

РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА/REGIONAL AND SECTORAL ECONOMICS

DOI: https://doi.org/10.60797/ECNMS.2026.13.3 EDN: GOUBRR

АДАПТАЦИЯ МЕЖДУНАРОДНОГО ОПЫТА ЦИФРОВОГО РИСК-МЕНЕДЖМЕНТА ДЛЯ РОССИЙСКОГО ФИНАНСОВОГО СЕКТОРА

Научная статья

Ханаева Д.П.[1, *]

[1] Сибирский федеральный университет, Красноярск, Российская Федерация

* Корреспондирующий автор (daria_hanaeva[at]mail.ru)

Предложена: 06.01.2026; Принята: 30.03.2026; Опубликована: 11.06.2026

Аннотация

В статье представлен комплексный анализ передовых международных практик цифрового управления финансовыми рисками и перспектив их адаптации для российского финансового рынка. Исследование охватывает опыт стран в области применения цифровых технологий для превентивного управления киберугрозами. Проведена сравнительная оценка различных регуляторных моделей с использованием метода взвешенных коэффициентов, выявлены ключевые направления цифровой трансформации риск-менеджмента. Особое внимание уделено специфике российского финансового сектора, включая региональные организации Красноярского края. Предложена концептуальная модель превентивного управления цифровыми финансовыми рисками, адаптированная к условиям ограниченных ресурсов и институциональных особенностей российской финансовой системы. Результаты исследования демонстрируют необходимость перехода от реактивного к превентивному подходу в управлении цифровыми рисками с использованием технологий искусственного интеллекта, поведенческой аналитики и систем раннего предупреждения.

Ключевые слова: цифровые финансовые риски, превентивное управление, киберугрозы, международный опыт, финансовый сектор.

ADAPTING INTERNATIONAL EXPERIENCE IN DIGITAL RISK MANAGEMENT FOR THE RUSSIAN FINANCIAL SECTOR

Research article

Hanaeva D.P.[1, *]

[1] Siberian Federal University, Krasnoyarsk, Russian Federation

* Corresponding author (daria_hanaeva[at]mail.ru)

Suggested: 06.01.2026; Accepted: 30.03.2026; Published: 11.06.2026

Abstract

The article presents a complex analysis of leading international practices in digital financial risk management and the prospects for their adaptation to the Russian financial market. The study examines the experience of various countries in the application of digital technologies for the preventive management of cyberthreats. A comparative evaluation of various regulatory models was carried out using the weighted coefficient method, and key areas for the digital transformation of risk management were identified. Particular attention is paid to the specific characteristics of the Russian financial sector, including regional organisations in Krasnoyarsk Krai. A conceptual model for the preventive management of digital financial risks is suggested, adapted to the conditions of limited resources and the institutional characteristics of the Russian financial system. The research results demonstrate the need to transition from a reactive to a preventive approach in digital risk management, using artificial intelligence technologies, behavioural analytics and early warning systems.

Keywords: digital financial risks, preventive management, cyberthreats, international experience, financial sector.

Введение

Цифровая трансформация финансовых систем развитых стран создает новые вызовы для устойчивости финансовых институтов. Цифровые финансовые риски, включающие киберугрозы, мошенничество и DDoS-атаки, становятся одним из главных факторов дестабилизации финансовых рынков. По данным исследований, российские финансовые организации, особенно банки и страховые компании, все чаще становятся жертвами кибератак [1], что обусловливает актуальность формирования эффективных подходов к превентивному управлению цифровыми рисками.

Международный опыт применения цифровых технологий для управления финансовыми рисками представляет особую ценность для формирования отечественных подходов к защите финансовых систем. Однако прямое копирование зарубежных практик неэффективно в силу различий в институциональной среде, технологической базе и регуляторных требованиях [2]. Это определяет необходимость селективной адаптации международного опыта с учетом национальной специфики.

Целью исследования является анализ передовых международных практик цифрового риск-менеджмента и предложение концептуального подхода к их адаптации для российского финансового рынка, ориентированного на превентивное управление цифровыми финансовыми рисками.

Методы и принципы исследования

Методологическую основу исследования составляет комплексный подход, включающий сравнительный анализ международных практик, метод взвешенных коэффициентов для оценки эффективности различных моделей управления рисками, систематизацию регуляторных подходов. В исследовании использованы данные международных финансовых организаций [3], [4], регуляторных органов ведущих стран [5], [6], научные публикации в области цифровой безопасности финансовых систем [7], [8].

Для количественной оценки международных подходов применен метод взвешенных коэффициентов с выделением пяти ключевых критериев. Приоритетными определены предиктивная эффективность и адаптируемость, поскольку именно они определяют способность системы прогнозировать риски и интегрироваться в российские условия.

Эмпирическую базу исследования составляют данные о специфике финансовых организаций Красноярского края [9], представляющих репрезентативную выборку для апробации концептуальной модели. Выбор регионального уровня обусловлен необходимостью учета особенностей организаций, не обладающих достаточными ресурсами для создания полноценных систем кибербезопасности.

Основные результаты

Проведенный анализ международной практики показывает, что различные страны выбирают специфические приоритеты в области цифрового управления финансовыми рисками. Европейские страны акцентируют внимание на защите персональных данных и прозрачности алгоритмов, что отражено в регламенте Digital Operational Resilience Act и методологии TIBER-EU [5], [6]. Анализ показывает, что европейский подход формирует высокую степень нормативной определенности и стандартизации процедур, однако одновременно увеличивает нагрузку на финансовые организации за счёт усложнения требований к операционной устойчивости. США и Великобритания фокусируются на обмене информацией через платформы FS-ISAC и NCSC, реализуя принцип коллективной защиты. Можно сказать, что эффективность данной модели обусловлена высокой зрелостью частного сектора и развитостью механизмов саморегулирования. Однако перенос данной практики в российские условия ограничен иной структурой надзора и меньшей ролью горизонтальных ассоциаций. Азиатские страны активно внедряют передовые технологии, включая квантовую криптографию в Японии и комплексную оценку технологических рисков в Сингапуре. Анализ позволяет сделать вывод, что именно сочетание государственной координации и технологической масштабируемости делает азиатскую модель наиболее адаптивной в системах с высокой централизацией управления.

Таблица 1 - Практики цифрового риск-менеджмента в международном финансовом секторе

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.1

Модель / страны	Ключевые инициативы	Передовые практики	Технологии
Европейский союз	Digital Operational Resilience Act; методология TIBER-EU	Комплексная оценка рисков; управление третьими сторонами; регулярные стресс-тесты	Предиктивная аналитика; тестирование на проникновение; обмен данными об угрозах
Великобритания	Инициативы NCSC; режим безопасности IoT	Secure by Design; профилирование атак; коллективное реагирование	Каталогизация уязвимостей; агрегирование инцидентов
США	NIST Cybersecurity Framework; FS-ISAC	Интеграция киберрисков в корпоративное управление; многоуровневая защита	Платформы обмена информацией; мониторинг аномалий
Азия (Сингапур, Китай, Япония)	TRM (Сингапур); централизованные системы идентификации; отраслевые ISAC	Сегментация сетей; скоринг транзакций; системы раннего предупреждения	ИИ; машинное обучение; биометрия; федеративное обучение
Австралия и Индия	Национальные центры реагирования; технологии верификации платежей	SOC; оценка зрелости; раннее предупреждение	Большие данные; автоматизация блокировок; постквантовая криптография
Канада и Тайвань	Национальные центры финразведки; отраслевые платформы обмена	Анализ транзакций; многоуровневая защита	Машинное обучение; анализ больших данных
Россия	ФинЦЕРТ; стандарты Банка России; курс на	Централизованный мониторинг угроз;	Отечественная криптография; системы

Модель / страны	Ключевые инициативы	Передовые практики	Технологии
	технологический суверенитет	нормативная стандартизация	раннего предупреждения

Примечание: составлено автором на основе [1], [2], [5], [7]

Сравнительный анализ передовых практик выявляет несколько общих направлений развития цифрового риск-менеджмента. Во-первых, все развитые юрисдикции переходят от реактивного реагирования к комплексной оценке рисков с регулярным тестированием устойчивости систем. Во-вторых, активно развиваются технологии поведенческой аналитики и предиктивного анализа киберугроз, что свидетельствует о смене парадигмы управления рисками — от фиксации инцидента к прогнозированию его вероятности [3]. В-третьих, формируются устойчивые платформы обмена информацией между участниками финансового рынка, что позволяет минимизировать асимметрию данных и снижать системные риски [4].

Особый интерес представляет опыт стран, реализовавших системы раннего предупреждения. Австралия внедрила технологию NameCheck для верификации получателей платежей в реальном времени, что позволило сократить уровень мошеннических операций. Малайзия создала платформу FinTIP для мониторинга киберпространства, а Китай разработал сервис FOFA с использованием искусственного интеллекта и биометрической аутентификации. Анализ данных практик позволяет заключить, что эффективность систем раннего предупреждения определяется не только технологией, но и институциональной встроенностью в финансовую инфраструктуру.

Технологические платформы международного уровня демонстрируют конвергенцию решений в области цифрового риск-менеджмента. Системы обмена информацией на базе протоколов STIX/TAXII получили распространение в ЕС, США и Великобритании, что указывает на формирование глобальных стандартов в сфере киберугроз. Технологии искусственного интеллекта для предиктивной аналитики активно применяются в США, Китае и Швейцарии [3]. Квантовые технологии для защиты данных внедряются в Японии, Индии и Канаде. Таким образом, наблюдается конвергенция технологических решений при сохранении различий в институциональных моделях их применения.

Регуляторные подходы к управлению цифровыми финансовыми рисками формируют три основные модели. Европейская модель характеризуется детализированными требованиями, единым подходом и акцентом на защите персональных данных [5]. Англо-саксонская модель основана на саморегулировании, активности отраслевых организаций и интенсивном обмене информацией. Азиатская модель предполагает активное государственное регулирование, стимулирование технологических инноваций и высокую степень централизации процессов управления рисками. Сопоставление данных моделей показывает, что их эффективность определяется соответствием национальной институциональной структуре, а не универсальностью технологических инструментов.

Российский финансовый сектор характеризуется значительной дифференциацией в уровне применения цифровых технологий управления рисками. Крупные государственные банки демонстрируют продвинутый уровень технологической зрелости, используя собственные AI-платформы для скоринга кредитных рисков и фрод-мониторинга [10]. Частные банки средней величины применяют готовые решения от IT-интеграторов, что ограничивает глубину аналитики. Небанковские кредитные организации и малые банки находятся на начальном уровне цифровизации. Таким образом, российская система в целом демонстрирует фрагментарность развития, что снижает её совокупную устойчивость [11].

Таблица 2 - Последствия кибератак на российские организации за 2024 г.

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.2

Категория последствий	Доля, %	Описание
Утечка конфиденциальной информации	50	Утечки конфиденциальных данных из-за кибератак
Нарушения в работе сервисов	28	Сбои в работе сервисов, предоставляемых компаниями
Дефейс веб-ресурсов	8	Несекционное изменение веб-сайтов и контента

Примечание: составлено автором по данным Банка России [11]

Региональная специфика финансовых организаций обусловливает особую актуальность превентивного подхода к управлению рисками. Для организаций Красноярского края характерны ограниченные ресурсы для создания полноценных систем кибербезопасности [9], что делает реактивное реагирование на инциденты потенциально катастрофичным. По данным исследований, ущерб от кибератак на региональные телекоммуникационные компании может достигать десятков миллионов рублей. В этих условиях реактивная модель реагирования на инциденты способна привести к высоким экономическим потерям. Следовательно, превентивное управление приобретает не рекомендательный, а стратегический характер.

Региональные коммерческие банки сталкиваются с высоким уровнем цифровизации при необходимости соответствия регуляторным требованиям Банка России [11]. Страховые компании обрабатывают чувствительные

персональные данные с интеграцией в государственные системы. Инвестиционные и управляющие компании нуждаются в защите торговых операций и интеграции с биржевыми системами. Телекоммуникационные компании с финансовыми услугами требуют комплексной защиты мобильных платежей и цифровых кошельков. Такая двойственная нагрузка формирует ситуацию повышенной регуляторной чувствительности: чем выше уровень цифровых сервисов, тем больше уязвимостей и тем жестче контроль. На практике это приводит к тому, что значительная часть ресурсов направляется на соблюдение нормативов, а не на развитие превентивной аналитики.

Таблица 3 - Категории финансовых организаций Красноярского края для внедрения модели превентивного управления цифровыми рисками

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.3

Категория организаций	Характеристика деятельности	Специфика цифровых рисков	Потребность в превентивном управлении	Основные преимущества
Региональные коммерческие банки	Банковские услуги для корпоративных и частных клиентов, интеграция с межбанковскими системами	Высокий уровень цифровизации, обработка больших объемов персональных данных, требования ЦБ РФ	Необходимость соответствия регуляторным требованиям, защита клиентских данных	Раннее выявление угроз, снижение операционных рисков
Страховые компании	Страхование имущества, жизни, здоровья, обязательные виды страхования	Обработка чувствительных персональных данных, интеграция с государственными системами	Защита конфиденциальной информации, соответствие требованиям к обработке персональных данных	Защита персональных данных, обеспечение непрерывности процессов
Инвестиционные и управляющие компании	Управление инвестиционными портфелями, операции с ценными бумагами	Торговые платформы, интеграция с биржевыми системами, обработка финансовых данных	Защита инвестиционных активов, обеспечение безопасности торговых операций	Защита инвестиционных активов, обеспечение безопасности торговых операций
Телекоммуникационные компании с финансовыми услугами	Предоставление телекоммуникационных услуг с элементами финансовых операций (мобильные платежи, цифровые кошельки)	Обработка платежных данных через телекоммуникационные каналы, интеграция финансовых и телекоммуникационных систем	Защита от мошенничества в мобильных платежах, обеспечение безопасности цифровых кошельков	Комплексная защита телекоммуникационных и финансовых процессов

Примечание: составлено автором

Таким образом, специфика цифровых рисков определяется не отраслевой принадлежностью как таковой, а глубиной интеграции организации в финансово-технологическую инфраструктуру.

Текущее состояние российских решений в области цифрового управления рисками характеризуется сочетанием институциональной устойчивости и технологических ограничений. К достоинствам относятся изначальное соответствие требованиям Банка России [11], использование отечественных AI-платформ [10], органичная интеграция с национальной финансовой инфраструктурой [12]. Это обеспечивает высокий уровень системной совместимости и снижает зависимость от внешних поставщиков решений. Однако анализ показывает, что жесткость регуляторных рамок ограничивает скорость внедрения инновационных инструментов предиктивной аналитики. Система во многом замкнута на национальном контуре, что снижает интенсивность трансграничного обмена информацией об угрозах. В результате управление рисками носит преимущественно реактивный характер, ориентированный на фиксацию и локализацию инцидентов, а не на их опережающее прогнозирование [1].

Для количественной оценки различных международных моделей управления цифровыми финансовыми рисками применен метод взвешенных коэффициентов. Наибольший вес (0,30) присвоен предиктивной эффективности, поскольку способность системы прогнозировать и предотвращать риски до их проявления является ключевым

фактором устойчивости финансовой системы [7]. Адаптируемость к российским условиям (0,25) занимает второе место по значимости, так как любая зарубежная методика может быть полезна только при возможности ее интеграции в отечественную инфраструктуру.

В таблицах 4 и 5 весовые коэффициенты сформированы на основе аналитического подхода с учетом приоритетности критериев для российских условий функционирования финансового сектора. В частности, при определении значимости критериев учитывались:

– результаты анализа научных публикаций в области цифрового риск-менеджмента;
– рекомендации международных организаций по управлению киберрисками;
– специфика российского финансового рынка, включая ограниченность ресурсов региональных организаций;
– целевая направленность исследования на превентивное управление рисками.

Ключевым критериям предиктивной эффективности и адаптируемости присвоены наибольшие веса (0,30 и 0,25 соответственно), поскольку именно они определяют способность системы не только выявлять, но и предупреждать риски в условиях российской институциональной среды. Остальные коэффициенты распределены пропорционально их влиянию на практическую реализуемость и экономическую эффективность предлагаемых решений.

Таблица 4 - Оценки критериев эффективности системы с использованием метода взвешенных коэффициентов

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.4

Критерий	Содержание	Вес
Предиктивная эффективность	Способность системы выявлять риски до их реализации с использованием технологий искусственного интеллекта, Big Data и SupTech-инструментов	0,30
Адаптируемость к российским условиям	Соответствие существующей правовой и институциональной среде, возможность применения без значительной перестройки регуляторных механизмов	0,25
Экономическая эффективность	Соотношение затрат на внедрение и ожидаемого эффекта	0,20
Технологическая зрелость	Степень отработанности решений и уровень автоматизации	0,15
Интеграционная совместимость	Возможность взаимодействия с отечественными цифровыми системами (СБП, НСПК, ФинЦЕРТ, ЕСИА)	0,10

Примечание: составлено автором

Для сопоставления были выбраны модели Европейского союза, США, Китая и России.

Таблица 5 - Сравнительная оценка международных подходов к цифровому управлению финансовыми рисками

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.5

Страна / модель	Предиктивная эффективность	Адаптируемость к РФ	Экономичность	Тех. зрелость	Интеграция	Итоговый индекс
Европейский союз (DORA, TIBER-EU)	5	4	3	5	4	4,4
США (NIST, FS-ISAC)	5	3	4	5	3	4,1
Китай (PBOC, Big Data, AI Risk Monitoring)	4	5	4	4	5	4,4

Страна / модель	Предиктивная эффективность	Адаптируемость к РФ	Экономичность	Тех. зрелость	Интеграция	Итоговый индекс
Россия (ФинЦЕРТ, НСПК, RegTech)	3	5	4	3	5	3,9

Примечание: составлено автором

Результаты сравнительной оценки показывают, что европейская модель получила итоговый индекс 4,4 балла благодаря высокой предиктивной эффективности и технологической зрелости [5], [6], однако характеризуется высокой стоимостью внедрения и сложностью адаптации [2]. Модель США получила 4,1 балла, отличаясь высокой технологической зрелостью, но слабой адаптируемостью к централизованной российской системе регулирования. Китайская модель с результатом 4,4 балла продемонстрировала наиболее сбалансированное сочетание предиктивности, адаптируемости и экономичности [3]. Российские решения получили 3,9 балла, демонстрируя высокий уровень интеграции и адаптируемости [11], [12], но сохраняя преимущественно реактивный характер управления рисками [1].

Анализ весовых коэффициентов позволяет выявить ключевые факторы успешности систем цифрового риск-менеджмента. Для России приоритетными являются предиктивность и адаптируемость. Именно сочетание этих факторов определяет возможность трансформации системы от реактивной к проактивной модели. Экономическая эффективность приобретает особую значимость в контексте региональных организаций, где чрезмерно капиталоемкие решения оказываются практически неприменимыми [9].

Адаптация международного опыта для российского финансового рынка требует учета как технологических возможностей, так и институциональных ограничений. Формирование подхода к превентивному управлению цифровыми финансовыми рисками должно основываться на нескольких ключевых принципах: практическая применимость в условиях ограниченных ресурсов, опора на публично доступные данные о киберугрозах, автоматизация процессов мониторинга и анализа, персонализация рекомендаций для различных типов организаций, интеграция с существующей российской инфраструктурой [12].

Таблица 6 - Основные принципы подхода для российских организаций

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.6

Принцип	Описание
Проактивность	Предотвращение рисков до их материализации через прогнозную аналитику
Автоматизация	Минимизация человеческого фактора через ИИ-алгоритм
Соответствие требованиям	Учет российского законодательства и требований ЦБ РФ
Адаптивность	Настройка под специфику конкретной организации и региона деятельности

Примечание: составлено автором

Концептуальная модель превентивного управления включает четыре взаимосвязанных компонента. Система сбора и анализа угроз осуществляет автоматический мониторинг публичных отчетов о киберинцидентах, бюллетеней безопасности, исследований угроз от международных организаций [1]. Интеллектуальный классификатор рисков на базе искусственного интеллекта определяет релевантность угроз для российского финансового рынка и конкретных типов организаций [10]. Прогнозная аналитика предсказывает развитие угроз во времени на основе анализа жизненных циклов киберугроз в международной практике [3]. Генератор превентивных мер автоматически предлагает конкретные защитные меры до материализации угрозы. Ключевое отличие предложенного подхода состоит в переносе центра тяжести с нормативного усиления контроля на алгоритмическое опережающее выявление угроз. Тем самым формируется система, способная снижать вероятность материализации риска до его фактического проявления.

Таблица 7 - Суть и ключевая идея предлагаемого подхода к управлению цифровыми финансовыми рисками

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.7

Суть подхода	Ключевая идея
Непрерывно отслеживает открытые источники информации о киберугрозах; Анализирует паттерны развития угроз с помощью искусственного интеллекта; Прогнозирует вероятность материализации рисков для конкретных типов организаций; Автоматически генерирует превентивные рекомендации по защите	Использовать коллективные знания мирового финансового сообщества о киберугрозах для создания системы, которая «видит угрозу до того, как она материализуется» у российской организации

Примечание: составлено автором

Формируемый в рамках исследования подход к превентивному управлению цифровыми финансовыми рисками включает четыре взаимосвязанных компонента, обеспечивающих раннюю идентификацию угроз, их анализ, прогнозирование развития и автоматическую генерацию защитных мер с учётом международного опыта.

Таблица 8 - Алгоритм функционирования подхода

DOI: https://doi.org/10.60797/ECNMS.2026.13.3.8

№	Этап	Описание
1	Мониторинг	Система ежедневно собирает информацию из сотен открытых источников — отчеты международных банков, исследования кибербезопасности, бюллетени CERT-организаций. Это создает постоянно обновляемую картину глобального ландшафта угроз
2	Анализ	ИИ-алгоритмы анализируют собранную информацию, выявляют новые типы атак, определяют их потенциальную опасность для российских финансовых организаций, строят связи между различными инцидентами
3	Прогнозирование	На основе исторических данных о развитии аналогичных угроз система прогнозирует вероятность и временные рамки появления угрозы в российском финансовом секторе
4	Предупреждение	Система генерирует персонализированные рекомендации для разных типов организаций с указанием конкретных мер защиты, которые нужно принять до материализации угрозы

Примечание: составлено автором

Ключевая идея подхода заключается в использовании коллективных знаний мирового финансового сообщества о киберугрозах для создания системы, которая выявляет угрозу до ее материализации у российской организации. Система непрерывно отслеживает открытые источники информации о киберугрозах, анализирует паттерны их развития с помощью искусственного интеллекта [10], прогнозирует вероятность материализации рисков для конкретных типов организаций и автоматически генерирует превентивные рекомендации по защите.

Заключение

Проведённый анализ позволил выявить три тенденции международного цифрового управления финансовыми рисками: технологическую конвергенцию, усиление превентивной направленности и формирование экосистемных механизмов обмена информацией. Проведена сравнительная оценка моделей Европейского союза, США, Китая и России, показавшая, что для российских условий наиболее релевантна китайская модель. Сформирована концептуальная модель превентивного управления цифровыми финансовыми рисками, адаптированная к условиям российских финансовых организаций с ограниченными ресурсами.

Международный опыт цифрового управления финансовыми рисками демонстрирует эффективность превентивного подхода, основанного на применении передовых цифровых технологий. Однако прямое копирование зарубежных практик неприменимо для российского финансового рынка в силу институциональных, регуляторных и технологических различий.

Предложенная концептуальная модель ориентирована на практическое применение в организациях с ограниченными ресурсами. Ключевым преимуществом подхода является использование публично доступной информации о киберугрозах, что снижает барьеры входа для региональных финансовых организаций.

Дальнейшие исследования должны быть направлены на практическую апробацию предложенного подхода в реальных условиях российских финансовых организаций и разработку механизмов институциональной поддержки превентивного управления цифровыми финансовыми рисками на национальном уровне.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Резников Р. Киберугрозы финансовой отрасли: прогноз на 2025–2026 г. / Р. Резников // Positive Technologies. — 2025. — URL: https://ptsecurity.com/ru-ru/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения: 10.12.2025).

2. PwC Research. — 2025. — URL: https://www.pwc.com/us/en/library.html (accessed: 25.12.2025).

3. Зюзин А.В. Локализация и диверсификация российской экономики: региональные и отраслевые особенности / А.В. Зюзин, О.А. Демидова, Т.Г. Долгопятова // Пространственная экономика. — 2020. — Т. 16. — № 2. — С. 39-69. — DOI: 10.14530/se.2020.2.039-069. — EDN CBKNOO.

4. Индекс готовности приоритетных отраслей экономики Российской Федерации к внедрению искусственного интеллекта. Аналитический доклад. — Москва : Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации, 2024. — https://letaibe.media/wp-content/uploads/2024/12/digital_otchet_indeks_2024_0212.pdf?ysclid=mq7m4funr9895466340 (дата обращения: 10.12.2025).

5. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года // Positive Technologies. — 2023. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 22.12.2025).

6. Козубекова Р.Р. Банковский риск-менеджмент в условиях развития финансовых технологий / Р.Р. Козубекова // Интеллектуальные ресурсы – региональному развитию. — 2023. — № 1. — С. 540–545. — EDN EWRQTW.

7. Основные направления развития технологий SupTech и RegTech на период 2021–2023 годов. — Москва, 2021. — URL: http://biscotto.ru/wp-content/uploads/2021/08/ОСНОВНЫЕ-НАПРАВЛЕНИЯ-РАЗВИТИЯ-ТЕХНОЛОГИЙ-SUPTECH-И-REGTECH-НА-ПЕРИОД-2021-–-2023-ГОДОВ.pdf (дата обращения: 23.12.2025).

8. Регулирование генеративного ИИ: правовой анализ и риски для РФ // Национальный портал в сфере искусственного интеллекта. — 2024. — URL: https://ai.gov.ru/knowledgebase/investitsionnaya-aktivnost/2024_regulirovanie_generativnogo_ii_pravovoy_analiz_i_riski_dlya_rf_yakov_i_partnery/ (дата обращения: 23.12.2025).

9. Тургаева А.А. Риск-менеджмент эффективности бизнес-процессов организации / А.А. Тургаева // Проблемы экономики и юридической практики. — 2024. — Т. 20. — № 2. — С. 292–296. — EDN XOROKU.

10. Финансовый риск-менеджмент : учебник / под общ. ред. Л.А. Латышевой, Л.А. Латышева, Ю.М. Склярова [и др.]. — Ставрополь, 2021. — 376 с.

11. Центральный банк Российской Федерации. — 2025. — URL: https://www.cbr.ru/ (дата обращения: 28.12.2025).

12. Абашкин В.Л. Цифровая экономика: 2024 : краткий статистический сборник / В.Л. Абашкин, Г.И. Абдрахманова, К.О. Вишневский [и др.]. — Москва : ИСИЭЗ ВШЭ, 2024. — 124 с.

Список литературы на английском языке / References in English

1. Reznikov R. Kiberugrozi finansovoi otrasli: prognoz na 2025–2026 g. [Cyber threats to the financial industry: forecast for 2025-2026] / R. Reznikov // Positive Technologies. — 2025. — URL: https://ptsecurity.com/ru-ru/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (accessed: 10.12.2025). [in Russian]

2. PwC Research. — 2025. — URL: https://www.pwc.com/us/en/library.html (accessed: 25.12.2025).

3. Zyuzen A.V. Lokalizatsiya i diversifikatsiya rossiyskoy ekonomiki: regionalnye i otraslevye osobennosti [Localization and diversification of Russian economy: regions' and industries' peculiarities] / A.V. Zyuzen, O.A. Demidova, T.G. Dolgopyatova // Prostranstvennaya ekonomika [Spatial Economics]. — 2020. — Vol. 16. — № 2. — P. 39–69. — DOI: 10.14530/se.2020.2.039-069. — EDN CBKNOO. [in Russian]

4. Indeks gotovnosti prioritetnyh otraslej ekonomiki Rossijskoj Federacii k vnedreniyu iskusstvennogo intellekta. Analiticheskij doklad [The index of readiness of priority sectors of the economy of the Russian Federation for the introduction of artificial intelligence. Analytical report]. — Moscow : National Center for the Development of Artificial Intelligence under the Government of the Russian Federation, 2024. — https://letaibe.media/wp-content/uploads/2024/12/digital_otchet_indeks_2024_0212.pdf?ysclid=mq7m4funr9895466340 (accessed: 10.12.2025). [in Russian]

5. Kiberugrozy finansovoj otrasli: promezhutochnye itogi 2023 goda [Cyber threats to the financial industry: interim results of 2023] // Positive Technologies. — 2023. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (accessed: 22.12.2025). [in Russian]

6. Kozubekova R.R. Bankovskij risk-menedzhment v usloviyah razvitiya finansovyh tekhnologij [About digital transformation of bank business models] / R.R. Kozubekova // Intellektual'nye resursy – regional'nomu razvitiyu [Intellectual resources for regional development]. — 2023. — № 1. — P. 540–545. — EDN EWRQTW. [in Russian]

7. Osnovnye napravleniya razvitiya tekhnologij SupTech i RegTech na period 2021–2023 godov [The main directions of development of SupTech and RegTech technologies for the period 2021–2023]. — Moscow, 2021. — URL: http://biscotto.ru/wp-content/uploads/2021/08/ОСНОВНЫЕ-НАПРАВЛЕНИЯ-РАЗВИТИЯ-ТЕХНОЛОГИЙ-SUPTECH-И-REGTECH-НА-ПЕРИОД-2021-–-2023-ГОДОВ.pdf (accessed: 23.12.2025). [in Russian]

8. Regulirovanie generativnogo II: pravovoj analiz i riski dlya RF [Regulation of generative AI: legal analysis and risks for the Russian Federation] // Nacional'nyj portal v sfere iskusstvennogo intellekta [National Portal in the Field of Artificial Intelligence]. — 2024. — URL: https://ai.gov.ru/knowledgebase/investitsionnaya-aktivnost/2024_regulirovanie_generativnogo_ii_pravovoy_analiz_i_riski_dlya_rf_yakov_i_partnery/ (accessed: 23.12.2025). [in Russian]

9. Turgaeva A.A. Risk-menedzhment effektivnosti biznes-processov organizacii [Risk management of the effectiveness of the organization's business processes] / A.A. Turgaeva // Problemy ekonomiki i yuridicheskoj praktiki [Problems of economics and legal practice]. — 2024. — Vol. 20. — № 2. — P. 292–296. — EDN XOROKU. [in Russian]

10. Finansovyj risk-menedzhment [Financial risk management] : textbook / edited by L.A. Latysheva, L.A. Latysheva, Yu.M. Sklyarova [et al.]. — Stavropol, 2021. — 376 p. [in Russian]

11. Tsentralnyj bank Rossijskoj Federatsii [The Central Bank of the Russian Federation]. — 2025. — URL: https://www.cbr.ru/ (accessed: 28.12.2025). [in Russian]

12. Abashkin V.L. Cifrovaya ekonomika: 2024 [Digital Economy: 2024] : kratkij statisticheskij sbornik [a short statistical collection] / V.L. Abashkin, G.I. Abdrakhmanova, K.O. Vishnevsky [et al.]. — Moscow : ISIEZ HSE, 2024. — 124 p. [in Russian]