ДЕНЬГИ, КРЕДИТ, БАНКИ

УДК 378.018.44: 004 doi 10.29039/2312-5330-2025-2-75-87

Бойченко Олег Валериевич,
доктор технических наук, профессор,
профессор кафедры бизнес-информатики и математического моделирования,
Физико-технический институт,
Крымский федеральный университет имени В. И. Вернадского,
г. Симферополь, Российская Федерация.
Фадина Юлия Юрьевна,
ассистент кафедры бизнес-информатики и математического моделирования
Физико-технический институт,
Крымский федеральный университет имени В. И. Вернадского,
г. Симферополь, Российская Федерация.

Boychenko Oleg Valeriyevich,
Doctor of Technical Sciences, Professor,
Professor of the Department of Business Informatics and Mathematical Modelling,
Institute of Physics and Technology,
V.I. Vernadsky Crimean Federal University,
Simferopol, Russian Federation.
Fadina Yulia Yuryevna,
Assistant of the Department of Business Informatics and Mathematical Modelling,
Institute of Physics and Technology,
V.I. Vernadsky Crimean Federal University,
Simferopol, Russian Federation.

КИБЕРБЕЗОПАСНОСТЬ ДАННЫХ ЦИФРОВОЙ ПЛАТФОРМЫ В ДЕЯТЕЛЬНОСТИ БАНКОВ

CYBERSECURITY OF DIGITAL PLATFORM DATA IN BANKING ACTIVITIES

В статье проведено исследование проблематики кибербезопасности цифровых платформ информационных систем банков в условиях цифровой трансформации. Особое внимание уделяется человеческому фактору, технологическим уязвимостям (облачные среды, IoT-устройства) и регулятивным мерам. Установлено, что банковская сфера является важной целью киберприступников из-за высокой значимости данных и сложности инфраструктур. В исследовании подчеркивается, что 55% киберинцидентов инициируются действиями самих сотрудников информационных систем (фишинг, социальная инженерия), а внешние атаки составляют 23,8%, что выделяет необходимость пересмотра подходов к минимизации рисков. Отдельное внимание уделено анализу технологических уязвимостей, включая облочные среды и IoT-устройства, расширяющие область атак.

Изучая область кибербезопасности данных цифровой платформы в деятельности банков было выявлено, что система защиты должна быть адаптивной. Интегируя искусственный интеллект (ИИ) с целью анализа и обнаружения аномалий, автоматизации реагирования на инциденты, улучшения механизмов аутентификации, платформа сможет предотвращать утечки и нарушения операционной деятельности банковских систем. Показано, что внедрение ИИ сокращает время обнаружения угроз на 40-60%, а также платформы кибербезопасности SIEM/SOAR обеспечивают мониторинг угроз в режиме реального времени. Критически важным элементом выделяется обучение сотрудников, подчеркивается важность программ обучения с симуляцией фишинга, снижающим восприимчивость к фишингу с 30% до 2%, что подтверждается статистикой организаций, которые уже внедрили такие программы.

По данным исследования, проведенного на платформе RB.ru , в большинстве компаний во время первых учений около 30% сотрудников попадаются на фишинг. Однако регулярные тренинги с имитацией атак позволяют снизить этот показатель до 2% и ниже. Аналогичные результаты подтверждены в обзоре средств для симуляции фишинговых атак, где отмечено, что периодические учебные атаки повышают осведомленность сотрудников и минимизируют риски социальной инженерии.

Обоснована необходимость регуляторных мер, включая решения RegTech/Suptech, для автоматизации аудита и соответствия стандартам. В частности, требования Банка России к платформе цифрового рубля предусматривают механизмы обнаружения аномалий в транзакциях и использование российской криптографии. В качестве результатов исследований предложено формирование целостной стратегии безопасности, сочетающей ИИ-технологии, непрерывное обучение персонала и адаптивные политики, что позволяет укрепить защиту в условиях растущей сложности цифровых экосистем в банковской деятельности.

Ключевые слова: кибербезопасность банковских систем, цифровые платформы финансовых организаций, человеческий фактор, фишинг, искусственный интеллект, облачная безопасность, уязвимости, риски, платформы безопасности, обучение сотрудников.

The article examines the issues of cybersecurity of digital platforms of information systems of banks in the context of digital transformation. Special attention is paid to the human factor, technological vulnerabilities (cloud environments, IoT devices) and regulatory measures. It has been established that the banking sector is an important target for cybercriminals due to the high importance of data and the complexity of infrastructures. The study highlights that 55% of cyber incidents are initiated by the actions of information systems employees themselves (phishing, social engineering), and external attacks account for 23.8%, which highlights the need to review approaches to minimizing risks. Special attention is paid to the analysis of technological vulnerabilities, including installation environments and IoT devices that expand the scope of attacks.

Studying the field of cybersecurity of digital platform data in the activities of banks, it was revealed that the protection system should be adaptive. By integrating artificial intelligence (AI) to analyze and detect anomalies, automate incident response, and improve authentication mechanisms, the platform will be able to prevent leaks and operational disruptions in banking systems. It has been shown that the introduction of Ai reduces the threat detection time by 40-60%, as well as the SIEM/SOAR cybersecurity platforms provide real-time threat monitoring. Employee training is highlighted as a critical element, emphasizing the importance of phishing simulation training programs that reduce phishing susceptibility from 30% to 2%, which is confirmed by statistics from organizations that have already implemented such programs.

According to research conducted on the platform RB.ru In most companies, during the first exercises, about 30% of employees fall for phishing. However, regular training with simulated attacks can reduce this figure to 2% or lower. Similar results were confirmed in a review of tools for simulating phishing attacks, which noted that periodic training attacks increase employee awareness and minimize the risks of social engineering.

The necessity of regulatory measures, including RegTech/Suptech solutions, for audit automation and compliance with standards is substantiated. In particular, the requirements of the Bank of Russia for the digital ruble platform provide for mechanisms for detecting anomalies in transactions and the use of Russian cryptography. The results of the research suggest the formation of a holistic security strategy combining AI technologies, continuous staff training and adaptive policies, which makes it possible to strengthen protection in the face of the growing complexity of digital ecosystems in banking.

Keywords: cybersecurity of banking systems, digital platforms of financial organizations, human factor, phishing, artificial intelligence, cloud security, vulnerabilities, risks, security platforms, employee training.

ВВЕДЕНИЕ

Проведенные исследования показывают, что современные аспекты цифровой трансформация представляют из себя не только комплексную программу внедрения современных цифровых технологий в процессы информационных систем банков (чат ботов, искусственного интеллекта, анализа больших данных и т.д.), но и представляет собой преобразование всей структуры финансовой организации, наряду с изменением стратегий, способа и формата предоставления услуг, а также сервисов и продуктов. При этом некомплексный подход к переходу на «цифровые рельсы» бизнес-процессов в компании открывает новые и довольно масштабные возможности для злоумышленников [1]. При этом, главным виновником утраты критически важных информационных ресурсов являются сотрудники банка (34% сотрудников не знают базовых правил кибербезопасности, а 74% утечек произошли по вине рядовых сотрудников).

Однако в 2025 году цифровая трансформация банковского сектора сталкивается с новыми вызовами, связанными с ужесточением требований к защите данных. По данным ФСТЭК России, в 2025 году вступают в силу более строгие национальные стандарты в сфере защиты информации, которые предусматривают обязательное использование российских криптографических алгоритмов и усиленный контроль за облачными средами [2]. Параллельно растет количество атак на цепочки поставок (supply chain attacks), что угрожает не только банкам, но и их партнерам [3]. Особенно актуальна проблема киберугроз, связанных с внедрением технологий цифрового рубля, где требуется комплексная защита транзакций от аномалий и мошеннических действий[4].

Активное внедрение современных технологий дает новые возможности как потребителям финансовых услуг, так и тем, кто их предоставляет: скорость, доступность, комфорт получения разного рода сервисов постоянно увеличиваются. Однако новые технологии несут и новые угрозы — киберриски.

К киберрискам относятся:

- хищение средств клиентов финансовых организаций,
- финансовые потери самих участников рынка,
- нарушение надежности и непрерывности предоставления финансовых услуг,
- развитие системного кризиса из-за кибератак, поразивших крупнейшие банки.

Чтобы киберриски не приводили к таким серьезным последствиям, Банк России следит за киберустойчивостью финансовых организаций, предупреждает их о возможных новых типах атак и способах реагирования на них.

Исследованию проблемных вопросов кибербезопасности данных цифровой платформы, актуальных угроз и поиску решений посвящены работы Козловой Н. Ш., Довгаля В. А., Лебедя С. В., Скворцова И. П., Титарева А. О., Хакимова А. А. и др.

В частности, в работе [5] Козлова Н. Ш. в соавторстве с Довгалем В. А. подчеркивается роль методов защиты данных в условиях растущих угроз, поднимаются темы влияния кибербезопасности в функционировании организаций и проблем, возникающих в сфере кибербезопасности. Также Довгаль В. А. анализирует риски информационной безопасности, акцентируя внимание на необходимости интеграции технологий и регуляторных мер.

Лебедь С. В. в своем исследовании [6] рассматривает роль инновационных технологий в обеспечении кибербезопасности цифровых платформ, подчеркивая важность их адаптации к современным угрозам.

Скворцов И. П. и Титарев А. О. в своей статье [7] утверждают, что непонимание сотрудниками особенностей взаимодействия элементов и процессов информационных систем со средствами защиты информации влечет за собой неосознанное повышение угроз информационной безопасности, возникающих вследствие влияния человеческого фактора. Авторы, в качестве примера, приводят исследование, проведенное “Лабораторией Касперского”, которое ставит человеческий фактор на второе место причин происшествий в области информационной безопасности.

Также, Хакимов А. А. в своем исследовании [8] поднимает вопрос влияние искусственного интеллекта в кибербезопасности и приходит к выводам, что ИИ позволит усилить защиту от киберугроз, способен улучшить обнаружение и реагирование на киберугрозы, сделать процессы аутентификации и авторизации более надежным, а также предотвратить фишинг.

ПОСТАНОВКА ЗАДАЧИ

Работа посвящена анализу проблем кибербезопасности данных цифровой платформы в контексте растущих киберугроз и цифровой трансформации информационных систем банков. Особое внимание уделяется исследованию взаимосвязи между человеческим фактором, технологическими уязвимостями и недостатками в системах защиты, а также их влиянием на устойчивость цифровых экосистем.

Цель работы состоит в исследовании проблем, связанных с современными особенностями безопасности данных цифровой платформы, включая анализ причин инцидентов, оценку эффективности существующих мер защиты и разработку минимизации рисков, связанных с утечкой информации в информационных системах банков.

Задачи работы определены целью исследования и направлены на изучение основных особенностей современных угроз цифровым платформам в банковской сфере, включая атаки на основе социальной инженерии, фишинга и эксплуатацию уязвимостей в облачных средах, IoT-устройствах и периферийных системах, анализе причин доминирования человеческого фактора в киберинцидентах, изучения методик повышения осведомленности сотрудников через имитационные тренинги. Важное внимание уделяется исследованию роли искусственного интеллекта в обнаружении аномалий, автоматизации реагирования на инциденты и усиление механизмов аутентификации, а также оценке эффективности интеграции платформ кибербезопасности для анализа угроз и управления инцидентами в реальном времени.

Достижение указанных задач позволит сформировать системный подход к противодействию угрозам, используя как технологические аспекты, так и человеческий фактор, что соответствует требованиям цифровой трансформации и регуляторным стандартам.

МЕТОДЫ

В исследовании был использован комплекс методов:

- метод системного анализа применен для изучения взаимосвязей между человеческим фактором, технологическими уязвимостями, включая облачные среды, IoT-устройства и периферийные системы, и регуляторными требованиями в контексте кибербезопасности цифровых платформ в деятельности банков;
- метод статистического анализа использован для обработки данных о киберинцидентах, включая долю утечек по вине сотрудников и эффективность имитационных тренингов;
- метод сравнительного анализа использован для оценки эффективности внедрения искусственного интеллекта в область кибербезопасности;
- метод синтеза задействован при разработке рекомендаций по интеграции платформ кибербезопасности, объединяющих мониторинг, анализ угроз и управление инцидентами в реальном времени, а также для получения обобщенных результатов исследования, формулировки выводов и общих заключений.

РЕЗУЛЬТАТЫ

Сегодня обеспечение кибербезопасности необходимо для защиты, во-первых, данных, хранящихся и обрабатывающихся на ресурсах информационных систем банков, во-вторых, всех цифровых процессов. Только ИБ-ориентированный подход к реализации стратегии может обеспечить успех трансформации на каждом ее этапе.

Первостепенные задачи — внедрение методов и политик, направленных на предотвращение нежелательного доступа, обнаружение нарушений и успешное и своевременное реагирование на инциденты безопасности. Сетевая безопасность, безопасность конечных точек, шифрование данных, контроль доступа, планы реагирования на инциденты и обучение сотрудников, а также общее повышение осведомленности пользователей систем и приложений — одни из компонентов комплексного подхода к построению архитектуры кибербезопасности.

Банк России развивает системы мониторинга, интегрирующие данные об инцидентах информационной безопасности, результаты аудита и сценарии киберучений. Современные методы исследований планируют использование RegTech- и SupTech- решений для анализа рисков, что позволит совершенствовать системы внешнего аудита информационной безопасности. Систему внешнего аудита планируется воплотить в отношении:

- аудита по вопросам защиты информации и операционной надежности;
- аудита поставщиков облачных сервисов;
- аудита безопасности приложений.

В том числе, Банк России планирует внедрение системы мониторинга и анализа операционных рисков организаций, благодаря чему будут проработаны вопросы разработки, тестирования и последующей корректировки методики оценки возможностей банков выявлять инциденты информационной безопасности и операционной надежности, реагировать на них и восстанавливаться в случае их реализации. Это позволяет прогнозировать угрозы и минимизировать последствия атак [4].

Однако, несмотря на довольно развитую систему нормативно-правового регулирования мероприятий киберзащиты, наряду с продвинутыми технологическими разработками, киберинциденты в госсекторе и предприятиях малого и среднего бизнеса характеризуются ростом. При этом, причинами инцидентов в 23,8 % случаев являются внешние атаки, а в 55% случаев — действия сотрудников (социальная инженерия).

Социальная инженерия выделяется среди ключевых угроз, по итогам IV квартала 2024 года стала причиной 50 % кибератак на организации и 88% на частных лиц. Первостепенным каналом социальной инженерии для организаций является электронная почта (84%). Злоумышленники используют в атаках утекшие персональные данные, взломанные аккаунты организаций и могут создавать на их основе поддельные. За рассматриваемый период в результате 53% успешных атак на организации была раскрыта конфиденциальная информация, а нарушение основной деятельности компаний наблюдалось в 32% инцидентов. Это требует пересмотра подходов к обучению сотрудников и клиентов распознаванию фишинговых атак и манипулятивных схем.

Новые виды атак, такие как deepfake-звонки для мошенничества, также требуют адаптации мер защиты. По данным экспертов по ИБ, банки, внедряющие биометрическую аутентификацию, основанную на ИИ, смогли снизить риск таких атак. Сбербанк внедрил голосовую биометрию для верификации клиентов, что позволило сократить количество инцидентов, связанных с телефонным мошенничеством на 80% за 2024 год [9]. Банк «Открытие» интегрировал голосовую биометрию в систему верификации клиентов, что позволило предотвратить $15 млн потерь от телефонного мошенничества в 2025 году [10].

Среди современных методов социальной инженерии особое внимание заслуживают атаки, использующие AI-генераторы для создания фишинговых писем. Эти письма отличаются высокой точностью и способны обходить даже продвинутые системы фильтрации. По данным Kaspersky за 2025 год, 53% успешных атак приводят к утечкам данных, а 32% — к нарушению основной деятельности компаний [11].

Фишинг (от англ. fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого получение идентификационных данных пользователей. Согласно интенет-записям, впервые термин «phishing» был использован и зафиксирован 2 января 1996 г. Упоминание об этом произошло в группе новостей Usenet под названием «AOHell» [12].

В настоящее время существует множество методов фишинга. Следует добавить, что фишинг-атака, при помощи сотрудников компании, может применять методы социальной инженерии. Как правило, защите от данного вида атак компании уделяют мало внимания.

Социальная инженерия определяется как действие по манипулированию людьми в совершении действий или разглашении конфиденциальной информации [13].

Обучение информационной безопасности сотрудников, не имеющих базовых представлений, является трудоемким процессом. Для снижения рисков социальной инженерии финансовые организации внедряют регулярные тренинги с имитацией фишинговых атак. Существуют три варианта обучению антифишингу:

1) электронные ресурсы с мультипликационным фильмом;

2) обучающий тест с элементами инфографики;

3) инструкция о противодействии фишингу.

Согласно исследованию А. В. Вилкова, В. М. Литвишкова и Б. А. Швырева внедрение в организацию встроенного подхода к обучению с использованием обучающих моментов в сочетании с наглядными и действенными учебными материалами позволило минимизировать шансы быть подвергнутыми фишинговым атакам на 50%, чем у тех организаций, кто не проходил обучение [14].

Проблема устойчивости сотрудников любой организации к фишинговым атакам актуальна и требует качественной проработки. Помимо представленных выше вариантов обучению антифишингу на рынке представлен ряд программных средств, позволяющих провести симуляцию фишинговой атаки, а также проанализировать полученные результаты, что также может стать отличным инструментом для обучения сотрудников на практике, к примеру:

1) Портал Microsoft Defender;

2) Sophos Phish Threat;

3) Cymulate;

4) Phishing Readiness;

5) Gophish и др.

Эти симуляции проверяют политики и методики безопасности, а также обучают сотрудников повышению их осведомленности и снижению их восприимчивости к атакам.

По статистике, в большинстве компаний во время первых учений около 30% сотрудников попадаются на фишинг, однако благодаря периодическим учебным атакам эта цифра снижается до 2% и ниже [15].

Внедрение искусственного интеллекта (ИИ) в системы мониторинга угроз уже демонстрирует значительные результаты. Например, банк «Альфа» сократил время реагирования на инциденты на 50% после интеграции ИИ в платформы SIEM/SOAR, что подтверждается статистикой Microsoft Security за 2025 год [16]. Эффективность обучения сотрудников также подтверждается: в Citibank уровень уязвимости к фишингу снизился с 25% до 1,5% за год благодаря имитационным тренингам [17]. Однако новые угрозы, такие как атаки с использованием deepfake-аудио для имитации голоса CEO, требуют адаптации существующих мер защиты [3].

Последствия успешных кибератак в IV квартале прошедшего года имели разные исходы, которые затронули как отдельных пользователей, так и организации.

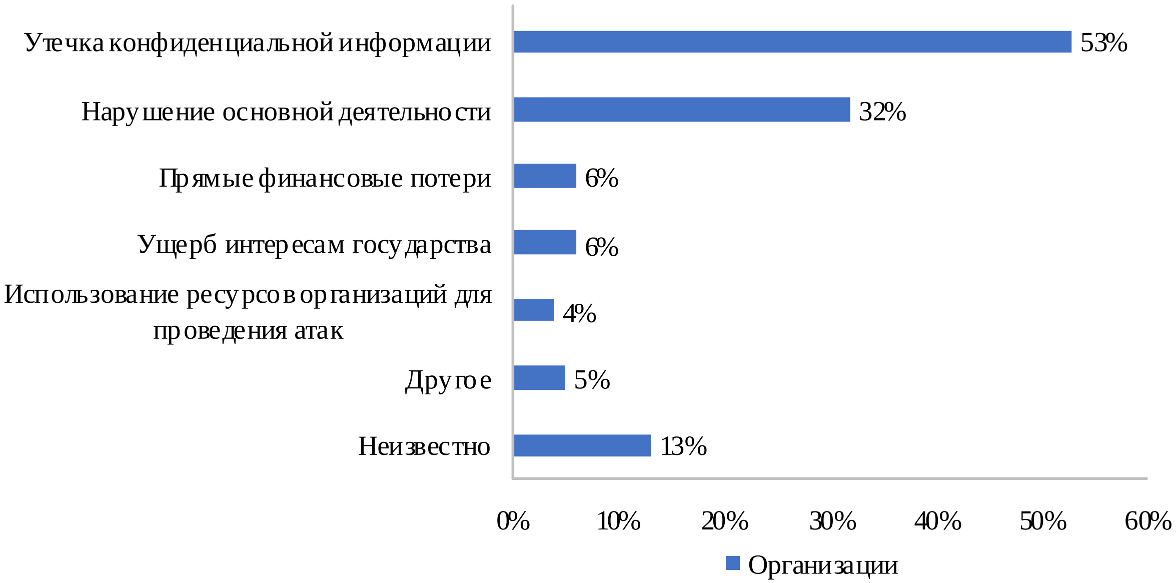

Рис. 1. Последствия атак по доле успешных атак [11].

Преступники, как и весь год, сосредоточивали свое внимание на краже конфиденциальной информации (53% успешных атак) и нарушении основной деятельности (32%) (Рис. 1) [11].

Государственное регулирование является важным аспектом в обеспечении киберустойчивости. С целью создания условий для безопасного внедрения цифровых технологий и обеспечения технологического суверенитета Банк России формирует требования к защите данных для платформы цифрового рубля, включая:

- механизмы обнаружения аномалий в транзакциях (мониторинг операций с целью выявления аномалий, указывающих на возможные мошеннические действия, а также компрометацию участников платформы);
- использование российских криптографических стандартов;
- тестирование аппаратных модулей безопасности [4].

Особую актуальность приобретают угрозы, связанные с внедрением технологий цифрового рубля. По данным Банка России, требования к платформе цифрового рубля включают обязательное использование российских криптографических стандартов и механизмы обнаружения аномалий в транзакциях . Например, тестирование аппаратных модулей безопасности (HSM) показало, что их интеграция с платформами кибербезопасности снижает риск компрометации данных на 50%. Это связано с тем, что HSM обеспечивают защищенное хранение криптографических ключей и выполнение операций шифрования, исключая их экспозицию в программной среде.

Платформа кибербезопасности создана для того, чтобы компании могли объединять в единое целое мониторинг, анализ и контроль всех источников данных, на всех уровнях безопасности, а также повышать уровень защиты, масштабируемость и производительность.

Важным преимуществом применения платформы кибербезопасности является расширенная видимость. В процессе цифрового преобразования банки часто сталкивается с проблемами из-за разнобоя своих цифровых ресурсов и необходимости поддерживать пользователей, облачные развертывания, сети и устройства с различными операционными системами, в различных средах и локациях [18].

Критическими остаются уязвимости в облачных средах и IoT-устройствах. По данным исследований, 20% компаний по всему миру уже в 2018 году сталкивались с атаками на IoT-устройства, а рост их числа продолжает увеличивать риски [19]. Современные исследования подтверждают, что уязвимости в IoT и облачных сервисах остаются ключевыми угрозами для банковской сферы [20]. Для минимизации таких рисков банки внедряют системы управления идентификацией и доступом (IAM), которые позволяют контролировать доступ к облачным ресурсам и снижать вероятность несанкционированных запросов [21].

Платформы безопасности предоставляют широкий функционал для сбора данных, обеспечивая видимость по всем векторам: облако, электронная почта, сеть, конечные и мобильные устройства, веб-службы и устройства IoT. Платформы должны вписываться в корпоративную ИТ-экосистему и в бизнес-процессы, а также интегрироваться с продуктами партнеров, дополняя свои возможности. К ним относятся: SIEM/SOAR, управление идентификацией и доступом, оценка уязвимостей, процесс управления исправлениями, системы обработки обращений в ИТ-службу, аналитические данные об угрозах и многое другое (рис. 2).

Благодаря расширенной видимости и консолидированным функциям безопасности платформа кибербезопасности помогает банкам лучше понимать киберриски, обмениваться информацией о них и управлять ими, а централизованный анализ является важнейшим условием для обеспечения безопасности всей компании.

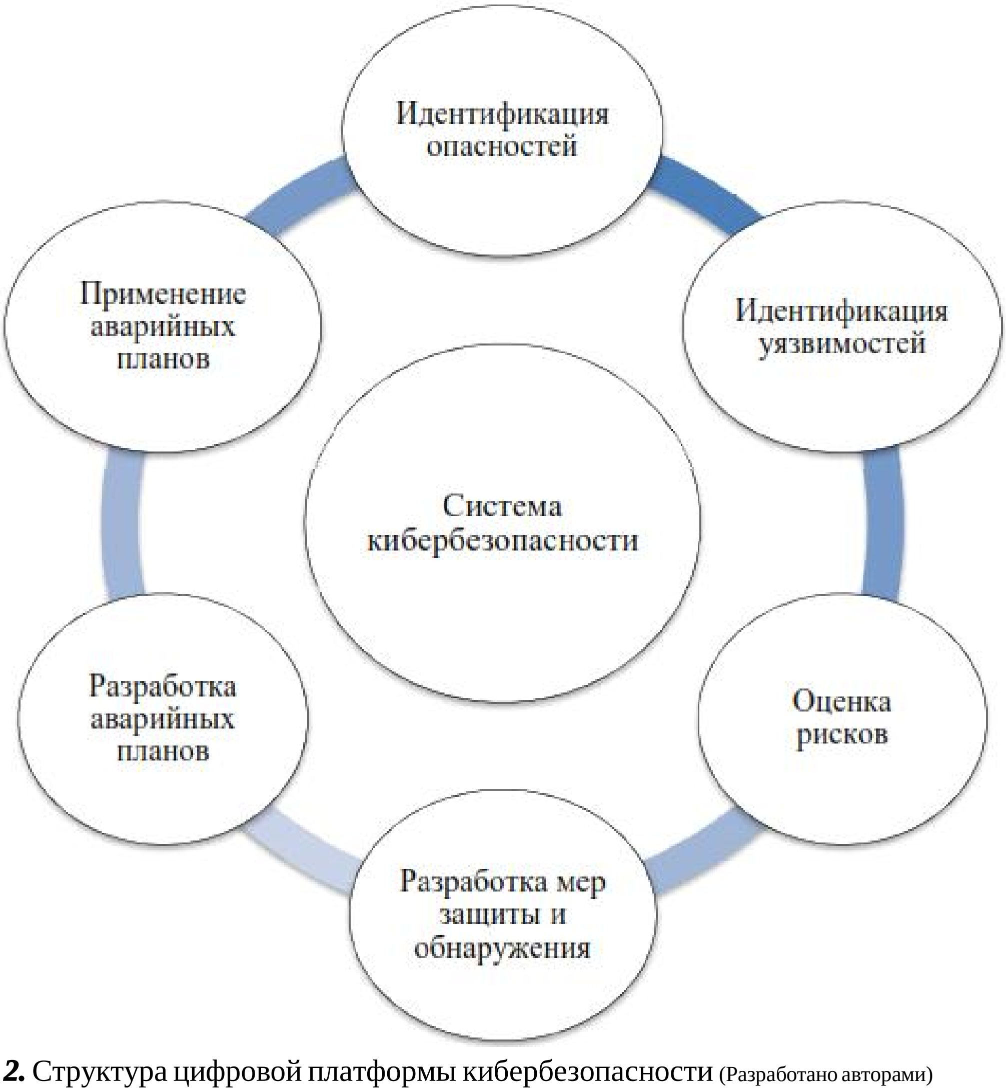
Идентификация опасностей
Идентификация уязвимостей
Оценка рисков
Разработка мер защиты и обнаружения
Разработка аварийных планов
Применение аварийных планов
Система кибербезопасности

Рис. 2. Структура цифровой платформы кибербезопасности (Разработано авторами)

Непрерывная оценка рисков и угроз позволяет видеть и устранять всю подозрительную активность. Единый механизм анализа безопасности, который используется на платформе, облегчает выполнение этой задачи, централизованно анализируя данные, поступающие как от собственных средств обеспечения безопасности, так и от сторонних решений. Кроме того, преимуществами платформы кибербезопасности является обеспечение всесторонней видимости и непрерывная оценка киберрисков, что позволяет создать условия для устранения киберугроз и снижать последствия атак.

А. С. Алпеев, М. М. Безкоровайный и А. Л. Татузов в своих работах выделяют проактивную систему реагирования на внутренние и внешние вызовы и угрозы киберпространства, которая основывается на гибкой методологии Agile, для адаптации команды под новые источники киберугроз [22].

Благодаря интеграции всех уровней безопасности появляется возможность вести анализ рисков, получать проанализированные данные о них и предпринимать практические шаги по устранению различных видов рисков, которым подвергается банк. Если угроза обнаружена, аналитики ИБ могут определить ее тип и источник, узнать, получили ли злоумышленники доступ к системе, обнаружить точку входа, отследить дальнейшее перемещение угрозы по организации и то, какие действия предпринимались — все эти возможности предоставляет единая консоль. Поскольку платформа коррелирует данные и анализирует картину в целом, компания может быстро выявлять события и реагировать на них. Это позволяет минимизировать последствия атаки и совершенствовать протоколы безопасности, чтобы предотвратить следующие атаки (Рис. 3) [23].

До появления платформ кибербезопасности банкам приходилось использовать множество точечных решений для защиты отдельных бизнес-процессов. Однако, чем больше разрозненных

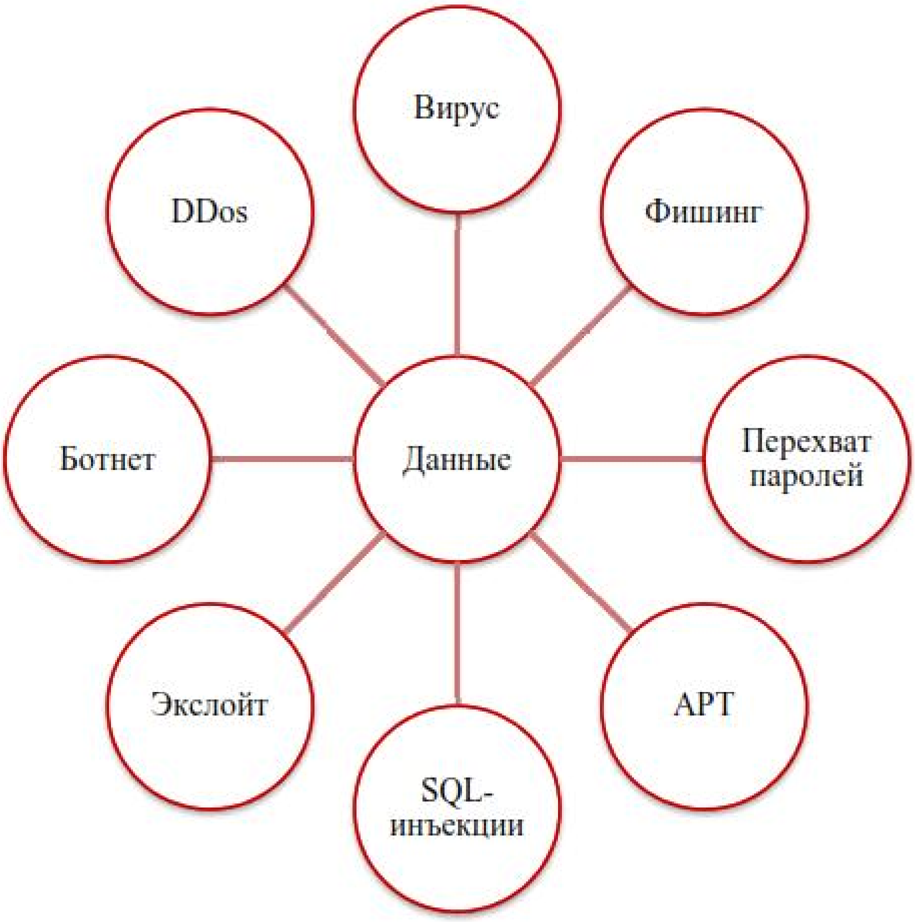

Рис. 3. Угрозы кибербезопасности данных цифровой платформы [23]

инструментов кибербезопасности используется, тем менее эффективна защита. Применение отдельных разрозненных решений приводит к появлению брешей в системе безопасности, которыми могут воспользоваться злоумышленники, потому важна консолидация данных и аналитика в масштабах всей организации, что позволяет выявлять аспекты, которые отдельные механизмы защиты обнаружить не в состоянии [24].

Современные платформы кибербезопасности активно внедряют искусственный интеллект для анализа поведения пользователей и обнаружения аномалий. Варианты использования безопасности ИИ, где он будет наиболее эффективен (табл. 1).

Таблица 1. Варианты использования безопасности ИИ *

Распространенные случаи использования безопасности ИИ	Описание
Контроль доступа и аутентификации пользователей	Системы ИИ проверяют паттерны поведения пользователей при входе в систему для выявления аномального поведения, автоматически активируют дополнительные проверки (принудительная двухфакторная аутентификация) или сброс пароля при выполнении определенных условий, временное ограничение входа пользователя в систему при вероятности компрометации аккаунта.
Защиты периферийных устройств	Алгоритмы ИИ отслеживают все устройства организации, контролируют активность их ПО и антивирусной защиты, автоматически обнаруживают признаки вредоносной активности и другие доказательства кибератаки на устройства организации.
Облачная безопасность	ИИ помогает командам безопасности получить представление о рисках и уязвимостях в их мультиоблачной среде.
Обнаружение киберугроз	Расширенное обнаружение и реагирование (XDR) и информация о безопасности и решения для управления событиями (SIEM) для выявления киберугроз по всему предприятию. Решения XDR отслеживают конечные точки, электронную почту, идентификационные данные и облачные приложения на предмет аномального поведения и сообщают команде об инцидентах или реагируют автоматически в зависимости от правил, определенных операциями безопасности.
Защита информации	ИИ для идентификации и маркировки конфиденциальных данных во всей среде (инфраструктуре организации или в облачное приложение), обнаружении попыток вывода данных из компании, блокировке и сообщении о проблеме.
Расследование инцидентов и реагирование на них	ИИ помогает идентифицировать и сопоставлять наиболее полезные события из нескольких источников данных, экономя драгоценное время специалистов. Генеративный ИИ еще больше упрощает расследование, переводя анализ на естественный язык и отвечая на вопросы также на естественном языке.

* Составлено авторами

Особое внимание в результатах исследования уделено анализу эффективности внедрения искусственного интеллекта (ИИ) в системы кибербезопасности. По данным Microsoft Security за 2025 год, банки, интегрировавшие ИИ в платформы SIEM/SOAR, сократили время обнаружения угроз на 60 %, а автоматизация реагирования на инциденты позволила минимизировать последствия атак на 45 %. Например, банк «Альфа» внедрил алгоритмы машинного обучения для анализа транзакций цифрового рубля, что позволило выявлять мошеннические операции в режиме реального времени с точностью 98 %

Для платформ кибербезопасности искусственный интеллект может стать незаменимым инструментом, преобразуя подходы к защите данных и инфраструктуры. Автоматизация паттернов поведения пользователей, мониторинг устройств организации, обнаружение угроз в облаке и оперативное реагирование на инциденты позволяют банкам не только противостоять сложным атакам, но и предугадывать риски. Внедрение ИИ с решениями XDR, SIEM и системами защиты данных повышает точность обнаружения аномалий, сокращает время реагирования и снижает нагрузку на специалистов информационной безопасности [10].

Сейчас использование единых платформ кибербезопасности еще более важно, чем когда-либо, поскольку банки и специалисты по ИБ сталкиваются с постоянно растущей сложностью обеспечения кибербезопасности. Это связано с цифровой трансформацией информационных систем, с растущим числом сотрудников, которые работают удаленно за периметром корпоративной сети, а также с необходимостью обеспечить конфиденциальность данных и соответствие требованиям регуляторов. В результате поверхность кибератаки постоянно развивается и усложняется, так что для целостного, простого и эффективного контроля рисков и угроз кибербезопасности необходим единый подход [25].

По мере роста поверхности атаки растут и возможности атакующих. Поскольку действия злоумышленников постоянно совершенствуются, банки должны постоянно помнить о возникающих рисках и сознавать их опасность для создания системы проактивной защиты от угроз, а также оперативно выявлять уязвимости и реагировать на события безопасности.

ВЫВОДЫ

Таким образом, применение целостного подхода к жизненному циклу поверхности кибератаки, благодаря централизованной системе цифровой платформы кибербезопасности данных и обучению сотрудников распознавать киберугрозы, возможно создание условий для детализированной аналитики киберугроз в составе:

1. Данные о поверхности атаки (наглядное представление о своих кибер-активах и о возможных векторах атаки);
2. Оценка риска (аналитическая информация об уязвимостях и подверженности риску);
3. Снижение ущерба по последствиям атаки (задействование защитных средств с принятием ответных мер);
4. Унификация и упрощение аналитики и контроля (повышение общей безопасности, наряду с улучшением эффективности, масштабируемости и производительности системы в целом).

Для устойчивости к будущим угрозам банки должны инвестировать в платформы кибербезопасности, объединяющие мониторинг, анализ и реагирование в едином интерфейсе. Это сократит время реагирования на инциденты на 60 % и повысит доверие клиентов, как показано в исследованиях Trend Micro [26]. Кроме того, внедрение программ непрерывного обучения сотрудников, включая симуляции фишинговых атак, позволит снизить восприимчивость к мошенничеству до 2 %. Важно также учитывать рост удаленной работы и IoT-устройств, которые расширяют поверхность атак и требуют адаптации стратегий защиты.

В заключение отметим, что платформа кибербезопасности в деятельности банков включает в себя инструменты для эффективного предотвращения, обнаружения и реагирования, которые позволяют управлять снижением рисков по всей поверхности кибератаки. Она требует баланса между технологиями, людьми и регуляторными механизмами. Успех обеспечивается не только внедрением передовых решений, но и системным подходом к обучению, аудиту и адаптации к развивающимся угрозам. Исследование подтверждает, что только комплексная стратегия, учитывающая все аспекты цифровой экосистемы, способна минимизировать риски и обеспечить устойчивость в условиях глобальной цифровой трансформации информационных систем банков.

СПИСОК ЛИТЕРАТУРЫ

1. Кибербезопасность и цифровая трансформация: 3 главных тенденции защиты данных. — URL: cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (дата обращения: 17.04.2025).

2. Семенычев, А. Прогноз развития рынка информационной безопасности в 2025 году / Алексей Семенычев // CNews. — 2025. — URL: safe.cnews.ru/news/line/2025-03-06_garda_prognoz_razvitiya (дата обращения: 17.04.2025).

3. Санкции и шпионаж: какие киберриски угрожают бизнесу и пользователям в 2025 году // Forbes. — 2025. — URL: www.forbes.ru/tekhnologii/531090-santaz-i-spionaz-kakie-kiberriski-ugrozaut-biznesu-i-pol-zovatelam-v-2025-godu (дата обращения: 17.04.2025).

4. Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на 2023–2025 годы. — М.: ЦБ РФ, 2023.

5. Козлова, Н. Ш. Кибербезопасность и информационная безопасность: сходства и отличия / Н. Ш. Козлова, В. А. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2021. — № 3(286). — С. 88-97. — DOI 10.53598/2410-3225-2021-3-286-88-97. — EDN VSEERU.

6. Лебедь, С. В. Инновационные технологии в сфере кибербезопасности / С. В. Лебедь // Современные информационные технологии и ИТ-образование. — 2022. — Т. 18, № 2. — С. 383-390. — DOI 10.25559/SITITO.18.202202.383-390. — EDN KPPPAC.

7. Скворцов, И. П. О проблеме человеческого фактора в обеспечении информационной безопасности / И. П. Скворцов, А. О. Титарев // Воздушно-космические силы. Теория и практика. — 2022. — № 23. — С. 106-113. — EDN HYFMVI.

8. Хакимов, А. А. роль искусственного интеллекта в кибербезопасности / А. А. Хакимов // Universum: технические науки. — 2023. — № 11-1(116). — С. 58-59. — EDN JVXBHC.

9. Осторожно: дипфейк! Как узнать мошенника на видео // Сбербанк. — 2025. — URL: www.sberbank.ru/ru/person/kibrary/articles/ostorozhno-dipfejk-kak-uznat-moshennika-na-video (дата обращения: 18.04.2025).

10. Что такое ИИ для кибербезопасности? — URL: www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity (дата обращения: 14.03.2025).

11. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. — URL: www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 11.03.2025).

12. History of Phishing / phishing.org. — URL: www.phishing.org/history-of-phishing (date of the application: 16.03.2025).

13. Баева, У. М. Обзор средств для симуляции фишинговых атак / У. М. Баева, В. И. Кураков, А. С. Худадян // Вестник науки. — 2022. — Т. 2, № 5(50). — С. 71-77. — EDN EAUCNA.

14. Вилкова, А. В. Встроенное обучение как элемент непрерывного обучения информационной безопасности / А. В. Вилкова, В. М. Литвишков, Б. А. Швырев // Пенитенциарная наука. — 2020. — Т. 14, № 1(49). — С. 135-141. — DOI 10.24411/2686-9764-2020-10044. — EDN XIDPSR.

15. Как взломать своих сотрудников с помощью фишинга и зачем вам это делать. — URL: rb.ru/opinion/hacking-for-good/ (дата обращения: 15.03.2025).

16. 5 основных тенденций, с которыми ИТ-отделы должны справиться в 2025 году. — ББР Банк, 2025. — URL: bbr.ru/about/press-center/kompiuterra-5-osnovnykh-tendentsii-s-kotorymi-it-otdely-dolzhny-spravitsia-v-2025-godu (дата обращения: 17.04.2025).

17. Ахмеев, А. Кибербезопасность в банковской сфере: вызовы 2025 года / Алексей Ахмеев // Spark. — 2025. — URL: spark.ru/startup/svoi-ru/blog/249815/kiberbezopasnost-v-bankovskoj-sfere-vizovi-2025-goda (дата обращения: 17.04.2025).

18. Что такое платформа кибербезопасности? — URL: www.trendmicro.com/ru_ru/what-is/cybersecurity-platform.html (дата обращения: 14.03.2025).

19. Откуда ждать угрозу уязвимости интернета вещей // Jetinfo. — 2024. — URL: www.jetinfo.ru/otkuda-zhdat-ugrozu-uyazvimosti-interneta-veshhej/ (дата обращения: 15.04.2025).

20. Мадиярбекова, А. Кибербезопасность в устройствах IOT: уязвимости, риски и стратегии снижения рисков / А. Мадиярбекова // Вестник науки. — 2024. — Т. 5, № 12-1(81). — С. 698-706. — EDN PEURQM.

21. Бессараб, М. Всепроникающая безопасность: какие облачные ИБ-решения будут востребованы в 2025 году / Михаил Бессараб, Вадим Католик, Алексей Антонов // K2 Cloud. — 2024. — URL: k2cloud.cnews.ru/articles/2024-10-06_vsepronikayushchaya_bezopasnost_kakie (дата обращения: 17.04.2025).

22. Шкодинский, С. В. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике / С. В. Шкодинский, М. Н. Дудин, Д. И. Усманов // Финансовый журнал. — 2021. — Т. 13, № 3. — С. 38-53. — DOI 10.31107/2075-1990-2021-3-38-53. — EDN MHVBTK.

23. Плохута, К. Д. Особенности количественной оценки рисков в информационной безопасности / К. Д. Плохута // Тенденции развития науки и образования. — 2024. — № 110-16. — С. 80-83. — DOI 10.18411/trnio-06-2024-870. — EDN IONLDX.

24. Никульченкова, Е. В. Проблемы противодействия киберпреступности в России / Е. В. Никульченкова // Психопедагогика в правоохранительных органах. — 2023. — Т. 28, № 3(94). — С. 345-352. — DOI 10.24412/1999-6241-2023-394-345-352. — EDN JMCBEF.

25. Назарова, А. Д. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации / А. Д. Назарова, В. В. Шведов // Столыпинский вестник. — 2023. — Т. 5, № 5. — EDN XYOZYG.

26.Что такое платформа кибербезопасности? // Trend Micro. — 2025. — URL: www.trendmicro.com/ru_ru/what-is/cybersecurity-platform.html (дата обращения: 13.04.2025).

SPISOK LITERATURY

1. Kiberbezopasnost' i tsifrovaya transformatsiya: 3 glavnykh tendentsii zashchity dannykh. — URL: cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (data obrashcheniya: 17.04.2025).

2. Semenychev, A. Prognoz razvitiya rynka informatsionnoy bezopasnosti v 2025 godu / Aleksey Semenychev / / CNews. — 2025. — URL: safe.cnews.ru/news/line/2025-03-06_garda_prognoz_razvitiya (data obrashcheniya: 17.04.2025).

3. Sanktsii i shpionazh: kakiye kiberriski ugrozhayut biznesu i pol'zovatelyam v 2025 godu // Forbes. — 2025. — URL: www.forbes.ru/tekhnologii/531090-santaz-i-spionaz-kakie-kiberriski-ugrozaut-biznesu-i-pol-zovatelam-v-2025-godu (data obrashcheniya: 17.04.2025).

4. Bank Rossii. Osnovnyye napravleniya razvitiya informatsionnoy bezopasnosti kreditno-finansovoy sfery na 2023–2025 gody. — M.: TSB RF, 2023.

5. Kozlova, N. Sh. Kiberbezopasnost' i informatsionnaya bezopasnost': skhodstva i otlichiya / N. Sh. Kozlova, V. A. Dovgal' // Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-matematicheskiye i tekhnicheskiye nauki. — 2021. — № 3(286). — S. 88-97. — DOI 10.53598/2410-3225-2021-3-286-88-97. — EDN VSEERU.

6. Lebed', S. V. Innovatsionnyye tekhnologii v sfere kiberbezopasnosti / S. V. Lebed' // Sovremennyye informatsionnyye tekhnologii i IT-obrazovaniye. — 2022. — T. 18, № 2. — S. 383-390. — DOI 10.25559/SITITO.18.202202.383-390. — EDN KPPPAC.

7. Skvortsov, I. P. O probleme chelovecheskogo faktora v obespechenii informatsionnoy bezopasnosti / I. P. Skvortsov, A. O. Titarev // Vozdushno-kosmicheskiye sily. Teoriya i praktika. — 2022. — № 23. — S. 106-113. — EDN HYFMVI.

8. Khakimov, A. A. rol' iskusstvennogo intellekta v kiberbezopasnosti / A. A. Khakimov // Universum: tekhnicheskiye nauki. — 2023. — № 11-1(116). — S. 58-59. — EDN JVXBHC.

9. Ostorozhno: dipfeyk! Kak uznat' moshennika na video // Sberbank. — 2025. — URL: www.sberbank.ru/ru/person/kibrary/articles/ostorozhno-dipfejk-kak-uznat-moshennika-na-video (data obrashcheniya: 18.04.2025).

10. Chto takoye II dlya kiberbezopasnosti? — URL: www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity (data obrashcheniya: 14.03.2025).

11. Aktual'nyye kiberugrozy: IV kvartal 2024 goda – I kvartal 2025 goda. — URL: www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (data obrashcheniya: 11.03.2025).

12. History of Phishing / phishing.org. — URL: www.phishing.org/history-of-phishing (date of the application: 16.03.2025).

13. Bayeva, U. M. Obzor sredstv dlya simulyatsii fishingovykh atak / U. M. Bayeva, V. I. Kurakov, A. S. Khudadyan // Vestnik nauki. — 2022. — T. 2, № 5(50). — S. 71-77. — EDN EAUCNA.

14. Vilkova, A. V. Vstroyennoye obucheniye kak element nepreryvnogo obucheniya informatsionnoy bezopasnosti / A. V. Vilkova, V. M. Litvishkov, B. A. Shvyrev // Penitentsiarnaya nauka. — 2020. — T. 14, № 1(49). — S. 135-141. — DOI 10.24411/2686-9764-2020-10044. — EDN XIDPSR.

15. Kak vzlomat' svoikh sotrudnikov s pomoshch'yu fishinga i zachem vam eto delat'. — URL: rb.ru/opinion/hacking-for-good/ (data obrashcheniya: 15.03.2025).

16. 5 osnovnykh tendentsiy, s kotorymi IT-otdely dolzhny spravit'sya v 2025 godu. — BBR Bank, 2025. — URL: bbr.ru/about/press-center/kompiuterra-5-osnovnykh-tendentsii-s-kotorymi-it-otdely-dolzhny-spravitsia-v-2025-godu (data obrashcheniya: 17.04.2025).

17. Akhmeyev, A. Kiberbezopasnost' v bankovskoy sfere: vyzovy 2025 goda / Aleksey Akhmeyev // Spark. — 2025. — URL: spark.ru/startup/svoi-ru/blog/249815/kiberbezopasnost-v-bankovskoj-sfere-vizovi-2025-goda (data obrashcheniya: 17.04.2025).

18. Chto takoye platforma kiberbezopasnosti? — URL: www.trendmicro.com/ru_ru/what-is/cybersecurity-platform.html (data obrashcheniya: 14.03.2025).

19. Otkuda zhdat' ugrozu uyazvimosti interneta veshchey // Jetinfo. — 2024. — URL: www.jetinfo.ru/otkuda-zhdat-ugrozu-uyazvimosti-interneta-veshhej/ (data obrashcheniya: 15.04.2025).

20. Madiyarbekova, A. Kiberbezopasnost' v ustroystvakh IOT: uyazvimosti, riski i strategii snizheniya riskov / A. Madiyarbekova // Vestnik nauki. — 2024. — T. 5, № 12-1(81). — S. 698-706. — EDN PEURQM.

21. Bessarab, M. Vsepronikayushchaya bezopasnost': kakiye oblachnyye IB-resheniya budut vostrebovany v 2025 godu / Mikhail Bessarab, Vadim Katolik, Aleksey Antonov // K2 Cloud. — 2024. — URL: k2cloud.cnews.ru/articles/2024-10-06_vsepronikayushchaya_bezopasnost_kakie (data obrashcheniya: 17.04.2025).

22. Shkodinskiy, S. V. Analiz i otsenka kiberugroz natsional’noy finansovoy sisteme Rossii v tsifrovoy ekonomike / S. V. Shkodinskiy, M. N. Dudin, D. I. Usmanov // Finansovyy zhurnal. — 2021. — T. 13, № 3. — S. 38-53. — DOI 10.31107/2075-1990-2021-3-38-53. — EDN MHVBTK.

23. Plokhuta, K. D. Osobennosti kolichestvennoy otsenki riskov v informatsionnoy bezopasnosti / K. D. Plokhuta // Tendentsii razvitiya nauki i obrazovaniya. — 2024. — № 110-16. — S. 80-83. — DOI 10.18411/trnio-06-2024-870. — EDN IONLDX.

24. Nikul’chenkova, Ye. V. Problemy protivodeystviya kiberprestupnosti v Rossii / Ye. V. Nikul’chenkova // Psikhopedagogika v pravookhranitel’nykh organakh. — 2023. — T. 28, № 3(94). — S. 345-352. — DOI 10.24412/1999-6241-2023-394-345-352. — EDN JMCBEF.

25. Nazarova, A. D. Vyzovy i resheniya v oblasti kiberbezopasnosti v epokhu tsifrovoy transformatsii / A. D. Nazarova, V. V. Shvedov // Stolypinskiy vestnik. — 2023. — T. 5, № 5. — EDN XYOZYG.

26. Chto takoye platforma kiberbezopasnosti? // Trend Micro. — 2025. — URL: www.trendmicro.com/ru_ru/what-is/cybersecurity-platform.html (data obrashcheniya: 13.04.2025).

Статья поступила в редакцию 30 апреля 2025 года

Статья одобрена к печати 4 сентября 2025 года