ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004

DOI: 10.21822/2073-6185-2025-52-2-107-115 Обзорная статья/ Review article

Стратегии защиты от угроз безопасности: развитие системы обеспечения кибербезопасности

Г.И. Качаева[1], Н.Г. Султанов[2]
[1]Дагестанский государственный технический университет,
[1]367015, г. Махачкала, проспект Имама Шамиля 70, Россия,
[2]Дагестанский государственный университет,
[2]367000, г. Махачкала, ул. М. Гаджиева, 43-а , Россия

Резюме. Цель. Актуальность исследования обусловлена стремительным развитием цифровой экономики и ростом киберугроз, угрожающих безопасности персональных данных и финансовых операций. Целью научного исследования является анализ современных стратегий защиты от киберугроз и развитие системы кибербезопасности в условиях цифровой трансформации. **Метод.** Методы исследования включают анализ литературы, статистических данных и практических кейсов. **Результат.** Рассмотрены основные типы кибератак (фишинг, DDoS, вредоносные программы, кибершпионаж) и ключевые технологии защиты, включая шифрование AES-256, многофакторную аутентификацию (MFA) и системы обнаружения вторжений (IDS). Особое внимание уделено стратегиям: проактивной защите, адаптивной безопасности и архитектуре «нулевого доверия», с примерами их применения в России (Сбербанк, Ростелеком, медучреждения). Изучены механизмы предотвращения атак и повышения киберустойчивости, включая роль ГосСОПКА, обработавшей в 2023 году свыше 500 тысяч инцидентов. Выявлены уязвимости систем и предложены способы их минимизации, такие как модернизация технических средств, развитие кадрового потенциала и совершенствование нормативной базы. **Вывод.** Практическая значимость заключается в разработке рекомендаций по внедрению стратегий, позволивших сократить ущерб от атак на 18% в 2023 году, и повышению эффективности защиты данных. Необходим системный подход к интеграции инноваций и координации усилий для обеспечения устойчивого развития кибербезопасности в России.

Ключевые слова: кибербезопасность, цифровая экономика, киберугрозы, проактивная защита, адаптивная безопасность, нулевое доверие, защита данных, ГосСОПКА.

Для цитирования: Г.И. Качаева, Н.Г. Султанов. Стратегии защиты от угроз безопасности: развитие системы обеспечения кибербезопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(2):107-115. DOI:10.21822/2073-6185-2025-52-2-107-115

Security threat protection strategies: development of a cybersecurity system

G.I. Kachaeva[1], N.G. Sultanov[2]
[1]Daghestan State Technical University,
[1]70 I. Shamil Ave., Makhachkala 367015, Russia,
[2]Daghestan State University,
[2]43-a M. Gadzhieva St., Makhachkala 367000, Russia

Abstract. **Objective**. The relevance of this study stems from the rapid advancement of the digital economy and the escalating cyber threats that jeopardize the security of personal data and financial transactions. The aim of the scientific research is to analyze modern strategies for protecting against cyber threats and to advance the development of a cybersecurity system in the context of digital transformation. **Method.** Research methods encompass literature review, statistical

analysis, and case studies. **Result.** The paper considers the types of cyberattacks (phishing, DDoS, malware, cyber espionage) and key security technologies, including AES-256 encryption, multi-factor authentication (MFA), and intrusion detection systems (IDS). Attention is paid to the following strategies: proactive defense, adaptive security, and zero trust architecture, with examples of their application in Russia (Sberbank, Rostelecom, medical institutions). The paper studies the mechanisms for preventing attacks and increasing cyber resilience, including the role of GosSOPKA, which processed over 500 thousand incidents in 2023. The paper identifies system vulnerabilities and proposes ways to minimize them: upgrading technical equipment, developing human resources, and improving the regulatory framework. **Conclusion.** The practical significance lies in the development of recommendations for the implementation of strategies that reduced damage from attacks by 18% in 2023. A systematic approach is needed to integrate innovations and coordinate efforts to ensure sustainable development of cybersecurity in Russia.

Keywords: cybersecurity, digital economy, cyber threats, proactive defense, adaptive security, zero trust, data protection, GosSOPKA

For citation: G.I. Kachaeva, N.G. Sultanov. Security threat protection strategies: development of a cybersecurity system. Herald of Daghestan State Technical University. Technical Sciences.2025;52(2):107-115. (In Russ) DOI:10.21822/2073-6185-2025-52-2-107-115

Введение. В условиях стремительной цифровизации экономики информационные технологии становятся ключевым элементом практически всех сфер деятельности. С каждым годом увеличивается количество цифровых сервисов, используемых как в повседневной жизни граждан, так и в бизнесе, и государственном управлении. Однако вместе с ростом технологических возможностей увеличиваются и риски, связанные с киберугрозами. Мошенники и злоумышленники активно применяют новые технологии для доступа к конфиденциальной информации и финансовым ресурсам. Это делает кибербезопасность одной из важнейших задач современного общества и бизнеса.

Постановка задачи. Защита данных и обеспечение безопасности информационных систем становятся приоритетными направлениями в цифровой трансформации [1-3]. В связи с этим необходимо разрабатывать комплексные стратегии и методы защиты от кибератак, чтобы минимизировать риски и повысить устойчивость к угрозам.

Степень изученности проблемы кибербезопасности в России на современном этапе высока и охватывает множество аспектов, связанных с цифровизацией и защитой информационных систем. Сегодня активно исследуются как теоретические, так и практические вопросы обеспечения кибербезопасности, особенно в контексте банковского сектора и промышленных предприятий. Исследования, проводимые такими авторами, как Вахрушев и Липовская (2019), Кобец (2024), и Ронжина с Глазатовым (2023), выделяют особенности формирования рынка услуг кибербезопасности, а также основные угрозы, с которыми сталкиваются различные организации. Наиболее актуальными становятся вопросы интеграции новых технологий и методов защиты в условиях растущих киберугроз и финансовых рисков, что освещают работы Поляковой (2019) и Шкодинского с соавторами (2021). Научные исследования, проведенные Ноговицыным (2023) и Обуховой с Пияльцевым (2020), акцентируют внимание на необходимости комплексного подхода к защите информационных данных и систем в условиях цифровой трансформации.

Эти исследования подчеркивают важность создания стратегий для повышения уровня кибербезопасности на уровне отдельных компаний и в масштабах национальной экономики. Накопленный опыт и результаты научных изысканий позволяют утверждать, что проблемы кибербезопасности не только активно изучаются, но и требуют дальнейшего внимания с учетом быстро меняющегося цифрового ландшафта и новых вызовов, связанных с киберугрозами.

Методы исследования. В условиях стремительного роста киберугроз разработка и внедрение современных стратегий защиты становятся ключевым фактором обеспечения кибербезопасности. Среди наиболее эффективных подходов выделяются следующие:

1. Проактивная защита – стратегия, направленная на активный поиск угроз до того, как они проявят себя. Это включает мониторинг аномалий в сетевом трафике и поведении пользователей с использованием систем на основе искусственного интеллекта (ИИ). Например, в 2023 году крупные российские банки, такие как Сбербанк, внедрили системы Threat Hunting, что позволило снизить количество успешных фишинговых атак на 15% (по данным Центрального банка РФ).
2. Адаптивная безопасность – подход, предполагающий гибкость защитных систем и их способность адаптироваться к новым угрозам в реальном времени. Он включает использование многоуровневых систем защиты, таких как межсетевые экраны нового поколения (NGFW) и системы предотвращения вторжений (IPS). В России такие решения активно применяются в телекоммуникационном секторе: операторы связи, например «Ростелеком», используют адаптивные системы для защиты от DDoS-атак, что сократило время простоя сервисов на 30% в 2023 году.
3. Архитектура «нулевого доверия» – стратегия, основанная на принципе «никому не доверяй, всегда проверяй». Она требует обязательной аутентификации и проверки каждого пользователя и устройства, даже внутри корпоративной сети. Этот подход набирает популярность в медицинских учреждениях России: после серии атак на базы данных в 2022–2023 годах ряд клиник внедрил Zero Trust, что снизило утечки данных на 25% (по данным Росздравнадзора).

Эти стратегии требуют интеграции современных технологий, таких как шифрование AES-256, многофакторная аутентификация (MFA) и системы обнаружения вторжений (IDS). По данным компании «Лаборатория Касперского», в 2023 году использование MFA в российских организациях выросло на 40%, что значительно снизило риски компрометации учетных данных. Практическая значимость таких подходов подтверждается их способностью не только реагировать на угрозы, но и предотвращать их на ранних стадиях.

В условиях цифровизации экономики информационные технологии становятся одной из главных опор в ее ускоренном развитии. Инновационное развитие предполагает как доступность новейших информационных технологий, так и их непрекращающееся усложнение. Сегодня мы вошли в эпоху глобальной цифровизации жизнедеятельности индивида. Не использовать цифровые сервисы уже практически невозможно. Они охватили почти все сферы от проведения банковских платежей до обеспечения общественной безопасности [1]. Но со стремительным проникновением таких технологий в жизнь индивида увеличивается количество персональной информации, которая собирается и анализируется операторами. Поэтому особое внимание необходимо уделять обеспечению кибербезопасности. Без нее ценность любых современных технологий девальвируется, а экономический эффект от их применения стремится к нулю. Поэтому кибербезопасность сегодня стала важным элементом в государственном управлении с последующим ее каскадированием на коммерческие и некоммерческие организации.

Цифровая экономика характеризуется повсеместным внедрением информационных технологий. В финансовом секторе они приобретают особое значение. Ведь большинство услуг, оказываемых финансовыми организациями, невозможно без представления пользователем полной информации о себе. Ярким примером является страхование жизни, где помимо сведений о своих документах клиент предоставляет организации информацию о состоянии своего здоровья [5]. Третьи лица могут использовать эти данные для совершения мошеннических операций. Поэтому обеспечение кибербезопасности становится важным фактором при цифровой трансформации [2]. Киберугрозы стали одним из глобальных вызовов настоящего времени. Мошенники активно используют современные технологии

для того, чтобы завладеть денежными средствами граждан. Появляются новые виды мошенничества.

Фишинговые методы - одни из самых распространенных видов мошенничества в сети Интернет. Коммуницируя с человеком посредством переписки по электронной почте или в мессенджерах, злоумышленник пытается выдать себя за представителя официальной организации, чтобы получить конфиденциальную информацию о человеке и далее завладеть его денежными средствами. Наиболее распространены массовые рассылки по электронной почте, они получили название «Нигерийские письма», потому что на ранних стадиях их использования мошенники выдавали себя за крупного экс-чиновника из Нигерии, которому необходимо получить доступ к своим средствам, размещенным в иностранном банке, а ввиду отсутствия у него сейчас возможности оплатить необходимые сборы, он готов поделиться частью своих средств с получателем письма (суммы называются как правильно внушительные: от нескольких десятков до миллионов долларов США). Чтобы принять его предложение достаточно перевести необходимую ему сумму по указанным в письме реквизитам. После получения денежных средств мошенник прерывает коммуникацию.

Другой распространенный вид кибермошенничества - рассылка программ, содержащих вредоносный код. Устанавливая такое программное обеспечение, пользователь предоставляет злоумышленнику доступ к своей конфиденциальной информации, а в ряде случаев - и напрямую к банковским счетам. Такой способ применяется как для осуществления атак на персональные компьютеры, так и на смартфоны. DDOS-атаки осуществляются на онлайн-сервисы крупных организаций. Из-за них владелец ресурса не может осуществлять свою персональную деятельность, что приводит к реализации финансовых и репутационных рисков. Значительная часть потребителей сегодня предпочитает приобретать товары онлайн, поэтому постоянные подобные атаки могут привести к прекращению деятельности организации. Зачастую мошенники предлагают прекратить совершать DDOS-атаки, получив вознаграждение [4]. Кибершпионаж используется для получения корпоративных или государственных закрытых данных, которые в дальнейшем мошенник использует в своих корыстных интересах. Так могут быть украдены технологические разработки, стратегические документы и другие объекты интеллектуальной собственности. Также мошенники взламывают базы данных с помощью SQL-инъекций. Таким образом они получают доступ к логину и паролям пользователей и к другим персональным данным. В условиях цифровизации кибербезопасность стала неотъемлемой частью инфраструктуры почти любого коммерческого предприятия вне зависимости от масштабов его деятельности и финансовых показателей [8]. Больше всего подвергаются атакам злоумышленников следующие сферы:

– финансы – банки, брокерские и инвестиционные компании, страховщики, платежные системы;

– энергетика – компании-поставщики электроэнергии, топлива, газа;

– промышленность – машиностроение, автомобилестроение, производство транспортной техники;

– телекоммуникационные компании – провайдеры связи и интернета, онлайн-сервисы;

– в сфере государственного сервиса – сайты различных ведомств и учреждений;

– в образовании – вузы, научно-исследовательские институты.

Кибератаки способны подорвать репутацию предприятий и ведут к следующим последствиям:

1. Получение мошенниками конфиденциальной информации о клиентах и сотрудниках.

2. Прерывание деятельности организации и вывод из строя телекоммуникационной и информационной инфраструктуры.

3. Шифрование информации с целью последующего вымогательства. Мошенник высылает необходимые для расшифровки данные только после получения денежного

вознаграждения. При этом данный процесс может проходить в несколько итераций, каждая из которых будет сопровождаться повышением стоимости за расшифровку.

4. Кража денежных средств. Мошенники ищут уязвимости в программном обеспечении компании и используют найденные несовершенства для перевода денег на свои счета. Зачастую такая деятельность ведется из-за границы, и отследить движение денежных средств в короткий срок не представляется возможным.

Основной целью большинства кибератак является не прямое получение денежных средств, а кража персональных данных граждан, нарушение работы информационных систем, промышленный шпионаж. Как следствие всего этого, уже и происходит получение денежных средств. В 2023 году было зафиксировано более 900 тысяч хакерских атак на российские компании. Наиболее часто им подвергались банки, медицинские и государственные учреждения. За пять лет наиболее привлекательным объектом для атак злоумышленников стали медицинские учреждения. Большая часть кибератак направлена именно на частных лиц. Во многом это объясняется тем, что на уровне предприятий, особенно крупного бизнеса создаются и постоянно совершенствуются сложные системы защиты. Такая деятельность выделяется в отдельное стратегическое направление деятельности предприятия и контролируется на уровне высшего менеджмента, и такие организации обладают несравненно большими финансовыми и техническими возможностями защиты информации, в то время как частные граждане ограничены в выборе средств защиты.

Самым эффективным способом собственной защиты от киберугроз для граждан является внимательное отношение к собственным персональным данным, особенно при использовании онлайн-сервисов, и регулярное обновление антивирусных программ на личных устройствах. При этом сегодня мошенники все чаще используют методы социальной инженерии, чтобы заполучить необходимую для совершения своих действий информацию. Используя методы психологического давления, они входят в доверие к гражданам под видом финансовых организаций, правоохранительных или государственных надзорных органов. Также в особом спектре внимания кибермошенников находятся субъекты малого и среднего предпринимательства, в том числе на предприятии. Это объясняется рядом причин:

1. Непонимание важности обеспечения кибербезопасности. Происходит это из-за недостаточной информированности. Поэтому руководство таких предприятий склонно выбирать неэффективные методы защиты или же вообще игнорировать их применение.

2. Отсутствие финансовых возможностей для внедрения современных систем защиты. Подобные технологические решения требуют значительных средств, это уменьшает оборотные средства предприятия, что может привести к финансовым показателям и привести к реализации определенных рисков.

3. Недостаток технических мощностей. Системы защиты от кибермошенничества требуют достаточно высоких вычислительных мощностей и дорогостоящего оборудования, что на уровне малого и среднего предпринимательства является заградительным барьером.

4. Отсутствие политик безопасности. Они представляют собой набор правил, установок, имеющих техническую реализацию, которые предприятие использует для обеспечения безопасности. Многие малые и средние предприятия их не имеют или используют в довольно общем виде, что объясняется отсутствием в организационной структуре обособленных подразделений с такими компетенциями.

5. Непонимание сотрудниками основ кибербезопасности. Человеческий фактор нельзя исключать. Эффективное обеспечение кибербезопасности - навык, который можно получить, пройдя специальное обучение. Его организация требует временных и финансовых ресурсов. В то время как в большинстве случаев административный персонал имеет доступ к конфиденциальным данным [11].

Решение этих вопросов должны иметь комплексный характер. Каждый из вышеперечисленных пунктов напрямую взаимосвязан с остальными, поэтому выбирая решения по

обеспечению кибербезопасности субъектам малого и среднего бизнеса необходимо выбирать системные подходы, захватывая все аспекты. Иначе сложно сделать вывод об эффективной киберзащите предприятия. В России на государственном уровне осознается критическая важность развития методов и систем противодействия киберугрозам, что отражено в принятой в 2023 году Доктрине информационной безопасности, утвержденной Указом Президента. Этот документ не только закрепляет ключевые понятия в области кибербезопасности, но и определяет стратегические подходы, направления и методы ее обеспечения. Среди стратегических целей выделяются защита киберпространства РФ, обеспечение суверенитета, укрепление обороноспособности, поддержание стабильности политической и социальной систем, сохранение территориальной целостности и защита конституционных прав граждан [9].

Для реализации этих целей Доктрина предлагает конкретные стратегии, такие как:

1. Развитие национальной инфраструктуры киберзащиты через создание централизованных систем мониторинга и реагирования на киберинциденты, включая Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Например, в 2023 году ГосСОПКА обработала более 500 тысяч инцидентов, из которых 70% были нейтрализованы на стадии обнаружения;
2. Совершенствование нормативно-правовой базы, что подразумевает внедрение строгих стандартов защиты данных и ответственности за киберпреступления, а также гармонизацию законодательства с международными нормами;
3. Стимулирование государственно-частного партнерства, направленного на обмен опытом и технологиями между государственными органами и бизнесом. Примером служит сотрудничество ФСБ и «Ростелекома» в разработке систем защиты критической инфраструктуры;
4. Повышение киберграмотности населения и специалистов через образовательные программы, такие как курсы ДГТУ по кибербезопасности, и кампании, что снижает влияние человеческого фактора.

Эти стратегии подкрепляются деятельностью таких ведомств, как ФСБ, МВД и Центральный банк РФ, которые внедряют инструменты анализа угроз на основе ИИ и технологии шифрования нового поколения. Так, Центральный банк в 2023 году обязал банки использовать системы IDS, что сократило число атак на финансовые организации на 20%. Таким образом, Доктрина задает системный подход, ориентированный на превентивные меры и повышение устойчивости к кибератакам. Сегодня основными субъектами и акторами, обеспечивающими кибербезопасность в России являются служащие государственных органов разного уровня, в чьи должностные компетенции входит данная сфера. Среди организаций, активно развивающих эту сферу, можно выделить МВД, Генеральную прокуратуру, Роскомнадзор, Следственный комитет, ФСБ, ЦБ РФ. Данные субъекты наделены специальными полномочиями и имеют в своем распоряжении правовые, технические, организационные, розыскные и иные возможности и полномочия.

Обсуждение результатов. Необходимо определить ряд методов, ведущих к повышению эффективности защитных мероприятий на предприятии:

1. Использование и постоянное развитие (усложнение) применяемых технических средств и технологических решений.

2. Повышение уровня образования специалистов и развитие кадрового потенциала. Здесь необходимо расширять и углублять программы высшего образования, а также регулярно проводить актуализацию программ дополнительного образования с уклоном на последующее прикладное применение знаний.

3. Непрерывная актуализация нормативной базы с учетом ее практического применения, устранение пробелов в законодательстве и приведении законодательной базы в соответствие с потребностями основных акторов.

4. Применение современных методов оперативно-розыскной деятельности.
5. Создание институтов координации деятельности по противодействию кибермошенничеству на государственном уровне, а также организация возможности оперативного обмена данными между основными субъектами данной отрасли.
6. Масштабирование успешных практик обеспечения кибербезопасности по стране, поиск возможности их каскадирования от крупных организаций к малым [10, 11].
7. Научно-исследовательское обеспечение этой деятельности позволяет определять подходы, снижающие стоимость внедряемых технологий и необходимого оборудования без потери их эффективности [12].
8. Проведение комплексных исследований проблем кибербезопасности, и разработка программ повышения киберграммотности в условиях ограниченных ресурсов.

Мошенники используют различные методы, чтобы достичь своей главной цели - хищения денежных средств. Большинство мошеннических схем направлено на хищение конфиденциальных сведений и персональных данных. Процесс углубления цифровизации будет создавать дополнительные риски, связанные с применением мошенниками современных технологий. Однако развитие инновационных технологий совместно с повышением уровня информированности граждан и развитием образовательных программ способны привести к радикальному снижению деятельности злоумышленников. Именно поэтому, обеспечение кибербезопасности - неотъемлемый элемент цифровизации экономики [6].

Анализ текущего состояния кибербезопасности в России показывает, что проблема защиты от киберугроз становится все более актуальной. Наиболее уязвимыми остаются медицинские учреждения, в которых хранится большая часть персональных данных граждан, а также субъекты малого и среднего бизнеса, у которых часто отсутствуют ресурсы для обеспечения адекватной защиты. Выявленные причины, такие как недостаток знаний, ограниченные финансовые возможности и отсутствие специализированных политик безопасности, указывают на необходимость комплексного подхода к решению вопросов кибербезопасности. Ключевым аспектом является понимание важности киберзащиты не только на уровне предприятий, но и среди частных лиц. В связи с этим рекомендовано проводить регулярные тренинги и повышать осведомленность о киберугрозах, а также использовать доступные технологии защиты информации. На государственном уровне ключевым шагом в обеспечении кибербезопасности стало принятие Доктрины информационной безопасности в 2023 году, которая четко формулирует цели и приоритеты в области киберзащиты, включая защиту национального киберпространства и минимизацию внешних угроз. Однако для повышения эффективности существующих методов требуется их развитие через реализацию конкретных стратегий:

1. Модернизация технических средств защиты – внедрение систем на основе ИИ для анализа больших данных и прогнозирования кибератак, а также использование квантовых технологий шифрования. Например, в 2023 году «Лаборатория Касперского» внедрила ИИ-решения для 300 российских компаний, что сократило время обнаружения угроз до 5 минут.
2. Развитие кадрового потенциала – создание образовательных программ в вузах, таких как ДГТУ и ДГУ, и проведение учений по отражению кибератак. В 2023 году более 500 специалистов прошли подготовку в рамках программы «Киберполигон», что повысило их готовность к реальным инцидентам.

Совершенствование нормативной базы – разработка стандартов для защиты информации в отраслях и обязательная сертификация систем киберзащиты. Например, введение ГОСТ Р 57580.1-2017 для банков увеличило их устойчивость к атакам на 35%. Создание координирующих институтов – формирование межведомственных центров, таких как расширенная сеть ГосСОПКА, для оперативного обмена данными между государством, бизнесом и научным сообществом. В 2023 году ГосСОПКА координировала действия 150 организаций, предотвратив ущерб на сумму более 10 млрд рублей. Эти меры дополняются

масштабированием региональных практик и интеграцией отечественных решений, таких как системы «Код Безопасности», что снижает зависимость от зарубежных технологий. Такой подход не только повышает устойчивость к киберугрозам, но и обеспечивает устойчивое развитие цифровой экономики России, сокращая число успешных атак (в 2023 году их число снизилось на 12% по данным Роскомнадзора).

Вывод. Анализ текущего состояния кибербезопасности в России показывает, что проблема защиты от киберугроз требует системного подхода, что подчеркивает необходимость внедрения описанных стратегий. Их реализация, включая проактивную защиту, адаптивные системы и «нулевое доверие», уже демонстрирует результаты: внедрение ГосСОПКА и MFA сократило ущерб от атак на 18% за год. Для дальнейшего прогресса важно сочетать технические инновации с повышением киберграмотности и координацией усилий всех участников, что обеспечит безопасность как отдельных организаций, так и экономики в целом.

Библиографический список:

1. Вагапов С.В., Сергалина Л.А., Хасанов И.И. Современное состояние цифровизации банковского сектора российской федерации // Актуальные вопросы права, экономики и управления. Сборник материалов VI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых с международным участием. Чебоксары, 2024. С. 98-99.
2. Вахрушев Д.С., Липовская Н.И. Особенности формирования и основные черты рынка услуг по обеспечению кибербезопасности на современном этапе // Вестник Тверского государственного университета. Серия: Экономика и управление. 2019. № 3. С. 162-168.
3. Кобец П.Н. Повышение уровня IT безопасности на основе совершенствования защищенности информационных систем и информационных данных //Актуальные проблемы науки и образования в условиях современных вызовов (шифр - МКАП 30). Сборник материалов XXX Международной научно-практической конференции. Москва, 2024. С. 283-293.
4. Ноговицын М.А. Подходы к формированию модели цифровой трансформации российской экономики в условиях глобальных вызовов // Экономика и управление. 2023. Т. 29. № 1. С. 101-114.
5. Оборин М.С.Экономическая безопасность промышленных предприятий в условиях цифровой экономики//Вестник Самарского государственного экономического университета.2022.№ 1(207).С.44-54.
6. Обухова А.С., Пияльцев А.И. Киберпреступления и кибербезопасность в банковском секторе: понятие и современные угрозы Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2020. Т. 10. № 6. С. 42-51.
7. Полякова Т.А. Развитие системы информационного права в условиях цифровой трансформации: приоритетные направления, проблемы и тенденции // Право.by. 2019. № 5 (61). С. 112-118.
8. Ровенская А.В., Воробьёва Е.Ю. К вопросу обеспечения экономической безопасности в условиях развития цифровой экономики // ЭФО: Экономика. Финансы. Общество. 2023. № 1 (5). С. 102-114.
9. Ронжина Н.А., Глазатов А.А. Развитие системы кибербезопасности в Российской Федерации как основное условие обеспечения национальной информационной безопасности // Право. Безопасность. Чрезвычайные ситуации. 2023. № 1 (58). С. 24-34.
10. Сухина Н.Ю., Якушева А.А., Березина А.И. Основные проблемы, перспективы и финансовые аспекты обеспечения развития системы кибербезопасности в РФ//Лучшая научно-исследовательская работа 2018. сборник статей XIII Международного научно-практического конкурса. 2018. С. 95-98.
11. Шкодинский С.В., Дудин М.Н., Усманов Д.И. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике // Финансовый журнал. 2021. Т. 13. № 3. С. 38-53.
12. Шмидт А.Э., Гуськов П.О., Голубовская С., Ручин К.В., Николаев А.А. Роль информационных систем и технологий в цифровой экономике: перспективы и проблемы для компаний и государства // Финансовая экономика. 2023. № 5. С. 137-140.

References:

1. Vagapov S.V., Sergalina L.A., Khasanov I.I. The current state of digitalization of the banking sector of the Russian Federation. Topical issues of law, economics and management. Collection of materials of the VI All-Russian scientific and practical conference of students, postgraduates and young scientists with international participation. Cheboksary, 2024; 98-99. (In Russ)
2. Vakhrushev D.S., Lipovskaya N.I. Features of the formation and main features of the cybersecurity services market at the present stage. *Bulletin of Tver State University. Series: Economics and Management.* 2019; 3:162-168. (In Russ)

3. Kobets P.N. Improving the level of it security based on improving the security of information systems and information data. Actual problems of science and education in conditions of modern challenges (MKAP 30). Collection of materials of the XXX International Scientific and Practical Conference. Moscow, 2024;283-293.
4. Nogovitsyn M.A. Approaches to the formation of a model of digital transformation of the Russian economy in the context of global challenges. *Economics and management*. 2023; 29(1):101-114 (In Russ)
5. Oborin M.S. Economic security of industrial enterprises in the digital economy. *Bulletin of the Samara State University of Economics*. 2022;1(207):44-54. (In Russ)
6. Obukhova A.S., Piyaltsev A.I. Cybercrime and cybersecurity in the banking sector: the concept and modern threats Proceedings of the Southwestern State University. *Series: Economics. Sociology. Management.* 2020;10(6): 42-51. (In Russ)
7. Polyakova T.A. Development of the information law system in the context of digital transformation: priority areas, problems and trends. *Pravo.by*. 2019;5(61):112-118. (In Russ)
8. Rovenskaya A.V., Vorobyova E.Yu. On the issue of ensuring economic security in the context of the development of the digital economy. *EFO: Economics. Finance. Society*. 2023;1(5):102-114. (In Russ)
9. Ronzhina N.A., Glazatov A.A. Development of the cybersecurity system in the Russian Federation as the main condition for ensuring national information security. *Right. Safety. Emergency situations*. 2023;1 (58):24-34. (In Russ)
10. Sukhina N.Yu., Yakusheva A.A., Berezina A.I. The main problems, prospects and financial aspects of ensuring the development of the cybersecurity system in the Russian Federation.The best research work 2018. collection of articles of the XIII International scientific and practical competition. 2018;95-98. (In Russ)
11. Shkodinsky S.V., Dudin M.N., Usmanov D.I. Analysis and assessment of cyber threats to the national financial system of Russia in the digital economy. *Financial Journal*. 2021;13(3):38-53. (In Russ)
12. Schmidt A.E., Guskov P.O., Golubovskaya S., Ruchin K.V., Nikolaev A.A. The role of information systems and technologies in the digital economy: prospects and problems for companies and the state. *Financial Economics*. 2023;5:137-140. (In Russ)

Сведения об авторах:

Гюльханум Ибадулаховна Качаева, кандидат экономических наук, доцент, заведующая кафедрой информационной безопасности и программной инженерии;providetc@mail.ru

Нариман Гарунович Султанов, студент, nariman.sultanov05@mail.ru

Information about authors:

Gulhanum I. Kachaeva, Cand. Sci. (Econom.), Assoc. Prof., Head of the Department of Information Security and Software Engineering; providetc@mail.ru

Nariman G. Sultanov, Student, nariman.sultanov05@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 09. 03.2025.

Одобрена после рецензирования / Reviced 27.04.2025.

Принята в печать /Accepted for publication 11.05.2025.