Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2024-1-104-122

ВЫЯВЛЕНИЕ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ СИСТЕМАТИЧЕСКОГО ОБЗОРА ЛИТЕРАТУРЫ

Брюханов Владислав Андреевич.
Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, Россия.
✉Грызунов Виталий Владимирович;
Шестаков Александр Викторович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉viv1313r@mail.ru

Аннотация. Область информационной безопасности охватывает широкий спектр технических, организационных и социальных аспектов, требуя от специалистов по защите информации уникального и всестороннего подхода при разработке, поддержке, эксплуатации, оценке и совершенствовании систем управления информационной безопасностью. Важным элементом успешной защиты информации является точная идентификация и оценка рисков и уязвимостей, которые могут стать источником угроз. В существующих публикациях, как правило, подразумевается, что специалисты обладают необходимыми опытом и знаниями для проведения риск-анализа. Однако в динамичном мире информационных технологий и угроз, специалист по информационной безопасности сталкивается с огромным объемом информации и потенциальными рисками, которые непрерывно эволюционируют. В силу этого держать в голове всевозможные угрозы информационной безопасности непосильная задача.

На основе метода систематического обзора литературы выявлены актуальные проблемы информационной безопасности, потенциально выступающие источниками риска информационной безопасности. В частности, выявлено 73 актуальные проблемы информационной безопасности, которые должен учитывать в своей деятельности специалист по защите информации. Понимание этих проблем позволяет разрабатывать более эффективные стратегии защиты, а также принимать обоснованные и взвешенные решения при разработке и применении мер безопасности.

Ключевые слова: идентификация рисков, информационная безопасность, защита информации, поддержка принятия решений, управление информационной безопасностью, источники риска, актуальные угрозы

Для цитирования: Брюханов В.А., Грызунов В.В., Шестаков А.В. Выявление проблем информационной безопасности методом систематического обзора литературы // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 1. С. 104–122. DOI: 10.61260/2218-13X-2024-1-104-122.

Research article

IDENTIFICATION OF INFORMATION SECURITY PROBLEMS BY A SYSTEMATIC LITERATURE REVIEW

Bryukhanov Vladislav A.
Emperor Alexander I Saint-Petersburg state transport university, Saint-Petersburg, Russia.
✉Gryzunov Vitaly V.;
Shestakov Alexander V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉viv1313r@mail.ru

Abstract. The field of information security covers a wide range of technical, organizational and social aspects, requiring information security specialists to take a unique and comprehensive approach to the development, support, operation, evaluation and improvement of information security management systems. An important element of successful information protection is the accurate identification and assessment of risks and vulnerabilities that may become a source of threats. In existing publications, as a rule, it is assumed that specialists have the necessary experience and knowledge to conduct risk analysis. However, in the dynamic world of information technology and threats, an information security specialist faces a huge amount of information and potential risks that are constantly evolving. Because of this, it is an impossible task to keep in mind all kinds of threats to information security.

The purpose is to identify actual problems of information security, potentially acting as sources of information security risk, based on the method of systematic review of the literature. Results: 73 actual problems of information security have been identified, which an information security specialist should take into account in his activities. Understanding these issues makes it possible to develop more effective protection strategies, as well as to make informed and informed decisions when developing and applying security measures.

Keywords: risk identification, information security, information protection, decision support, information security management, risk sources, current threats

For citation: Bryukhanov V.A., Gryzunov V.V., Shestakov A.V. Identification of information security problems by a systematic literature review // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 1. P. 104–122. DOI: 10.61260/2218-13X-2024-1-104-122.

Введение

Информационные технологии, используемые человечеством, трансформировались от громоздких мэйнфреймов с перфокартами к облачным технологиям хранения и обработки данных и применению ботов, от кнопочных телефонов – к смартфонам со встроенными электронными сим-картами, от бытовой техники и простых станков – к устройствам Интернета вещей (*IoT*) и Интернету промышленных вещей (*IIoT*), от аналитических и творческих способностей человека – к технологиям искусственного интеллекта, близким к возможностям человека в некоторых областях.

Развитие технологий порождает лавинообразный рост потоков передаваемых данных и обусловливает возникновение новых угроз информационной безопасности (ИБ). Злоумышленники активно используют преимущества новых технологий в своих целях [1], сокращают затраты времени на планирование, подготовку и реализацию атак. Это проявляется не только в количестве, но и в качестве угроз. Они становятся более интеллектуальными и сложными.

На этапе идентификации рисков специалист ИБ постоянно задаёт себе вопрос: «Что ещё я не учел, и с какими проблемами ИБ организация и пользователи могут столкнуться в будущем?». При этом по большей части, как показывают результаты анализа существующих практик поиска, сбора и механизмов обработки данных об уровне защищенности информационной инфраструктуры, объектов информатизации, информационных объектов и процедур выявления рисков ИБ, идентификация рисков опирается исключительно на опыт и мировоззрение специалиста ИБ, выполняющего идентификацию. Опыт других исследователей зачастую остаётся за пределами его внимания.

Настоящее исследование направлено на выявление актуальных проблем ИБ, опираясь на которое, процесс идентификации рисков станет системным и обоснованным.

Systematic Literature Review (SLR): проблемы информационной безопасности

Процесс исследования разделен на три этапа:
1. Поиск и отбор литературы.
2. Анализ литературы.
3. Обобщение результатов, формирование заключения исследования.

SLR: Поиск и отбор

В процессе исследования выявлено, что некоторые авторы освещают проблемы информационной безопасности через задачи, которые предстоит решить, поэтому в итоговом запросе к базам данных использовались и «проблемы ИБ», и «задачи ИБ».

Описание процесса поиска и отбора методом *SLR* представлено в табл. 1.

Таблица 1

Систематический обзор литературы проблем ИБ

№	Этап	Входные данные	Обоснование	N
1	Выбор цифровых библиотек	– *eLibrary.ru* – *Google* Академия	В рамках первой попытки осуществить *SLR* были выбраны общедоступные цифровые библиотеки. Данные ресурсы включают и журналы из перечня ВАК, и источники проиндексированных в международных базах данных *SCOPUS, WoS* и др.	–
2	Определение поисковых запросов	– «Проблемы информационной безопасности» | «задачи информационной безопасности» | «*information security problem*» | «*information security task*»	Большинство научных статей использует термин «информационная безопасность», а потому принято решение не использовать сокращения «ИБ», «инфобез»	**~22863**
3	Критерии включения и исключения	× Исследованию больше пяти лет × Исследование написано не на русском/английском языке × Отсутствует полный доступ × Не статья в журнале ✓ В названии публикации, ключевых словах или аннотации присутствуют искомые фразы	Указанные критерии подбирались на основании поставленной цели исследования «охватить МНОЖЕСТВО АКТУАЛЬНЫХ проблем…»	**143**
4	Удаление дубликатов	– Итого дубликатов найдено: 13	–	**130**

N – количество рассматриваемых статей

Итого в результате поиска было отобрано 130 научных исследований для процедуры дальнейшего анализа и синтеза полученной информации.

SLR: Анализ

Не каждая статья содержала актуальные или искомые данные, а некоторые исследования дублировали друг друга. В результате анализа разработана интеллект-карта проблем ИБ (рис.), а также табл. 2, описывающая суть указанных проблем. Следует отметить, что разработанная интеллект-карта не является классификацией и содержит некоторую агрегацию данных из отобранных публикаций.

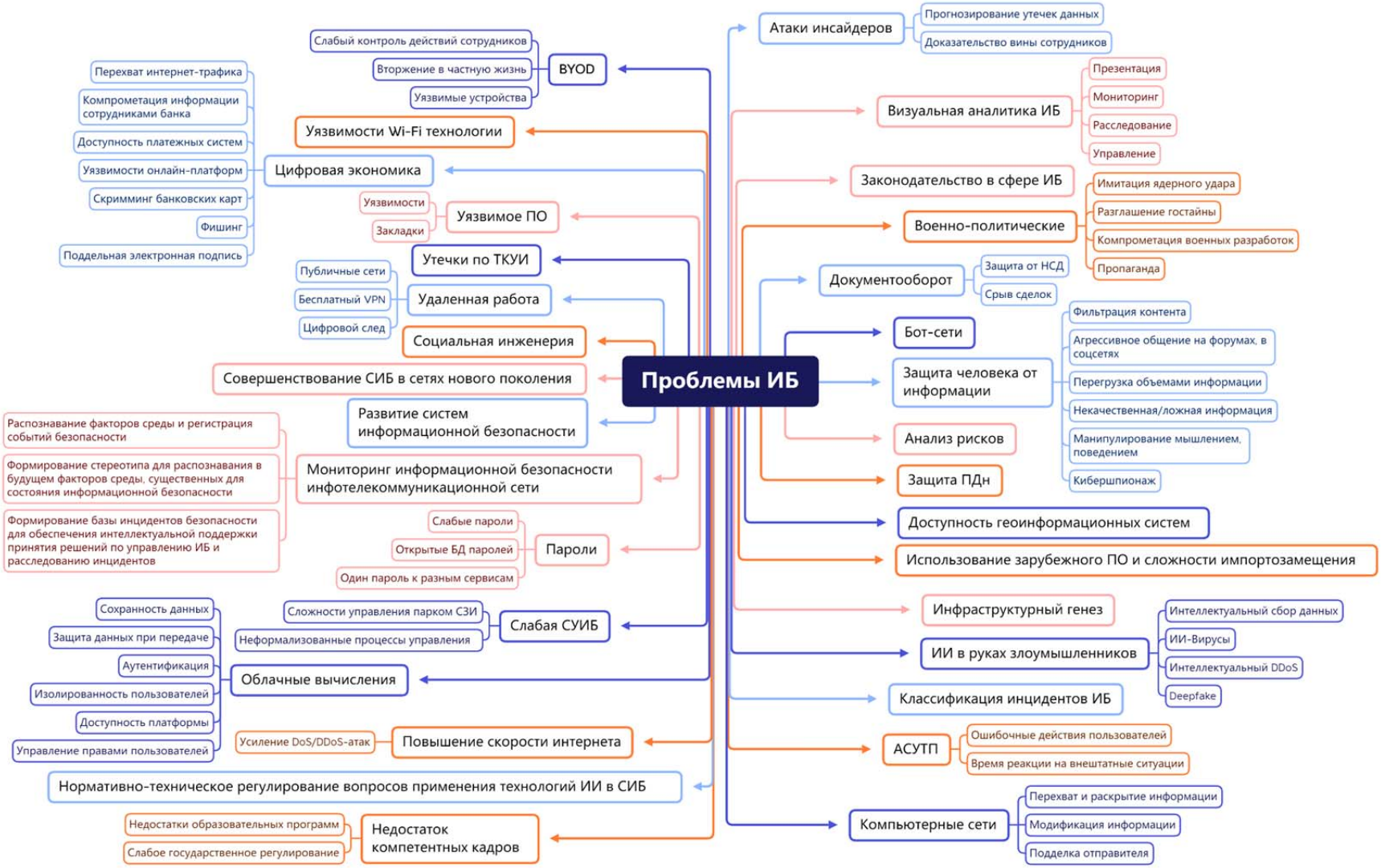

Рис. **Интеллект-карта проблем ИБ (ИИ – искусственный интелект; ПДн – персональные данные; ПО – программное обеспечение; БД – база данных; СЗИ – средства защиты информации; АСУТП – автоматизированная система управления технологическим процессом; СУИБ – система управления ИБ; ТКУИ – техничсекий канал утечки информации; СИБ – система ИБ; НСД – несанкционированный доступ)**

Таблица 2

Проблемы ИБ

№	Проблема ИБ	Описание
1	Анализ рисков [2–4]	Анализ рисков необходим для определения направлений развития системы защиты информации. Процесс анализа рисков требует задействования компетентных специалистов разных профилей. Однако собрать такую группу экспертов очень сложно, отчего оценка рисков может быть не точной. Кроме того, отсутствует единая методика расчета информационных рисков
2	АСУТП	
2.1	Ошибочные действия пользователей [5]	Некорректные действия пользователей могут привести к сбоям в системе и серьезным последствиям, таким как прекращение производственного процесса, повреждение оборудования и т.д.
2.2	Время реакции на внештатные ситуации [5]	Время реакции на аварии и сбои имеет решающее значение для минимизации ущерба и приведения системы в штатное состояние
3	Атаки инсайдеров	
3.1	Прогнозирование утечек данных [6]	Раньше системы мониторинга событий ИБ действовали по принципу скорейшего устранения последствий, однако бизнес нуждается в средствах защиты, способных на ранних этапах выявлять потенциальную атаку
3.2	Доказательство вины сотрудников [6]	*DLP*-системы отличное средство для детектирования несанкционированных действий сотрудников. Однако практика судебных разбирательств показательна в том плане, что не любая информация может служить доказательной базой [7]. Если в процессе расследования инцидента будет нарушена тайна личной переписки и любая чувствительная информация, то организации и специалистам по ИБ грозят существенные санкции
4	Бот-сети [8]	Ботнет предоставляет огромные вычислительные возможности для генерации *DDoS*-атак
5	Визуальная аналитика ИБ	
5.1	Презентация [9]	Наглядная демонстрация упрощает процесс понимания сложных данных, связанных с ИБ. С помощью графиков и диаграмм возможно выявить тренды и прогнозы в отношении различных аспектов ИБ организации. Наглядные показатели могут быть использованы в отчетах и документах для прозрачного представления работы служб ИБ
5.2	Мониторинг [9]	Визуальное отображение данных необходимо для повышения эффективности мониторинга состояния системы ИБ и принятия мер в случае возникновения угроз
5.3	Расследование [9]	Использование визуализации для поиска связей и паттернов в данных, связанных с инцидентами ИБ, помогает исследователям лучше понимать инцидент и принимать меры для предотвращения подобных ситуаций в будущем
5.4	Управление [9]	Визуализация помогает принимать обоснованные решения в области ИБ
6	Военно-политические	
6.1	Имитация ядерного удара [10]	Подобным методом злоумышленники могут вызвать панику

		и ответные действия «атакуемой» стороны
6.2	Разглашение гостайны [10]	Раскрытие государственной тайны может нанести непоправимый ущерб национальной безопасности
6.3	Компрометация военных разработок [10]	Информации о разработках, применяемых в военных целях, может быть использована противником для создания противодействующих средств или улучшения своего вооружения
6.4	Пропаганда [10–13]	Ложная или искаженная военно-политическая информация оказывает сильное влияние на настроения в обществе и формирует напряженную политическую обстановку
7	Документооборот	
7.1	Защита от НСД [14]	Проблема заключается в том, что злоумышленники могут получить НСД к конфиденциальным и чувствительным данным посредством кражи учетных записей и ключей доступа
7.2	Срыв сделок [14]	Перегрузка облачных сервисов электронного документооборота, нарушение целостности отправляемых документов, взлом учетных записей отправителей организации могут привести к срыву сделок и крупным репутационным и материальным потерям организаций
8	Доступность геоинформационных систем [15–17]	Геоинформационные системы как информационные системы, обрабатывающие пространственные данные, лежат в основе практически всех информационных систем. Нарушение доступности их ресурсов влечёт за собой нарушение работы систем ИБ и обеспечение других аспектов ИБ: целостности, конфиденциальности и т.д., становится невозможным
9	Законодательство в сфере ИБ [18–20]	Проблема связана с излишними, недостаточными или неактуальными требованиями ИБ. С одной стороны, не все организации в виду малых бюджетов могут позволить себе соответствовать действующим нормативно-правовым актам. С другой, выполнение требований не гарантирует должную степень защищенности, отчего крупные компании предпочитают использовать риск-ориентированные модели построения системы защиты
10	Защита персональных данных [21–24]	Практически каждая компания так или иначе осуществляет обработку персональных данных, а потому обязана следовать требованиям законодательства по защите персональных данных
11	Защита человека от информации	
11.1	Фильтрация контента [23–27]	Одним из важнейших направлений государства является защита человека, а особенно молодого поколения от неуместного контента, такого как пропаганда насилия, порнография и др.
11.2	Агрессивное общение на форумах, в соцсетях [26–28]	Проблема, которая может привести к дискриминации, кибербуллингу и другим формам онлайн-насилия
11.3	Перегрузка объемами информации [27]	С каждым годом интернет все больше напоминает свалку всевозможной информации, в том числе ложной. Десятки тысяч страниц, генерируемых поисковыми системами, являются избыточными для восприятия пользователя
11.4	Некачественная/ложная информация [27]	
11.5	Манипулирование мышлением, поведением [11, 26, 29]	Проблема, связанная с использованием алгоритмов рекомендации в целях воздействия на поведение и мышление личности
11.6	Кибершпионаж [25, 26]	Проблема связана с кражей личной информации, путем взлома

		аккаунтов или перехвата персональных данных
12	ИИ в руках злоумышленников	
12.1	Интеллектуальный сбор данных [30]	Злоумышленники могут использовать технологии ИИ для сбора, анализа и сортировки большого объема данных из различных источников, включая социальные сети, открытые БД утечек информации и др.
12.2	ИИ-Вирусы [30]	Вирусы могут использовать алгоритмы машинного обучения и другие методы ИИ для адаптации к различным условиям программной среды в целях противодействия обнаружению антивирусными средствами защиты
12.3	Интеллектуальный *DDoS* [30]	Технологии ИИ могут быть использованы для создания более эффективных и сложных атак на отказ в обслуживании. Такие атаки могут использовать инструменты для адаптации к защите
12.4	*Deepfake* [30]	ИИ научился динамически подменять данные видеокамер с точностью, достаточной для компрометации личности. Злоумышленники способны заключать сделки от имени фирмы, притворяясь уполномоченным лицом, а также наносить ущерб репутации людей в целях кибербуллинга
13	Инфраструктурный генез [31]	В процессе своего развития информационные системы становятся настолько сложными, что появляется вероятность возникновения деструктивных воздействий инфраструктурного генеза. В этом случае межэлементное взаимодействие внутри информационной системы выступает источником проблем ИБ
14	Использование зарубежного программного обеспечения и сложности импортозамещения [32, 33]	Использование программного обеспечения политически мотивированных иностранных организаций ведет к существенным рискам. В современных реалиях российские компании вынуждены планировать переход на отечественные решения. Однако заместить все используемое зарубежное ПО и оборудование российскими аналогами – трудоемкая задача
15	Классификация инцидентов ИБ [34]	Классификация инцидентов ИБ необходима для выработки перечня действий по обработке инцидента
16	Компьютерные сети	
16.1	Перехват и раскрытие информации [35]	Нарушение конфиденциальности передаваемых сообщений в следствии перехвата трафика
16.2	Модификация информации [35]	Нарушение целостности передаваемых сообщений в следствие модификации пакетов данных
16.3	Подделка отправителя [35]	Взлом почтовых серверов или регистрация домена, похожего на домен компрометируемой организации, с целью отправки фишинговых писем
17	Мониторинг ИБ инфотелекоммуникационной сети	
17.1	Распознавание факторов среды и регистрация событий безопасности [36]	Задача заключается в постоянном анализе информационной среды и обнаружении любых изменений, которые могут привести к угрозам ИБ. Это могут быть попытки несанкционированного доступа, внедрение вредоносных программ, атаки на сеть и т.д. Регистрация событий безопасности позволяет быстро обнаружить и предотвратить любые потенциальные угрозы
17.2	Формирование стереотипа для распознавания в будущем факторов среды, существенных для	Задача заключается в сборе и анализе информации о факторах, которые могут оказывать влияние на безопасность информации. Это могут быть технологические изменения, изменения в политике безопасности, изменения

	состояния ИБ [36]	в законодательстве и т.д. Формирование стереотипа позволяет быстро распознавать новые угрозы и принимать меры по их предотвращению
17.3	Формирование базы инцидентов безопасности для обеспечения интеллектуальной поддержки принятия решений по управлению ИБ и расследованию инцидентов [36]	Задача заключается в сборе и анализе информации об инцидентах безопасности, которые произошли в прошлом. Формирование базы данных позволяет изучать причины и последствия произошедших инцидентов, определять эффективность принятых мер и вырабатывать стратегии для предотвращения подобных инцидентов в будущем
18	Недостаток компетентных кадров	
18.1	Недостатки образовательных программ [18]	В новостях часто мелькают сообщения о том, что компании жалуются на подготовку выпускников-специалистов по ИБ. Во многом упрекают действующие образовательные стандарты
18.2	Слабое государственное регулирование [18]	Потребность в специалистах ИБ на текущий момент в разы выше, чем количество обучаемых студентов
19	Нормативно-техническое регулирование вопросов применения технологий искусственного интеллекта в системах ИБ [37]	Общая цель задачи – обеспечить безопасное и эффективное использование искусственного интеллекта в системах ИБ, а также устранить потенциальные угрозы, связанные с неправомерным использованием этой технологии
20	Облачные вычисления	
20.1	Сохранность данных [38, 39]	Данные на облачных серверах должны храниться в виде, исключающем их компрометацию или несанкционированное удаление/изменение
20.2	Защита данных при передаче [38]	При передаче данных облачному сервису необходимо обеспечить сохранность и конфиденциальность информации
20.3	Аутентификация [38]	Пользователь или служба должны пройти аутентификацию на сервере и тем самым подтвердить принадлежность передаваемых данных
20.4	Изолированность пользователей [38, 39]	Данные разных пользователей/организаций могут храниться на одном физическом сервере, однако иметь доступ они должны только к своим данным
20.5	Доступность платформы [39]	Облачные сервисы могут выполнять ключевые функции организации, а отсутствие беспрепятственного доступа чревато большими потерями для бизнеса
20.6	Управление правами пользователей [39]	Сервер должен обеспечить контроль прав пользователей и исключить их неправомерное изменение
21	Пароли	
21.1	Слабые пароли [40]	В любых открытых базах данных паролей присутствуют такие популярные комбинации, как *Admin123, user, love, Qwerty123* и т.д. Использование подобных значений огромный риск для пользователя и организации
21.2	Открытые БД паролей [40]	Хакерские форумы часто публикуют информацию о наличии у них БД паролей определенных компаний. Использование таких баз данных злоумышленниками может нанести непоправимый ущерб жертвам атаки
21.3	Один пароль к разным сервисам [22, 40]	Метод, используемый пользователями сети, для упрощения авторизации. Пользователь придумывает сложный пароль и использует его на всевозможных сервисах, часть из которых может пренебрегать правилами безопасного хранения учетных данных. В результате кражи пароля, злоумышленник получает

		доступ к аккаунтам разных сайтов
22	Повышение скорости интернета	
22.1	Усиление *DoS/DDoS*-атак [41]	DDoS – один из самых простых и эффективных видов атак. Повышение скорости интернета может расширить возможности злоумышленников по генерации вредоносного трафика
23	Развитие систем ИБ [42]	Развитие системы ИБ является неотъемлемой частью стратегии ИБ, которая должна постоянно адаптироваться к новым угрозам и требованиям
24	Слабая СУИБ	
24.1	Сложности управления парком средств защиты информации [43]	Для сопровождения эффективной системы управления ИБ необходимы внушительные затраты трудовых, материальных и временных ресурсов. Помочь в решении проблемы может автоматизированное и централизованное управление разнородными средствами защиты информации. Однако универсального способа организации такого решения не существует
24.2	Неформализованные процессы управления [44]	Отсутствие четких правил, регламентов и инструкций может привести к ошибочным, несанкционированным или несвоевременным действиям сотрудников
25	Совершенствование систем ИБ в сетях нового поколения [45]	Задача заключается в обеспечении защиты и конфиденциальности данных, передаваемых по сети, в условиях быстрого развития технологий и увеличения количества угроз
26	Социальная инженерия [46–48]	Атаки с использованием методов социальной инженерии – самый популярный и эффективный способ достижения целей злоумышленников. Она позволяет обходить даже самую дорогостоящую и архитектурно-правильную систему защиты
27	Удаленная работа	
27.1	Публичные сети [48, 49]	Компании, в срочном порядке вынужденные переводить сотрудников на удаленную работу, могут ошибочно или в качестве временного решения разрешить доступ пользователей к инфраструктуре организации через незащищенные сети
27.2	Бесплатный *VPN* [48, 49]	Как только организация осознает опасность передачи корпоративных данных по открытым сетям, то она задумывается о необходимости защиты. И в данном случае проще всего воспользоваться общедоступным *VPN*-сервисом. Однако разработчики бесплатных *VPN*-приложений тоже хотят заработать на своем продукте, а потому в ход идёт реклама, а также сбор и продажа передаваемых данных
27.3	Цифровой след [48]	И даже когда в компании организована частная *VPN*-сеть от сертифицированного криптопровайдера, то и это не гарантирует абсолютную безопасность. Сотрудник может совмещать работу через выделенную *VPN*-сеть и серфинг в интернете. И по итогу цифровой след может содержать как личные, так и корпоративные данные
28	Утечки по ТКУИ [50]	Злоумышленник применяет технические средства (например, электромагнитные излучения, акустические волны, инфракрасное излучение) для получения конфиденциальной информации, передаваемой через компьютерные системы, сети связи, а также другие электронные устройства
29	Уязвимое ПО	

29.1	Уязвимости [51, 52]	Уязвимости, возникающие в процессе разработки, трудно устранимы после выпуска программного обеспечения в производственную среду. Применение методологии безопасной разработки не гарантирует отсутствия уязвимостей в готовом продукте
29.2	Закладки [51, 52]	Программисты из различных соображений могут оставлять закладки в собственных разработках или забывать о их наличии. Данными особенностями кода могут воспользоваться злоумышленники в целях обхода стандартных форм аутентификации
30	Уязвимости *Wi-Fi* технологии [53]	Отсутствие или использование устаревших (*WEP*) протоколов шифрования, слабые пароли точек *Wi-Fi*, использование *PIN*, подделка *mac*-адреса устройства – всё это создаёт угрозу компрометации конфиденциальной информации
31	Цифровая экономика	
31.1	Перехват интернет-трафика [54]	Проблема связана с возможностью злоумышленников перехватывать и анализировать интернет-трафик, который может содержать платежные данные и иную конфиденциальную информацию
31.2	Компрометация информации сотрудниками банка [54, 55]	Сотрудники банка могут раскрывать конфиденциальную информацию третьим лицам вследствие шантажа, подкупа, обиды
31.3	Доступность платежных систем [54]	Проблемы с доступностью платежных систем могут возникнуть из-за технических сбоев, кибератак или других факторов. В результате простоя сервисов могут быть нарушены критичные для бизнеса транзакции, что в итоге сильно отразится на репутации и доверии клиентов к банку
31.4	Уязвимости онлайн-платформ [56]	В следствии уязвимостей кода или используемой системы управления контентом (*CMS*) онлайн-платформы могут стать объектом кибератак и мошенничества
31.5	Скримминг банковских карт [55, 57]	Скримминг является формой мошенничества, при которой злоумышленники получают доступ к данным банковских карт посредством считывания магнитных полос
31.6	Фишинг [55, 57]	Фишинг является одной из самых распространённых форм мошенничества в финансовой сфере, при которой злоумышленники пытаются получить данные банковских карт, посредством поддельных веб-страниц, имитирующих реальные сайты
31.7	Поддельная электронная подпись [20]	Злоумышленник регистрирует фирму «однодневку» и при помощи краденных персональных данных оформляет поддельную электронную подпись
32	*BYOD*	
32.1	Слабый контроль действий сотрудников [58]	Использование сотрудниками собственных устройств затрудняет контроль за их действиями, ввиду потенциальной возможности вторжения в частную жизнь работников. В судебной практике есть прецеденты, когда использование DLP-систем признавалось незаконным [7], вследствие чего организации несли материальные и репутационные потери
32.2	Вторжение в частную жизнь [58]	
32.3	Уязвимые устройства [58]	Личные устройства сотрудников менее защищены в сравнении с корпоративными рабочими станциями с установленным средствами защиты

В результате анализа доступной литературы было выявлено 73 актуальных проблем ИБ.

SLR: Обобщение результатов, формирование заключения исследования

На этом этапе обобщены результаты и сформулированы следующие выводы:

1. Методом систематического обзора литературы подтверждено многообразие направлений деятельности по ИБ.
2. Ряд направлений и отдельные проблемы информационной безопасности перекликаются между собой (например, пункт 28 табл. 2 является составляющей подпункта 31.3 табл. 2).
3. Для эффективного устранения пробелов в системах защиты информации необходим инструмент, способный определять приоритетные направления развития ИБ организации с учетом контекста.
4. Уязвимости новых технологий обязательно станут объектом пристального внимания со стороны злоумышленников.
5. Традиционно известные методы атак, такие как социальная инженерия или регистрация побочных электромагнитных излучений и наводки, не потеряли своей актуальности. Следовательно, можно ожидать рост разнообразия угроз ИБ.
6. Современные и перспективные практики ведения бизнеса (*BYOD*, облачные сервисы, электронный документооборот и т.д.) – потенциальный источник угроз безопасности информации. Организациям стоит учитывать это при смене парадигмы управления.

Заключение

В результате исследования на основе применения метода систематического обзора литературы к выявлению актуальных проблем ИБ проанализировано 130 источников. В итоговую выборку включены данные из 56 источников. Выявлено 73 проблемы ИБ, агрегированные в 32 направления. Результаты настоящего исследования показывают, что применение методического аппарата на основе *SLR* позволяет специалисту в области ИБ подойти к вопросу идентификации потенциальных проблем и оцениванию рисков ИБ организации системно и обоснованно.

Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России по тематике «Киберсреда».

Список источников

1. Как чат-боты ChatGPT изменят кибербезопасность. URL: https://www.kaspersky.ru/blog/chatgpt-cybersecurity/34561/ (дата обращения: 12.02.2024).
2. Бурькова Е.В., Извекова Л.А. Применение метода кластеризации данных для решения задачи оценки рисков информационной безопасности // Национальная безопасность и стратегическое планирование. 2019. № 2 (26). С. 81–86. EDN VPZHMI.
3. Крутов А.Н., Крутова Н.А., Иванчина О.В. Проблема анализа рисков в управлении информационной безопасностью предприятия // Вестник СамГУПС. 2019. № 1 (43). С. 96–103. EDN DZDIEW.
4. Смирнов И.Н. Задачи службы информационной безопасности предприятия в современных условиях // Фундаментально-прикладные проблемы безопасности, живучести, надежности, устойчивости и эффективности систем: материалы II Междунар. науч.-практ. конф., посвящ. 105-летию со дня рождения Адмирала флота СССР дважды героя Советского Союза Сергея Георгиевича Горшкова. Елец: Елецкий гос. ун-т им. И.А. Бунина, 2018. С. 197–200. EDN XTNJNJ.

5. Вольхина М.Н., Стойчин К.Л. Проблемы информационной безопасности в АСУ ТП // Безопасность информационного пространства – 2017. Екатеринбург: Уральский федеральный ун-т имени первого Президента России Б.Н. Ельцина, 2018. С. 96–99. EDN SQLENV.

6. Косов Н.А., Голубов Н.А. Способы защиты от инсайдерских атак // Инновационные решения социальных, экономических и технологических проблем современного общества: сб. науч. статей по итогам круглого стола со всероссийским и международным участием, М.: ООО «КОНВЕРТ», 2021. Т. 8. С. 149–151. EDN TFZVIG.

7. DLP вне закона! Так решил суд! URL: https://lukatsky.ru/legislation/dlp-vne-zakona-tak-reshil-sud.html (дата обращения: 11.01.2024).

8. Чернокнижный Г.М., Лукин Е.И. К вопросу об угрозах ботнет-сетей // Конвергенция цифровых и материальных миров: экономика, технологии, образование: сб. науч. статей Междунар. науч. конф. / под ред. В.В. Трофимова, В.Ф. Минакова. СПб.: С.-Петерб. гос. эконом. ун-т, 2018. С. 225–230. EDN YPXZWX.

9. Визуальная аналитика для информационной безопасности: области применения, задачи и модели визуализации / И.В. Котенко [и др.] // Вопросы кибербезопасности. 2021. № 4 (44). С. 2–15. DOI: 10.21681/2311-3456-2021-4-2-15. EDN LVCIOR.

10. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 2–9. DOI: 10.21681/2311-3456-2019-1-2-9. EDN VWBWZC.

11. Белов Д.Е. Некоторые аспекты проблемы информационной безопасности Российской Федерации // Проблемы массовой коммуникации: новые подходы. 2019. С. 77–79.

12. Жигадло В.Э. Задачи и функции информационной безопасности в условиях информационного противоборства и «ментальных» войн // Информационная безопасность регионов России (ИБРР-2021): материалы XII С.-Петерб. межрегион. конф. СПб.: Регион. общ. организ. «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 21–23. EDN VTGRGO.

13. Лапшинова К.В., Подольская А.А. Проблемы информационной безопасности России в контексте отношения молодежи к информационной войне // Социально-гуманитарные технологии. 2020. № 2 (14). С. 44–53. EDN KXJXAE.

14. Кириленко В.В. Проблемы защиты информации в системах электронного документооборота. 2021. № 4 (34). EDN LKOUGY.

15. Бурлов В.Г., Грызунов В.В., Сипович Д.Е. Адаптивное управление доступностью в геоинформационной системе, использующей туманные вычисления // International Journal of Open Information Technologies. 2021. Т. 9. № 9. С. 76–89.

16. Грызунов В.В. Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 101–115. DOI: 10.31854/1813-324X-2022-8-3-101-116.

17. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability. Informatsionno-upravliaiushchie sistemy [Information and Control Systems]. 2022. № 1. P. 19–29. DOI: 10.31799/1684-8853-2022-1-19-29.

18. Белов Е.Б., Лось В.П., Малюк А.А. Цифровая экономика и актуальные проблемы совершенствования системы подготовки кадров в области информационной безопасности // Безопасность информационных технологий. 2018. Т. 25. № 4. С. 6–22. EDN YQNKMX.

19. Зиновьева В.В. Анализ инцидентов нарушения безопасности конфиденциальной информации в России и мире в I полугодии 2022 года. Правовые проблемы информационной безопасности и пути их решения // Цифровые технологии и право: сб. науч. трудов I Междунар. науч.-практ. конф. / под ред. И.Р. Бегишева [и др.]. Казань: Изд-во «Познание», 2022. Т. 1. С. 107–113. EDN HX: LZCA.

20. Ионкина А.В., Крохалев А.А. Проблемы информационной безопасности в цифровой экономике // Молодежь и наука. 2021. № 7. EDN IMKDYD.

21. Herlambang P.M., dudiyanty T.R. Cybersecurity challenges. in the implementation of a hospital management information system // Eubios journal of Asian and international bioethics. Christchurch. 2017. Vol. 28. № 3. P. 151–154.

22. Маврин А.В. Современные проблемы информационной безопасности, связанные с защитой персональных данных пользователя // StudNet. 2022. Т. 5. № 6. С. 109. EDN GTXRCU.

23. Наумова И.В. Проблемы информационной безопасности образовательного процесса в современных условиях // Безопасная образовательная среда: проблемы проектирования и перспективы развития: сб. науч. трудов по материалам Всерос. науч.-практ. конф. 2018. С. 49–52.

24. Современные проблемы обеспечения информационной безопасности документооборота на предприятии / С.С. Салтыш [и др.] // Безопасность информационного пространства: сб. трудов XIX Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. Екатеринбург: Уральский гос. экон. ун-т, 2021. С. 116–120. EDN RPFRVI.

25. Писаренко В.И., Писаренко И.В. Потенциал педагогической науки в решении проблемы информационной безопасности студентов при взаимодействии с интернет-пространством // На пути цифровизации общества: психологические и педагогические основы: сб. статей по итогам Междунар. науч.-практ. конф. Стерлитамак: ООО «Агентство международных исследований», 2020. С. 29–32. EDN QHLJZK.

26. Фотиева И.В. Этический аспект проблемы информационной безопасности // Нацразвитие: материалы Междунар. науч. конф. СПб., 2020. С. 175–177. DOI: 10.37539/APR290.2020.28.46.008. EDN HGMKPZ.

27. Яковлева В.В., Савчук В.С. Проблемы информационной безопасности несовершеннолетних в образовательном процессе // Социально-экономическое развитие регионов: проблемы и перспективы внедрения инноваций: сб. материалов Межрегион. науч.-практ. конф., посвящ. 50-летию Бурятского филиала СибУПК и 95-летию Бурятского республиканского союза потребительских обществ / под ред. Е.Н. Лищук. Новосибирск: Сибирский ун-т потребительской кооперации, 2018. С. 321–325. EDN EHZYAJ.

28. Фидченко Е.В. Проблемы информационной безопасности человека: философский аспект // Дальневосточная весна – 2019: материалы 17 Междунар. науч.-практ. конф. по проблемам экологии и безопасности. Комсомольск-на-Амуре: Комсомольский-на-Амуре гос. ун-т, 2019. С. 274–276. EDN HFMPYN.

29. Kilishbayevich B.J. Philosophical analysis of manipulation and information security problems // Sustainability of education, socio-economic science theory. 2023. Т. 1. № 6. С. 149–152.

30. Николаев Е.Н. Проблемы информационной безопасности в аспекте развития искусственного интеллекта // 2021. № 48. С. 1428–1434. EDN NDICRE.

31. Максимова Е.А. Методы выявления и идентификации источников деструктивных воздействий инфраструктурного генеза // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 86–99. EDN KTYQJE.

32. Григорьев Д.А. Проблемы информационной безопасности // Системы безопасности: материалы Междунар. науч.-техн. конф. 2019. № 28. С. 128–130. EDN PILHUR.

33. Карасева Т.Н., Мишанин М.А. Проблемы импортозамещения в сфере информационной безопасности // Лучшая исследовательская статья 2023: сб. статей Междунар. науч.-исслед. конкурса. Пенза: Наука и Просвещение, 2023. С. 38–40. EDN QLFXTY.

34. Михайлова Е.А. Решение задачи классификации инцидентов информационной безопасности на основе прецедентного анализа // Технические и математические науки. Студенческий научный форум: сб. статей по материалам XVIII студ. Междунар. науч.-практ. конф. М.: ООО «Международный центр науки и образования», 2019. Т. 7 (18). С. 76–77. EDN ZZFJKH.

35. Кужаев М.Р., Золкин А.Л. Проблемы информационной безопасности в компьютерных сетях // Безопасность информационного пространства: сб. трудов XIX Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. Екатеринбург: Уральский гос. эконом. ун-т, 2021. С. 120–123. EDN AICFNM.

36. Худайназаров Ю.К., Пермяков А.С., Лепешкин Е.О. Задачи системы интеллектуального мониторинга информационной безопасности инфотелекоммуникационной сети // Нейрокомпьютеры и их применение: тезисы докладов XVIII Всерос. науч. конф. М.: Московский гос. психол.-пед. ун-т, 2020. С. 198–200. EDN BMBERB.

37. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. № 3 (43). С. 68–83. DOI: 10.21681/2311-3456-2021-3-68-83. EDN UVMXAZ.

38. Антипова Р.В., Сосновский Г.О. Проблемы информационной безопасности облачных вычислений // Междисциплинарные исследования. Современное состояние и перспективы. 2018. С. 6–9.

39. Huang K. Information Security Problems and Solutions in Cloud Era // Journal of Physics: Conference Series. IOP Publishing. 2021. Т. 2066. № 1. (012005).

40. Глебов В.В., Кузнецова В.Ю. Проблема использования слабых паролей и ее программное решение // Каспий в цифровую эпоху: материалы Нац. науч.-практ. конф. с междунар. участием в рамках Междунар. науч. форума «Каспий – 2021: пути устойчивого развития». Астрахань: Изд. дом «Астраханский университет», 2021. С. 496–500. EDN BSSUUG.

41. Радченко О.Л., Гаязова Е.Э. Проблемы безопасности 5G // Электронная наука. 2021. Т. 2. № 2. EDN EGFSWI.

42. Дерябина О.С. Основные задачи развития системы информационной безопасности // Молодой ученый. 2019. № 25 (263). С. 19–21. EDN MVMHPA.

43. Максудов М.О., Дорошенко И.Е., Селифанов В.В. Проблемы формирования структуры функций системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 143–148.

44. Антипов В.Е., Селифанов В.В. Проблемы формализации процессов систем управления информационной безопасностью. 2022. Т. 6. С. 3–8. DOI: 10.33764/2618-981X-2022-6-3-8. EDN AQJZQN.

45. Микрюков А.А., Кулагина Е.С. Задачи совершенствования систем информационной безопасности в сетях нового поколения // Молодежь в науке: Новые аргументы: сб. науч. работ IV Междунар. молодеж. науч. конф. / отв. ред. А.В. Горбенко. Липецк: Научное партнерство «Аргумент», 2018. Ч. I. С. 75–77. EDN YUWTCI.

46. Грызунов В.В., Шкреба О.С. Особенности применения технологических методов в социальной инженерии // Технико-технологические проблемы сервиса. 2018. № 4 (46). С. 90–94. EDN YSWYUX.

47. Gryzunov V.V., Bondarenko I.Y. A Social Engineer in Terms of Control Theory // Proceedings of the 3rd International Conference Ergo-2018: Human Factors in Complex Technical Systems and Environments, Ergo 2018. SPb., 2018. P. 202–204. DOI: 10.1109/ERGO.2018.8443835. EDN YBNLBR.

48. Макаревич В.А., Минюкович Е.А., Мулярчик К.С. Проблемы информационной безопасности при организации удаленной работы сотрудников // Актуальные проблемы науки XXI века. 2020. № 9. С. 12–16. EDN JWFZYB.

49. Диль М.А. Задачи обеспечения информационной безопасности бизнеса // Горинские чтения. Инновационные решения для АПК: материалы Междунар. студ. науч. конф. Майский: Белгородский гос. аграрный ун-т им. В.Я. Горина, 2022. Т. 3. С. 227–228. EDN DNTVSN.

50. Третьяков И.А., Рушечников Я.И. Проблемы информационной безопасности электромагнитных излучений и наводок в средствах вычислительной техники //

Информационные системы и технологии: материалы Междунар. науч. конгресса по информатике. Минск: Белорусский гос. ун-т, 2022. Ч. 1. С. 108–112. EDN GTKGIM.

51. Карпухина Е.К. Основные проблемы информационной безопасности в условиях цифровой трансформации инфокоммуникационных технологий // Современные проблемы проектирования, производства и эксплуатации радиотехнических систем: сб. науч. трудов / отв. ред. В.Е. Дементьев. Ульяновск: Ульяновский гос. техн. ун-т, 2021. Вып. 13. С. 108–110. EDN FNCVOE.

52. Осипов М.Д., Кладов В.Е. Современные проблемы информационной безопасности и технические средства защиты // Безопасность информационного пространства: сб. трудов XVII Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых: Челябинск: Челябинский гос. ун-т, 2018. Т. 2. С. 146–154. EDN IRMJIU.

53. Летавина А.С., Богачев А.Ю. Проблемы информационной безопасности в беспроводных компьютерных сетях технологии Wi-Fi: характеристики, подключение и способы защиты // Российская наука и образование сегодня: проблемы и перспективы. 2020. № 2 (33). С. 83–87. EDN OZLHOF.

54. Мухаммадиев М.У. Проблемы информационной безопасности в электронных платежных системах // I-TOM. 2021. С. 241–243.

55. Беккалиева Н.К., Голубь В.С. Актуальные проблемы информационной безопасности в банковской деятельности // Использование инновационных технологий в разработке и реализации. экономических реформ: сб. статей Междунар. науч.-практ. конф. Челябинск: ООО «Аэтерна», 2018. С. 15–20. EDN MIHWIH.

56. Проблемы безопасности современных CMS / О.М. Бакунова [и др.] // Web of Scholar. 2018. Т. 1. № 1 (19). С. 11–13. EDN YMVBXS.

57. Хомякова У.В. Проблемы информационной безопасности банковских карт // Перспективы науки и общества в условиях инновационного развития: сб. статей Всерос. науч.-практ. конф. с междунар. участием. УФА: ООО «Аэтерна», 2022. С. 98–103. EDN URSKRQ.

58. Смирнов П.В., Стойчин К.Л. Проблемы информационной безопасности при использовании концепции BYOD // Безопасность информационного пространства – 2017. Екатеринбург: Уральский фед. ун-т им. первого Президента России Б.Н. Ельцина, 2018. С. 129–132. EDN MKMSMP.

References

1. Kak chat-boty ChatGPT izmenyat kiberbezopasnost'. URL: https://www.kaspersky.ru/blog/chatgpt-cybersecurity/34561/ (data obrashcheniya: 12.02.2024).

2. Bur'kova E.V., Izvekova L.A. Primenenie metoda klasterizacii dannyh dlya resheniya zadachi ocenki riskov informacionnoj bezopasnosti // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2019. № 2 (26). S. 81–86. EDN VPZHMI.

3. Krutov A.N., Krutova N.A., Ivanchina O.V. Problema analiza riskov v upravlenii informacionnoj bezopasnost'yu predpriyatiya // Vestnik SamGUPS. 2019. № 1 (43). S. 96–103. EDN DZDIEW.

4. Smirnov I.N. Zadachi sluzhby informacionnoj bezopasnosti predpriyatiya v sovremennyh usloviyah // Fundamental'no-prikladnye problemy bezopasnosti, zhivuchesti, nadezhnosti, ustojchivosti i effektivnosti sistem: materialy II Mezhdunar. nauch.-prakt. konf., posvyashch. 105-letiyu so dnya rozhdeniya Admirala flota SSSR dvazhdy geroya Sovetskogo Soyuza Sergeya Georgievicha Gorshkova. Elec: Eleckij gos. un-t im. I.A. Bunina, 2018. S. 197–200. EDN XTNJNJ.

5. Vol'hina M.N., Stojchin K.L. Problemy informacionnoj bezopasnosti v ASU TP // Bezopasnost' informacionnogo prostranstva – 2017. Ekaterinburg: Ural'skij federal'nyj un-t imeni pervogo Prezidenta Rossii B.N. El'cina, 2018. S. 96–99. EDN SQLENV.

6. Kosov N.A., Golubov N.A. Sposoby zashchity ot insajderskih atak // Innovacionnye resheniya social'nyh, ekonomicheskih i tekhnologicheskih problem sovremennogo obshchestva:

sb. nauch. statej po itogam kruglogo stola so vserossijskim i mezhdunarodnym uchastiem, M.: OOO «KONVERT», 2021. T. 8. S. 149–151. EDN TFZVIG.

7. DLP vne zakona! Tak reshil sud! URL: https://lukatsky.ru/legislation/dlp-vne-zakona-tak-reshil-sud.html (data obrashcheniya: 11.01.2024).

8. Chernoknizhnyj G.M., Lukin E.I. K voprosu ob ugrozah botnet-setej // Konvergenciya cifrovyh i material'nyh mirov: ekonomika, tekhnologii, obrazovanie: sb. nauch. statej Mezhdunar. nauch. konf. / pod red. V.V. Trofimova, V.F. Minakova. SPb.: S.-Peterb. gos. ekonom. un-t, 2018. S. 225–230. EDN YPXZWX.

9. Vizual'naya analitika dlya informacionnoj bezopasnosti: oblasti primeneniya, zadachi i modeli vizualizacii / I.V. Kotenko [i dr.] // Voprosy kiberbezopasnosti. 2021. № 4 (44). S. 2–15. DOI: 10.21681/2311-3456-2021-4-2-15. EDN LVCIOR.

10. Romashkina N.P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. № 1 (29). S. 2–9. DOI: 10.21681/2311-3456-2019-1-2-9. EDN VWBWZC.

11. Belov D.E. Nekotorye aspekty problemy informacionnoj bezopasnosti Rossijskoj Federacii // Problemy massovoj kommunikacii: novye podhody. 2019. S. 77–79.

12. Zhigadlo V.E. Zadachi i funkcii informacionnoj bezopasnosti v usloviyah informacionnogo protivoborstva i «mental'nyh» vojn // Informacionnaya bezopasnost' regionov Rossii (IBRR-2021): materialy XII S.-Peterb. mezhregion. konf. SPb.: Region. obshch. organiz. «Sankt-Peterburgskoe Obshchestvo informatiki, vychislitel'noj tekhniki, sistem svyazi i upravleniya», 2021. S. 21–23. EDN VTGRGO.

13. Lapshinova K.V., Podol'skaya A.A. Problemy informacionnoj bezopasnosti Rossii v kontekste otnosheniya molodezhi k informacionnoj vojne // Social'no-gumanitarnye tekhnologii. 2020. № 2 (14). S. 44–53. EDN KXJXAE.

14. Kirilenko V.V. Problemy zashchity informacii v sistemah elektronnogo dokumentooborota. 2021. № 4 (34). EDN LKOUGY.

15. Burlov V.G., Gryzunov V.V., Sipovich D.E. Adaptivnoe upravlenie dostupnost'yu v geoinformacionnoj sisteme, ispol'zuyushchej tumannye vychisleniya // International Journal of Open Information Technologies. 2021. T. 9. № 9. S. 76–89.

16. Gryzunov V.V. Metody adaptivnogo upravleniya dostupnost'yu resursov geoinformacionnyh sistem v usloviyah destruktivnyh vozdejstvij // Trudy uchebnyh zavedenij svyazi. 2022. T. 8. № 3. S. 101–115. DOI: 10.31854/1813-324X-2022-8-3-101-116.

17. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability. Informatsionno-upravliaiushchie sistemy [Information and Control Systems]. 2022. № 1. P. 19–29. DOI: 10.31799/1684-8853-2022-1-19-29.

18. Belov E.B., Los' V.P., Malyuk A.A. Cifrovaya ekonomika i aktual'nye problemy sovershenstvovaniya sistemy podgotovki kadrov v oblasti informacionnoj bezopasnosti // Bezopasnost' informacionnyh tekhnologij. 2018. T. 25. № 4. S. 6–22. EDN YQNKMX.

19. Zinov'eva V.V. Analiz incidentov narusheniya bezopasnosti konfidencial'noj informacii v Rossii i mire v I polugodii 2022 goda. Pravovye problemy informacionnoj bezopasnosti i puti ih resheniya // Cifrovye tekhnologii i pravo: sb. nauch. trudov I Mezhdunar. nauch.-prakt. konf. / pod red. I.R. Begisheva [i dr.]. Kazan': Izd-vo «Poznanie», 2022. T. 1. S. 107–113. EDN HX: LZCA.

20. Ionkina A.V., Krohalev A.A. Problemy informacionnoj bezopasnosti v cifrovoj ekonomike // Molodezh' i nauka. 2021. № 7. EDN IMKDYD.

21. Herlambang P.M., dudiyanty T.R. Cybersecurity challenges. in the implementation of a hospital management information system // Eubios journal of Asian and international bioethics. Christchurch. 2017. Vol. 28. № 3. P. 151–154.

22. Mavrin A.V. Sovremennye problemy informacionnoj bezopasnosti, svyazannye s zashchitoj personal'nyh dannyh pol'zovatelya // StudNet. 2022. T. 5. № 6. S. 109. EDN GTXRCU.

23. Naumova I.V. Problemy informacionnoj bezopasnosti obrazovatel'nogo processa v sovremennyh usloviyah // Bezopasnaya obrazovatel'naya sreda: problemy proektirovaniya i perspektivy razvitiya: sb. nauch. trudov po materialam Vseros. nauch.-prakt. konf. 2018. S. 49–52.

24. Sovremennye problemy obespecheniya informacionnoj bezopasnosti dokumentooborota na predpriyatii / S.S. Saltysh [i dr.] // Bezopasnost' informacionnogo prostranstva: sb. trudov XIX Vseros. nauch.-prakt. konf. studentov, aspirantov i molodyh uchenyh. Ekaterinburg: Ural'skij gos. ekon. un-t, 2021. S. 116–120. EDN RPFRVI.

25. Pisarenko V.I., Pisarenko I.V. Potencial pedagogicheskoj nauki v reshenii problemy informacionnoj bezopasnosti studentov pri vzaimodejstvii s internet-prostranstvom // Na puti cifrovizacii obshchestva: psihologicheskie i pedagogicheskie osnovy: sb. statej po itogam Mezhdunar. nauch.-prakt. konf. Sterlitamak: OOO «Agentstvo mezhdunarodnyh issledovanij», 2020. S. 29–32. EDN QHLJZK.

26. Fotieva I.V. Eticheskij aspekt problemy informacionnoj bezopasnosti // Nacrazvitie: materialy Mezhdunar. nauch. konf. SPb., 2020. S. 175–177. DOI: 10.37539/APR290.2020.28.46.008. EDN HGMKPZ.

27. Yakovleva V.V., Savchuk V.S. Problemy informacionnoj bezopasnosti nesovershennoletnih v obrazovatel'nom processe // Social'no-ekonomicheskoe razvitie regionov: problemy i perspektivy vnedreniya innovacij: sb. materialov Mezhregion. nauch.-prakt. konf., posvyashch. 50-letiyu Buryatskogo filiala SibUPK i 95-letiyu Buryatskogo respublikanskogo soyuza potrebitel'skih obshchestv / pod red. E.N. Lishchuk. Novosibirsk: Sibirskij un-t potrebitel'skoj kooperacii, 2018. S. 321–325. EDN EHZYAJ.

28. Fidchenko E.V. Problemy informacionnoj bezopasnosti cheloveka: filosofskij aspekt // Dal'nevostochnaya vesna – 2019: materialy 17 Mezhdunar. nauch.-prakt. konf. po problemam ekologii i bezopasnosti. Komsomol'sk-na-Amure: Komsomol'skij-na-Amure gos. un-t, 2019. S. 274–276. EDN HFMPYN.

29. Kilishbayevich B.J. Philosophical analysis of manipulation and information security problems // Sustainability of education, socio-economic science theory. 2023. T. 1. № 6. S. 149–152.

30. Nikolaev E.N. Problemy informacionnoj bezopasnosti v aspekte razvitiya iskusstvennogo intellekta // 2021. № 48. S. 1428–1434. EDN NDICRE.

31. Maksimova E.A. Metody vyyavleniya i identifikacii istochnikov destruktivnyh vozdejstvij infrastrukturnogo geneza // Elektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KubGTU». 2022. № 2. S. 86–99. EDN KTYQJE.

32. Grigor'ev D.A. Problemy informacionnoj bezopasnosti // Sistemy bezopasnosti: materialy Mezhdunar. nauch.-tekhn. konf. 2019. № 28. S. 128–130. EDN PILHUR.

33. Karaseva T.N., Mishanin M.A. Problemy importozameshcheniya v sfere informacionnoj bezopasnosti // Luchshaya issledovatel'skaya stat'ya 2023: sb. statej Mezhdunar. nauch.-issled. konkursa. Penza: Nauka i Prosveshchenie, 2023. S. 38–40. EDN QLFXTY.

34. Mihajlova E.A. Reshenie zadachi klassifikacii incidentov informacionnoj bezopasnosti na osnove precedentnogo analiza // Tekhnicheskie i matematicheskie nauki. Studencheskij nauchnyj forum: sb. statej po materialam XVIII stud. Mezhdunar. nauch.-prakt. konf. M.: OOO «Mezhdunarodnyj centr nauki i obrazovaniya», 2019. T. 7 (18). S. 76–77. EDN ZZFJKH.

35. Kuzhaev M.R., Zolkin A.L. Problemy informacionnoj bezopasnosti v komp'yuternyh setyah // Bezopasnost' informacionnogo prostranstva: sb. trudov XIX Vseros. nauch.-prakt. konf. studentov, aspirantov i molodyh uchenyh. Ekaterinburg: Ural'skij gos. ekonom. un-t, 2021. S. 120–123. EDN AICFNM.

36. Hudajnazarov Yu.K., Permyakov A.S., Lepeshkin E.O. Zadachi sistemy intellektual'nogo monitoringa informacionnoj bezopasnosti infotelekommunikacionnoj seti // Nejrokomp'yutery i ih primenenie: tezisy dokladov XVIII Vseros. nauch. konf. M.: Moskovskij gos. psihol.-ped. un-t, 2020. S. 198–200. EDN BMBERB.

37. Garbuk S.V. Zadachi normativno-tekhnicheskogo regulirovaniya intellektual'nyh sistem informacionnoj bezopasnosti // Voprosy kiberbezopasnosti. 2021. № 3 (43). S. 68–83. DOI: 10.21681/2311-3456-2021-3-68-83. EDN UVMXAZ.

38. Antipova R.V., Sosnovskij G.O. Problemy informacionnoj bezopasnosti oblachnyh vychislenij // Mezhdisciplinarnye issledovaniya. Sovremennoe sostoyanie i perspektivy. 2018. S. 6–9.

39. Huang K. Information Security Problems and Solutions in Cloud Era // Journal of Physics: Conference Series. IOP Publishing. 2021. T. 2066. № 1. (012005).

40. Glebov V.V., Kuznecova V.Yu. Problema ispol'zovaniya slabyh parolej i ee programmnoe reshenie // Kaspij v cifrovuyu epohu: materialy Nac. nauch.-prakt. konf. s mezhdunar. uchastiem v ramkah Mezhdunar. nauch. foruma «Kaspij – 2021: puti ustojchivogo razvitiya». Astrahan': Izd. dom «Astrahanskij universitet», 2021. S. 496–500. EDN BSSUUG.

41. Radchenko O.L., Gayazova E.E. Problemy bezopasnosti 5G // Elektronnaya nauka. 2021. T. 2. № 2. EDN EGFSWI.

42. Deryabina O.S. Osnovnye zadachi razvitiya sistemy informacionnoj bezopasnosti // Molodoj uchenyj. 2019. № 25 (263). S. 19–21. EDN MVMHPA.

43. Maksudov M.O., Doroshenko I.E., Selifanov V.V. Problemy formirovaniya struktury funkcij sistemy upravleniya informacionnoj bezopasnost'yu znachimogo ob"ekta kriticheskoj informacionnoj infrastruktury // Interekspo Geo-Sibir'. 2022. T. 6. S. 143–148.

44. Antipov V.E., Selifanov V.V. Problemy formalizacii processov sistem upravleniya informacionnoj bezopasnost'yu. 2022. T. 6. S. 3–8. DOI: 10.33764/2618-981X-2022-6-3-8. EDN AQJZQN.

45. Mikryukov A.A., Kulagina E.S. Zadachi sovershenstvovaniya sistem informacionnoj bezopasnosti v setyah novogo pokoleniya // Molodezh' v nauke: Novye argumenty: sb. nauch. rabot IV Mezhdunar. molodezh. nauch. konf. / otv. red. A.V. Gorbenko. Lipeck: Nauchnoe partnerstvo «Argument», 2018. Ch. I. S. 75–77. EDN YUWTCI.

46. Gryzunov V.V., Shkreba O.S. Osobennosti primeneniya tekhnologicheskih metodov v social'noj inzhenerii // Tekhniko-tekhnologicheskie problemy servisa. 2018. № 4 (46). S. 90–94. EDN YSWYUX.

47. Gryzunov V.V., Bondarenko I.Y. A Social Engineer in Terms of Control Theory // Proceedings of the 3rd International Conference Ergo-2018: Human Factors in Complex Technical Systems and Environments, Ergo 2018. SPb., 2018. P. 202–204. DOI: 10.1109/ERGO.2018.8443835. EDN YBNLBR.

48. Makarevich V.A., Minyukovich E.A., Mulyarchik K.S. Problemy informacionnoj bezopasnosti pri organizacii udalennoj raboty sotrudnikov // Aktual'nye problemy nauki XXI veka. 2020. № 9. S. 12–16. EDN JWFZYB.

49. Dil' M.A. Zadachi obespecheniya informacionnoj bezopasnosti biznesa // Gorinskie chteniya. Innovacionnye resheniya dlya APK: materialy Mezhdunar. stud. nauch. konf. Majskij: Belgorodskij gos. agrarnyj un-t im. V.Ya. Gorina, 2022. T. 3. S. 227–228. EDN DNTVSN.

50. Tret'yakov I.A., Rushechnikov Ya.I. Problemy informacionnoj bezopasnosti elektromagnitnyh izluchenij i navodok v sredstvah vychislitel'noj tekhniki // Informacionnye sistemy i tekhnologii: materialy Mezhdunar. nauch. kongressa po informatike. Minsk: Belorusskij gos. un-t, 2022. Ch. 1. S. 108–112. EDN GTKGIM.

51. Karpuhina E.K. Osnovnye problemy informacionnoj bezopasnosti v usloviyah cifrovoj transformacii infokommunikacionnyh tekhnologij // Sovremennye problemy proektirovaniya, proizvodstva i ekspluatacii radiotekhnicheskih sistem: sb. nauch. trudov / otv. red. V.E. Dement'ev. Ul'yanovsk: Ul'yanovskij gos. tekhn. un-t, 2021. Vyp. 13. S. 108–110. EDN FNCVOE.

52. Osipov M.D., Kladov V.E. Sovremennye problemy informacionnoj bezopasnosti i tekhnicheskie sredstva zashchity // Bezopasnost' informacionnogo prostranstva: sb. trudov XVII Vseros. nauch.-prakt. konf. studentov, aspirantov i molodyh uchenyh: Chelyabinsk: Chelyabinskij gos. un-t, 2018. T. 2. S. 146–154. EDN IRMJIU.

53. Letavina A.S., Bogachev A.Yu. Problemy informacionnoj bezopasnosti v besprovodnyh komp'yuternyh setyah tekhnologii Wi-Fi: harakteristiki, podklyuchenie i sposoby zashchity // Rossijskaya nauka i obrazovanie segodnya: problemy i perspektivy. 2020. № 2 (33). S. 83–87. EDN OZLHOF.

54. Muhammadiev M.U. Problemy informacionnoj bezopasnosti v elektronnyh platezhnyh sistemah // I-TOM. 2021. S. 241–243.

55. Bekkalieva N.K., Golub' V.S. Aktual'nye problemy informacionnoj bezopasnosti v bankovskoj deyatel'nosti // Ispol'zovanie innovacionnyh tekhnologij v razrabotke i realizacii. ekonomicheskih reform: sb. statej Mezhdunar. nauch.-prakt. konf. Chelyabinsk: OOO «Aeterna», 2018. S. 15–20. EDN MIHWIH.

56. Problemy bezopasnosti sovremennyh CMS / O.M. Bakunova [i dr.] // Web of Scholar. 2018. T. 1. № 1 (19). S. 11–13. EDN YMVBXS.

57. Homyakova U.V. Problemy informacionnoj bezopasnosti bankovskih kart // Perspektivy nauki i obshchestva v usloviyah innovacionnogo razvitiya: sb. statej Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem. UFA: OOO «Aeterna», 2022. S. 98–103. EDN URSKRQ.

58. Smirnov P.V., Stojchin K.L. Problemy informacionnoj bezopasnosti pri ispol'zovanii koncepcii BYOD // Bezopasnost' informacionnogo prostranstva – 2017. Ekaterinburg: Ural'skij fed. un-t im. pervogo Prezidenta Rossii B.N. El'cina, 2018. S. 129–132. EDN MKMSMP.

Информация о статье:
Статья поступила в редакцию: 18.02.2023; одобрена после рецензирования: 29.02.2024;
принята к публикации: 02.03.2024

The information about article:
The article was submitted to the editorial office: 18.02.2023; approved after review: 29.02.2024;
accepted for publication: 02.03.2024

Информация об авторах:
Брюханов Владислав Андреевич, аспирант кафедры «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I (190031, Санкт-Петербург, Московский пр., д. 9), e-mail: vladislove1925@mail.ru, ORCID 0009-0000-5237-5152, SPIN-код: 3912-2340
Грызунов Виталий Владимирович, профессор кафедры прикладной информатики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, доцент, e-mail: viv1313r@mail.ru, ORCID 0000-0003-4866-217X, SPIN-код: 9750-4417
Шестаков Александр Викторович, старший научный сотрудник, помощник начальника Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, e-mail: alexandr.shestakov01@yandex.ru, ORCID: 0000-0002-8462-6515, SPIN-код: 5831-5451

Information about authors:
Bryukhanov Vladislav A., post-graduate student of the department of Informatics and information security, Emperor Alexander I Saint-Petersburg state transport university (190031, Saint-Petersburg, Moskovsky ave., 9), e-mail: vladislove1925@mail.ru, ORCID 0009-0000-5237-5152, SPIN: 3912-2340
Gryzunov Vitaly V., associate professor of the department of information technologies and security systems of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of engineering sciences, e-mail: viv1313r@mail.ru, ORCID 0000-0003-4866-217X, SPIN: 9750-4417
Shestakov Alexander V., senior researcher, assistant chief of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of engineering sciences, e-mail: alexandr.shestakov01@yandex.ru, ORCID: 0000-0002-8462-6515, SPIN: 5831-5451