

В. А. Захаров^{1✉}, А. В. Троеглазова¹

Сравнительный анализ нормативных подходов и практик управления киберрисками в кредитно-финансовых организациях

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: vzakharov60@yandex.ru

Аннотация. В работе анализируются актуальные проблемы информационной безопасности финансового сектора, который испытывает нарастающее давление изоощренных кибератак. Отмечается, что рост числа инцидентов, уязвимостей и финансовых потерь, наряду с существенными затратами на внедрение рекомендованных стандартов (ГОСТ Р 57580.3-2022, ГОСТ Р 57580.4-2022), фактически сводит их применение к рекомендательному уровню. Особое внимание уделяется дефициту методик для оценки рисков, связанных с операциями без добровольного согласия, недостатками традиционных подходов к оценке рисков информационной безопасности в условиях динамично меняющегося ландшафта киберугроз. Подчеркивается возрастающая роль математического моделирования. Для повышения киберустойчивости финансовых организаций и эффективного управления рисками дальнейшая работа должна быть направлена на создание специализированных методик, развитие количественных подходов к оценке киберрисков и стимулирование интеграции систем управления ими в общую структуру риск-менеджмента.

Ключевые слова: кибер-риски, анализ рисков, управление рисками, операционная надежность, киберустойчивость, операция без добровольного согласия

V. A. Zakharov^{1✉}, A. V. Troeglazova¹

Comparative Analysis of Regulatory Approaches and Practices for Managing Cyber Risks in Credit and Financial Organizations

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: vzakharov60@yandex.ru

Abstract. The paper analyzes the current problems of information security in the financial sector, which is experiencing increasing pressure of sophisticated cyberattacks. It is noted that the growing number of incidents, vulnerabilities, and financial losses, along with the significant costs of implementing the recommended standards (GOST R 57580.3-2022, GOST R 57580.4-2022), effectively reduces their implementation to a recommended level. Special attention is paid to the lack of methods for assessing risks associated with operations without voluntary consent, and the shortcomings of traditional approaches to assessing information security risks in a dynamically changing cyberthreat landscape. The increasing role of mathematical modeling is emphasized. To enhance the cyber resilience of financial institutions and effectively manage risks, further efforts should focus on developing specialized methodologies, promoting quantitative approaches to cyber risk assessment, and encouraging the integration of cyber risk management systems into the overall risk management framework.

Keywords: cyber risks, risk analysis, risk management, operational reliability, cyber resilience, non-consensual operations

Введение

Современный финансовый рынок функционирует в условиях постоянного давления со стороны киберпреступности. Статистика последних пяти лет демонстрирует устойчивую тенденцию к увеличению интенсивности и сложности кибератак на финансовые организации. Несмотря на усиление мер защиты, в 2025 году количество целевых атак останется на критически высоком уровне, что свидетельствует об адаптации злоумышленников к современным системам безопасности.

Анализ данных за 2025 год по сравнению с 2024 годом выявил следующие количественные показатели:

1) Зафиксирован 20 % рост уязвимостей ПО в кредитно-финансовых организациях (рис. 1) [1];

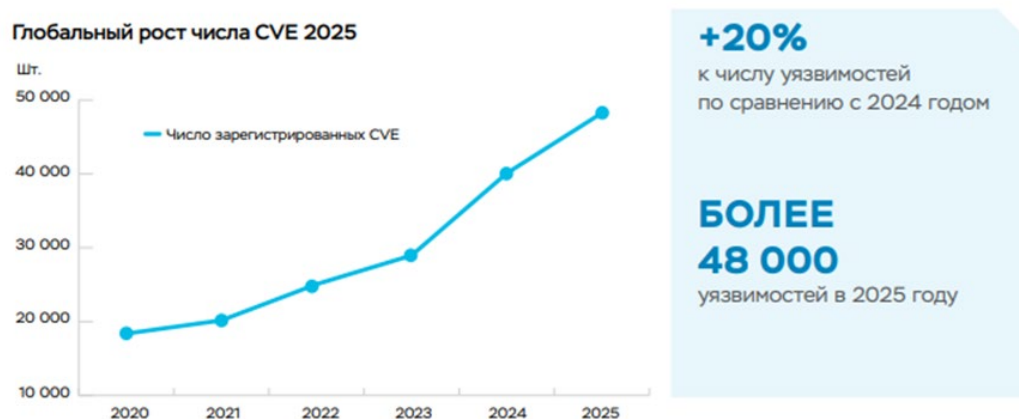


Рис. 1. Динамика зарегистрированных уязвимостей в 2025 году в организациях кредитно-финансовой сфере

2) Фиксируется рост инцидентов операционной надежности, связанных с невозможностью оказывать банковские и финансовые услуги, на 58 % по сравнению с 2024 годом (рис. 2) [1];

3) Объем похищенных денежных средств злоумышленниками у клиентов кредитных организаций вырос на 6,4 % (до 29,3 млрд руб.) [1].

Построение действенной системы обеспечения информационной безопасности в условиях ограниченных ресурсов, времени, а также с учетом ценности активов, их уязвимостей и потенциальных угроз, является критически важным. Выбор адекватных мер защиты для достижения необходимого уровня безопасности должен базироваться на результатах анализа рисков информационной безопасности. Эти результаты служат отправной точкой для внедрения и поддержания эффективного управления информационной безопасностью, а также играют ключевую роль при формировании политики безопасности и создании системы управления рисками. Снижение вероятности киберугроз требует от организаций способности к развитию своей деятельности, что обеспечивается готовностью противодействовать им, возможностью оперативного реагирования и наличием средств для восстановления после атак, то есть киберустойчивостью [3].



Рис. 2. Статистика инцидентов операционной надежности и их динамика 2024-2025 годы

Киберриски в финансовой сфере включают в себя прямые финансовые потери клиентов, подрывающие доверие к современным технологиям; нарушение операционной надежности, приводящее к репутационным ущербам и социальной напряженности; и, как следствие, возможность системного кризиса при возникновении серьезных инцидентов в значимых финансовых организациях.

Управление этими рисками предполагает наличие процедур для оценки, контроля и управления ими на уровне, соответствующем масштабам деятельности организации. Этот процесс включает:

- идентификацию активов, рисков, угроз и уязвимостей;
- анализ рисков путем оценки активов, последствий, вероятности угроз и степени уязвимостей;
- оценку уровня рисков для их последующего ранжирования.

Проведенный анализ литературных источников показал, что вопросы управления рисками информационной безопасности в кредитно-финансовой сфере широко представлены в публикациях: О.В. Бойченко [2, 3], А.А. Гуковской [4], Н.В. Щербаковой [5], М.А. Масловой [6], М.А. Польченко [7], Е.А. Беляева [8,9], М.Р. Белалова [10], Д.С. Кошкина [11], Н.В. Долбни [12] и других.

В контексте современной финансовой сферы представлен широкий спектр методик, стандартов, различных положений, разработанных для управления киберрисками. Примечательно, что, несмотря на наличие этих разнообразных подходов и накопленный опыт, наблюдается неуклонный рост самих киберугроз, что продолжает ставить перед организациями финансовой сферы сложные задачи по совершенствованию существующих моделей управления рисками информационной безопасности с учетом возникновения новых угроз.

В связи с этим целью настоящей работы является проведение сравнительного анализа нормативной базы, требований регуляторов в области защиты информации и сложившейся практики управления рисками информационной безопасности в кредитно-финансовых организациях. В рамках исследования будут рассмотрены преимущества и ограничения применяемых подходов в условиях

новых угроз, а также особенности их практической реализации, влияющие на возможности организаций по совершенствованию моделей управления рисками.

Анализ текущих подходов к управлению рисками развивает понимание киберрисков и проблем, указывая на потребность в совершенствовании существующих методов и практик управления киберрисками.

Материалы и методы исследования

Исследование опирается на системный подход к анализу нормативно-правового обеспечения информационной безопасности в финансовой сфере РФ (изучены и сопоставлены ключевые документы Банка России, ГОСТы). Использовались методы сравнительного анализа стандартов, регуляторных актов и практики управления рисками, экспертные оценки, а также изучение научной литературы, включая концепции цифровой экономики и системных рисков.

Результаты

При рассмотрении способов снижения вероятности возникновения киберугроз важным фактором является способность организации обеспечить развитие деятельности (устойчивость предприятия) за счет готовности противодействия к кибер-угрозам, возможности реагирования на них, средств восстановления после кибератак, называемая киберустойчивостью [2].

К важнейшим составляющим киберрисков в финансово-кредитной сфере можно отнести:

- прямые финансовые потери;
- нарушение операционной надежности и непрерывности предоставления финансовых услуг;
- развитие системного кризиса в случае возникновения инцидентов информационной безопасности [4].

Система управления рисками нарушения информационной безопасности предполагает установление процедур, обеспечивающих оценку, контроль и управление риском на том уровне, который соответствует масштабам деятельности банка и включает следующие этапы:

- 1) Идентификация риска: идентификация активов, рисков, значимых угроз, уязвимостей, существующих контролей;
- 2) Анализ рисков: оценка активов с учетом последствий от нарушения их свойств, вероятности реализации угроз и величины уязвимостей;
- 3) Оценка уровня рисков: оценка рисков заключается в определении количественных и качественных значений уровня риска, в формировании реестра рисков и их ранжировании [5, 7].

Оценка рисков начинается с определения ценных ИТ-активов, а сами риски возникают при реализации угроз через уязвимости, что требует анализа частоты событий, вероятности ущерба и его величины. Актуальность такого анализа обусловлена необходимостью защиты конфиденциальной информации, репутации и безопасности пользователей, поскольку угрозы, исходящие от их источников, могут привести к утрате свойств информационной безопасности активов [7].

В отличие от других сфер деятельности, организации кредитно-финансовой сферы находятся в зоне более сложного регулирования. Банк России разработал

Положение от 08.04.2020 года №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» [13], в котором особое внимание уделено управлению риском информационной безопасности и риском информационных систем. Положение определило необходимость в проведении различных оценок по информационной безопасности, использования новых стандартизированных подходов к оценке операционных рисков для расчета достаточности капиталов, требование к ведению баз данных о событии операционного риска, в том числе риска информационной безопасности [8, 9].

Процедура исследования данной работы строилась на поэтапном сравнительном анализе указанных методик с целью выявления их применимости, сильных и слабых сторон в условиях цифровизации финансовой сферы. В рамках работы был проведен анализ следующих документов и стандартов (табл. 1).

Таблица 1 – Сравнительный анализ методик, стандартов и нормативных документов по управлению рисками

Метод/ Краткое описание	Положительные стороны	Отрицательные стороны	Применимость
ГОСТ Р 71034-2023 «Менеджмент риска. Риск-аппетит и ключевые индикаторы риска». Описание концепции риск-аппетита и подходов к определению/использованию ключевых индикаторов риска	Универсален. Позволяет показать прямую взаимосвязь рисков и бизнес-целей. Может использовать существующие показатели. Способствует своевременному воздействию на риск. Позволяет анализировать показатели во времени. Определяет лимиты рисков. Использует качественные и количественные метрики	Может быть избыточным и труднореализуемым для малых организаций. Описывает общие подходы, не учитывает специфику отрасли	Универсальный (любая организация)
РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». Методика оценки рисков нарушения ИБ на основе качественных оценок степени возможности реализации угроз (СВР) и степени тяжести последствий (СТП)	Распространенность в организациях банковской сферы РФ. Позволяет оценивать риски в количественной (денежной) форме. Описаны защитные меры. Рекомендован для построения / совершенствования системы ИБ	Основана на экспертной оценке (зависимость от квалификации, субъективность). Привлечение внешних экспертов влечет финансовые расходы. Не отражает все современные векторы атак (документ 2009 года). Содержит устаревшие нормативные ссылки (СТО БР ИББС-1.0-2010 утратил силу)	Банковская сфера РФ

Окончание табл. 1

Метод/ Краткое описание	Положительные стороны	Отрицательные стороны	Применимость
ГОСТ Р ИСО/МЭК 27005-2010 «Информационные технологии. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности». Стандарт, предлагающий детальный структурированный подход к управлению рисками ИБ на протяжении всего жизненного цикла	Детальный, структурированный подход. Адаптивность. Основа для построения надежной системы. Применим к организациям всех типов. Описывает весь жизненный цикл управления рискам	Требует глубокого понимания теории и практики. Может быть объемным и ресурсоемким. Требует значительных ресурсов экспертизы.	Любые типы организаций
ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска». Руководство по выбору и применению технологий оценки риска; общий подход к оценке вероятности и последствий	Руководство по выбору технологий оценки риска. Общий подход к оценке вероятности и последствий. Полезен при принятии решений в условиях неопределенности. Устанавливает единый набор терминов Применим во всех сферах, где осуществляется управление рисками	Отсутствие описания процессов или практических инструкций. Не учитывает специфику отраслей	Универсальный (любая сфера)
Положения Банка России (№ 716-П, № 850-П и др.) и ФЗ № 161-ФЗ	Устанавливают обязательные нормативные требования. Охватывают ключевые области: операционный риск, надежность, защиту информации, платежные системы, противодействие переводам без согласия клиента	Фокус на регуляторных требованиях, может не охватывать все лучшие практики или новые угрозы. Специфичны для российского финансового сектора	Финансовый сектор РФ

Однако, несмотря на обилие исследований и наличие нормативно-правовой базы, практическое внедрение эффективных систем управления рисками информационной безопасности в финансовой сфере сталкивается с рядом нерешенных проблем.

Единственным документом, который определяет порядок оценки рисков информационной безопасности организаций кредитно-финансовой сферы, являются рекомендации в области стандартизации Банка России РС БР ИББС-2-2.2-2009 [14]. Методика разработана в 2009 году и в последующем не актуализировалась. Документ не содержит определенный перечень рассматриваемых угроз информационной безопасности, аналогичный банку данных угроз ФСТЭК [8].

В феврале 2023 года вступили в силу ГОСТ Р 57580.3-2022 «Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» [15] и ГОСТ Р 57580.4-2022 «Обеспечение операционной надежности. Базовый состав организационных и технических мер» [16]. Данные стандарты рекомендованы Банком России для управления рисками и обеспечения операционной надежности и призваны повысить устойчивость к кибератакам, а также улучшить качество обслуживания клиентов. Данные документы содержат положения политики управления рисками информационной безопасности, меры по их выявлению, оценке и мониторингу. В них описаны стратегии снижения рисков, планы реагирования на киберинциденты и восстановления после них, правила взаимодействия с поставщиками ИТ-услуг и проведения киберучений.

Настоящие стандарты применяются путем включения нормативных ссылок на них в нормативных актах Банка России и (или) прямого использования устанавливаемых в них требований во внутренних документах финансовых организаций, а также договорах [14,15]. В марте 2024 года Банк России утвердил методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности № 7-МР [17], которые предусматривают обеспечение реализации уровней защиты, определенных пунктом 6.8. раздела 6 ГОСТ Р 57580.3-2022. Таким образом, кредитным организациям рекомендуется осуществить внедрение данных ГОСТов до конца 2025 и 2026 годов в зависимости от значимости кредитной организации. Но до настоящего времени нет нормативных актов Банка России, содержащих ссылки на данные ГОСТы и официального документа, который бы регламентировал порядок и критерии оценки соответствия требованиям этих стандартов.

Необходимо отметить также, что стандартом Банка России СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств [18] событием риска реализации информационных угроз является операция без добровольного согласия, которая стала возможной в результате реализации атак социальной инженерии, либо в результате успешной реализации компьютерной атаки на информационную инфраструктуру клиента.

С точки зрения события операционного риска реализации угроз информационной безопасности, обусловленного с нарушением операционной надежности, основным критерием для классификации является превышение допустимой доли деградации технологического процесса, связанного с предоставлением банковских услуг. При этом событием риска является исключительно реализация информационных угроз в виде компьютерного инцидента. В настоящее время отсутствуют специализированные методики оценки рисков, связанных с операциями без добровольного согласия.

Обсуждение

Результаты исследования подтверждают эскалацию угроз кибербезопасности в финансовом секторе, что выражается в неуклонном росте как количества

кибератак, так и финансового ущерба от них. Рассматриваемые в работе актуальные проблемы в области оценки киберрисков подчеркивают необходимость совершенствования подходов к управлению рисками информационной безопасности в кредитно-финансовых организациях. Среди них можно выделить следующие ключевые аспекты.

1) Субъективность экспертных оценок и отсутствие прогнозирования угроз являются ключевыми методологическими недостатками в оценке рисков информационной безопасности. Милославская Н.Г. справедливо подчеркивает, что эти недостатки указывают на острую необходимость применения математического моделирования для более точной оценки таких рисков [20].

2) По мнению О.В. Бойченко и М.А. Масловой основой построения эффективной системы обеспечения информационной безопасности, особенно при ограниченных ресурсах (кадровых, финансовых), является грамотный анализ рисков. Их подход предполагает интеграцию как количественных методов (оценка последствий в числовом выражении), так и качественных (балльные шкалы для определения уровня риска и мер по его снижению). Такой комплексный подход, по их мнению, позволяет выбрать действительно оптимальные меры защиты информации [3, 6].

3) Исследования М.Р. Белалова, Д.С. Кошкина и Н.В. Долбени свидетельствуют о недостаточной проработке существующей методологической базы для количественной оценки киберрисков. Авторы указывают на нехватку стандартов в этой области, что, по их мнению, может привести к принятию ошибочных решений при выборе мер защиты [10–12].

4) Вопрос универсальности существующих методик оценки рисков информационной безопасности, исследовался в работах Е.А. Беляева, в которых он приходит к мнению, что не всегда они могут служить универсальным эталоном для всех сфер производственной деятельности [8].

Заключение

Настоящее исследование выявило ряд актуальных проблем обеспечения информационной безопасности, в условиях постоянно растущего числа и изощренности кибератак на финансовые организации:

1) динамика роста числа инцидентов, объем похищенных средств и увеличение уязвимостей в программном обеспечении за последние годы свидетельствуют о необходимости совершенствования существующих подходов к управлению рисками;

2) Существующие нормативные акты Банка России не содержат ссылки на ГОСТ Р 57580.3-2022, ГОСТ Р 57580.4-2022, следовательно, их соблюдение носит рекомендательный характер, что, в свою очередь, затрудняет их обязательное внедрение;

3) применение указанных стандартов требует значительных финансовых затрат на приобретение информационной системы управления рисками финансовой организации и интеграцию с системой управления рисками реализации ин-

формационных угроз, и на выделение необходимого ресурсного (кадрового и финансового) обеспечения;

4) в настоящее время отсутствуют специализированные методики оценки рисков, связанных с операциями без добровольного согласия. Используемые на практике методические рекомендации носят исключительно уведомительный характер, направленный на повышение осведомленности клиентов об актуальных угрозах в финансовом секторе, и не предлагают инструментов для формализованной оценки таких рисков;

5) существенно возрастает роль применения на практике математического моделирования оценки и прогнозирования рисков информационной безопасности в кредитно-финансовой сфере.

Для дальнейшего укрепления кибербезопасности финансового сектора представляется целесообразным:

- разработка специализированных методик оценки рисков, в особенности для операций без добровольного согласия;

- развитие количественных подходов к оценке киберрисков на основе математического моделирования;

- поиск эффективных путей интеграции систем управления рисками реализации информационных угроз в систему управления рисками финансовой организации, что в совокупности будет способствовать повышению общей устойчивости финансового сектора к киберугрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Центральный банк Российской Федерации. Аналитический отчет. Киберугрозы и кибератаки в 2025 году. Оценка рисков и тенденций. – 2024. – Текст : электронный // Официальный сайт Банка России. – URL: https://cbr.ru/Collection/Collection/File/59655/Attack_2025.pdf (дата обращения: 16.11.2025). – Режим доступа: свободный.

2. Бойченко, О.В. Киберустойчивость финансовых организаций / О. В. Бойченко, О. V. Boychenko // Научный вестник: финансы, банки, инвестиции. – 2025. – № 1 (70). – С. 105–114. – ISSN 2312-5330. – Текст : электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/372007> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

3. Бойченко, О.В. Система управления рисками кибербезопасности кредитно-финансовой деятельности / О. В. Бойченко, О. V. Boychenko // Научный вестник: финансы, банки, инвестиции. – 2024. – № 3 (68). – С. 55–65. – ISSN 2312-5330. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/368069> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

4. Гуковская, А.А. Оценка киберрисков: проблемы и методы. Актуальные проблемы управления в условиях цифровой экономики России: Всерос. науч. конф. Москва, 2020 г. : материалы конференции / под редакцией Н. И. Архиповой. – Москва : РГГУ, 2020 – Часть 1 : (VII Сперанские чтения; Гуманитарные чтения РГГУ – 2020) – 2020. – 220 с. – ISBN 978-5-7281-2883-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/384914> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

5. Щербакова, Н. В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы / Н. В. Щербакова // Вестник КемГУ. Серия: Политические, социологи-

ческие и экономические науки. – 2021. – № 1. – С. 136–146. – ISSN 2500-3372. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/323153> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

6. Маслова, М.А. Анализ и определение рисков информационной безопасности / М. А. Маслова // Научный результат. Информационные технологии. – 2019. – № 1. – С. 31–37. – ISSN 2518-1092. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/311845> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

7. Польшенко, М.А. Анализ рисков в информационной среде / М. А. Польшенко, М. А. Polchenko // Молодой исследователь Дона. – 2023. – № 3 (42). – С. 55–62. – ISSN 2500-1779. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/354992> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

8. Беляев, Е. А. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций / Е. А. Беляев, О. А. Емельянова, И. И. Лившиц // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21, № 3. – С. 437–441. – DOI 10.17586/2226-1494-2021-21-3-437-441. – EDN BCSBTV.

9. Беляев Е.А., Емельянова О.А. (науч. рук. Лившиц И.И.) Подходы к управлению рисками информационной безопасности в кредитно-финансовых организациях согласно рекомендациям базельского комитета (БАЗЕЛЬ III) // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб: Университет ИТМО, [2021]. URL: <https://kmu.itmo.ru/digests/article/6434> (дата обращения: 17.04.2026). – Режим доступа: для авториз. пользователей.

10. Белалов, М.Р. Киберриски как новый класс операционных рисков банков: экономическая оценка, моделирование потерь и оптимизация затрат на защиту / М. Р. Белалов // Вестник Евразийской науки. – 2025. – Т 17. – № s4. – URL: <https://esj.today/PDF/14FAVN425.pdf> (дата обращения: 17.04.2026).

11. Кошкин Д. С., Шерстов А. В., Фильо В. В. Киберриски: перспективные инструменты контроля (на примере киберстрахования) / Д. С. Кошкин // Искусство и общество. – 2023. – Т. 18. – № 1. – URL: <https://artsoc.jes.su/s207751800024767-2-1/> (дата обращения: 17.04.2026).

12. ЦИФРОВАЯ УЯЗВИМОСТЬ БИЗНЕСА: ЭВОЛЮЦИЯ КИБЕРУГРОЗ / Н. В. Долбня, N. Dolbnya, Г. Е. Шпак, G. Shpak // Новое в экономической кибернетике. – 2025. – № 4. – С. 93–110. – ISSN 2523-448X. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/375460> (дата обращения: 16.11.2025). – Режим доступа: для авториз. пользователей.

13. Положение № 716-П от 08 апреля 2020 г. «О требованиях к системе управления операционным риском в кредитной организации и банковской группе(с изменениями на 22 октября 2024 года): утверждено Центральным банком Российской Федерации (Банком России). – Москва: Центральным банком Российской Федерации (Банком России), 2009: введен впервые: дата введения 2020–04–08 / Центральным банком Российской Федерации (Банком России)–, 2019. – Текст : электронный // Консорциум Кодекс : сайт Электронный фондправовых и нормативно-технических документов. – URL: <https://docs.cntd.ru/document/564859689> (дата обращения: 16.11.2025). – Режим доступа: свободный.

14. РС БР ИББС-2.2-2009 РС БР ИББС-2.2-2009 Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушений информационной безопасности: утверждены и введены в действие распоряжением Банка России от 11 ноября 2009 г. № Р-1190: введены впервые: дата введения 2009–11–11 / разработаны Центральным банком Российской Федерации (Банком России). – Москва: Центральным банком Российской Федерации (Банком России), 2009. – Текст : электронный // ЦБ : сайт Центральный банк Российской Фе-

дерации (Банк России). – URL: https://cbr.ru/statichtml/file/59420/st22_09.pdf (дата обращения: 25.11.2025). – Режим доступа: свободный.

15. ГОСТ Р 57580.3 – 2022 Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 г. № 1548-ст: введен впервые: дата введения 2023–02–01 / разработан Центральным банком Российской Федерации (Банком России). – Москва: ФГБУ Институт стандартизации, 2023. – Текст : электронный // Росстандарт : сайт Федерального агентства по техническому регулированию и метрологии. – URL: <https://protect.gost.ru/gost/details/1c8a4cba-f1b9-4eec-a32b-cf6bf0637b72> (дата обращения: 16.11.2025). – Режим доступа : свободный.

16. ГОСТ Р 57580.4 – 2022 Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 г. № 1549-ст: введен впервые: дата введения 2023–07–01 / разработан Центральным банком Российской Федерации (Банком России). – Москва: ФГБУ Институт стандартизации, 2023. – Текст : электронный // Росстандарт : сайт Федерального агентства по техническому регулированию и метрологии. – URL: <https://protect.gost.ru/gost?year=2026&month=4&search=57580.4> (дата обращения: 17.04.2026). – Режим доступа: свободный.

17. Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности : № 7-МР от 21.03.2024. / Центральный банк Российской Федерации (Банк России). – Москва, 2024. – Текст : электронный // Официальный сайт Банка России. – URL: <https://cbr.ru/Crosscut/LawActs/File/7712> (дата обращения: 17.04.2026). – Режим доступа: свободный.

18. СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств : стандарт Банка России : официальное издание : принят и введен в действие Приказом Банка России от 1 марта 2023 г. № ОД-335 / разработан Центральным банком Российской Федерации (Банком России). – Москва : Центральный банк Российской Федерации, 2023. – Текст : электронный // Официальный сайт Банка России : сайт Центрального банка Российской Федерации. – URL: <https://cbr.ru/Crosscut/LawActs/File/6150> (дата обращения: 17.04.2026). – Режим доступа : свободный.

19. Беляев Е.А., Емельянова О.А. (науч. рук. Исаев А.С.) Проблемы применения методических документов Банка России при осуществлении оценки рисков информационной безопасности кредитно-финансовых организаций // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб: Университет ИТМО, [2020]. URL: <https://kmu.itmo.ru/digests/article/3887> (дата обращения: 17.04.2026). – Режим доступа: для авториз. пользователей.

20. Милославская, Н. Г. , Толстой А.И., Управление рисками информационной безопасности. Учебное пособие для вузов. – 4-е издание, переработанное и дополненное – Москва : Горячая линия – Телеком, 2024. – 292 с.: ил.– С. 126–128. – ISBN 978-5-9912-1037-9.

© В. А. Захаров, А. В.Троеглазова, 2026