УДК 004.056

КИБЕРУГРОЗЫ В БАНКОВСКОЙ СФЕРЕ И НАПРАВЛЕНИЯ ИХ СНИЖЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Лактюшина Ольга Викторовна[1],
канд. экон. наук, доцент,
e-mail: lakt-olga@mail.ru,

Горбачева Татьяна Александровна[2],
канд. экон. наук, доцент,
e-mail: t-gorbacheva@bk.ru,
[1]Московский университет имени С.Ю. Витте, г. Москва, Россия
[2]Финансовый университет при Правительстве РФ, г. Москва, Россия

Актуальность темы данного исследования обуславливается тем, что цифровая трансформация банковского бизнеса позволила клиентам по всему миру выйти на новый уровень доступности и удобства, однако за этим изменением последовал ряд новых угроз в области кибербезопасности. Финансовые учреждения должны быть готовы к угрозам, исходящим от злоумышленников, которые постоянно разрабатывают новые стратегии, чтобы воспользоваться недостатками банковских систем. Целью работы является исследование потенциальных киберугроз, существующих в банковской сфере, с целью выработки методов их выявления и противодействия. В статье показана разница в понятиях киберугроза, кибератака, киберпредставление. Изучены виды киберрисков в банковском секторе. Проанализированы значимые примеры кибератак на российские банки. На основе проведенного исследования представлены направления минимизации киберугроз в российском банковском секторе. В работе отмечается, что несмотря на постоянное появление новых и усовершенствование старых методов кибератак, знание видов угроз может значительно снизить их реализацию с помощью правильных средств контроля безопасности, что позволит банковскому сектору выйти на более высокий уровень киберустойчивости.

Ключевые слова: кибербезопасность, кибермошенничество, банк, электронные платежи, цифровая валюта, платежные карты, интернет-банкинг, киберугроза, мобильный банкинг, цифровое пространство

CYBER THREATS IN THE BANKING SECTOR AND WAYS TO REDUCE THEM IN THE RUSSIAN FEDERATION

Laktyushina O.V.[1],
candidate of economic sciences, associate professor,
e-mail: lakt-olga@mail.ru,

Gorbacheva T.A.[2],
candidate of economic sciences, associate professor,
e-mail: t-gorbacheva@bk.ru,
[1]Moscow Witte University, Moscow, Russia
[2]Financial University under the Government of the Russian Federation, Moscow, Russia

The relevance of the topic of this study is due to the fact that the digital transformation of the banking business has allowed customers around the world to reach a new level of accessibility and convenience, but this change has been followed by a number of new threats in the field of cybersecurity. Financial institutions must be prepared for the threats posed by intruders, who are constantly developing new strategies to take advantage of the shortcomings of banking systems. The purpose of the work is to study potential cyber threats existing in the banking sector in order to develop methods for their identification and counteraction. The article shows the difference in the concepts of cyber threat, cyber-attack, and cyber representation. The types of cyber risks in the banking

sector have been studied. Significant examples of cyber-attacks on Russian banks are analyzed. Based on the conducted research, the directions of minimizing cyber threats in the Russian banking sector are presented. It is noted in the article that despite the constant emergence of new and improved old methods of cyber-attacks, knowledge of the types of threats can significantly reduce their implementation with the right security controls, which gives organizations a higher level of cyber resilience.

Keywords: cybersecurity, cyber fraud, banking, electronic payments, digital currency, payment cards, internet banking, cyber threat, mobile banking, digital space

DOI 10.21777/2587-554X-2025-1-27-40

Введение

В эпоху непрерывных изменений в сфере информационных технологий финансовые институты и банки находятся в авангарде борьбы против угроз кибербезопасности. Как владельцы значительных объемов финансов и конфиденциальной информации, они привлекают внимание хакеров, стремящихся использовать все более сложные методы атак. Прогнозируемый рост глобального финансового рынка с годовым приростом на уровне 6 % с 2021 по 2025 год подвергает эти учреждения усиленным киберрискам [1].

Бурное развитие финансовой индустрии в сочетании с активными процессами цифровизации привело к значительному увеличению киберугроз, с которыми эта сфера начала сталкиваться. Процесс цифровой трансформации, делающий финансовые сервисы более удобными и эффективными, в то же время открыл широкие возможности для злоумышленников, осуществляющих кибератаки.

Уровень угрозы в секторе финансов возрос значительно. В 2022 году отмечено увеличение инцидентов с кибератаками на 38 % по сравнению с прошлым годом, причем средняя стоимость каждой инцидентной утечки данных составила 5,97 млн долларов[1]. Атаки варьировались от сложных схем вымогательства с использованием вредоносного ПО до масштабных нарушений безопасности данных, целями которых становились крайне чувствительные данные, включая личную финансовую информацию клиентов, защищенные авторским правом торговые алгоритмы и важнейшие бизнес-данные.

Изучение кибербезопасности в контексте банковской отрасли остается не только актуальным, но и играет ключевую роль в поддержании стабильности финансовых институтов.

Статья направлена на исследование потенциальных киберугроз, существующих в банковской сфере, с целью выработки методов их выявления и противодействия. Для реализации данной цели необходимо выполнить ряд задач:

1) исследовать виды киберугроз в банковском секторе;

2) проанализировать примеры кибератак на банковские структуры;

3) выявить направления минимизации киберугроз и повышения кибербезопасности.

В своем исследовании «Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы» ученые-экономисты М.Н. Дудин и С.В. Шкодинский провели всесторонний анализ организации кибербезопасности как в российской, так и в зарубежных банковских системах. Они выполнили многогранный статистический анализ угроз, связанных с кибербезопасностью для банков в России [2]. В результате были разработаны рекомендации и предложения, направленные на организационно-экономическое и правовое совершенствование защиты российских банков как от внутренних, так и внешних киберугроз. В другом своем исследовании авторы систематизировали различные подходы к ключевым категориям: «цифровой суверенитет» и «кибервойна» [3]. М.М. Безкоровайный, А.Л. Татузов исследовали подходы к понятию «кибербезопасность» и считают, что кибербезопасность в банковском секторе представляет собой проактивную систему, которая реагирует на угрозы и вызовы как внутреннего, так и внешнего характера в сфере киберпространства[2]. Банк международных расчетов

[1] IBM Security Cost of a Data Breach Report 2022. IBM. 2022. – URL: https://www.key4biz.it/wpcontent/uploads/2022/07/Cost-of-a-Data-BreachFull-Report-2022.pdf (дата обращения: 10.02.2025). – Текст: электронный.

[2] *Безкоровайный М.М., Татузов А.Л.* Кибербезопасность. Подходы к определению понятия // Вопросы кибербезопасности. – 2014. – № 1. – С. 22–27.

провел опрос членов Глобальной группы по киберустойчивости, посвященный киберрискам и связанным с ними вызовам для центральных банков. Опрос показывает, что с 2020 года центральные банки заметно увеличили свои инвестиции, связанные с кибербезопасностью, отдавая приоритет техническому контролю безопасности и отказоустойчивости[3].

Финансовая индустрия функционирует во все более сложной цифровой среде, интеграция инновационных решений становится не только желательной, но и необходимой для обеспечения целостности финансовых систем и поддержания общественного доверия перед лицом растущих киберугроз.

1. Виды киберугроз в банковском секторе

Цифровая трансформация в сфере банковских услуг значительно усовершенствовала доступность и оперативность их предоставления. Однако, параллельно этот процесс увеличил риски для участников рынка от множества киберпреступлений, подчеркивая критическую необходимость глубокого анализа этих рисков для создания эффективных защитных механизмов.

Киберугроза или угроза кибербезопасности представляет собой термин, который описывает вероятность осуществления кибератаки. Любая угроза, имеющая отношение к кибербезопасности и потенциально способная причинить вред системе, устройству, сети, индивиду или организации, классифицируется как киберугроза. Важно отметить, что киберугроза не обязательно должна приводить к атаке, чтобы считаться угрозой; просто должна существовать вероятность того, что атака может произойти[4].

Киберпреступления – незаконные действия, осуществляемые через применение передовых технологических средств с намерением получения материальной, политической либо другой формы выгоды [4]. Эти процессы осуществляются в том числе через кибератаки. Банковские и финансовые институты часто становятся целями для киберпреступников, подвергаясь их атакам.

Кибератака подразумевает вмешательство в устройства, системы или сети, совершаемое злоумышленниками в киберпространстве. Их целью является доступ к защищенной информации или ее кража с намерением извлечения выгоды, обычно финансового характера[5].

Каждая кибератака мотивирована либо амбицией получения конфиденциальных данных, либо стремлением причинить ущерб цифровой инфраструктуре, что осуществляется путем эксплуатации уязвимостей в системе защиты. Эффективность выполнения такой операции значительно опирается на умения хакера, значимость целевой информации, ограниченную квалификацию администратора кибербезопасности и недооценку важности информационной безопасности в пределах организации.

Атака типа «отказ в обслуживании» или DoS-атака (Denial-of-Service) – это тип кибератаки, который возникает, когда злоумышленник пытается сделать компьютер или другие сети недоступными для авторизованных пользователей путем кратковременного или постоянного прерывания нормальной работы хоста, подключенного к интернету. Другими словами, она происходит, когда киберпреступник лишает авторизованного пользователя доступа к своим личным данным или файлам. Как правило, при DoS-атаке используется один компьютер или группа компьютеров. Они негативно влияют на широкий спектр сервисов, включая онлайн-аккаунты, личные данные, электронную почту, веб-сайты и другие платформы, которые зависят от взломанного[6].

DDoS-атаки (Distributed Denial of Service), широко используемые в киберпреступности, отличаются от традиционных DoS-атак масштабом вовлечения зараженных устройств. Вместо единичного источника атака ведется с использованием сотен, тысяч, а иногда и десятков тысяч компьютеров и дру-

---

[3] *Doerr S., Gambacorta L., Leach T. and el.* Cyber risk in central banking // BIS Working paper. – 2022. – No 1039. – URL: https://www.bis.org/publ/work1039.htm (дата обращения: 10.02.2025). – Текст: электронный.

[4] *Ahmed Al-Zaidy.* What are Cyber-Trears, Cyber-Attacka and how to defend our Systems. Research Proposal Paper: Final Term Project Paper. Strayer University. 2014. – URL: https://www.researchgate.net/publication/349043516_What_are_Cyber-Threats_Cyber-Attacks_and_how_to_defend_our_Systems (дата обращения: 10.02.2025). – Текст: электронный.

[5] *Ahmed Al-Zaidy.* What are Cyber-Trears, Cyber-Attacka and how to defend our Systems. Research Proposal Paper: Final Term Project Paper. Strayer University. 2014. – URL: https://www.researchgate.net/publication/349043516_What_are_Cyber-Threats_Cyber-Attacks_and_how_to_defend_our_Systems (дата обращения: 10.02.2025). – Текст: электронный.

[6] Denial of Service (DoS) Attacks. EC-Counsil. March 2024. – URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-a-dos-attack-denial-of-service/ (дата обращения: 10.02.2025). – Текст: электронный.

гих подключенных устройств. Целью такой атаки является перегрузка сервера запросами до полного его обрушения, что делает невозможным обработку легитимного трафика. Хотя прямой целью DDoS не является кража данных, она может служить отвлекающим маневром для запуска иных атак, направленных на компрометацию безопасности системы. Например, в ходе DDoS-атаки может быть активирован вредоносный код, разработанный атакующими, для выполнения специфических задач, включая несанкционированный доступ или повреждение данных. Аналогичные уязвимости могут быть эксплуатированы и при взломе IoT-устройств («умных вещей»), когда злоумышленники используют их для генерации трафика, нацеленного на банковские и другие критичные инфраструктурные серверы, вызывая их перегрузку и отказ в обслуживании[7].

Вредоносное программное обеспечение, также известное как *malware*, представляет собой разнообразные виды программ, предназначенные для проникновения в банковские системы и кражи денег или конфиденциальной информации. Эта проблема значительно затронула такие страны, как Бразилия, Россия и Германия, что подчеркивает ее всемирную распространенность [5].

Фишинг, безусловно, остается наиболее распространенным способом первоначальной атаки. Традиционно фишинговые электронные письма использовались для того, чтобы обманом заставить пользователя запустить вредоносное вложение, после чего вредоносное ПО могло быть установлено на устройство пользователя. Фишинг учетных данных преследует другую цель. Это практика кражи комбинации логина и пароля пользователя, маскируясь под уважаемую или известную организацию в электронном письме, мгновенном сообщении или другом канале связи. Затем злоумышленники используют учетные данные жертвы для проведения атак на дополнительные цели с целью получения дальнейшего доступа[8]. Злоумышленники используют все более целенаправленные и специализированные вредоносные электронные письма, с помощью которых они могут либо скомпрометировать устройства конечных пользователей, либо получить привилегированный доступ к локальной инфраструктуре или облачным сервисам. Такой несанкционированный доступ может привести к крупным убыткам.

Программа-вымогатель – это тип вредоносного ПО, которое злоумышленники внедряют в компьютерную сеть жертвы для шифрования своих файлов и удержания их с целью получения выкупа. Обычно оно распространяется с взломанного устройства конечного пользователя по всей ИТ-среде организации. Это может поставить под угрозу не только доступность информации и ресурсов, но и их конфиденциальность и целостность. За последние несколько лет использование программ-вымогателей значительно возросло, и только за последний год число случаев утроилось. Программы-вымогатели в основном используются организованной преступностью[9].

Анализ, проведенный исследователями Р. Махарджан и Д. Чаттерджи в 2019 году, сфокусированный на кибербезопасности в финансовой отрасли Непала, выявил наиболее часто встречающиеся угрозы, включая XSS (Cross-Site Scripting), сети зараженных устройств (ботнеты) и подделку идентификационных данных (спуфинг). Эти атаки эксплуатируют уязвимости в программном обеспечении и сетевой архитектуре банков, позволяя злоумышленникам обходить меры защиты и незаконно проникать в финансовую инфраструктуру [6].

SQL-внедрение – сложная киберугроза, которая предполагает использование уязвимостей в кодовой структуре базы данных. Злоумышленник ловко манипулирует SQL-запросами системы баз данных веб-приложения, тем самым позволяя изменять и удалять записи – и все это без ведома или согласия пользователя[10].

Еще одна продвинутая киберугроза касается эксплоитов Zero-day. Это скрытые программные или аппаратные уязвимости, которые хакеры выявляют и используют до того, как разработчикам была

[7] *Ревенков П.В., Бердюгин А.А.* Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. – 2017. – № 3. – С. 16–23.

[8] Data Breach Investigations Report. Verizon. 2021. – URL: https://jre-training.com/WebSecurity/2021-DBIR-Summary.pdf (дата обращения: 10.02.2025). – Текст: электронный.

[9] *Doerr S., Gambacorta L., Leach T. and el.* Cyber risk in central banking // BIS Working paper. – 2022. – No 1039. – URL: https://www.bis.org/publ/work1039.htm (дата обращения: 10.02.2025). – Текст: электронный.

[10] *Mark Hill.* Cyber Threats Definition: A Comprehensive Study. – URL: https://cyberexperts.com/cyber-threats-definition/ (дата обращения: 10.02.2025). – Текст: электронный.

предоставлена возможность ответить патчем. Основываясь на их скрытности и скорости, эти атаки, как правило, очень успешны, что представляет собой насущную проблему для кибербезопасности[11].

В дополнение, работа Р. Менарда, Дж. Ботта и Р. Кросслера, опубликованная еще в 2017 году, акцентирует необходимость глубокого понимания поведенческих аспектов пользователей в контексте кибербезопасности. Применение ими теории мотивационной защиты демонстрирует, как важно осознание и применение знаний о мерах безопасности в повседневных действиях, связанных с кибербезопасностью, подчеркивая ключевую роль образовательных инициатив и повышения уровня информированности среди пользователей для эффективной защиты от кибератак[12].

В числе наиболее часто встречающихся форм киберпреступлений в России можно выделить мошенничество с онлайн-транзакциями, включая операции с применением похищенных данных банковских карт, создание фиктивных интернет-магазинов и незаконные манипуляции с банковскими переводами. Кроме того, распространены схемы обмана через социальные сети и мессенджеры, где преступники стремятся завладеть персональными данными или финансами пользователей [7].

В России активно борются с киберпреступлениями, применяя многоуровневый подход, включающий государственную и частную инициативу. Государственные органы, в том числе правоохранительные, осуществляют анализ тенденций киберугроз и разрабатывают стратегии для их нейтрализации. Финансовые учреждения, а также компании, работающие с конфиденциальной информацией, внедряют сложные системы кибербезопасности и используют передовые технологические решения для обеспечения защиты от вредоносных атак.

Тем не менее, ключевое значение имеет просвещение населения в сфере информационной безопасности, чтобы граждане были в курсе схем киберпреступлений и имели возможность принимать активные шаги для обеспечения защиты своей конфиденциальной информации и денежных средств [8].

Кибермошенничество в России представляет собой значительную угрозу, оказывая вред не только финансовым институтам, но и обычным гражданам, а также органам государственной власти. Согласно отчету Центра по информационной безопасности Банка России за 2020 год зарегистрировано свыше 500 тысяч инцидентов киберпреступлений, что на 23 % превышает показатели предыдущего года[13].

Кража конфиденциальной информации занимает одно из лидирующих мест среди методов киберпреступности в России, когда злоумышленники, представляясь сотрудниками финансовых учреждений или других компаний, требуют от потерпевших разглашения персональных данных или осуществления финансовых переводов на их реквизиты. В арсенале преступников также широко применяются методы использования вирусов и троянских программ, нацеленных на непосредственное изъятие финансовых активов с аккаунтов жертв [9].

Ещё один частый метод кибермошенничества в России – мошенничество с платёжными картами. Злоумышленники похищают информацию по картам и применяют ее для осуществления нелегальных операций.

В 2022 году произошел рост несанкционированных финансовых операций на 4,29 % по отношению к предыдущему году, что коррелирует с интенсификацией внедрения новейших методов проведения дистанционных платежей и увеличением объема выполняемых денежных транзакций (+39 %, до 1458,6 трлн руб.) через электронные платежные инструменты, включая карты, электронные кошельки и другие формы е-платежей. Однако, благодаря усиленным мерам безопасности, принимаемым банковскими учреждениями для предотвращения мошеннических действий, число таких операций в 2023 году сократилось на 15,31 %. К 2022 году доля неавторизованных операций от общего объема переводов снизилась до 0,00097 % (против 0,00130 % в предыдущем году), оставаясь заметно ниже нормативного значения в 0,005 %, заданного Центральным банком РФ для операций, осуществляемых с применением платежных карт (рисунок 1)[14].

[11] *Mark Hill.* Cyber Threats Definition: A Comprehensive Study. – URL: https://cyberexperts.com/cyber-threats-definition (дата обращения: 10.02.2025). – Текст: электронный.

[12] *Menar P., Bott G.J. and Crossler R.E.* User motivations in protecting information security: Protection motivation theory versus self-determination theory // Journal of Management Information Systems. – 2017. – № 34 (4). – P. 1203–1230.

[13] Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. Банк России. 2021. – URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 10.02.2025). – Текст: электронный.

[14] ЦБ РФ. Обзор операций, совершенных без согласия клиентов финансовых организаций. – URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 10.02.2025). – Текст: электронный.

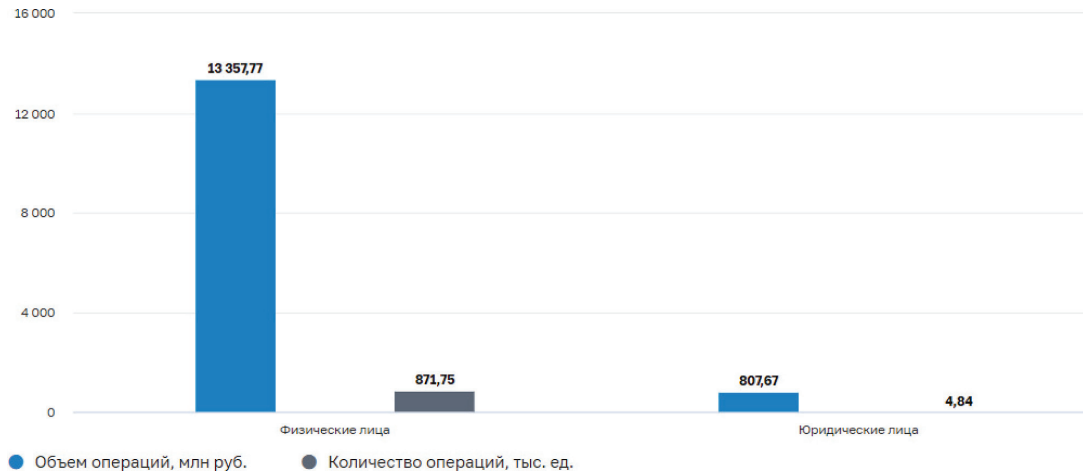

Рисунок 1 – Динамика операций без согласия клиентов в 2022 году: физические и юридические лица[15]

Преобладающим методом, применяемым мошенниками для присвоения финансов, продолжает быть социальная инженерия, при котором, под влиянием психологического давления, жертва испытывает принуждение к передаче финансов или конфиденциальных финансовых данных, что позволяет преступникам осуществить кражу. Процентное соотношение подобного вида мошенничества достигло в 2022 году 50,4 % в сравнении с 49,4 %. Согласно анализу Банка России, в 2022 году фиксируется рост средней величины ущерба от каждого случая кражи, осуществленного через социальную инженерию, что способствовало увеличению общего объема убытков от незаконных операций, произведенных без разрешения владельцев счетов (рисунок 2)[16].

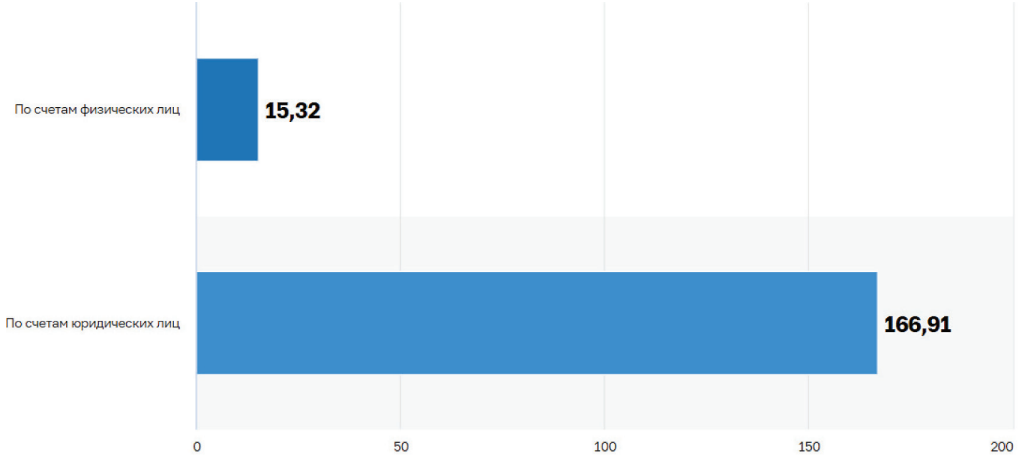

Рисунок 2 – Средняя сумма одной операции без согласия клиента в 2022 году (тыс. руб.)[17]

В 2022 году клиентам кредитных организаций возвратили 4,4 % (618,4 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия клиентов (в 2021 году данный показатель составил 6,8 % или 920,5 млн руб.)[18].

[15] ЦБ РФ. Обзор операций, совершенных без согласия клиентов финансовых организаций. – URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 10.02.2025). – Текст: электронный.
[16] ЦБ РФ. Обзор операций, совершенных без согласия клиентов финансовых организаций. – URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 10.02.2025). – Текст: электронный.
[17] ЦБ РФ. Средняя сумма одной операции без согласия клиента в 2022 году (тыс. руб.). – URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 10.02.2025). – Текст: электронный.
[18] ЦБ РФ. Средняя сумма одной операции без согласия клиента в 2022 году (тыс. руб.). – URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 10.02.2025). – Текст: электронный.

Таким образом, можно заметить, что киберугрозы становятся все более сложными для обнаружения, а цели злоумышленников – более разнообразными. В последние годы наблюдается увеличение числа атак, ориентированных на конкретные компании, особенно в банковской сфере, с основной целью – получение финансовой выгоды. Эти действия зачастую предваряются тщательным изучением хакерами своих жертв. Хотя успешность противодействия кибератакам возросла, убытки национальной банковской системы продолжают расти. Ситуация подчеркивает важность повышения устойчивости банковской системы и необходимости развития эффективных мер защиты от киберугроз, чтобы сохранить доверие населения.

2. Анализ примеров кибератак в РФ

Проанализируем несколько значимых кибератак, случившихся на территории России (таблица 1).

Таблица 1 – Значимые киберинциденты, зарегистрированные в Российской Федерации[19]

Банк	Украденные деньги/данные	Потери/убытки	Год
Центробанк России	2 млрд рублей ($31 млн)	2 млрд рублей ($31 млн)	2016
ПАО «Сбербанк»	Данные 200 тыс. кредитных карт	Более 2 млрд рублей	2019
Банки Татарстана	Более 1 млрд рублей	Более 1 млрд рублей	2018–2019
ПАО «Альфа-Банк»	Данные 700 тыс. клиентов	Не указано	2020

В июле 2016 года группа неопознанных киберпреступников осуществила масштабную хакерскую атаку на Банк России. Используя слабости в программном обеспечении, применяемом одним из его департаментов, злоумышленники проникли в его информационные системы. Далее, осуществив кражу финансовых средств, они перечислили похищенные активы на счета в местных банках, с последующим обналичиванием через банкоматы. Общий ущерб составил порядка 2 млрд рублей, эквивалентных приблизительно 31 млн долл. по курсу на момент преступления. Сразу после выявления проникновения Центральный банк оповестил компетентные органы, начав совместную работу по расследованию инцидента[20].

В июле 2019 года киберпреступники осуществили сложную атаку на информационные системы ПАО «Сбербанк», значительного игрока на финансовом рынке России, в результате чего были скомпрометированы данные свыше 200 тысяч держателей кредитных карт. Эксперты оценивают финансовые потери для банка от данного инцидента в размере свыше 2 млрд рублей[21].

Возникший инцидент был результатом взлома веб-платформы аффилированного с банком партнера, предоставляющего услуги по оформлению кредитных карт. Злоумышленники успешно преодолели защитные меры, нарушив целостность базы данных партнера, что привело к несанкционированному доступу к конфиденциальным сведениям. Данные включали номера карт, полные имена держателей, периоды их действия, а также трехзначные защитные CVV-коды более 200 тыс. учетных записей[22].

Немедленно после выявления нарушения «Сбербанк» проинформировал о происшествии правоохранительные органы и приступил к восстановлению своих информационных систем. Банк также объявил, что пострадавшие от утечки данных клиенты были оповещены о произошедшем и обеспечены заменой банковских карт на новые с изменёнными реквизитами.

Серия кибератак, направленная против финансовых учреждений в Татарстане, включая инциденты с «Банком Идея», происходила между 2018 и началом 2019 года. В ходе этих атак из систем банков было незаконно изъято более одного миллиарда рублей. Преступники применяли высокоэффективные

[19] Составлено авторами.
[20] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Банк России. 2017. – URL: https://cbr.ru/Collection/Collection/File/32089/GUBZI-4.pdf (дата обращения: 10.02.2025). – Текст: электронный.
[21] TASS. СБЕР предотвратил хищение средств клиентов на сумму более 25 млрд руб. – URL: https://tass.ru/ekonomika/6874941 (дата обращения: 10.02.2025). – Текст: электронный.
[22] TASS. СБЕР предотвратил хищение средств клиентов на сумму более 25 млрд руб. – URL: https://tass.ru/ekonomika/6874941 (дата обращения: 10.02.2025). – Текст: электронный.

методики социальной инженерии и фишинговые атаки для проникновения в банковские информационные системы.

В процессе расследования обнаружено, что ответственность за нападения несет китайская хакерская организация, получившая обозначения “APT10” и “Stone Panda”. Данная киберпреступная сеть имеет причастность к многочисленным глобальным киберинцидентам, среди которых значится взлом корпорации Hewlett Packard Enterprise в 2015 году[23].

В ответ на серию нападений на финансовые учреждения в Татарстане российские спецслужбы в кооперации с китайскими контрразведывательными агентствами осуществили комплекс международных антитеррористических операций. Их целью было идентифицировать и арестовать участников преступной сети. В ходе этих операций были успешно задержаны несколько ключевых фигур этой группы в различных уголках мира и экстрадированы в Российскую Федерацию для проведения уголовного процесса.

В 2020 году ПАО «Альфа-Банк» был подвержен кибератаке, в результате которой были украдены данные более чем 700 тысяч клиентов. Данное нарушение безопасности было осуществлено с использованием метода фишинга, основывающегося на распространении мошеннических электронных сообщений, имитирующих надежные источники, с целью обманным путем получить персональные данные от получателей.

В ходе атаки произошла утечка личной информации пользователей финансового учреждения, содержавшей контактные номера, места жительства и сведения о банковских картах. Тем не менее, представители банка подчеркнули, что критические данные, необходимые для совершения транзакций, не были затронуты и остались под надежной защитой [10].

После выявления нарушения банк активизировал процессы по обеспечению конфиденциальности информации клиентов, сотрудничая с правоохранительными структурами. Дополнительно были реализованы мероприятия по повышению уровня защиты информационных систем, в том числе осуществление аудиторских проверок и наращивание мер контроля доступа к конфиденциальным данным.

В России растет число кибернападений на ведущие предприятия и государственные структуры. Часто такие атаки связаны с попытками получения конфиденциальной информации или с целью вымогательства денег [11].

Таким образом, существует необходимость в усиленной работе по защите банковской инфраструктуры и данных клиентов, а также в координации мер по борьбе с киберпреступлениями как на национальном, так и на международном уровне.

3. Направления минимизации киберугроз и повышения кибербезопасности

В Российской Федерации действуют законодательные и подзаконные акты, направленные на регулирование кибербезопасности и защиты конфиденциальной информации. Ключевые документы в этой области – это Федеральный закон «О персональных данных» и нормативный акт Центрального банка, устанавливающий стандарты безопасности обработки персональных данных в информационных системах, применяемых в банковском секторе.

Российские банковские институты обязаны придерживаться нормативов информационной безопасности, установленных ЦБ РФ. Данные регламенты устанавливают критерии для обеспечения защиты информационных ресурсов, охватывая персональные данные вкладчиков, инфраструктурные элементы банков, а также цифровые коммуникационные каналы [12].

Банк России активно занимается противодействием киберпреступности, регулярно выпуская отчеты с рекомендациями и предложениями для укрепления экономической безопасности финансовых учреждений в контексте борьбы с киберугрозами.

В своих докладах Центральный банк РФ подчеркивает критическую важность разрабатывания и применения комплексных стратегий для обеспечения информационной безопасности, включая укре-

[23] PWC. With AI’s great power October 2019 comes great responsibility. – URL: https://www.pwc.in/assets/pdfs/consulting/technology/data-and-analytics/with-ai-s-great-power-comes-great-responsibility.pdf (дата обращения: 10.02.2025). – Текст: электронный.

пление защиты персональных данных пользователей, гарантию стабильности и безопасности выполнения финансовых транзакций, применение передовых технологий защиты информации и усиление контроля над активностью сотрудников банка.

Банк России настоятельно советует финансовым институтам активно применять инструменты мониторинга и аналитики данных для оперативного выявления и эффективного предотвращения киберугроз, осуществлять систематическую аудиторскую оценку информационных систем, а также непрерывно улучшать методы управления кибербезопасностью.

В дополнение Центральный банк РФ призывает банковские учреждения к усиленному взаимодействию в пределах профессиональных ассоциаций, а также к обмену данными о появляющихся рисках и способах обеспечения безопасности против них.

Начиная с 1 июля 2018 года, Банк России внес изменения в структуру отчетности об инцидентах, затрагивающих информационную безопасность. В отчетности будут указываться экономические последствия для операторов и их клиентов. Это позволит повысить достоверность данных о событиях, связанных с нарушением защиты информации, так как предоставляемая информация позволит более точно оценивать качество систем управления рисками и систем управления капиталом кредитных организаций [13].

Исходя из проблем, которые были выявлены, можно перейти к разработке предложений, которые могут помочь банкам повысить свою экономическую безопасность и противодействовать кибермошенничеству.

Повышение квалификации работников банка является ключевым элементом укрепления безопасности финансовых операций перед лицом роста киберпреступности. Оно способствует развитию профессиональных навыков сотрудников, углублению их понимания принципов информационной безопасности и освоению методик выявления и нейтрализации кибератак.

Для оптимизации и систематизации процесса обучения сотрудников рекомендуется выполнить ряд мероприятий. Необходимо провести анализ компетенций персонала по информационной безопасности. Для оценки уровня знаний сотрудников по информационной безопасности можно использовать различные методы и инструменты.

Одна из стратегий – организация проверки уровня квалификации сотрудников, которая может реализовываться как через внутренний аудит, осуществляемый самостоятельно финансовым учреждением, так и через аутсорсинг с привлечением внешних консалтинговых компаний. Аудит позволит выявить зоны риска, связанные с недостаточными знаниями персонала, и предложить рекомендации по улучшению обучения [14].

Еще одним методом оценки уровня знаний сотрудников может быть проведение тестирования. Реализация может проходить через онлайн-тесты на специализированных образовательных платформах или непосредственно в формате live-сессий, организуемых экспертами в области кибербезопасности. Анализ результатов такого тестирования позволяет выявить пробелы в профессиональных знаниях сотрудников, что дает возможность сфокусировать образовательные проекты на их исправлении.

Также можно использовать метод анонимного опроса сотрудников. Содержание анкет может охватывать вопросы осведомленности сотрудников о принципах и правилах информационной безопасности в финансовой организации, выявление их запросов и затруднений в этой сфере, а также определение вида киберугроз, которые они расценивают как наиболее значимые. Анализ полученных данных предоставляет возможность более целенаправленного и адаптированного к конкретным потребностям сотрудников усиления обучающих программ.

На основе результатов анализа знаний сотрудников необходимо разработать обучающие программы, которые позволят повысить уровень знаний и умений сотрудников. Программы могут включать в себя как теоретический материал, так и практические упражнения.

Систематическое развитие компетенций сотрудников в сфере кибербезопасности критично для их способности оперативно адаптироваться к новым угрозам информационной среды. Постоянное повышение квалификации в данной области представляет собой ключевой элемент стратегии обеспечения защиты финансовых учреждений от кибератак.

Чтобы обеспечить высокую результативность процесса обучения, важно придерживаться определённых основополагающих правил.

Во-первых, процесс обучения должен быть непрерывным, исключая возможность одноразовых мероприятий. Проведение тренингов необходимо с частотой минимум раз в год или квартал в сочетании с систематическим обновлением учебных материалов и ресурсов в области информационной безопасности.

Во-вторых, курсы по кибербезопасности должны быть доступны абсолютно всем сотрудникам, взаимодействующим с данными клиентов, включая не только IT-профессионалов, но и персонал, потенциально подверженный кибератакам, такой как работники отделов продаж и поддержки пользователей.

В-третьих, процесс обучения должен быть индивидуализирован, ориентирован на уникальные требования и интересы каждой группы работников. Так, курсы для IT-профессионалов будут включать в себя углубленное изучение технологических деталей, в то время как образовательные программы для персонала в сфере продаж могут акцентироваться на навыках распознавания манипулятивных техник и защиты от фишинга [13].

Наконец, обучение должно быть оценено для того, чтобы убедиться, что оно достаточно эффективно. Применение методов оценки, таких как экзамены для проверки усвоенных знаний, анкетирование и сбор отзывов участников, позволяет комплексно оценить достигнутый уровень подготовки. Используя данные оценки, можно совершенствовать учебный процесс, тем самым повышая эффективность защитных мер банковской системы против кибератак.

В секторе банковских услуг критически важным является применение передовых решений и инструментальных средств для борьбы с растущими угрозами кибербезопасности. В первую очередь, это включает в себя использование современных систем аутентификации и авторизации, таких как двухфакторная аутентификация, биометрическая идентификация и т.д. Подобные меры значительно повышают уровень защиты информации о счетах и транзакциях клиентов, в то же время уменьшая шансы на успешные атаки мошенников в киберпространстве.

Следует подчеркнуть, что инструменты обнаружения вторжений (Intrusion Detection Systems, IDS) представляют собой ключевой элемент защитной стратегии финансовых учреждений против киберпреступности. Эти системы способны анализировать сетевой трафик, выявлять неправомерные действия и оповещать IT-специалистов о возможных рисках для информационной безопасности. Разнообразие настроек IDS позволяет идентифицировать специфические виды атак, в том числе направленные против веб-приложений, нарушения границ сетевого периметра или компрометацию баз данных [15].

Также банки применяют криптографические методы для обеспечения безопасности секретной информации, транслируемой по сетевым каналам. Криптография обеспечивает защиту информации от несанкционированного доступа и использования, кодируя её в формат, нечитаемый для неуполномоченных лиц. Криптографические методы служат защитой для данных, пересылаемых через интернет, включая логины, банковские карты и прочую важную информацию.

Следует подчеркнуть, что применение инструментов для обнаружения несанкционированного доступа и криптографической защиты информации, хотя и существенно повышает уровень защищенности, не способно ее гарантировать от всех видов киберугроз. В комплексе с дополнительными мерами безопасности, включая методы двухэтапной верификации, проведение информационно-образовательных мероприятий для пользователей относительно правил безопасного поведения в сети, а также актуализацию программных решений, значительно снижается вероятность успешных хакерских атак.

Важно также регулярно обновлять и тестировать системы безопасности, чтобы убедиться в их эффективности и готовности к обнаружению и предотвращению киберугроз. Это включает в себя регулярное обновление программного обеспечения и аппаратных средств, а также проведение пенетрационного тестирования, которое может помочь выявить слабые места в системе и устранить их до того, как к ним смогут обратиться злоумышленники [16].

Применение передовых технологий в сфере безопасности считается ключевым элементом в предотвращении кибератак против банковских учреждений. Однако критически важно реализовать эту технологическую составляющую на фоне грамотно подготовленных специалистов и придерживаться строгих протоколов безопасности для достижения максимальной защищенности.

Мониторинг транзакций является важной составляющей в обеспечении безопасности финансовой деятельности банка. Целью мониторинга транзакций является выявление потенциальных мошеннических схем и предотвращение кражи средств с банковских счетов.

Мониторинг транзакций может проводиться как с использованием автоматизированных систем, так и вручную банковскими аналитиками. Автоматизация способствует скоростной и точной обработке обширных данных, в то время как ручная проверка позволяет идентифицировать более сложные мошеннические операции, которые могут оставаться незамеченными для алгоритмов.

При мониторинге транзакций используются различные методы анализа данных, такие как анализ поведения клиентов, анализ транзакционной активности и анализ сравнительных данных. Анализ поведения клиентов включает в себя сопоставление текущих транзакций с предыдущими операционными данными клиента, чтобы выявить любые аномалии в его поведении. Изучение транзакционной активности охватывает детализированный анализ операций по нескольким критериям, включая величину операций и географию отправителя и получателя с целью выявления любых необычных паттернов. Современные системы мониторинга транзакций также могут использовать аналитические инструменты и технологии, такие как машинное обучение и искусственный интеллект, для обнаружения мошеннических схем. Например, системы машинного обучения могут использоваться для построения моделей, которые могут автоматически выявлять аномалии и необычные паттерны в транзакционной активности клиентов.

Сотрудничество с правоохранительными органами является важной составляющей борьбы с киберпреступностью. Для повышения эффективности этого процесса важно разработать и внедрить систему сотрудничества с правоохранительными структурами, способную оперативно реагировать на инциденты кибербезопасности и уменьшать время на их урегулирование. Одним из способов оптимизации сотрудничества является заключение соглашений о взаимодействии с правоохранительными органами. Такие соглашения позволяют устанавливать четкие правила и процедуры взаимодействия, определять ответственность и обязанности каждой из сторон, а также определять механизмы обмена информацией [17].

Для повышения эффективности взаимодействия необходимо внедрить механизм оперативного уведомления органов правопорядка о происшествиях, угрожающих безопасности. Для этого необходимо разработать процедуры, которые позволят быстро определять и уведомлять о возможных кибератаках, а также регулярно проводить учебные тренировки и симуляции сотрудников, чтобы они знали, как быстро и правильно реагировать на инциденты [18].

Дополнительно, к укреплению кооперации с правоохранительными структурами, банки могут участвовать в совместных проектах по борьбе с киберпреступностью, а также оказывать экспертную помощь в разрешении инцидентов безопасности. Участие в таких межсекторальных проектах и исследованиях способствует повышению уровня взаимного понимания и уверенности между банковскими учреждениями и правоохранительными органами, а также помогает в развитии новых методов и технологий борьбы с киберпреступностью.

Развертывание системы обнаружения вторжений представляет собой критически важный элемент стратегии защиты от киберугроз. Эти системы сканируют трафик в сети на предмет аномалий, которые могут указывать на попытки неавторизованного доступа, и оповещают об этом. Но процесс интеграции IDS в инфраструктуру организации сложен, требует глубокого понимания информационной безопасности и умения работать с соответствующими технологиями.

Одним из первых шагов при внедрении системы IDS является оценка потребностей и возможностей компании. Необходимо определить, какие типы угроз могут возникнуть и какие уязвимости существуют в сети компании. На основе этих данных можно выбрать подходящую систему IDS и определить ее конфигурацию [19].

После выбора системы IDS необходимо ее установить и настроить. Это включает в себя определение параметров системы, настройку фильтров, настройку уведомлений и других настроек, которые обеспечивают оптимальную работу системы.

Следующий шаг – провести тренинги для персонала по работе с системой, включая правильное распознавание и реагирование на уведомления системы. Также важно проводить регулярные тесты работы системы IDS для определения ее эффективности и выявления возможных проблем.

Кроме того, для оптимизации процесса внедрения системы IDS можно привлечь сторонних экспертов в области информационной безопасности, которые помогут выбрать наиболее подходящую си-

стему IDS и настроить ее для оптимальной работы. Также можно использовать облачные сервисы для ускорения процесса установки и настройки системы IDS.

Сотрудничество между банками и другими организациями является ключевым фактором в борьбе с киберугрозами. Для улучшения и оптимизации данного процесса необходимо принять несколько мер.

Во-первых, нужно организовать создание платформы для обмена информацией о киберугрозах, это является важным шагом в повышении кибербезопасности в банковской сфере. Это позволит банкам и другим организациям быстро получать информацию о новых угрозах и обмениваться своими наработками по предотвращению кибератак.

Обмен данными о кибератаках возможен через интегрированные базы и инструменты аналитики. Это требует создания унифицированных норм для аккумуляции и интерпретации данных о киберопасности и налаживания координации в передаче сведений между субъектами сети.

Однако при создании такой платформы необходимо обеспечить высокий уровень конфиденциальности информации. Для этого можно использовать различные методы шифрования и механизмы защиты данных. Также важно установить жесткие правила доступа к информации, чтобы предотвратить утечки конфиденциальных данных.

Создание такой платформы не только повысит кибербезопасность в банковской сфере, но и способствует развитию сотрудничества между организациями в области кибербезопасности.

Вторым ключевым аспектом является оперативное и эффективное реагирование на кибератаки для сокращения потенциального урона. Критически важной мерой служит разработка процедур координирования действий между финансовыми учреждениями и другими заинтересованными сторонами. Это может включать в себя составление унифицированного плана реагирования на инциденты безопасности, а также организацию команды для эффективного управления кризисными ситуациями, обеспечивая тесное взаимодействие между участниками рынка.

Важно также, чтобы все организации имели доступ к актуальной информации о киберугрозах и могли быстро реагировать на новые угрозы. Для этого необходимо использовать современные системы мониторинга и обнаружения вторжений, а также создать платформу, которая позволит обмениваться информацией о киберугрозах между банками и другими организациями [20].

В-третьих, установление стандартов и протоколов обмена информацией о киберугрозах между банками и другими организациями может значительно упростить процесс обмена информацией и обеспечить единый подход к защите от киберугроз. Это может включать в себя установление единого формата для обмена информацией о киберугрозах, единого языка и терминологии, а также установление правил и процедур для обработки информации о киберугрозах.

Заключение

Таким образом, банковский и финансовый сектор сталкиваются с беспрецедентными вызовами в области кибербезопасности, которые требуют многогранного адаптивного подхода. Инциденты в финансовом секторе представляют угрозу не только ему, но и могут подорвать доверие в целом к финансовой системе Российской Федерации. Киберинциденты, которые нарушают оказание критически важных услуг, например, платежные сети, могут серьезно повлиять на экономическую активность страны. Поэтому финансовые учреждения должны быть начеку в связи с постоянно меняющимися рисками, исходящими от киберпреступников, которые постоянно придумывают новые способы проникновения в финансовые системы. Более гибкие и эффективные методы обнаружения мошенничества сейчас очень важны. Например, такие как: неконтролируемое обучение, позволяющее выявлять закономерности и отклонения в данных без четких указаний; разработка процедур реагирования и восстановления; применение эффективных протоколов реагирования и механизмов антикризисного управления.

Банки могут опережать развитие рисков и поддерживать целостность и безопасность своих цифровых транзакций, поддерживая эффективные процедуры мониторинга моделей и обратной связи, внедряя передовые подходы к машинному обучению и постоянно совершенствуя системы обнаружения аномалий. Использование неконтролируемого обучения имеет большой потенциал для защиты финансовых

активов, повышения квалификации в области выявления мошенничества в банковской отрасли и поддержания доверия потребителей к банковскому делу в эпоху цифровых технологий. Финансовые учреждения должны внедрять современные технологии и поддерживать активную стратегию кибербезопасности, чтобы оставаться на шаг впереди киберпреступников до тех пор, пока сохраняются киберугрозы.

Кроме новых технологий ключевые стратегии минимизации киберугроз включают в себя квалификационное повышение сотрудников, активное наблюдение за финансовыми операциями, взаимодействие с представителями правопорядка, разработку механизмов раннего оповещения, а также расширение партнерских отношений с коллегами по сектору и смежными учреждениями. Реализация каждой из упомянутых стратегий критична для гарантии защиты данных и минимизации вероятности финансовых убытков. Тем не менее, для достижения наивысшей эффективности их применение должно быть интегрированным и включать постоянное улучшение и оптимизацию процессов.

Список литературы

1. *Reddem P.* Cybersecurity in banking and finance: navigating the digital threat landscape // International Journal of Scienific Research in Computer Science, Engineering and Information Technology. – 2024. – Vol. 10, Iss. 5. – P. 852–861.
2. *Дудин М.Н., Шкодинский С.В.* Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы // Финансы: теория и практика. – 2022. – № 26 (6). – С. 52–71.
3. *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.
4. *Буз С.И.* Киберпреступления: понятие, сущность и общая характеристика // Юристъ-ПравоведЪ. – 2019. – № 4 (91). – С. 78–82.
5. *Goenka R., Chawla M. and Tiwari N.* A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy // International Journal of Information Security. – 2023. – No. 23 (1). – P. 1–30.
6. *Maharjan R. and Chatterjee J.M.* Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal // LBEF Research Journal of Science, Technology and Management. – 2019. – No. 1 (1). – P. 82–98.
7. *Качурин В.В., Ахмадеев Р.Г.* Повышение устойчивости информационной безопасности финансового сектора экономики // Вестник университета. – 2023. – № 5. – С. 151–160.
8. *Мажиев М.Х.* Киберпреступления как угроза национальной безопасности // Право и управление. – 2024. – № 5. – С. 526–530.
9. *Зайцева Т.В., Шершова Е.В.* Кибербезопасность как неотъемлемый инструмент противодействия киберпреступлениям в банковской сфере // Управленческий учет. – 2021. – № 10-3. – С. 623–628.
10. *Бойченко О.В., Польская С.И.* Аналитика проблем кибербезопасности критической информационной инфраструктуры банков // Научный вестник: финансы, банки, инвестиции. – 2023. – № 3 (64). – С. 22–32.
11. *Abdullaev E.A.O.* Cyber attaks and their impact on the digital economy // International Journal of Humanities and Natures Science. – 2024. – No. 3-2. – P. 121–130.
12. *Морозова Д.В., Прокопенко П.П.* Угрозы кибербезопасности банковской сферы Российской Федерации // Студенческий. – 2022.– № 41-4 (211). – С. 55–60.
13. *Комаров А.В.* Киберпреступность в банковской сфере: инновационные методы борьбы и противодействия // Финансовый бизнес. – 2021. – № 10 (220). – С. 35–37.
14. *Бабкин А.В., Бойченко О.В., Польская С.И.* Кибербезопасность кредитно-финансовой системы банков в условиях цифровой экономики // Вестник Академии знаний. – 2023. – № 3 (56). – С. 291–297.
15. *Магомедов Р.М.* О проблемах безопасности платежей при онлайн-торговле // Самоуправление. – 2023. – № 3 (136). – С. 466–469.
16. *Тарасова Н.В., Акиншина И.И.* Тенденции цифровой трансформации банковского сектора и проблемы обеспечения кибербезопасности // Первый экономический журнал. – 2023. – № 11 (341). – С. 159–166.
17. *Маныч Е.Г.* Киберпреступность в России: основные криминологические показатели и ее современные тенденции // Государство и право XXI веке. – 2021. – № 1. – С. 55–60.
18. *Богомолова Д.А.* Методы защиты от кибератак // Наука через призму времени. – 2023. – № 1 (70). – С. 5–7.

19. *Одинцов В.О.* Проблемы обеспечения кибербезопасности в коммерческих банках России в современных условиях // Горизонты экономики. – 2023. – № 3 (76). – С. 103–107.
20. *Гаврилова Э.Н., Данаева К.Л.А.* Банковский сектор России: современное состояние и тенденции развития // Вестник Московского университета имени С.Ю. Витте. Серия 1: Экономика и управление. – 2021. – № 1 (36). – С. 7–14.

References

1. *Reddem P.* Cybersecurity in banking and finance: navigating the digital threat landscape // International Journal of Scienific Research in Computer Science, Engineering and Information Technology. – 2024. – Vol. 10, Iss. 5. – P. 852–861.
2. *Dudin M.N., Shkodinskij S.V.* Vyzovy i ugrozy cifrovoj ekonomiki dlya ustojchivosti nacional'noj bankovskoj sistemy // Finansy: teoriya i praktika. – 2022. – № 26 (6). – S. 52–71.
3. *Shkodinskij S.V., Dudin M.N., Usmanov D.I.* Analiz i ocenka kiberugroz nacional'noj finansovoj sisteme Rossii v cifrovoj ekonomike // Finansovyj zhurnal. – 2021. – T. 13, № 3. – S. 38–53.
4. *Buz S.I.* Kiberprestupleniya: ponyatie, sushchnost' i obshchaya harakteristika // Yurist"-Pravoved". – 2019. – № 4 (91). – S. 78–82.
5. *Goenka R., Chawla M. and Tiwari N.* A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy // International Journal of Information Security. – 2023. – No. 23 (1). – P. 1–30.
6. *Maharjan R. and Chatterjee J.M.* Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal // LBEF Research Journal of Science, Technology and Management. – 2019. – No. 1 (1). – P. 82–98.
7. *Kachurin V.V., Ahmadeev R.G.* Povyshenie ustojchivosti informacionnoj bezopasnosti finansovogo sektora ekonomiki // Vestnik universiteta. – 2023. – № 5. – С. 151–160.
8. *Mazhiev M.H.* Kiberprestupleniya kak ugroza nacional'noj bezopasnosti // Pravo i upravlenie. – 2024. – № 5. – S. 526–530.
9. *Zajceva T.V., Shershova E.V.* Kiberbezopasnost' kak neot"emlemyj instrument protivodejstviya kiberprestupleniyam v bankovskoj sfere // Upravlencheskij uchet. – 2021. – № 10-3. – S. 623–628.
10. *Bojchenko O.V., Pol'skaya S.I.* Analitika problem kiberbezopasnosti kriticheskoj informacionnoj infrastruktury bankov // Nauchnyj vestnik: finansy, banki, investicii. – 2023. – № 3 (64). – S. 22–32.
11. *Abdullaev E.A.O.* Cyber attaks and their impact on the digital economy // International Journal of Humanities and Natures Science. – 2024. – No. 3-2. – P. 121–130.
12. *Morozova D.V., Prokopenko P.P.* Ugrozy kiberbezopasnosti bankovskoj sfery Rossijskoj Federacii // Studencheskij. – 2022.– № 41-4 (211). – S. 55–60.
13. *Komarov A.V.* Kiberprestupnost' v bankovskoj sfere: innovacionnye metody bor'by i protivodejstviya // Finansovyj biznes. – 2021. – № 10 (220). – S. 35–37.
14. *Babkin A.V., Bojchenko O.V., Pol'skaya S.I.* Kiberbezopasnost' kreditno-finansovoj sistemy bankov v usloviyah cifrovoj ekonomiki // Vestnik Akademii znanij. – 2023. – № 3 (56). – S. 291–297.
15. *Magomedov R.M.* O problemah bezopasnosti platezhej pri onlajn-torgovle // Samoupravlenie. – 2023. – № 3 (136). – S. 466–469.
16. *Tarasova N.V., Akinshina I.I.* Tendencii cifrovoj transformacii bankovskogo sektora i problemy obespecheniya kiberbezopasnosti // Pervyj ekonomicheskij zhurnal. – 2023. – № 11 (341). – S. 159–166.
17. *Manych E.G.* Kiberprestupnost' v Rossii: osnovnye kriminologicheskie pokazateli i ee sovremennye tendencii // Gosudarstvo i pravo XXI veke. – 2021. – № 1. – S. 55–60.
18. *Bogomolova D.A.* Metody zashchity ot kiberatak // Nauka cherez prizmu vremeni. – 2023. – № 1 (70). – S. 5–7.
19. *Odincov V.O.* Problemy obespecheniya kiberbezopasnosti v kommercheskih bankah Rossii v sovremennyh usloviyah // Gorizonty ekonomiki. – 2023. – № 3 (76). – S. 103–107.
20. *Gavrilova E.N., Danaeva K.L.A.* Bankovskij sektor Rossii: sovremennoe sostoyanie i tendencii razvitiya // Vestnik Moskovskogo universiteta imeni S.Yu. Vitte. Seriya 1: Ekonomika i upravlenie. – 2021. – № 1 (36). – S. 7–14.

Статья поступила в редакцию: 20.02.2025
Статья поступила для публикации: 27.02.2025
Received: 20.02.2025
Accepted: 27.02.2025