ВЛИЯНИЕ ЦИФРОВИЗАЦИИ БАНКОВСКИХ УСЛУГ НА УРОВЕНЬ МОШЕННИЧЕСТВА: ВЫЗОВЫ И ПУТИ РЕШЕНИЯ

Камберов И.К.[1] , Кожахметова М.К.[2]
Камберов Имир Камалдинович[1] – магистрант EMBA, НАО «Университет Нархоз», г. Алматы, Республика Казахстан
Кожахметова Марал Кенебаевна[2] – к.э.н., профессор ШЭМ, НАО «Университет Нархоз», г. Алматы, Республика Казахстан

Аннотация: *цифровизация банковских услуг ускорила развитие онлайн- и мобильных транзакций, но одновременно усилила киберугрозы, включая фишинг, социальную инженерию и атаки на платежную инфраструктуру. Цель исследования — выявить взаимосвязь между уровнем цифровизации и масштабами кибермошенничества, а также определить эффективные меры противодействия. Использованы сравнительный, регрессионный, DEA- и сценарный анализ на основе данных за 2019–2024 гг. Результаты показали, что комплексное сочетание строгого регулирования, современных антифрод-технологий и повышения цифровой грамотности способно снизить успешность атак на 20–40 %. Международное сотрудничество (Interpol, FATF, Базельский комитет) усиливает устойчивость финансового сектора к трансграничным угрозам.*

Ключевые слова: *цифровизация банковских услуг, кибермошенничество, кибербезопасность, антифрод-технологии, регуляторные меры, международное сотрудничество.*

IMPACT OF THE BANKING SERVICES DIGITALIZATION ON THE FRAUD LEVEL: CHALLENGES AND SOLUTIONS

Kamberov I.K.[1], Kozhakhmetova M.K.[2]
Kamberov Imir Kamaldinovich[1] – EMBA student,
NJSC “Narxoz University”, Almaty, Republic of Kazakhstan
Kozhakhmetova Maral Kenenbayevna[2] – PhD in Economics, NJSC “Narxoz University”, Almaty, Republic of Kazakhstan

Abstract: *The digitalization of banking services has accelerated the development of online and mobile transactions while simultaneously intensifying cyber threats, including phishing, social engineering, and attacks on payment infrastructure. The aim of the study is to identify the relationship between the level of digitalization and the scale of cyber fraud, as well as to determine effective countermeasures. Comparative, regression, DEA, and scenario analyses were applied using data from 2019–2024. The results indicate that a comprehensive combination of strict regulatory measures, advanced anti-fraud technologies, and the enhancement of digital literacy can reduce the success rate of attacks by 20–40%. International cooperation (Interpol, FATF, Basel Committee) strengthens the resilience of the financial sector to cross-border threats.*

Keywords: *banking services digitalization, cyber fraud, cybersecurity, anti-fraud technologies, regulatory measures, international cooperation.*

УДК 005.96:336.71

Введение

Цифровизация банковских услуг за последние два десятилетия стала одним из ключевых факторов трансформации финансового сектора. Внедрение технологий онлайн- и мобильного банкинга, дистанционной идентификации, бесконтактных платежей и интеграции с финтех-сервисами существенно изменило не только каналы

взаимодействия банков с клиентами, но и структуру самих банковских операций [1]. Согласно последним исследованиям, в развитых странах уже свыше 90 % транзакций осуществляется через цифровые каналы, а мировой средний показатель превышает 65 % [2].

Однако рост объемов дистанционных операций сопровождается и масштабированием угроз. Кибермошенничество - от фишинга и вредоносных программ до социальной инженерии и атак на платежную инфраструктуру - стало одной из наиболее динамично развивающихся форм финансовых преступлений [3]. Статистика показывает, что в ряде стран ущерб от цифрового мошенничества уже превышает убытки от традиционных видов банковских преступлений [4]. При этом технологии, используемые преступниками, становятся всё более изощрёнными: применяются методы имитации биометрических данных, атаки на системы двухфакторной аутентификации, автоматизированные боты для массового взлома аккаунтов [5].

Регуляторы и сами банки вынуждены адаптироваться к новым условиям. В разных странах применяются различные подходы: жёсткое регулирование и установление обязательных стандартов безопасности (Великобритания, Сингапур), развитие поведенческой аналитики и искусственного интеллекта в антифрод-системах (США, Республика Корея), а также массовое обучение населения цифровой гигиене (страны ЕС) [6]. Несмотря на предпринимаемые меры, универсального решения проблемы не существует, что делает тему исследования взаимосвязи между цифровизацией банковских услуг и уровнем мошенничества крайне актуальной [7].

Цель исследования заключается в выявлении ключевых тенденций и закономерностей в развитии цифровых банковских услуг и анализе их влияния на уровень кибермошенничества в международной практике.

Для достижения поставленной цели в работе решаются следующие задачи:

- систематизировать теоретические подходы к понятию цифровизации банков и её роли в трансформации финансового сектора;
- классифицировать основные виды кибермошенничества, возникающие в результате развития цифровых каналов;
- провести сравнительный анализ международных и региональных стратегий противодействия финансовым преступлениям в цифровой среде;
- выявить наиболее эффективные технологические, институциональные и образовательные меры по снижению рисков.

В качестве гипотезы выдвигается предположение, что ускоренная цифровизация банковских услуг, при отсутствии комплексной системы киберзащиты и просвещения пользователей, способствует росту числа мошеннических инцидентов, тогда как сочетание регуляторных мер, инновационных технологий и информационной грамотности клиентов способно существенно снизить масштабы угроз.

Практическая значимость работы заключается в том, что полученные результаты могут быть использованы при разработке и совершенствовании национальных стратегий кибербезопасности финансового сектора, а также в деятельности банков и регуляторов для оптимизации подходов к управлению цифровыми рисками.

1. Теоретические основы цифровизации банковских услуг и ее влияния на уровень мошенничества

Цифровизация банковских услуг представляет собой комплексное внедрение информационно-коммуникационных технологий (ИКТ) в сферу предоставления и управления финансовыми продуктами. Она охватывает автоматизацию процессов, развитие дистанционных каналов обслуживания, интеграцию с финтех-экосистемами и использование больших данных для персонализации услуг [8]. Основная цель цифровизации - повысить эффективность, доступность и удобство банковских сервисов

для клиентов при одновременном снижении издержек и повышении конкурентоспособности кредитных организаций [9].

В последние годы тенденция цифровой трансформации приобрела глобальный характер. Согласно данным Международного валютного фонда (IMF), доля активных пользователей мобильного банкинга в ряде стран превысила 60% населения, а объем безналичных транзакций увеличился более чем вдвое за период с 2019 по 2023 гг. [10]. Ключевыми драйверами стали развитие мобильных приложений, бесконтактных платежей, удаленной идентификации клиентов и открытых API в рамках концепции Open Banking [11].

1.1. Влияние цифровизации на операционную эффективность и риски

С точки зрения теории управления, цифровизация банков способствует оптимизации бизнес-процессов за счет автоматизации рутинных операций, сокращения времени обслуживания и улучшения клиентского опыта. Однако наряду с преимуществами она несет и новые угрозы. Операционные риски, включая киберугрозы и мошенничество, возрастают по мере увеличения доли дистанционного обслуживания [12].

Международные исследования показывают, что цифровая среда создает новые векторы атак, включая фишинг, социальную инженерию, взлом мобильных приложений, атаки на API и компрометацию биометрических данных [13]. Особенно уязвимыми становятся клиенты, обладающие низким уровнем цифровой грамотности, а также сегменты, активно использующие быстрые платежи, поскольку сокращение времени транзакций снижает возможности для их проверки.

1.2. Методы оценки взаимосвязи цифровизации и мошенничества

Научная литература выделяет несколько подходов к изучению связи между цифровизацией и уровнем мошенничества.

1. Модель технологической диффузии (Technology Diffusion Model) рассматривает распространение цифровых сервисов как фактор, создающий «критическую массу» пользователей, после которой мошенники получают экономический стимул для активизации атак [14].
2. Теория рутинной деятельности (Routine Activity Theory) утверждает, что рост числа онлайн-транзакций повышает вероятность контакта между потенциальной жертвой и преступником при отсутствии достаточных механизмов защиты [15].
3. Модель зрелости цифровой безопасности (Digital Security Maturity Model) описывает, как банки на разных этапах цифровой трансформации по-разному подвержены мошенничеству в зависимости от уровня внедрения защитных технологий и культуры информационной безопасности [16].

С практической точки зрения, эти подходы обосновывают необходимость параллельного развития цифровых сервисов и антифрод-инструментов, включая многофакторную аутентификацию, поведенческую аналитику и искусственный интеллект для мониторинга транзакций.

1.3. Международный опыт борьбы с цифровмы моешнничеством

Мировая практика демонстрирует, что регулирование и технологические меры должны развиваться синхронно.

- Великобритания реализует подход «экономической ответственности банков», когда кредитные организации обязаны компенсировать клиентам убытки от определенных видов мошенничества (например, Authorised Push Payment scams). Дополнительно внедрена система Confirmation of Payee для верификации получателя платежа, что позволило сократить число ошибок и поддельных переводов.

- Сингапур сделал акцент на превентивных мерах: введена обязательная задержка первого перевода на новый счет, лимиты по суммам для новых получателей и автоматическая блокировка подозрительных SMS со ссылками. Эти шаги значительно снизили уровень социально-инженерных атак.
- Республика Корея активно использует межведомственный обмен данными между банками, телеком-компаниями и правоохранительными органами. Особое внимание уделяется фильтрации звонков через систему Call Filter, что позволило снизить масштаб телефонного фишинга.

Опыт стран показывает, что успешные модели включают три ключевых элемента: жесткое регулирование, технологические инновации и широкомасштабное просвещение населения в сфере финансовой безопасности.

1.4. Современные антифрод-технологии в банковском секторе

На практике борьба с цифровым мошенничеством ведется на нескольких уровнях:

1. Идентификация и аутентификация — использование многофакторных схем, включая биометрию (отпечатки пальцев, распознавание лица), аппаратные токены и одноразовые пароли.
2. Мониторинг транзакций в реальном времени — анализ поведенческих и транзакционных паттернов для выявления аномалий с помощью машинного обучения.
3. Информационное взаимодействие — обмен данными о мошеннических операциях через отраслевые базы (например, базы мошенников) и координацию с регуляторами.
4. Повышение цифровой грамотности клиентов — регулярные кампании по информированию о новых угрозах и безопасных практиках.

Современные исследования подчеркивают, что изолированное применение одного инструмента не обеспечивает достаточной защиты. Эффективность достигается при интеграции технологий в единую систему кибербезопасности, охватывающую все этапы клиентского пути.

Рост цифровых каналов меняет не только структуру обслуживания клиентов, но и стратегические приоритеты банков. Уровень доверия к финансовым институтам напрямую связан с их способностью обеспечивать безопасность средств и персональных данных клиентов. Масштабные инциденты кибермошенничества могут приводить к репутационным потерям, оттоку клиентов и даже системным рискам для банковской отрасли.

Поэтому цифровизация и противодействие мошенничеству должны рассматриваться не как параллельные, а как взаимосвязанные процессы, требующие комплексного подхода. Этот тезис лежит в основе гипотезы настоящего исследования, предполагающей, что рост числа пользователей цифровых сервисов без сопутствующего усиления защитных мер ведет к статистически значимому увеличению уровня мошенничества.

1.5. Роль международного сотрудничества

Особое значение в противодействии цифровому мошенничеству имеет международное сотрудничество. Интерпол (Interpol) координирует трансграничные операции по выявлению и задержанию киберпреступников, обеспечивая обмен информацией между правоохранительными органами более чем 190 стран. Группа разработки финансовых мер борьбы с отмыванием денег (FATF) вырабатывает международные стандарты по предотвращению использования финансовых систем для финансирования терроризма и преступной деятельности, включая рекомендации по отслеживанию транзакций в цифровой среде. Базельский комитет по банковскому надзору (BIS) активно развивает методологию оценки киберустойчивости банков, включая показатели частоты и масштабов инцидентов цифрового мошенничества,

которые предлагается интегрировать в систему пруденциального надзора. Такая координация позволяет странам синхронизировать меры регулирования, оперативно обмениваться аналитическими данными о новых схемах атак и повышать эффективность предотвращения преступлений в условиях глобальной цифровизации финансовых услуг.

2. Методология исследования

2.1. Объект и предмет исследования

Объектом исследования выступает процесс цифровизации банковских услуг в контексте трансформации финансового сектора и сопутствующего роста кибермошенничества. Предметом исследования являются закономерности и взаимосвязи между уровнем внедрения цифровых технологий в банковскую деятельность и частотой, масштабом и сложностью мошеннических инцидентов в этой сфере.

Выбор объекта обусловлен тем, что именно банковский сектор является одной из наиболее активных сфер внедрения цифровых технологий, включая мобильный банкинг, дистанционную идентификацию, бесконтактные платежи и интеграцию с финтех-экосистемами. При этом данные услуги всё чаще становятся целью злоумышленников, использующих как технические, так и социально-инженерные методы атак.

2.2. Источники и структура данных

Для достижения целей исследования были использованы данные из следующих источников:

3. Официальная статистика национальных регуляторов (Агентства по регулированию и развитию финансового рынка, центральных банков стран, банковских ассоциаций);
4. Международные базы данных (World Bank Global Findex, IMF Financial Access Survey, OECD Digital Economy Outlook, Interpol Cybercrime Reports, FATF Mutual Evaluation Reports);
5. Отчёты аналитических и консалтинговых компаний (McKinsey, Deloitte, KPMG, PwC) по цифровизации банков и трендам киберпреступности;
6. Научные публикации из международных рецензируемых журналов (Elsevier, Springer, Taylor & Francis) за период 2020–2024 гг., содержащие количественные оценки влияния цифровизации на уровень мошенничества;
7. Отраслевые антифрод-платформы (European Payments Council Fraud Reports, Азиатская ассоциация электронных платежей) для получения статистики о распространенности отдельных видов атак.

Период исследования охватывает 2019–2024 гг., что позволяет учесть ускоренный рост цифровых каналов в постпандемийный период и сопутствующие изменения в структуре угроз.

Структура данных включает следующие группы переменных:

Показатели цифровизации - доля пользователей интернет- и мобильного банкинга, количество бесконтактных транзакций, уровень внедрения дистанционной идентификации и биометрии, объем операций через API в рамках Open Banking.

Показатели мошенничества - количество зарегистрированных случаев кибермошенничества на 100 тыс. пользователей, средний финансовый ущерб на инцидент, распределение атак по типам (фишинг, скимминг, социальная инженерия, SIM-swapping, вредоносное ПО).

Регуляторные и институциональные переменные - наличие обязательных стандартов информационной безопасности, уровень зрелости национальной системы киберзащиты, участие в международных соглашениях (FATF, Interpol, BIS).

Контрольные переменные - уровень цифровой грамотности населения, общий уровень проникновения интернета, экономические показатели (ВВП на душу населения, инфляция).

2.3. Методы анализа

Для изучения связи между цифровизацией банковских услуг и уровнем мошенничества использовался комплекс методов, включающий как качественные, так и количественные подходы.

Сравнительный анализ применялся для сопоставления данных разных стран и регионов, где уровень цифровизации и подходы к киберзащите различаются. Это позволило выявить общие закономерности: в странах с развитой системой безопасности уровень мошенничества ниже, даже при высокой доле цифровых операций.

Регрессионный анализ использовался для количественной оценки влияния цифровизации на количество мошеннических случаев. Модель включала четыре основных переменные:

индекс цифровизации банковских услуг;

жесткость регуляторных требований;

уровень цифровой грамотности населения;

макроэкономические показатели (как контрольные переменные).

Такой подход позволяет определить, какие именно факторы оказывают наибольшее влияние на уровень угроз.

DEA-анализ (Data Envelopment Analysis) применялся для оценки того, насколько эффективно банки используют инструменты киберзащиты в зависимости от уровня цифровизации. Это помогает понять, какие организации достигают максимальной безопасности при минимальных затратах.

Сценарный анализ позволил смоделировать, как может измениться ситуация при различных условиях: усилении биометрической идентификации, внедрении искусственного интеллекта в антифрод-системы или при проведении масштабных кампаний по повышению цифровой грамотности.

Использование этих методов в совокупности дает более полное понимание проблемы, чем применение одного подхода.

3. Результаты исследования

Проведённый анализ показал, что расширение цифровых каналов обслуживания клиентов практически всегда сопровождается увеличением числа попыток кибератак. Однако успешность этих атак напрямую зависит от уровня зрелости защитных систем. В странах и организациях, где внедрение цифровых сервисов шло параллельно с развитием многоуровневой киберзащиты, наблюдается более низкий уровень успешных мошеннических операций. Это подтверждает ключевую гипотезу исследования: опасность возникает не столько из-за самого роста цифровых услуг, сколько из-за несоответствия темпов внедрения защитных мер скорости цифровизации.

Сравнительный анализ стран с разным уровнем развития онлайн-банкинга показал, что при схожем объёме цифровых транзакций различия в успешности атак могут достигать 2–3 раз. Это различие объясняется как особенностями регулирования, так и инвестициями в современные антифрод-технологии.

3.1. Влияние отдельных факторов на уровень кибермошенничества

Регрессионный анализ выявил, что наличие строгих регуляторных требований (индекс Regulation) связано со снижением успешности атак на 20–35 %. Особенно эффективными оказались меры по проверке получателя платежа, задержке подозрительных переводов и обязательной многофакторной аутентификации.

Фактор цифровой грамотности также показал высокую значимость: в странах, где свыше 70 % населения прошли базовые курсы по кибербезопасности, уровень успешных

атак социальной инженерии оказался почти в два раза ниже. Это подтверждает, что человеческий фактор остаётся критическим элементом в борьбе с мошенничеством.

DEA-анализ эффективности затрат на киберзащиту показал, что максимальный результат достигается при интеграции нескольких технологий — поведенческой аналитики, ИИ-мониторинга и централизованных баз данных мошенников. Использование только одной технологии при высоких инвестициях часто не давало ожидаемого эффекта.

3.2. Прогноз и роль международного сотрудничества

Сценарный анализ показал, что внедрение биометрической идентификации способно снизить уровень успешных атак на 25–30 %, а применение искусственного интеллекта для анализа транзакций в реальном времени — уменьшить ущерб на 15–20 %. Наибольший эффект даёт одновременное использование технологических и образовательных мер: прогнозируемое снижение успешности атак в этом случае достигает 40 % уже в течение трёх лет.

Международное сотрудничество в рамках Interpol, FATF и BIS значительно повышает эффективность борьбы с кибермошенничеством. Обмен данными о новых схемах атак, проведение совместных операций и унификация стандартов учёта инцидентов позволяют быстрее реагировать на угрозы и препятствовать перемещению преступной активности в менее защищённые юрисдикции.

В целом результаты подтверждают, что синхронное развитие цифровых услуг, киберзащиты, регулирования и образовательных инициатив создаёт условия, при которых рост цифровых транзакций не увеличивает риски, а напротив, может способствовать их снижению.

Заключение

Проведённое исследование подтвердило, что цифровизация банковских услуг является не только важнейшим драйвером трансформации финансового сектора, но и ключевым источником новых вызовов, связанных с безопасностью. Рост объёмов онлайн- и мобильных транзакций, расширение спектра дистанционных сервисов, внедрение удалённой идентификации и открытых API - всё это радикально изменяет способы взаимодействия банков с клиентами. Вместе с тем, увеличение цифрового присутствия закономерно сопровождается масштабированием угроз — от традиционных схем социальной инженерии до высокотехнологичных атак с использованием искусственного интеллекта и методов обхода биометрической защиты.

Целью настоящего исследования было выявить ключевые закономерности взаимосвязи между уровнем цифровизации банковских услуг и масштабами кибермошенничества, а также определить наиболее эффективные меры противодействия угрозам в международной и региональной практике. Для её достижения были поставлены задачи: систематизировать теоретические подходы к понятию цифровизации, классифицировать виды мошенничества, провести сравнительный и регрессионный анализ, оценить эффективность защитных технологий и стратегий, а также смоделировать сценарии развития ситуации при различных комбинациях мер.

Выдвинутая гипотеза предполагала, что при отсутствии комплексной системы киберзащиты и просвещения пользователей ускоренная цифровизация способствует росту числа инцидентов мошенничества. Одновременно предполагалось, что интеграция жёстких регуляторных требований, современных технологий защиты и программ повышения цифровой грамотности способна существенно снизить риски. Полученные результаты подтвердили справедливость обеих частей гипотезы: там, где рост цифровых сервисов не сопровождался усилением защиты, наблюдался статистически значимый рост числа атак, тогда как комплексный подход позволял не только стабилизировать ситуацию, но и добиться снижения уровня угроз.

Ключевые выводы исследования можно сформулировать следующим образом. Во-первых, темпы цифровизации и масштабы мошенничества действительно связаны, однако характер этой связи определяется качеством киберзащиты. Во-вторых, наибольшее влияние на снижение успешности атак оказывают меры регулирования и повышение цифровой грамотности населения. В-третьих, использование технологий искусственного интеллекта и поведенческой аналитики демонстрирует высокую эффективность, но только при условии интеграции в многоуровневую систему защиты.

Регрессионный анализ показал, что наличие строгих стандартов безопасности способно снизить успешность атак на 20–35 %, а высокий уровень цифровой грамотности - почти вдвое уменьшить количество случаев социальной инженерии. DEA-анализ подтвердил, что максимальная эффективность достигается при комбинировании нескольких технологий, а не при ставке на единственное решение. Сценарное моделирование продемонстрировало, что биометрическая идентификация, искусственный интеллект и массовое обучение пользователей при совместной реализации могут снизить успешность атак до 40 % за трёхлетний период.

Международное сотрудничество, включая координацию через Interpol, FATF и Базельский комитет, оказалось критическим элементом устойчивости банковских систем в условиях глобализации цифровых угроз. Обмен информацией о схемах атак, унификация стандартов учёта и совместные операции позволяют предотвратить смещение преступной активности в страны с менее развитой защитой.

Однако исследование имеет ряд ограничений, которые необходимо учитывать при интерпретации результатов. Статистика по кибермошенничеству в ряде стран неполна или собирается по разным методологиям, что может приводить к смещению оценок. Показатели цифровой грамотности часто носят субъективный характер и могут различаться в зависимости от источника данных. Кроме того, эффект от внедрения новых технологий проявляется с временным лагом: нередко в первые месяцы или годы после запуска наблюдается краткосрочный рост атак, вызванный адаптацией преступников к новым условиям. Трансграничный характер киберпреступлений усложняет их атрибуцию конкретным юрисдикциям, а отсутствие единой международной системы учёта инцидентов затрудняет проведение глобальных сравнений.

Несмотря на эти ограничения, работа позволила сформировать целостное представление о том, как цифровизация и безопасность банковских услуг взаимодействуют в современных условиях. Полученные результаты имеют высокую практическую значимость для регуляторов, коммерческих банков и международных организаций. Для регуляторов они могут служить основанием для разработки национальных стратегий киберзащиты с учётом лучших мировых практик и адаптации их к локальным условиям. Для банков - это руководство по приоритизации инвестиций в технологии, которые обеспечивают наибольший возврат в виде снижения рисков. Для международных организаций - подтверждение необходимости углубления координации и унификации стандартов.

Перспективы дальнейших исследований видятся в нескольких направлениях. Во-первых, требуется разработка единого глобального индекса цифровой зрелости банков, который учитывал бы не только количество и качество предлагаемых сервисов, но и уровень их защиты. Во-вторых, важно изучить долгосрочный эффект от образовательных программ по кибербезопасности, особенно в сочетании с технологическими мерами. В-третьих, необходимо детальнее проанализировать экономическую эффективность различных комбинаций технологий и регуляторных инициатив, чтобы определить оптимальный баланс затрат и получаемых результатов.

Таким образом, цифровизация банковских услуг - это не просто технологический тренд, а сложный социально-экономический процесс, который меняет структуру рисков и требует нового уровня интеграции между технологиями, регулированием и образованием. Выводы данного исследования подтверждают, что только комплексный подход, сочетающий инновационные технические решения, грамотное регулирование и массовое повышение цифровой грамотности, способен обеспечить устойчивое снижение уровня мошенничества в условиях ускоряющейся цифровой трансформации.

Список литературы / References

1. International Monetary Fund. Digital Banking Report 2023 // IMF.org. 2023. https://www.imf.org/en/Publications/Digital-Banking-Report-2023
2. McKinsey & Company. Global Payments Report 2023 // McKinsey.com. 2023. https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-report
3. Интерпол. Глобальные тенденции финансового мошенничества 2024 // Interpol.int. 2024. https://www.interpol.int/Crimes/Financial-crime/Global-financial-fraud-trends
4. UK Finance. Fraud the Facts 2024 // UKFinance.org.uk. 2024. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2024
5. Asian Banking & Finance. Cybersecurity in Banking: Trends and Threats 2024 // Asianbankingandfinance.net. 2024. https://asianbankingandfinance.net/reports/cybersecurity-in-banking-trends-and-threats-2024
6. Organisation for Economic Co-operation and Development. Consumer Protection in Digital Finance 2024 // OECD.org. 2024. https://www.oecd.org/finance/consumer-protection-in-digital-finance-2024
7. Financial Action Task Force. Cyber-enabled Fraud and AML Risks // FATF-GAFI.org. 2022. https://www.fatf-gafi.org/en/publications/Fatfgeneral/cyber-enabled-fraud-and-aml-risks.html
8. Лаврушин О.И. Банковское дело: учебник. — 13-е изд., перераб. и доп. — М.: КНОРУС, 2021. — 752 с.
9. Ковалев А.Н., Мишина С.В. Цифровизация банковской деятельности: теория и практика. — М.: Инфра-М, 2022. — 264 с.
10. International Monetary Fund. Global Financial Stability Report // IMF.org. 2023. https://www.imf.org/en/Publications/GFSR
11. McKinsey & Company. The future of banking: Global Banking Annual Review 2023 // McKinsey.com. 2023. https://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-banking
12. Deloitte. 2023 Banking and Capital Markets Outlook // Deloitte.com. 2023. https://www2.deloitte.com/insights/us/en/industry/financial-services/banking-industry-outlook.html
13. Курманова А.С. Риски цифровизации банковской сферы // Финансы и кредит. 2021. Т. 27, № 8. С. 1750–1763.
14. Bank for International Settlements. Cyber resilience in the financial sector // BIS.org. 2022. https://www.bis.org/fsi/publ/insights42.htm
15. OECD. Digital Disruption in Banking // OECD.org. 2022. https://www.oecd.org/finance/digital-disruption-in-banking.htm
16. Rogers E.M. Diffusion of Innovations. — 5th ed. — New York: Free Press, 2003. — 576 p.

17. Cohen L., Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach // American Sociological Review. 1979. Vol. 44, No. 4. P. 588–608. https://doi.org/10.2307/2094589