, which is based on the use of neural networks, is justified. For the sentiment analysis of information flows, a program has been developed in the high-level programming language Python based of ready-made trained neural networks. The stem dictionary is used. Information flows are divided into tokens represented as vectors. In detail, the examples show the use of various neural networks to determine the tonality of the text. The results of the two text analysis codes are compared using the probability of obtaining the correct level of negativity

of the text. The expediency of using site blockers as methods to protect against cyberbullying as well as the use of datasets for training neural networks are justified.
Keywords: cyberbullying, site blocker, firewall, negative information, sentiment analysis, neural networks.
For citation: EVSEEV, Vladimir L.; SADEKOVA, Rufiya Sh. Countering cyberbullying in social networks. IT Security (Russia), [S.l.], v. 28, n. 3, p. 92–102, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1366. DOI: http://dx.doi.org/10.26583/bit.2021.3.08.

Введение

Пандемия коронавируса повлияла не только на экономику, но и на коммуникации в обществе. Межличностное общение вне социальных сетей асимптотически приблизилось к нулю. Общение людей перешло из реального мира в виртуальный мир посредством только социальных сетей. Из-за травли в интернете у многих наблюдается стресс, импульсивность, что наносит вред обществу. И, как результат, во всем мире значительно возросло обращение людей в службы психологической поддержки [1]. Гибридное воздействие злоумышленников на личности возросло на несколько порядков [2]. Одним из его проявлений является кибербуллинг – это агрессия, травля, направленные жертве с помощью средств электронной коммуникации [3]. На государственном уровне встала проблема – как защитить социум от данного негативного воздействия.

Чтобы пользователи социальных сетей не подвергались воздействию кибербуллинга, они должны уметь его распознавать, знать меры защиты от такого воздействия, а государство – должно направлять свои усилия на предотвращение кибербуллинга. С этой целью требуется разработать специальную программу выполняющую анализ тональности текста, позволяющий определять показатели и уровни негативности и являющийся основным элементом блокировщика сайтов.

За 2020 г. кибербуллинг стал одной из самых разрушительных форм онлайн-атак на субъекты. Агрессивные злоумышленники, используя IT-технологии, эмоционально давят на свою жертву, чтобы причинить ей сильнейшую психологическую травму и добиться своих целей [4]. Последствия реализации этих угроз зачастую трагичны и наносят значительный вред обществу.

Как же защищаться от кибербуллера? С нашей точки зрения целесообразно использовать следующие меры:

- организационные меры (общие рекомендации можно взять из программы Калифорнийского университета по борьбе с травлей) [5];
- правовые меры (статьи Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях [6], Федеральные Законы РФ);
- технические меры [7] (компьютерные программы, противодействующие кибербуллингу).

Рассмотрим технические меры защиты от кибербуллинга.

1. Защита интернета от кибербуллинга

Для защиты пользователей социальных сетей от влияния кибербуллинга целесообразно использовать блокировщик сайтов, в основе которого лежит специальная программа выполняющую анализ тональности текста. Данная программа будет выдавать управляющее воздействие в межсетевой экран для блокировки URL-адреса нежелательного сайта. Рассмотрим работу подобной программы, написанной на объектно-ориентированном высокоуровневом языке программирования Python, ориентированного на обеспечение переносимости написанных на нём программ.

Блокировщик сайтов целесообразно использовать, например, в государственных образовательных учреждения, т.к. он позволяет полностью оградить обучающихся от

негативной информации и предостеречь обучающихся от кибербуллинга во время нахождения их в учебном заведении (они не видят даже URL-адреса нежелательных сайтов).

Кроме специальной программы в блокировщике требуется использовать систему предотвращения вторжений (Intrusion Prevention System, IPS). IPS позволяет формировать и отсылать новые конфигурации в межсетевой экран, на основе которых межсетевой экран будет фильтровать трафик от нежелательного контента, т.е. кибербуллинга.

Работа блокировщика сайтов основывается на определении доли негативной информации сайта. Чтобы определить, какая доля текста является негативной, введем показатель негативности, который будет лежать в диапазоне от 0 до 1 с дискретностью 0,1. Для систематизации результатов работы блокировщика, определим пороги негативности данного показателя, относящиеся к определенным уровням:

- 0 – 0,3 – низкий уровень негативности;
- 0,31 – 0,6 – средний уровень негативности;
- 0,61 – 0,8 – высокий уровень негативности;
- 0,81 – 1 – критический уровень негативности.

Блокировщик сайтов работает следующим образом:

На вход блокировщика подается URL-адрес некоторого сайта, контент (текст) которого требуется оценить на наличие негативной информации.

Копируется текст данного сайта.

Происходит анализ тональности текста.

Определяется уровень негативности текста и происходит отнесение его к тому или иному уровню негативности.

Если выявлен средний, высокий или критический уровень негативности, то IPS выдает сигнал в межсетевой экран на блокировку URL-адреса сайта, а затем его адрес заносится в базу запрещенных сайтов программы.

Если же был получен критический уровень негативности текста, то целесообразно заблокировать сайт и на государственном уровне. Для этого необходимо отправить заявку в Роскомнадзор на сайте Единого реестра сайтов, содержащих запрещенную информацию, заполнив форму сообщения вручную.

Подобный порядок действий программы можно сравнить с межсетевым экраном Китайской Народной Республики, который блокирует на государственном уровне любую информацию негативного подтекста [8].

В основе работы разработанной программы блокировщика сайтов лежит анализ тональности текста (сентимент-анализ), позволяющий определять показатели и уровни негативности. Как происходит анализ эмоциональной окраски текста? Остановимся более подробно на работе сентимент-анализа.

В основе сентимент-анализа лежит подход, основанный на машинном обучении. Традиционно в данной сфере выделяют различные задачи обучения, но в анализе тональности обычно используется только обучение с учителем [9]. А этого недостаточно.

За последние годы количество методов машинного обучения значительно возросло, все чаще применяются различные нейронные сети [10].

Для сентимент-анализа информационных потоков была разработана программа на высокоуровневом языке программирования Python с внедрением в нее готового модуля, например, Dostoevsky, в котором используется уже обученная нейронная сеть [11]. Для ее обучения была использована база данных 2018 г. RuSentiment, в которую входят комментарии из социальной сети ВКонтакте [12].

Далее, надо определить – какая из баз данных является более эффективной и влияет ли база данных на качество правильного выполнения анализа тональности текста?

Как же в блокировщике сайтов происходит оценка тональности с помощью нейронной сети? Для примера возьмем два предложения, которые могут встречаться в социальных сетях:

1. Я купила новую книгу, но она мне абсолютно не понравилась, ужасный сюжет.
2. Мальчик купил бабушке цветы, это так мило!

По данным предложениям формируем словарь, не по словам, а по стемам (stem – основа слова без суффиксов и окончаний), что позволит избегать повторений слов в разных падежах, числах, словоформах (например, стем слова «легендарный» – «легенд»). Также важно учитывать из предложения – какой тональности каждый стем. Это будет учитываться в дальнейшем в нейронной сети. Чтобы рассмотреть, как определяется тональность текста с помощью нейронной сети, для примера возьмем третье предложение – Милый мальчик купил мне книгу. Представим в виде нулевого вектора все стемы из словаря. Соответственно, размерность вектора определяется количеством стем из словаря. Разобьем третье предложение на токены, т.е. на уникальные слова, и выделим стемы. Если стем из словаря присутствует в предложении, то элемент вектора этого стема будет равен 1, в противном случае – 0.

Далее этот вектор подается на вход нейронной сети и на выходе получаем два нейрона: первый отвечает за долю позитивного текста, второй – за долю негативного.

Развитие нейронных сетей повлекло за собой появление в 2015 г. крупных модулей с нейросетями – TensorFlow и Keras [13].

2. Анализ тональности текста с использованием модуля TensorFlow

Проанализируем эмоциональную окраску текста с помощью модуля TensorFlow. Для обучения нейронной сети понадобятся базы данных с позитивными и негативными текстами. В качестве таких текстов воспользуемся русскоязычными постами микроблогинговой площадки Twitter [14], которые были собраны в 2014 г.

В качестве входных данных будем использовать 7 предложений:

1. Давай дружить.
2. Я люблю тебя.
3. Ты очень красивый.
4. У меня все прекрасно.
5. На улице играют дети.
6. В школе ребенок подрался с одноклассником.
7. Какая у тебя ужасная внешность!

Последние два предложения явно негативные, а остальные – нейтральные или положительные. В дальнейшем определим уровень негативности этих предложений [15].

Порядок анализа текста, с помощью этого модуля, выполняется по следующему алгоритму:

1. Импортирование необходимых модулей.
2. Загрузка данных из баз с негативными и позитивными твитами.
3. Создание стеммера (функции, определяющей стем слова), где regex отсеивает смайлы и символы в твитах (рис. 1).

```
stemer = RussianStemmer()
regex = re.compile('[^а-яА-Я ]')
stem_cache = {}

def get_stem(token):
    stem = stem_cache.get(token, None)
    if stem:
        return stem
    token = regex.sub('', token).lower()
    stem = stemer.stem(token)
    stem_cache[token] = stem
    return stem
```

Рис. 1. Программный код создания стеммера
Fig. 1. The program code for creating a stemmer

4. Формирование словарей с уникальными словами из позитивных и негативных твитов.
5. Формирование словаря, который используется для преобразования токена в число.
6. Определение функции преобразования твита в вектор, который подается в нейронную сеть (рис. 2).

```
def tweet_to_vector(tweet, show_unknowns=False):
    vector = np.zeros(VOCAB_SIZE, dtype=np.int_)
    for token in tokenizer.tokenize(tweet):
        stem = get_stem(token)
        idx = token_2_idx.get(stem, None)
        if idx is not None:
            vector[idx] = 1
        elif show_unknowns:
            print("Unknown token: {}".format(token))
    return vector
```

Рис. 2. Программный код определения функции преобразования твита в вектор
Fig. 2. The program code for defining a function for converting a tweet into a vector

7. Формирование матрицы из преобразованных твитов в векторы.
8. Формирование выходного вектора (рис. 3).

```
labels = np.append(
    np.zeros(len(negative_tweets), dtype=np.int_),
    np.ones(len(positive_tweets), dtype=np.int_))
```

Рис. 3. Программный код формирования выходного вектора
Fig. 3. The program code for formation of the output vector

9. Формирование данных для обучения.
10. Построение нейронной сети (рис. 4).

```
def build_model(learning_rate=0.1):
    tf.compat.v1.reset_default_graph()

    net = tflearn.input_data([None, VOCAB_SIZE])
    net = tflearn.fully_connected(net, 125, activation='ReLU')
    net = tflearn.fully_connected(net, 25, activation='ReLU')
    net = tflearn.fully_connected(net, 2, activation='softmax')
    regression = tflearn.regression(
        net,
        optimizer='sgd',
        learning_rate=learning_rate,
        loss='categorical_crossentropy')

    model = tflearn.DNN(net)
    return model

model = build_model(learning_rate=0.75)
```

Рис. 4. Программный код построения нейронной сети
Fig. 4. The program code for building a neural network

11. Обучение и тестирование нейронной сети (рис. 5).

```
model.fit(
    X_train,
    y_train,
    validation_set=0.1,
    show_metric=True,
    batch_size=128,
    n_epoch=30)


predictions = (np.array(model.predict(X_test))[:,0] >= 0.5).astype(np.int_)
accuracy = np.mean(predictions == y_test[:,0], axis=0)
```

Рис. 5. Программный код обучения и тестирования нейронной сети
Fig. 5. The program code for training and testing a neural network

12. Анализ тональности входящих высказываний и вывод уровня негативности у каждого высказывания (рис. 6).

Результаты сентимент-анализа:

1. Давай дружить – низкий уровень негативности текста.
2. Я люблю тебя – средний уровень негативности текста.
3. Ты очень красивый – низкий уровень негативности текста.
4. У меня все прекрасно – низкий уровень негативности текста.
5. На улице играют дети – высокий уровень негативности текста.
6. В школе ребенок подрался с одноклассником – критический уровень негативности текста.
7. Какая же у тебя ужасная внешность! – критический уровень негативности текста.

```
def level(tweet):
    tweet_vector = tweet_to_vector(tweet, True)
    p = model.predict([tweet_vector])[0][0]
    if p < 0.3:
        print("низкий уровень негативности текста")
    elif p < 0.6:
        print("средний уровень негативности текста")
    elif p < 0.8:
        print("высокий уровень негативности текста")
    else: print("критический уровень негативности текста")

messages = [
    'Давай дружить',
    'Я люблю тебя',
    'Ты очень красивый',
    'У меня все прекрасно',
    'На улице играют дети',
    'В школе ребенок подрался с одноклассником',
    'Какая же у тебя ужасная внешность!'
]

for message in messages:
    print(message, '-', end=' ')
    level(message)
```

Рис. 6. Программный код анализа тональности входящих высказываний (messages) и вывод результатов анализа
Fig. 6. The program code for sentiment analysis of incoming messages and output of analysis results

Анализ данных результатов показал – у пяти из семи предложений программный код верно определил оценку тональности. Следовательно, вероятность получения правильного уровня негативности текста при использовании программного кода сентимент-анализа с помощью модуля TensorFlow равна $P_1=5/7\approx0,71$.

3. Анализ тональности текста с использованием модуля Dostoevsky

Проанализируем эмоциональную окраску текста с помощью модуля Dostoevsky Данный модуль использует уже обученную нейронную сеть и датасет, содержащий посты из социальной сети ВКонтакте за 2018 г. При этом посты из данной базы категорированы на пять типов:

- negative (негативное настроение);
- positive (позитивное настроение);
- neutral (нейтральное поведение);
- speech (разговорный формат, в который входят поздравления, благодарственные посты, приветствия);
- skip (непонятные случаи, когда у текста нельзя определить настроение).

На вход программного кода, основанного на данном модуле, подаются предложения, использованные в предыдущем программном коде [11] (рис. 7).

После выполнения программного кода получаем следующие уровни негативности предложений:

1. Давай дружить – низкий уровень негативности текста.
2. Я люблю тебя – низкий уровень негативности текста.
3. Ты очень красивый – низкий уровень негативности текста.

4. У меня все прекрасно – низкий уровень негативности текста.
5. На улице играют дети – низкий уровень негативности текста.
6. В школе ребенок подрался с одноклассником – низкий уровень негативности текста.
7. Какая же у тебя ужасная внешность! – критический уровень негативности текста.

```
from dostoevsky.tokenization import RegexTokenizer
from dostoevsky.models import FastTextSocialNetworkModel

tokenizer = RegexTokenizer()
model = FastTextSocialNetworkModel(tokenizer=tokenizer)

messages = [
    'Давай дружить',
    'Я люблю тебя',
    'Ты очень красивый',
    'У меня все прекрасно',
    'На улице играют дети',
    'В школе ребенок подрался с одноклассником',
    'Какая же у тебя ужасная внешность!'
]

results = model.predict(messages, k=5)

def level(p):
        if p < 0.3:
                print("низкий уровень негативности текста")
        elif p < 0.6:
                print("средний уровень негативности текста")
        elif p < 0.8:
                print("высокий уровень негативности текста")
        else: print("критический уровень негативности текста")



for message, sentiment in zip(messages, results):
        print(message, '-', end=' ')
        level(sentiment['negative'])
```

Рис. 7. Программный код анализа тональности текста с помощью модуля Dostoevsky
Fig. 7. Program code for text sentiment analysis using the Dostoevsky module

Данный программный код анализа тональности текста с помощью модуля Dostoevsky достаточно правильно оценил предложения на позитивность и негативность – верно определил оценку тональности у шести из семи предложений. Ошибка с определением негативности только у шестого предложения. Анализ показывает, что вероятность получения правильного уровня негативности текста равна $P_2=6/7\approx0{,}86$.

4. Сравнение результатов работы программных кодов

Результаты выполнения двух программных кодов анализа текста (в первом коде использовался модуль TensorFlow, в которой нейронная сеть обучается на базах данных 2014 г., содержащие позитивные и негативные тексты, во втором коде – модуль Dostoevsky, в котором нейронная сеть была обучена на базе данных 2018 г., классифицирующихся на 5 категорий) приведены в табл. 1.

Таблица 1. Результаты выполнения программных кодов анализа текста

Предложение	Уровень негативности текста, определенный с помощью первого программного кода (P_1≈0,71)	Уровень негативности текста, определенный с помощью второго программного кода (P_2≈0,86)
Давай дружить	Низкий	Низкий
Я люблю тебя	Средний	Низкий
Ты очень красивый	Низкий	Низкий
У меня все прекрасно	Низкий	Низкий
На улице играют дети	Высокий	Низкий
В школе ребенок подрался с одноклассником	Критический	Низкий
Какая же у тебя ужасная внешность	Критический	Критический

По результатам анализа табл. 2 можно сделать вывод: наиболее достоверным является программный код с модулем Dostoevsky, так как вероятность получения верного уровня негативности у предложений среди других полученных вероятностей является максимальной (P_2≈0,86). Это связано с тем, что данный модуль использует более актуальную базу данных, содержащую наиболее современные слова в текстах, и обученную ею нейронную сеть. Также в результате выполнения программного кода с использованием модуля Dostoevsky можно получить оценку тональности предложений по 5 категориям, что позволяет точнее определить эмоциональную окраску входящего текста.

Заключение

В работе показано, что для защиты от кибербуллинга, пользователям сети Интернет целесообразно, в дополнение к организационным и правовым мерам защиты, использовать технические меры защиты – блокировщики сайтов. В основе их работы лежит программа блокирования URL-адресов сайтов с текстом негативного характера. Алгоритм разработанной программы основан на анализе тональности текста (сентимент-анализ), позволяющий определять показатели и уровни негативности. Важнейшей частью разработанной программы является модуль анализа тональности текста, определяющий уровень негативности, который определяет эффективность работы блокировщика сайтов. Проведено сравнение результатов выполнения двух программных кодов сентимент-анализа предложений (первый программный код основан на модуле TensorFlow, второй – на модуле Dostoevsky), сделан вывод о целесообразности применения модуля Dostoevsky, использующего обученную нейронную сеть и усовершенственную базу данных, содержащую пять типов категорий.

В дальнейшем целесообразно использовать для обучения нейронных сетей датасеты, собранные государственными структурами, которые должны периодически обновляться новыми текстами, содержащими актуальную лексику. Это связано с увеличением количества неологизмов русского языка, чему способствует повышение значимости зарубежных социальных сетей.

СПИСОК ЛИТЕРАТУРЫ:

1. Volkova O.V., Shesternya P.A. Parallel pandemic: psychological facilitation in medical assistance // Сибирский психологический журнал. 2020. № 78. С. 156–167. URL: https://cyberleninka.ru/article/n/parallel-pandemic-psychological-facilitation-in-medical-assistance (дата обращения: 02.03.2021). DOI: http://dx.doi.org/10.17223/17267080/78/10.

2. Мацкевич И.М., Бочкарева Е.В. Пандемия и криминализация общества: как помешать появлению порочного круга. Часть 1 // Мониторинг правоприменения. 2020. URL: https://cyberleninka.ru/article/n/pandemiya-i-kriminalizatsiya-obschestva-kak-pomeshat-poyavleniyu-porochnogo-kruga-chast-1 (дата обращения: 02.03.2021). DOI: http://dx.doi.org/10.21681/2226-0692-2020-3-81-87.
3. Sobkin V.S., Fedotova A.V. Teenagers in social networks: patterns of usage and aggressiveness // Journal of Siberian Federal University. Humanities & Social Sciences. 2019. № 9. P. 1733–1752. URL: https://cyberleninka.ru/article/n/teenagers-in-social-networks-patterns-of-usage-and-aggressiveness (дата обращения: 02.03.2021). DOI: http://dx.doi.org/10.17516/1997-1370-0480.
4. Зинцова А.С. Социальная профилактика кибербуллинга. Вестник Нижегородского университета им. Н.И. Лобачевского. 2014. № 3. С. 122–128. URL: https://cyberleninka.ru/article/n/sotsialnaya-profilaktika-kiberbullinga (дата обращения: 02.03.2021).
5. Волкова Е.Н., Цветкова Л.А., Волкова И.В. Методологические основания для разработки программ профилактики подросткового буллинга // Сибирский психологический журнал. 2019. № 74. С. 88–100. URL: https://cyberleninka.ru/article/n/metodologicheskie-osnovaniya-dlya-razrabotki-programm-profilaktiki-podrostkovogo-bullinga (дата обращения: 07.03.2021). DOI: http://dx.doi.org/10.17223/17267080/74/5.
6. Барей Н.С., Мальцева В.А. Информационная безопасность детей в виртуальном пространстве. Кибербуллинг как стигматизационный фактор // Теория и практика общественного развития. 2020. №1 (143). С. 102–106. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-detey-v-virtualnom-prostranstve-kiberbulling-kak-stigmatizatsionnyy-faktor-1 (дата обращения: 02.03.2021).
7. Пахонина Е.В. К проблеме дистанционной коммуникации. Международный научно-исследовательский журнал. 2020. № 9–2 (99). URL: https://cyberleninka.ru/article/n/k-probleme-distantsionnoy-kommunikatsii (дата обращения: 04.03.2021). DOI: http://dx.doi.org/10.23670/IRJ.2020.99.9.048.
8. McMahon R., Bennett I. U.S. Internet Providers and the «Great Firewall of China» // Council on Foreign Relations. 23.02.2011. URL: https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china (дата обращения: 10.03.2021).
9. Shah A. Sentiment analysis of product reviews using supervised learning // RT&A. 2021. №SI 1 (60). P. 243–253. URL: https://cyberleninka.ru/article/n/sentiment-analysis-of-product-reviews-using-supervised-learning (дата обращения: 07.03.2021).
10. Sak H., Senior A., Beaufays F. Long short-term memory recurrent neural network architectures for large-scale acoustic modeling // Proceedings of the Annual Conference of the International Speech Communication Association. 2014. P. 338–342. URL: https://www.isca-speech.org/archive/archive_papers/interspeech_2014/i14_0338.pdf (дата обращения: 07.03.2021).
11. Силаева А.Э., Габриелян Г.А., Исаева И.А., Никульчев Е.В. Интеллектуальный анализ текстовых ответов в массовых опросах // Cloud of Science. 2019. Т. 6. № 4. С. 779–788. URL: https://cyberleninka.ru/article/n/intellektualnyy-analiz-tekstovyh-otvetov-v-massovyh-oprosah (дата обращения: 07.03.2021).
12. Rogers A., Romanov A., Rumshisky A., Volkova S., Gronas M., Gribov A. RuSentiment: An Enriched Sentiment Analysis Dataset for Social Media in Russian // Proceedings of the 27th International Conference on Computational Linguistics. 2018. P. 755–763. URL: https://www.aclweb.org/anthology/C18-1064.pdf (дата обращения: 07.03.2021).
13. Druki A.A., Spitsyn V.G., Arkalykov E.U. Semantic segmentation algorithms of the earth's surface pictures based on neural network methods // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2020. № 51. URL: https://cyberleninka.ru/article/n/algoritmy-semanticheskoy-segmentatsii-snimkov-zemnoy-poverhnosti-na-osnove-neyronnyh-setey (дата обращения: 07.03.2021). DOI: http://dx.doi.org/10.17223/19988605/51/8.
14. Рубцова Ю.В. Построение корпуса текстов для настройки тонового классификатора // Программные продукты и системы. 2015. № 1 (109). С. 72–78. URL: http://www.swsys.ru/index.php?page=article&id=3962&lang= (дата обращения: 05.03.2021). DOI: http://dx.doi.org/10.15827/0236-235X.109.072-078.
15. Karuchit W. Negative effects of digital media on Thai youngsters: Case studies from Thailand and abroad // International Journal of Media and Information Literacy. 2016. № 2. URL: https://cyberleninka.ru/article/n/negative-effects-of-digital-media-on-thai-youngsters-case-studies-from-thailand-and-abroad (дата обращения: 05.03.2021). DOI: http://dx.doi.org/10.13187/ijmil.2016.2.122.

REFERENCES:

[1] Volkova O.V., Shesternya P.A. Parallel pandemic: psychological facilitation in medical assistance. Siberian Psychological Journal. 2020. No. 78. P. 156–167. URL: https://cyberleninka.ru/article/n/parallel-pandemic-

psychological-facilitation-in-medical-assistance (accessed: 02.03.2021). DOI: http://dx.doi.org/10.17223/17267080/78/10.

[2] Matskevich I.M., Bochkareva E.V. Pandemic and criminalization of society: how to prevent the emergence of a vicious circle. Part 1. Monitoring enforcement. 2020. URL: https://cyberleninka.ru/article/n/pandemiya-i-kriminalizatsiya-obschestva-kak-pomeshat-poyavleniyu-porochnogo-kruga-chast-1 (accessed: 02.03.2021). DOI: http://dx.doi.org/10.21681/2226-0692-2020-3-81-87 (in Russian).

[3] Sobkin V.S., Fedotova A.V. Teenagers in social networks: patterns of usage and aggressiveness. Journal of Siberian Federal University. Humanities & Social Sciences. 2019. No. 9. P. 1733–1752. URL: https://cyberleninka.ru/article/n/teenagers-in-social-networks-patterns-of-usage-and-aggressiveness (accessed: 02.03.2021). DOI: http://dx.doi.org/10.17516/1997-1370-0480.

[4] Zintsova A.S. Social prevention of cyberbullying. Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevsky. 2014. No. 3. P. 122–128. URL: https://cyberleninka.ru/article/n/sotsialnaya-profilaktika-kiberbullinga (accessed: 02.03.2021) (in Russian).

[5] Volkova E.N., Tsvetkova L.A., Volkova I.V. Methodological grounds for the development of programs for the prevention of teenage bullying. Siberian psychological journal. 2019. No. 74. P. 88–100. URL: https://cyberleninka.ru/article/n/metodologicheskie-osnovaniya-dlya-razrabotki-programm-profilaktiki-podrostkovogo-bullinga (accessed: 07.03.2021). DOI: http://dx.doi.org/10.17223/17267080/74/5 (in Russian).

[6] Barei N.S., Maltseva V.A. Information security of children in the virtual space. Cyberbullying as a stigmatization factor. Theory and practice of social development. 2020. No. 1 (143). P. 102–106. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-detey-v-virtualnom-prostranstve-kiberbulling-kak-stigmatizatsionnyy-faktor-1 (accessed: 02.03.2021) (in Russian).

[7] Pakhonina E.V. On the problem of remote communication. International Scientific Research Journal. 2020. No. 9–2 (99). URL: https://cyberleninka.ru/article/n/k-probleme-distantsionnoy-kommunikatsii (accessed: 04.03.2021). DOI: https://doi.org/10.23670/IRJ.2020.99.9.048 (in Russian).

[8] McMahon R., Bennett I. U.S. Internet Providers and the «Great Firewall of China». Council on Foreign Relations. 23.02.2011. URL: https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china (accessed: 10.03.2021).

[9] Shah A. Sentiment analysis of product reviews using supervised learning. RT&A. 2021. No. SI 1 (60). P. 243–253. URL: https://cyberleninka.ru/article/n/sentiment-analysis-of-product-reviews-using-supervised-learning (дата обращения: 07.03.2021).

[10] Sak H., Senior A., Beaufays F. Long short-term memory recurrent neural network architectures for large-scale acoustic modeling. Proceedings of the Annual Conference of the International Speech Communication Association. 2014. P. 338–342. URL: https://www.isca-speech.org/archive/archive_papers/interspeech_2014/i14_0338.pdf (accessed: 07.03.2021).

[11] Silaeva A.E., Gabrielyan G.A., Isaeva I.A., Nikulchev E.V. Intelligent analysis of text responses in mass polls. Cloud of Science. 2019. Vol. 6 No. 4. P. 779–788. URL: https://cyberleninka.ru/article/n/intellektualnyy-analiz-tekstovyh-otvetov-v-massovyh-oprosah (accessed: 07.03.2021) (in Russian).

[12] Rogers A., Romanov A., Rumshisky A., Volkova S., Gronas M., Gribov A. RuSentiment: An Enriched Sentiment Analysis Dataset for Social Media in Russian. Proceedings of the 27th International Conference on Computational Linguistics. 2018. P. 755–763. URL: https://www.aclweb.org/anthology/C18-1064.pdf (accessed: 07.03.2021).

[13] Druki A.A., Spitsyn V.G., Arkalykov E.U. Semantic segmentation algorithms of the earth's surface pictures based on neural network methods // Bulletin of Tomsk State University. Management, Computer Engineering and Informatics. 2020. No. 51. URL: https://cyberleninka.ru/article/n/algoritmy-semanticheskoy-segmentatsii-snimkov-zemnoy-poverhnosti-na-osnove-neyronnyh-setey (accessed: 07.03.2021). DOI: http://dx.doi.org/10.17223/19988605/51/8.

[14] Rubtsova Yu. Building a text corpus for tuning a tone classifier // Software products and systems. 2015. No. 1 (109). P. 72–78. URL: http://www.swsys.ru/index.php?page=article&id=3962&lang= (accessed: 05.03.2021). DOI: http://dx.doi.org/10.15827/0236-235X.109.072-078 (in Russian).

[15] Karuchit W. Negative impact of digital media on Thai youth: Case studies from Thailand and abroad. International Journal of Media and Information Literacy. 2016. No. 2. URL: https://cyberleninka.ru/article/n/negative-effects-of-digital-media-on-thai-youngsters-case-studies-from-thailand-and-abroad (accessed: 05.03.2021). DOI: http://dx.doi.org/10.13187/ijmil.2016.2.122.

Поступила в редакцию – 29 марта 2021 г. Окончательный вариант – 25 Августа 2021г.
Received – March 29, 2021. The final version – August 20, 2021.

Алексей А. Сиротский[1], Сергей А. Резниченко[2]
[1]Московский государственный технологический университет «СТАНКИН»,
Вадковский пер., 1, Москва, 127055, Россия
[2]Финансовый университет при правительстве РФ,
Ленинградский пр–кт, 49, Москва, 125993, Россия
[1]e-mail: hotwater2009@yandex.ru, https://orcid.org/0000-0002-9343-7185
[2]e-mail: rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457

ФОРМАЛИЗОВАННАЯ МОДЕЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ПРЕДМЕТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТАНДАРТОВ

DOI: http://dx.doi.org/10.26583/bit.2021.3.09

Аннотация. Задача аудита информационной безопасности заключается в проверке соответствия системы защиты объекта совокупности критериев, определяющих требования к уровню защищенности. В этой связи необходимо определить и формализовать совокупность критериев, отражающих уровень защищенности объекта и выявление показателей, по которым можно провести объективные процедуры проверки. Аудит информационной безопасности проводится на предмет соответствия требованиям любых стандартов в области информационной безопасности. В связи с отсутствием практико-ориентированных инструктивно-методических материалов аудиторской деятельности по оценке соответствия информационной безопасности организаций требованиям ключевых документов и стандартов, были проведены исследования содержательности и формализуемости требований на примере стандарта ГОСТ Р ИСО/МЭК 17799-2005 в части разработки метода проведения аудита ИБ на предмет соответствия данному стандарту и инструкции по его реализации. Целью работы является формирование формализованной методики при проведении аудита информационной безопасности на предмет соответствия стандартам и нормативным требованиям по информационной безопасности. В статье представлена формализованная модель аудита информационной безопасности организации, которая базируется на принципах независимости и объективности аудиторской деятельности. Предложен подход, на основе системы объективных показателей, сопоставимых с функциями защиты, и заключающийся в формировании чек-листов с соответствующими критериями соотнесения показателей. В основу предлагаемого метода, и в целях повышения объективности результатов аудиторской работы, положен принцип подтверждения фактов, выявляемых в результате аудиторской проверки. В рамках метода предложена инструкция по разработке чек-листов, пригодная и адаптируемая для любого описательного стандарта, на предмет соответствия, которому может проводиться процедура аудиторской проверки.

Ключевые слова: аудит, информационная безопасность, стандарт, модель, контроль, показатели, методика, формализация.

Для цитирования: СИРОТСКИЙ, Алексей А.; РЕЗНИЧЕНКО, Сергей А. ФОРМАЛИЗОВАННАЯ МОДЕЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ПРЕДМЕТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТАНДАРТОВ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 103–117, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1368. DOI: http://dx.doi.org/10.26583/bit.2021.3.09.

Alexei A. Sirotskiy[1], Sergei A. Reznichenko[2]
[1]Moscow State University of Technology «STANKIN»,
Vadkovskiy pereulok, 1, Moscow, 127055, Russia
[2]Financial University under the Government of the Russian Federation,
Leningradsky Prospekt, 49, Moscow, 125993, Russia
[1]e-mail: hotwater2009@yandex.ru, https://orcid.org/0000-0002-9343-7185
[2]e-mail: rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457

A formalized model of an organization information security audit for compliance with the requirements of standards

DOI: http://dx.doi.org/10.26583/bit.2021.3.09

Abstract. In general the overall task of an information security audit is to verify that the security system of an object meets the set of criteria that determine the requirements for the security level. In this regard, it is necessary to define and to establish a set of criteria reflecting the security level of the facility and to identify indicators for which objective verification procedures can be carried out. Information security audits can be conducted to ensure compliance with all information security standards. Due to the lack of instructional methodologies for auditing activities to assess the compliance of organization information security with the requirements of systemically important generally applicable documents and standards, studies were carried out on the content and formalizability of requirements using the example of the GOST R ISO/IEC 17799-2005 standard in terms of the building an instructional methodology for auditing IS possibility for compliance with this standard. The purpose of the study is to form a formalized audit methodology when conducting an audit of information security for compliance with standards and regulatory requirements for information security in the absence of developed and generally accepted methods. In the following a formalized model for auditing the organization's information security for compliance with the requirements of standards is developed. The model is based on the principles of maximum independence and objectivity of audit activities. The authors of the paper suggest an approach, which is based on a system of objective indicators comparable to protection functions, and consists in the formation of check lists with appropriate criteria for the correlation of indicators and methods of proving the facts revealed as a result of an audit. On the basis of the proposed model and methodology, it is possible to develop the check lists for any descriptive standard for which an audit is required.

Keywords: audit, information security, standard, model, control, indicators, methodology, formalization.
For citation: SIROTSKIY, Alexei A.; REZNICHENKO, Sergei A. A formalized model of an organization information security audit for compliance with the requirements of standards. IT Security (Russia), [S.l.], v. 28, n. 3, p. 103–117, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1368. DOI: http://dx.doi.org/10.26583/bit.2021.3.09.

1. Введение

Аудит информационной безопасности (ИБ), как системное действие, направлено на контроль и проверку состояния ИБ объекта защиты (в частности, организации), а также оценку адекватности применяемых средств и методов защиты информации в соответствии с существующими угрозами.

Общая задача аудита ИБ заключается в проверке соответствия системы защиты объекта совокупности критериев, определяющих требования к уровню защищенности.

В этой связи возникает необходимость определения и формализации совокупности критериев, отражающих уровень защищенности объекта и выявление показателей, по которым возможно провести объективные процедуры проверки. Критерии должны быть чётко определяемыми и по возможности измеряемыми [1, 2].

Объектами аудита ИБ могут быть любые объекты и процессы, например:

– деятельность компании в целом;

– автоматизированная или информационная система, либо их отдельные компоненты;

– организационно-управленческие процессы;

– технические средства;

– бизнес-процедуры [3, 4].

По форме проведения, аудит ИБ может быть организационно-нормативным [5] (когда предметом анализа являются мероприятия и нормативные документы по

обеспечению ИБ) и техническим (когда предметом анализа являются технические средства обработки информации).

Совокупность методов анализа рисков ИБ базируется на двух моделях:

– первая модель определяет риск на основе сопоставления соответствия объекта защиты набору требований по ИБ, которые исходят из стандартов, нормативно-правовых актов и условий эксплуатации систем;

– вторая модель определяет риск на основе оценки вероятностей реализации угроз и атак, а также величин потенциально возможного материального ущерба.

В рамках концептуальной модели аудита ИБ [5], можно выделить три практических и три теоретических подхода к проведению аудита ИБ.

Практическими подходами являются:

– аудит на основе анализа рисков;

– аудит на основе анализа стандартов ИБ;

– аудит на основе экспериментальных исследований объекта.

Теоретическими подходами являются:

– аудит на основе моделирования процессов;

– аудит на основе модели оценки;

– аудит на основе модели зрелости.

Исходя их этого, невозможно дать универсальные формализованные показатели и критерии проведения аудита, применимые во всех задачах и видах аудита.

Одним из наиболее распространённых методов является подход на основе анализа стандартов ИБ, хотя бы потому, что стандарты формируют совокупность требований и рекомендаций по обеспечению ИБ на основе накопленного профессионального опыта, а также являются регламентирующими документами, применяемыми в профессиональном сообществе. Кроме того, по ряду отраслей существуют обязательные к применению отраслевые стандарты. Примером обязательных к применению стандартов являются стандарты Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» и СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». Отраслевые стандарты определяют специфические задачи управления и обеспечения ИБ в своей сфере. Типичной является финансово-кредитная сфера, характеризующаяся ярко выраженными индивидуальными особенностями [6, 7].

Примерами общепримени мых основополагающих стандартов являются национальный стандарт российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» и международный стандарт ISO / IEC 27002-2013 «Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью».

Аудит ИБ может проводиться на предмет соответствия требованиям стандартов необходимых организации в соответствии с заданием на аудит. И если применительно к требованиям стандартов СТО БР ИББС-1.0 и СТО БР ИББС-1.1 Банком России разработана методика аудиторской проверки, изложенная в стандарте Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014», то применительно к общепримени мым стандартам ГОСТ Р ИСО/МЭК и ISO/IEC таких методик как правило нет. Можно отметить модель, реализованную в стандартах

ISO/IEC 15504-3 «Информационная технология. Оценка процесса», ISO/IEC 21827 «Инжиниринг безопасности систем – модель зрелости возможностей», COBIT (Control Objectives for Information and related Technology), но она не может быть прямо перенесена на другие стандарты и нормативные документы, в частности на стандарт ГОСТ Р ИСО/МЭК 17799-2005. В то же время стандарты ГОСТ Р ИСО/МЭК 17799-2005 и ISO / IEC 27002-2013 являются базовыми документами, определяющими основные направления обеспечения информационной безопасности организаций, и во множестве случаев могут быть основой для проводимой аудиторской проверки.

Целью работы является формирование формализованной аудиторской методики и практико-ориентированной инструкции, при проведении аудита ИБ на предмет соответствия стандартам и нормативным требованиям по ИБ. В рамках предлагаемой методики возможна разработка аналогичных инструкций применительно к любому стандарту.

2. Формализация проведения аудита информационной безопасности

Следует заметить, что подавляющее большинство базовых стандартов в области обеспечения ИБ объектов защиты и управлению ИБ на предприятиях, имеет явно выраженный описательный характер с указаниями по совокупности руководящих действий, и не содержат:

- критериев полноты руководящих действий;
- дискретных, однозначно трактуемых показателей выполнимости и результативности действий;
- методов достижения результатов;
- инструкций по реализации проверок на соответствие.

Основная трудность в проведении аудита ИБ на предмет соответствия требованиям стандартов заключается в отсутствии чёткой и последовательной методики аудита. В свою очередь при аудите ИБ следует исключить субъективности, исходя из понимания, что результаты аудита будут тем достовернее, чем в большей степени они будут формализованы. Исключить субъективности полностью, к сожалению, неосуществимо.

Формализация аудиторских процессов является актуальным и пока ещё мало изученным направлением исследований. Предпринимались различные попытки формализации, в основном применительно к отдельным аспектам аудита и с применением так называемого «аудиторского подхода на основе эталонной модели» [8, 9].

Задача формализации аудиторского процесса преследует цель повторяемости и независимости процедур и результатов аудита.

Одной из наилучших практик можно назвать создание так называемых «чек-листов» (контрольных карт), отражающих последовательность проведения аудиторской процедуры, проверяемые процессы и их дискретизированные показатели.

Рассмотрим аудиторские задачи и действия в рамках оценки соответствия ИБ организации требованиям стандарта ГОСТ Р ИСО/МЭК 17799-2005, которые по аналогии коррелируют и со стандартом ISO / IEC 27002-2013. Данный стандарт определяет требования к безопасности с учётом следующих факторов:

- оценка рисков ИБ;
- нормативные требования;
- специфические принципы, характерные для среды организации.

Стандарт ГОСТ Р ИСО/МЭК 17799-2005 выделяет три ключевые категории информации, защита которых должна обеспечиваться первостепенно:

- персональные данные;

– учётные данные организации;
– интеллектуальная собственность.

Совокупность мероприятий определена следующим образом:

– наличие политик ИБ;
– распределение обязанностей по обеспечению ИБ;
– обучение по вопросам ИБ;
– информирование об инцидентах ИБ;
– управление непрерывностью бизнеса.

Защита персональных данных и персональной информации происходит из неприкосновенности личности и частной жизни, что имеет высокую актуальность в современном общественном устройстве [10–13]. Выделение данной категории в стандарте актуально ввиду наличия отдельного Федерального Закона[1] и подкрепляет практические аспекты реализации его требований.

В отношении каждой из категорий информации необходимы защитные мероприятия. Также и наоборот: защитные мероприятия должны быть направлены на обеспечение защиты всех категорий информации. Составим обобщённую матрицу защиты (табл. 1), в которой определим 15 функций защиты F_{11} … F_{53}, каждую из которых можно оценить по совокупности соответствия требованиям.

Таблица 1. Обобщённая матрица защиты

Мероприятия	Категории информации		
	Персональные данные	Учётные данные организации	Интеллектуальная собственность
Политики ИБ	F_{11}	F_{12}	F_{13}
Распределение обязанностей	F_{21}	F_{22}	F_{23}
Обучение персонала	F_{31}	F_{32}	F_{33}
Информирование об инцидентах	F_{41}	F_{42}	F_{43}
Управление непрерывностью бизнеса	F_{51}	F_{52}	F_{53}

Процессы управления ИБ в стандарте ГОСТ Р ИСО/МЭК 17799-2005 разделены на 10 направлений:

– политика безопасности;
– организация информационной безопасности;
– управление активами;
– безопасность человеческих ресурсов;
– физическая безопасность и безопасность окружения;
– управление передачей данных и операционной деятельностью;
– контроль доступа;
– разработка и обслуживание систем;
– управление непрерывностью бизнеса;
– соответствие требованиям.

Сопоставляя совокупность рекомендованных мероприятий и управленческих процессов, можно отметить, что частично они совпадают.

Непосредственные действия аудитора направлены на выявление соответствия защищённости объекта по указанным 10 направлениям. При этом проверки необходимо

[1]Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.

выполнять максимально объективными и повторяемыми методами. Разработанная модель аудиторского контроля, в рамках выделенных направлений, приведена на рис. 1.

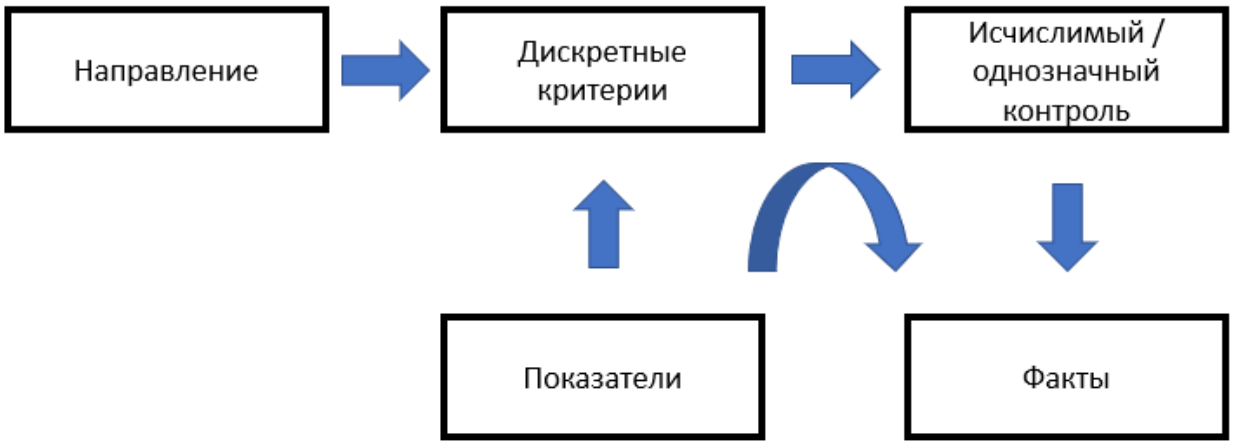


Рис. 1. Модель аудиторского контроля
Fig. 1. Audit control model

Согласно предлагаемой модели, аудитор:

– определяет факты, относящиеся к проверяемым процедурам и методам защиты информации;

– собирает доказательства (подтверждения) определяемых фактов;

– использует исключительно объективные дискретные критерии;

– фиксирует результаты проверки в виде однозначно трактуемых или исчислимых показателей.

Принципиальным является вопрос о системе объективных показателей и критериев аудиторского контроля. В этих целях аудиторы, в частности, могут руководствоваться стандартом ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности», который существует в редакциях 2006 г. и 2013 г., которые имеют существенные отличия в части подходов к организации управления информационной безопасностью на предприятиях. Процедуры аудита по совокупности требований системы стандартов ISO 2700x и в рамках цикла PDCA имеют самостоятельную концепцию [14] и в данном случае не рассматриваются.

Стандарт ГОСТ Р ИСО/МЭК 27001-2006 в рекомендуемом приложении «А» приводит цели и меры управления, соответствующие направлениям, сформулированным в стандарте ГОСТ Р ИСО/МЭК 17799-2005, а стандарт ISO/IEC 27001-2013 в рекомендуемом приложении «А» приводит аналогичные цели и меры управления, соответствующие направлениям, сформулированным в стандарте ISO/IEC 27002-2013. Они имеют частичные совпадения и соответствия, поскольку перечень направлений, определяемых в ГОСТ Р ИСО/МЭК 17799-2005 и ISO/IEC 27002-2013 имеет различия.

В табл. 2 приведён в качестве примера перечень целей и мер управления из стандарта ГОСТ Р ИСО/МЭК 27001-2006 для направления «Политика информационной безопасности» стандарта ГОСТ Р ИСО/МЭК 17799-2005. Такие перечни целей и мер определены для всех направлений стандарта.

Таблица 2. Цели и меры управления политикой информационной безопасностью

A.5.1.1	Документирование политики информационной безопасности	Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций
A.5.1.2	Анализ политики информационной безопасности	Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности

Приведённая информация, безусловно, является определяющей для аудиторской оценки соответствия, поскольку указывает на необходимые факты, которые аудитором должны быть или подтверждены, или опровергнуты, но не содержит критериев проверки.

Таким образом, имеется потребность в создании формализованной схемы и/или алгоритма аудиторских действий, базирующейся на дискретных критериях и однозначно определяемых объективных исчисляемых показателях. Подобная модель может быть представлена в виде «чек-листов» однозначно поставленных вопросов, на которые могут быть даны только предельно чёткие ответы, исключающие субъективность.

Для создания чек-листов соответствующих ответов воспользуемся как сформулированными в стандарте ГОСТ Р ИСО/МЭК 27001-2006 целями и мерами, так и совокупностью требований, изложенных в стандарте ГОСТ Р ИСО/МЭК 17799-2005. Рассмотрим предлагаемое решение на примере направления «Политика информационной безопасности». Согласно указанным стандартам, цель политики ИБ – обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением ИБ в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.

В действующем законодательстве нет прямых требований по форме и содержанию политик ИБ, в связи, с чем можно наблюдать довольно разнообразные подходы организаций к формированию политик ИБ. В тоже время именно ГОСТ Р ИСО/МЭК 17799-2005 содержит указания на минимальные требования к содержательности политики ИБ, которая должна включать следующее:

а. определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б. изложение целей и принципов информационной безопасности, сформулированных руководством;

в. краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;
2) требования в отношении обучения вопросам безопасности;
3) предотвращение появления и обнаружение вирусов и другого вредоносного ПО;
4) управление непрерывностью бизнеса;
5) ответственность за нарушения политики безопасности;
6) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;
7) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных

информационных систем, а также правила безопасности, которым должны следовать пользователи.

Требования по управлению политикой ИБ следующие:

1. Необходимо, чтобы в организации назначалось ответственное за политику безопасности должностное лицо, которое отвечало бы за ее реализацию и пересмотр в соответствии с установленной процедурой.

2. Указанная процедура должна обеспечивать осуществление пересмотра политики информационной безопасности в соответствии с изменениями, влияющими на основу первоначальной оценки риска, например, путем выявления существенных инцидентов нарушения информационной безопасности, появление новых уязвимостей или изменения организационной или технологической инфраструктуры.

3. Периодические пересмотры должны осуществляться в соответствии с установленным графиком и включать:

– проверку эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности;

– определение стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность бизнеса;

– оценку влияния изменений в технологиях.

На основе совокупности перечисленных требований и указаний, аудитором составляется перечень вопросов, которые составят чек-лист, и на которые он будет искать ответы в виде доказательств и подтверждающих фактов в процессе проведения аудита.

Поскольку в рамках предлагаемой модели необходимы объективные, дискретные, исчисляемые, однозначно трактуемые критерии, то к перечню вопросов, входящих в чек-лист, предъявляются те же требования: ответом на вопрос может быть только неоспоримое и проверяемое утверждение, но ни в коем случае не рассуждение.

В табл. 3 приведено примерное содержание чек-листа для аудиторской проверки по направлению «Политика информационной безопасности». Предлагаемый чек-лист может быть расширен аудитором под конкретные задачи [15]. Поясним принципы составления чек-листа. Все вопросы сгруппированы по трём уровням (количество уровней может быть и больше). Идея уровней в том, что при отрицательном ответе на вопрос более высокого (например, первого) уровня, нет смысла искать ответы на вопросы более низкого (в данном случае – второго) уровня. Существуют также и альтернативные модели уровневого представления оценок безопасности объектов в процессе проведения аудита [16, 17].

Как видно из табл. 3, все собираемые подтверждающие сведения представляются либо в виде дискретных значений (да/нет, присутствует/отсутствует, соответствует/не соответствует, и т.п.), либо в исчисляемых (средний балл по тестированию [18], процент ознакомленных или обученных сотрудников, и т.п.). Не следует путать проверку (методом тестирования) знаний содержания конкретной политики ИБ организации как внутреннего локального нормативного документа и знаний сотрудниками теории и методологии защиты информации в целом.

Таблица 3. Чек-лист работы аудитора

№ п/п	Уровень	Вопрос для определения контрольного показателя	Ответ		Способ подтверждения факта
			Дискретный	Исчисляемый	
1	1	Есть ли политика безопасности как документ?	Да/нет	-	Наличие документа
2	2	Утверждена ли политика безопасности руководством (надлежащим образом)	Да/нет	-	Наличие реквизитов, подписей, печати
3	2	Размещена ли политика безопасности в свободном доступе, в том числе для сторонних контрагентов	Да/нет	-	а) место размещения; б) способ доступа
4	2	Доведена ли политика безопасности до всех сотрудников организации?	-	% ознакомленных сотрудников	а) лист ознакомления с подписями б) интервью с сотрудниками
5	2	Соответствуют ли изложенные в политике меры и процедуры обеспечения безопасности реально применяемым мерам в совокупности с видами защищаемой информации?	-	Полностью/ В большей мере/ Наполовину/ В меньшей мере/ Не соответствуют	Сопоставление указанных в политике ИБ видов защищаемой информации, должностей сотрудников, процедур взаимодействия, используемых средств обработки и защиты информации реальным бизнес-процессам организации
6	2	Соответствует ли политика ИБ требованиям стандарта	Да/нет (/частично)	-	Наличие отражённых вопросов согласно перечню стандарта
7	3	Понимают ли сотрудники содержание и требования политики безопасности?	-	% компетентных сотрудников	Тестирование сотрудников
8	3	Есть ли процедура пересмотра политики ИБ?	Да/нет	-	Наличие соответствующей записи в политике ИБ или отдельном локальном документе
9	1	Есть ли ответственное лицо за реализацию политики ИБ?	Да/нет	-	1. Наличие: а) должностной инструкции; б) приказа о назначении; в) трудового договора; 2. Проведение интервью с ответственным лицом
10	2	Распределены ли обязанности по обеспечению ИБ между сотрудниками?	-	% сотрудников, имеющих должностные функции по контролю за безопасностью	Наличие должностных инструкций для сотрудников (по категориям) с записями в них о действиях по обеспечению ИБ

Таблица 3. Чек-лист работы аудитора (продолжение)

№ п/п	Уровень	Вопрос для определения контрольного показателя	Ответ		Способ подтверждения факта
11	1	Есть ли методика оценки рисков ИБ в организации?	Да/нет	-	Наличие внутреннего локального документа
12	2	Регулярно ли проводится оценка рисков ИБ?	а) Да/нет; б) соответствует периодичности / не соответствует периодичности	-	а) наличие внутреннего нормативного документа организации с определенным порядком и периодичностью оценки рисков б) наличие отчётов о предыдущих оценках рисков
13	2	Принимались ли решения по результатам переоценки рисков?	Да/нет	-	а) наличие датированных документов по коррекции защитных мер; б) наличие датированных документов о закупке дополнительных средств защиты; в) наличие договоров об оказании услуг в области ИБ
14	3	Изменение количества инцидентов информационной безопасности за отчётный период	-	%	Исследование журналов регистрации инцидентов информационной безопасности.
15	3	Изменение количества предотвращённых событий нарушения информационной безопасности за отчётный период	-	%	Исследование записей о зарегистрированных попытках нарушения информационной безопасности, в том числе создаваемых автоматически в программных средах.
16	1	Обучались ли сотрудники по тематике ИБ?	-	% обучившихся сотрудников	Наличие документов о повышении квалификации и профессиональной переподготовке
17	2	Каков уровень знаний сотрудников в области ИБ?	-	Средний балл	Тестирование сотрудников с оценкой в виде набранных баллов
18	1	Есть ли регламент реагирования на инциденты ИБ?	Да/нет		Наличие внутреннего локального документа

Можно сформулировать следующие принципы составления чек-листов:

– выполнение каждого требования нормативного документа определяется контрольным показателем;

– каждый контрольный показатель выражается в виде предельно чёткого, однозначно трактуемого вопроса, предполагающего однозначный объективный ответ;

– ответ на вопрос может быть либо дискретным, либо в измеримых исчисляемых значениях;

– все вопросы, формирующие контрольные показатели, делятся на уровни;

– вопросы первого (высшего) уровня определяют глобально факты исполнения требований;

– вопросы второго и последующих (низших) уровней детализируют степень исполнения требований и характеризуют уровень защищённости;

– аудитор собирает ответы на вопросы с целью подтверждения фактов;

– при отрицательных ответах на вопросы верхних уровней, проверять утверждения по вопросам нижних уровней не имеет смысла;

– качество формулировок контрольных вопросов определяется их объективностью, выражающейся в неоспоримости ответов даже с позиций сторонней заинтересованности.

В общем случае, исходя из изложенного принципа формирования чек-листов, каждый вопрос (показатель) S_i описывается в виде следующей функции:

$$S_i(j) \quad = \{X_i \,|\, Z_i\},$$

где i – номер вопроса, j – уровень вопроса, X – дискретное значение ответа (1 – «да», «выполняется», «есть»; 0 – «нет», «не выполняется», «отсутствует»); Z – исчисляемое значение ответа (в долях, процентах или иных единицах, а также в градациях, например: 1 – «полностью соответствует», 0,75 – «в большей мере, 0,5 – «наполовину», 0,25 – «в меньшей мере», 0 – «не соответствует»).

Для контроля первого уровня целесообразно применять вопросы только с дискретными ответами. Требованиями по прохождению аудита будет являться 100% результаты по критериям первого уровня: $S_i(1) = 1$ и набор минимальной (заранее установленной до начала аудита) результативности по второму и последующему уровням.

Для второго и последующих уровней задаются минимальные пороги результативности, которые могут быть сформулированы следующим образом:

– для второго уровня: не менее чем на 80% вопросов должны быть получены положительные ответы;

– для третьего уровня: не менее чем на 60% вопросов должны быть получены положительные ответы.

При подготовке к аудиту должны быть составлены чек-листы по всем имеющимся в стандарте 10 направлениям, причём, каждый из вопросов $S_i(n)$ ставится в соответствие с решаемой функцией (функциями) F_{11} … F_{53}, в виде матрицы соответствия (табл. 4). Следует достигать максимальной связности показателей и функций, для чего вычисляется общее количество соответствий по горизонталям t и вертикалям k.

Таблица 4. Матрица соответствия функций защиты по чек-листам

	F_{11}	……	……	……	F_{53}	Итого
S_1 (1)	+					t_1 (1)
S_i (1)		+	+			……
……	……	……	……	……	……	……
S_1 (2)			+			……
S_i (2)		+		+		……
……	……	……	……	……	……	……
S_1 (3)					+	……
S_i (3)	+					t_i (3)
Итого	k_1	……	……	……	k_{15}	-

Вычисляются суммы всех ответов для каждого уровня:

$$C_N = \sum t(j)_i,$$

где j – текущий уровень.

Вычисляются количество соответствий ответов и функций:

$$D_i = \sum S(j)_i,$$

Релевантность составленной модели оценивается по принципу однородности, т.е. полученные значения C_N и D_i не должны существенно отличаться друг от друга (для случая с 15-ю функциями F_{11} … F_{53}, C_N ориентировочно лежит в диапазоне 3 … 5).

В процессе проверки аудитор для выявления адекватности и действенности мер по защите информации, может также включать в чек-листы проверочные мероприятия (либо организовать их в виде отдельной программы исследования безопасности). К таким мероприятиям могут относиться тесты на стойкость организационной структуры к информационно-психологическим или информационно-техническим воздействиям.

И если оценка стойкости к информационно-техническим воздействиям проводится в рамках технического и инструментального аудита, то оценка стойкости к информационно-психологическим воздействиям может оказаться полезным дополнением к документарному аудиту для выявления практического уровня стойкости коллектива организации в отношении угроз информационной безопасности. Такие тестовые мероприятия могут быть разработаны аудитором на основе структурных моделей социально-психологических угроз безопасности информации.

Предложенный метод проведения аудита заключается в формализации матрицы защиты и разработке объективных чек-листов. При этом сформированы принципы составления таких чек-листов и оценки их релевантности.

Таким образом, аудит информационной безопасности на основе сформированной и описанной модели, при его практическом применении даст не только объективный повторимый и однозначный результат оценки уровня информационной безопасности организации, но и позволит выявить слабые стороны в системе защиты и сформировать рекомендации по повышению уровня защищённости объекта. Поэтому применение данной модели целесообразно при проведении аудита информационной безопасности в государственных структурах.

Заключение

В данной работе сформирована формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов, которая базируется на принципах независимости и объективности аудиторской деятельности.

Предложен подход, опирающийся на систему объективных показателей, сопоставимых с функциями защиты, и заключающийся в формировании чек-листов с соответствующими критериями соотнесения показателей и методами подтверждения фактов, выявляемых в результате аудиторской проверки.

На основе предложенной модели возможна разработка чек-листов применительно для любого стандарта и нормативного документа, на предмет соответствия, которому может быть востребовано проведение аудиторской проверки.

СПИСОК ЛИТЕРАТУРЫ:

1. Сиротский А.А. Метрический подход к оценке информационной безопасности в организациях банковской сферы. Системы безопасности, 2016. №25. С. 126–129. URL: https://www.elibrary.ru/item.asp?id=28884138 (дата обращения: 01.04.2021).
2. Курило А.П. и др. Построение структуры показателей эффективности противодействия угрозам информационной безопасности в интересах оценки защищенности информационных. Безопасность информационных технологий, [S.l.], Т. 17. № 2. С. 16–18. 2010. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/720 (дата обращения: 01.04.2021).
3. Сиротский А.А. Технологии конкурентоспособного управления предприятиями машиностроения. Ученые записки РГСУ, 2013. №5. Т. 2. С. 177–181. URL: https://www.elibrary.ru/item.asp?id=21408309 (дата обращения: 01.04.2021).
4. Hajo A. Reijers. Business Process Management: The evolution of a discipline, Computers in Industry, Vol. 126, 2021, 103404, ISSN 0166-3615. DOI: https://doi.org/10.1016/j.compind.2021.103404.
5. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности, 2018. №1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения: 01.04.2021). DOI: http://dx.doi.org/10.24411/2410-9916-2018-10101.
6. Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security. Vol. 68, 2017. P. 145–159, ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.04.009.
7. Nelli V. Syreyshchikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing. Vol. 32, 2019. P. 278–285. ISSN 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2019.02.215.
8. Oladko V.S The Model of Information Security Audit in the Information Systems of E-Commerce Type of B2E // Sochi Journal of Economy, 2016. Vol. 4, Issue 2. P. 117–126. URL: https://www.elibrary.ru/item.asp?id=26747087 (дата обращения: 01.04.2021).
9. Воеводин В.А. Эталонная модель аудита информационной безопасности // Информатика, вычислительная техника и управление, серия «Естественные и технические науки», 2019. №9. С. 56–61. URL: http://www.nauteh-journal.ru/files/718b40fd-8a0d-4d9b-ace4-c9f2c25cbb98 (дата обращения: 12.08.2021).
10. Liudmila Liutsko, Josep Maria Tous, Aleksander Veraksa, Sergey Leonov, Proprioceptive Indicators (Precision, Speed and Personality) of Age-depended Differences for Traffic Security, Procedia - Social and Behavioral Sciences, Volume 187, 2015. P. 491–496. ISSN 1877-0428. DOI: https://doi.org/10.1016/j.sbspro.2015.03.092.
11. Dontsov A.I., Drozdova A.V., Gritskov Y.V. Visual Culture and Personality Psychological Security, Procedia - Social and Behavioral Sciences. Vol. 86, 2013. P. 70–75. ISSN 1877-0428. DOI: https://doi.org/10.1016/j.sbspro.2013.08.527.
12. Дураковский А.П., Петров В.Р. О защите персональных данных в СКУД. Безопасность информационных технологий, [S.l.]. Т. 19, № 1. С. 95–97, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/547.
13. Сиротский А.А. Исследование угроз и организация менеджмента информационной безопасности в финансово-кредитных организациях // Информационные технологии. Радиоэлектроника.

Телекоммуникации (ITRT-2016): сб. статей VI международной заочной научно-технической конференции. Ч.2. / Поволжский гос. ун-т сервиса. – Тольятти: Изд-во: ПВГУС, 2016. С. 213–221. URL: https://ies.unitech-mo.ru/files/upload/publications/15844/a0d8c6cae8ae62dea212e274d18ba2ef.pdf (дата обращения: 01.04.2021).

14. Бабуркина А.С., Широкова С.В., Ильяшенко О.Ю. Разработка процедуры проведения аудита безопасности информационной системы для ООО «Клиника современной косметологии» / Фундаментальные и прикладные исследования в области управления, экономики и торговли. Сборник трудов научной и учебно-практической конференции. СПб., 2017. С. 15–22. URL: https://elibrary.ru/item.asp?id=29373585 pdf (дата обращения: 01.04.2021).
15. Зефиров С.Л., Щербакова А.Ю. Оценка информационной безопасности объекта при проведении аудита информационной безопасности / Информационные системы и технологии ИСТ-2020. Сборник материалов XXVI Международной научно-технической конференции. Нижегородский государственный технический университет им. Р.Е. Алексеева. Н. Новгород, 2020. С. 517–522.
16. Лившиц И.И. Методика определения активов при внедрении и сертификации СМИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001-2006 и СТО Газпром серии 4.2 // Вопросы защиты информации, 2015. № 4(111). С. 43–51. URL: https://elibrary.ru/item.asp?id=25484325 pdf (дата обращения: 01.04.2021).
17. A.J. Burns, Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, Computers in Human Behavior. Vol. 68, 2017. P. 190–209. ISSN 0747-5632. DOI: https://doi.org/10.1016/j.chb.2016.11.018.
18. Ткачева А.Ю., Вигдорчик И.Э., Дубовик А.И. Аудит информационной безопасности и материально-техническое обеспечение ОВД как меры обеспечения информационной безопасности в ОВД // Успехи современной науки, 2016. №10. Т. 2. С. 102–104. URL: https://elibrary.ru/item.asp?id=27433173 pdf (дата обращения: 01.04.2021).

REFERENCES:

[1] Sirotskiy A.A. Metric approach to assessing information security in banking organizations. Sistemy bezopasnosti, 2016. No. 25. P. 126–129. URL: https://www.elibrary.ru/item.asp?id=28884138 (accessed: 01.04.2021) (in Russian).
[2] Kurilo A.P. et al. Construction of Structure of Indicators of Efficiency of Counteraction to Threats of Information Safety in Interests of the Estimation of Security of Information Processes in Computer Systems. IT Security (Russia), [S.l.]. Vol. 17, no. 2. P. 16–18, 2010. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/720 (accessed: 01.04.2021) (in Russian).
[3] Sirotskiy A.A. Technologies of competitive management of engineering enterprises. Uchenye zapiski RSSU, 2013. No. 5. Vol. 2. P. 177–181. URL: https://www.elibrary.ru/item.asp?id=21408309 (accessed: 01.04.2021) (in Russian).
[4] Hajo A. Reijers, Business Process Management: The evolution of a discipline, Computers in Industry, Vol. 126, 2021, 103404, ISSN 0166-3615. DOI: https://doi.org/10.1016/j.compind.2021.103404.
[5] Makarenko S.I. Information security audit: milestones, conceptual framework, classification of activities. Sistemy upravleniya, svyazi i bezopasnosti, 2018. No. 1. P. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (accessed: 01.04.2021). DOI: http://dx.doi.org/10.24411/2410-9916-2018-10101 (in Russian).
[6] Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security. Vol. 68, 2017. P. 145–159, ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.04.009.
[7] Nelli V. Syreyshchikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing. Vol. 32, 2019. P. 278–285. ISSN 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2019.02.215.
[8] Oladko V.S. The Model of Information Security Audit in the Information Systems of E-Commerce Type of B2E. Sochi Journal of Economy, 2016. Vol. 4, Issue 2. P. 117–126. URL: https://www.elibrary.ru/item.asp?id=26747087 (accessed: 01.04.2021).
[9] Voevodin V.A. Reference model of information security audit. Computer Science, computer engineering and management, series "Natural and Technical Sciences", 2019. No. 9. P. 56–61. URL: http://www.nauteh-journal.ru/files/718b40fd-8a0d-4d9b-ace4-c9f2c25cbb98 (accessed: 12.08.2021) (in Russian).
[10] Liudmila Liutsko, Josep Maria Tous, Aleksander Veraksa, Sergey Leonov, Proprioceptive Indicators (Precision, Speed and Personality) of Age-depended Differences for Traffic Security, Procedia - Social and Behavioral Sciences. Vol. 187, 2015. P. 491–496, ISSN 1877-0428. DOI: https://doi.org/10.1016/j.sbspro.2015.03.092.

[11] Dontsov A.I., Drozdova A.V., Gritskov Y.V. Visual Culture and Personality Psychological Security, Procedia - Social and Behavioral Sciences. Vol. 86, 2013. P. 70–75. ISSN 1877-0428. DOI: https://doi.org/10.1016/j.sbspro.2013.08.527.

[12] Durakovskiy A.P., Petrov V.R. On the Protection of Personal Data in the Access Control System. IT Security (Russia), [S.l.]. Vol. 19, no. 1. P. 95–97, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/547 (in Russian).

[13] Sirotskiy A.A. Threat Research and Organization of Information Security Management in Financial and Credit Organizations. Informacionnye technologii. Radioelectronika. Telekommunikacii (ITRT-2016): Articles of the VI International Correspondence Scientific and Technical Conference. Vol. 2. Povolzhskiy gos. Un-t servisa. – Toliatti: PVGUS, 2016. P. 213–221. URL: https://ies.unitech-mo.ru/files/upload/publications/15844/a0d8c6cae8ae62dea212e274d18ba2ef.pdf (accessed: 01.04.2021) (in Russian).

[14] Baburkina A.S., Shirokova S.V., Ilyashenko O.Yu. Development of procedure of information system security audit for OOO "Clinic of modern cosmetology". Fundamentalnye I prikladnye issledovaniya v oblasti upravleniya, ekonomiki i torgovli. Collection of works of scientific and educational-practical conference. SPb., 2017. P. 15–22. URL: https://elibrary.ru/item.asp?id=29373585 (accessed: 01.04.2021) (in Russian).

[15] Zefirov S.L., Scherbakova A.Yu. Assessment of information security of an object during an information security audit / Informacionnye sistemy I technologii IST-2020. Collection of materials of the XXVI International Scientific and Technical Conference. Nizhny Novgorod State Technical University named after R.E. Alekseev. N. Novgorod, 2020. P. 517–522 (in Russian).

[16] Livshits I. I. Methods of assets determination for ISMS implementation and certification in accordance with the requirements GOST R ISO/IEC 27001-2006 and STO Gazprom series 4.2. Voprosy zaschity informacii, 2015. № 4(111). P. 43–51. URL: https://elibrary.ru/item.asp?id=25484325 (accessed: 01.04.2021) (in Russian).

[17] A.J. Burns, Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, Computers in Human Behavior. Vol. 68, 2017. P. 190–209, ISSN 0747-5632. DOI: https://doi.org/10.1016/j.chb.2016.11.018.

[18] Tkacheva A.Yu., Vigdorchik I.E., Dubovik A.I. Information security audit and OVD logistics as information security measures in OVD. Uspehi sovremennoi nauki, 2016. No. 10. Vol.2. P. 102–104. URL: https://elibrary.ru/item.asp?id=27433173 (accessed: 01.04.2021) (in Russian).

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

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

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

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

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами, кегель 12); далее сведения об авторах – организация с почтовым адресом, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив, кегель 11); затем название статьи (по центру, ПРОПИСНЫМИ буквами, кегель 12), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом, кегель 11) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив, кегель 11); аннотация (100 – 250 слов, по ширине, строчными буквами – см. **правила оформления аннотации**);

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

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

– в статью включают **Введение** и **Заключение**, а также вводятся **Разделы** с их нумерацией (прописные по центру, полужирно, кегль 12);

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

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы литературы (по ширине, строчные, кегль 10), оформленный в соответствии с действующими стандартами и указанием идентификатора DOI (как правило, не менее 15 наименований в научной статье и 50 в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные авторов и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации на латиницу.

Правила оформления аннотации

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

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

Аннотация включает следующие аспекты содержания статьи**:**

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

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

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

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

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

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

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи

и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

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

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (файл *.doc) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

The articles submitted to the editors must meet the following requirements:

– the topic of the article should be relevant, have scientific or practical significance and be published by the authors for the first time;

– the manuscript should be formatted only in * .doc or pdf format, A4 strip, size 12, TimesNewRoman font, one-and-a-half interval;

– in the beginning of the article there are information about the article in English: I.O. Name of authors (centered, lower case); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– further information on the article is in Russian: I.O. The authors' surname (for jubilus, lower case letters); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– then the text of the article is in Russian or English, size 12, interval one and a half, the recommended total volume of the article should not exceed 10 pages, including tables, illustrations;

– at the end of the article the LIST OF LITERATURE is given, in which the bibliographic list of sources of literature is indicated, drawn up in accordance with the current standards (as a rule, not less than 15 titles);

– after the list of literature is REFERENCES, in which these bibliographic sources should be written in Latin (ie Latin letters).

Rules to write a scientific abstract

Abstract is a source of information about the content of the paper and its research results. The structure of the abstract should correspond to the structure of the paper and should be not less than 100 words, but not more than 250 words.

The abstract includes the following aspects of the paper:

- subject and purpose of the paper;
- method or methodology described in the paper;
- results;
- discussion.

The abstract plays the following role:

- allows you to establish the main content of the paper, determine its relevance and decide whether to read the full text of the paper;
- provides information about the paper and eliminates the need to read the full text of the paper if the paper is of secondary interest to the reader;
- used in information systems, including automated ones, to search for documents and information (title, abstract and keywords are translated into English, and foreign readers judge the content of the paper by them).

The abstract should be informative (not contain general wordings) and original. The information contained in the title of the paper should not be repeated in the text of the abstract. The text of the abstract should not contain an interpretation of the content of the paper, criticisms and the author's point of view, as well as information that is not included in the paper. You should avoid unnecessary introductory phrases (for example, " the author is considering..."). Historical references, if they do not constitute the main content of the paper, the description of previously published works and well-known provisions are not given in the abstract.

The text of the abstract should use syntactic constructions peculiar to the language of scientific and technical documents, avoid complex grammatical structures.

The text of the abstract should use significant (key) words from the text of the paper.

The method or methodology of the work should be described if they are new or of interest from the point of view of this work. In the abstract of the paper describing the experimental work, indicate the data sources and the specific features of their processing.

The results are described very accurately and informative. The main theoretical and experimental results, actual data, discovered interrelations and regularities are presented. At the same time, preference is given to new results and data of long-term importance, important discoveries, conclusions that refute existing theories, as well as data that, in the author's opinion, have practical value.

Conclusions may be accompanied by recommendations, assessments, suggestions, hypotheses described in the paper.

Terms of publication of the article

– the article should be sent by e-mail;

– the editorial board of the journal follows the ethical standards adopted in the international scientific community, relying on the recommendations of the Ethics Committee of scientific publications that do not contradict the norms of Russian legislation in the field of regulation of the activities of the media and copyright;

– articles that do not meet the requirements for presentation and processing are not considered or published;

– in one issue of the journal, as a rule, only one author's article is published, including co-authors;

– authors should provide only original works, if text or graphic information obtained from other persons is used, references to the relevant publications or the author's written permission are necessary;

– the decision to publish the manuscript is made by the editorial board on the basis of the result of peer review and expert evaluation by qualified specialists in the field of information security;

– in the case of receipt of the manuscript for publication, the author must promptly give answers to editorial questions related to comments on the article;

– in case of refusal to publish, the editorial board should provide the author with a copy of the review and justification for refusing the publication;

– submitting an article to more than one journal is simultaneously regarded as unethical behavior and is unacceptable;

– articles are published for free.

Rules for publication of texts

1. Articles must be submitted electronically (* .doc or * .rtf) with a printout (or a file in * .pdf format) - to avoid inaccuracies in reading the formulas.
2. Pictures, graphics, photographs and other types of illustrations should, if possible, not only be included in the text, but also separate files in the original format (not integrated into the Word document).
3. Abbreviations and abbreviations, which are not on the list of abbreviations, should be disclosed (in parentheses or in a footnote).
4. By providing links to formulas, expressions or restrictions in the text of the article, please make sure that the relevant objects in the article are numbered and numbered.
5. References to the literature should be given in the text in square brackets, in the case of citations, with pages.
6. When preparing a list of literature, it is desirable to pay attention to the availability of output data of works and to avoid repeated instructions of the same work under different numbers.
7. References to laws, regulations, confessions and so on should be indicated in the prescribed form: the Law of the Russian Federation "__" of x month xxxx, No. ___. Art. ___.
8. Foreign words, terms and surnames, the spelling of which allows variants, please write within the same article the same way.

Submission Preparation Checklist

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the "About the journal" page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Privacy Statement

The names and email addresses entered in this journal site page will be used exclusively for the purposes specified by this journal and will not be used for any other purposes or will not be given over to another individuals and organizations.

СПИСОК СОКРАЩЕНИЙ, ПРИНЯТЫХ В ЖУРНАЛЕ

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
БЧ – блокчейн
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КПО – комплекс программного обеспечения
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОКСО – Общероссийский классификатор специальностей по образованию
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СБЧ – система блокчейн
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись
ФГОС – федеральный государственный образовательный стандарт
ФУМО ИБ – федеральное учебно-методическое объединение по образованию в области информационной безопасности

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 8277

Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 8277
E-mail: BIT@mephi.ru
Сайт журнала: https://bit.mephi.ru

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

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

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Ответственный редактор И.М. Ядыкин
Технический редактор П.А. Золотухина

Подписано в печать 01.09.2021. Формат 60x84 1/8
Печ. л. 15,5. Уч.-изд. л. 15,5. Тираж 500 экз. Изд. № 002 – 3

Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»
(АО «ЭНПО СПЭЛС»)
Каширское ш., 31, строение 44, этаж 3, пом. IV, ком. 4, Москва, 115409, Россия

Joint Stock Company «Experimental Scientific and Production Association
SPECIALIZED ELECTRONIC SYSTEMS»
(JSC «ENPO SPELS»)
Kashirskoe shosse, 31, building 44, floor 3, pom. IV, room 4, Moscow, 115409, Russia

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