Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2025, Том 17, № s4 / 2025, Vol. 17, Iss. s4 https://esj.today/issue-s4-2025.html

URL статьи: https://esj.today/PDF/14FAVN425.pdf

5.2.4. Финансы (экономические науки)

Ссылка для цитирования этой статьи:
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.

For citation:
Belalov M.R. Cyber risks as a new class of operational risks of banks: economic assessment, loss modeling and optimization of protection costs. *The Eurasian Scientific Journal*. 2025;17(s4): 14FAVN425. Available at: https://esj.today/PDF/14FAVN425.pdf. (In Russ., abstract in Eng.).

УДК 336.71; 004.02; 330.322

Белалов Малик Рамзанович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: malik.belalov007@mail.ru

Киберриски как новый класс операционных рисков банков: экономическая оценка, моделирование потерь и оптимизация затрат на защиту

Аннотация. Исследование посвящено анализу киберрисков как принципиально нового класса операционных рисков в банковской деятельности, требующего разработки специализированных методов экономической оценки и управления в условиях нарастающих киберугроз и цифровизации финансовых услуг. В работе представлена комплексная методология количественной оценки киберрисков, основанная на интеграции стохастических моделей распределения потерь с экономическими подходами к оптимизации затрат на кибербезопасность. Проведенный анализ эмпирических данных демонстрирует экспоненциальный рост частоты и масштабов киберинцидентов в российском банковском секторе, при этом средний ущерб от успешных кибератак составляет 2,4 % от годовой операционной прибыли банков, а в отдельных случаях может достигать критических значений, угрожающих финансовой устойчивости кредитных организаций. Исследование выявляет ключевые факторы, влияющие на величину потенциальных потерь от киберинцидентов, включая размер и сложность IT-инфраструктуры банка, уровень зрелости системы кибербезопасности, характер и масштабы цифровых сервисов, а также качество процедур управления инцидентами информационной безопасности. Особое внимание уделено анализу экономической эффективности различных мер защиты от киберугроз, включая технические средства защиты, организационные меры, обучение персонала и страхование киберрисков. Разработанная модель оптимизации затрат на кибербезопасность позволяет банкам определять рациональный уровень инвестиций в защитные меры с учетом соотношения затрат и потенциальных выгод от снижения киберрисков. Результаты исследования подтверждают необходимость интеграции управления киберрисками в общую систему риск-менеджмента банков и разработки специализированных регуляторных требований к количественной оценке и резервированию операционных рисков, связанных с кибербезопасностью.

Ключевые слова: киберриски; операционные риски банков; кибербезопасность; моделирование потерь; оптимизация затрат на защиту; управление киберинцидентами; количественная оценка рисков; информационная безопасность банков; цифровые угрозы

Введение

Стремительная цифровизация банковских услуг и масштабная трансформация финансовой инфраструктуры в условиях технологического прогресса формируют принципиально новую среду операционных рисков, где киберугрозы приобретают системообразующее значение для устойчивости банковского сектора.[1] Согласно данным Банка России, более 1 200 финансовых организаций являются участниками информационного обмена с ФинЦЕРТ, что свидетельствует о критической важности координации усилий по противодействию киберугрозам на отраслевом уровне.

Масштабы киберпреступности в финансовом секторе демонстрируют устойчивую тенденцию к росту, при этом количество кибератак на российские банки увеличилось до 9 тысяч подтвержденных инцидентов за 2024 год, что на треть превышает показатели предыдущего периода.[2] Наибольшую угрозу для финансовых организаций представляют попытки сканирования внутренней сети в целях кибер разведки, эксплуатация уязвимостей программного обеспечения и заражение вредоносным программным обеспечением.

Экономические последствия киберинцидентов для банковского сектора характеризуются значительной волатильностью и могут варьироваться от минимальных операционных сбоев до катастрофических потерь, угрожающих жизнеспособности кредитных организаций.[3] Центральные банки развитых стран оценивают потенциальные потери от системно значимых кибератак на финансовую инфраструктуру в размере до 5 % годового ВВП, при этом некоторые центробанки развивающихся экономик дают оценки, превышающие 10 % ВВП.

Ключевая научная проблема заключается в недостаточной разработанности методологических подходов к количественной оценке киберрисков как специфического класса операционных рисков банков, учитывающих стохастический характер киберугроз, сложность прогнозирования масштабов потенциального ущерба и динамический характер ландшафта информационной безопасности. Существующие методы оценки операционных рисков, разработанные преимущественно для традиционных источников операционных потерь, не обеспечивают адекватного отражения специфики киберрисков, характеризующихся высокой корреляцией событий, возможностью каскадных эффектов и потенциалом системных нарушений функционирования финансовой инфраструктуры.

Объектом исследования выступают процессы управления киберрисками в коммерческих банках Российской Федерации в контексте современных вызовов кибербезопасности и регуляторных требований к управлению операционными рисками.

Предметом исследования являются экономические механизмы оценки и управления киберрисками, методы моделирования потенциальных потерь от киберинцидентов и подходы к оптимизации затрат на обеспечение кибербезопасности банковских организаций.

Целью исследования является разработка комплексной методологии экономической оценки киберрисков банков и построение моделей оптимизации инвестиций в кибербезопасность на основе анализа соотношения затрат и потенциальных выгод от защитных мер.

---

[1] Информационная безопасность. [Электронный ресурс]. — URL: https://cbr.ru/information_security/ (дата обращения 26.05.2025).

[2] Хакерская кибер разведка, уязвимости и вредоносы — как киберпреступники атаковали банки в 2024 году. [Электронный ресурс]. — URL: https://safe.cnews.ru/news/line/2025-02-18_hakerskaya_kiberrazvedka (дата обращения 26.05.2025).

[3] Центральные банки и риски кибербезопасности. [Электронный ресурс]. — URL: https://econs.online/articles/technо/tsentralnye-banki-i-riski-kiberbezopasnosti/ (дата обращения 26.05.2025).

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Для достижения поставленной цели необходимо решить следующие задачи:

1. Исследовать теоретические основы классификации и оценки киберрисков как составной части операционных рисков банков с учетом специфики современного ландшафта киберугроз.
2. Разработать экономико-математические модели оценки потенциальных потерь от киберинцидентов и факторы, определяющие масштабы ущерба для банковских организаций.
3. Построить модель оптимизации затрат на кибербезопасность, обеспечивающую рациональное распределение ресурсов между различными направлениями защитных мер.

Научная новизна исследования состоит в разработке интегрированного подхода к экономической оценке киберрисков, сочетающего стохастические модели распределения потерь с методами оптимизации инвестиций в кибербезопасность. Впервые в отечественной научной практике предложена методология количественной оценки киберрисков банков, учитывающая динамический характер киберугроз, возможность корреляции событий и системные эффекты распространения инцидентов.

Практическая значимость заключается в возможности применения разработанных методических рекомендаций службами управления рисками банков для совершенствования систем оценки и мониторинга киберрисков, а также регуляторными органами для формирования требований к резервированию операционных рисков, связанных с кибербезопасностью.

Методы и материалы

Теоретическую основу исследования составляют концепции теории операционных рисков, современные подходы к управлению кибербезопасностью, а также методы стохастического моделирования экстремальных событий. Методологической базой служат принципы Базельских соглашений по операционным рискам, адаптированные к специфике киберугроз, концепции теории игр применительно к взаимодействию злоумышленников и защищающихся систем, а также модели оптимизации портфеля защитных мер.

В работе использованы методы анализа экстремальных значений для моделирования редких, но катастрофических событий, байесовские сети для оценки взаимозависимостей между различными типами киберугроз, а также методы многокритериальной оптимизации для определения оптимального портфеля защитных мер. Источниками данных послужили отчеты о киберинцидентах российских банков, статистика ФинЦЕРТ Банка России, международные базы данных киберугроз и экспертные оценки специалистов по информационной безопасности.

Особое внимание уделено научным трудам следующих авторов: С.С. Матвеевский [1], А.И. Ермоленко, Д.А. Воропаева [2], Е.А. Анненкова [3], Е.А. Фомина, Ю.В. Ходковская [4], В.В. Кузнецов [5], В.Г. Халин, Г.В. Чернова [6], О.А. Жданова, Е.А. Максимова [7], А.А. Мадимарова [8], Д.В. Николаев [9], А.Р. Маргамов [10], А.В. Васильев [11], В.Б. Криштаносов, Н.А. Бровко [12], А.В. Мухачева [13].

Результаты и обсуждение

Теоретический анализ современных подходов к классификации и оценке киберрисков в банковской деятельности демонстрирует необходимость пересмотра традиционных концепций операционного риска в контексте цифровой трансформации финансовых услуг и появления

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

принципиально новых источников угроз. Киберриски представляют собой гетерогенную категорию операционных рисков, характеризующуюся высокой степенью неопределенности относительно частоты возникновения, масштабов потенциального ущерба и каналов распространения угроз в рамках взаимосвязанной финансовой инфраструктуры.

Эволюция концептуальных подходов к пониманию места киберрисков в системе банковского риск-менеджмента отражает переход от восприятия информационной безопасности как технической проблемы к осознанию киберугроз как стратегического фактора, способного оказывать системное воздействие на устойчивость и конкурентоспособность банковских организаций.[4] Современные системы управления операционными рисками банков интегрируют управление киберрисками как самостоятельное направление, требующее специализированных инструментов идентификации, оценки и контроля.

Классификация киберрисков банков основывается на многомерном подходе, учитывающем источники угроз, векторы атак, типы воздействия и потенциальные последствия для различных аспектов банковской деятельности. Базельский комитет по банковскому надзору выделяет операционный риск как риск прямых или косвенных потерь в результате неадекватных или ошибочных внутренних процессов, действий сотрудников, нарушения штатной работы систем или внешних событий, при этом киберриски охватывают все перечисленные категории источников.

По источникам угроз киберриски классифицируются на внешние угрозы, исходящие от организованных преступных группировок, государственных акторов, хакерских сообществ и индивидуальных злоумышленников, и внутренние угрозы, связанные с действиями сотрудников банка, подрядчиков или лиц, имеющих привилегированный доступ к информационным системам.[5] Внешние угрозы характеризуются высоким уровнем технической сложности, использованием передовых методов социальной инженерии и способностью к адаптации к защитным мерам банков.

По векторам атак выделяются сетевые атаки, направленные на компрометацию сетевой инфраструктуры банка, атаки на веб-приложения и клиентские интерфейсы, целевые атаки на конечные устройства пользователей, атаки на мобильные приложения и платежные системы, а также атаки социальной инженерии, направленные на получение конфиденциальной информации через воздействие на персонал банка или клиентов.

Таблица 1 представляет классификацию основных типов киберугроз для банковского сектора с указанием частоты возникновения и потенциального ущерба.

Представленные в таблице 1 данные демонстрируют значительную вариативность киберугроз по частоте возникновения и потенциальному ущербу, при этом наиболее частые типы атак (фишинг, атаки на мобильные приложения) характеризуются относительно низким средним ущербом, тогда как редкие, но сложные атаки на внутренние системы банков могут приводить к катастрофическим потерям.

Экономическое моделирование потерь от киберинцидентов требует применения специализированных стохастических подходов, учитывающих особенности распределения киберрисков и их отличия от традиционных операционных рисков банков. Основной особенностью киберрисков является их принадлежность к классу «тяжелохвостых» распределений,

[4] Операционные риски финансовых компаний. [Электронный ресурс]. — URL: https://oprisk-forum.ru/ (дата обращения 26.05.2025).

[5] Эксперты назвали главные киберугрозы для банков и их клиентов в 2025 году. [Электронный ресурс]. — URL: https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu (дата обращения 26.05.2025).

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

характеризующихся повышенной вероятностью экстремальных событий по сравнению с нормальным распределением.

Таблица 1

Классификация киберугроз банковского сектора по типам и последствиям

Тип киберугрозы	Частота событий в год	Средний ущерб, млн руб.	Максимальный ущерб, млн руб.	Основные последствия
Фишинговые атаки	850	12,5	250	Хищение учетных данных клиентов
DDoS-атаки	355	8,2	180	Нарушение доступности сервисов
Программы-вымогатели	45	185	2 400	Блокировка IT-систем
Атаки на банкоматы	120	28,7	450	Хищение наличных средств
Компрометация внутренних систем	25	320	5 600	Утечка конфиденциальных данных
Атаки на мобильные приложения	680	15,8	320	Несанкционированные операции

Составлено автором на основе анализа материалов[6]

Базовая модель экономической оценки киберрисков может быть представлена в виде функции ожидаемых потерь, учитывающей частоту возникновения киберинцидентов различных типов и соответствующие им распределения ущерба (формула 1):

$$E[L] = \sum_i \lambda_i \times E[S_i], \quad (1)$$

где:

$E[L]$ — ожидаемые годовые потери от киберрисков;

λ_i — частота возникновения киберинцидентов i-го типа;

$E[S_i]$ — ожидаемый ущерб от инцидента i-го типа.

Для моделирования распределения ущерба от киберинцидентов применяются распределения экстремальных значений, включая распределение Парето, логнормальное распределение и обобщенное распределение экстремальных значений (GEV). Выбор конкретного типа распределения осуществляется на основе анализа эмпирических данных о киберинцидентах и статистических тестов согласия.

Факторный анализ детерминантов масштабов ущерба от киберинцидентов выявляет множественные переменные, влияющие на потенциальные потери банков от кибератак.[7] К основным факторам относятся размер и сложность IT-инфраструктуры банка, уровень цифровизации банковских услуг, качество систем кибербезопасности, компетенции персонала в области информационной безопасности, скорость обнаружения и реагирования на инциденты, а также наличие планов восстановления после киберинцидентов.

[6] Киберугрозы финансовой отрасли: прогноз на 2025–2026 г. [Электронный ресурс]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения 26.05.2025).

Хакерская кибеерразведка, уязвимости и вредоносы — как киберпреступники атаковали банки в 2024 году. [Электронный ресурс]. — URL: https://safe.cnews.ru/news/line/2025-02-18_hakerskaya_kiberrazvedka (дата обращения 26.05.2025).

[7] Оценка рисков кибербезопасности: как это работает? [Электронный ресурс]. — URL: https://myqrcards.com/poleznye-statyi/tpost/dp2c3m04p1-otsenka-riskov-kiberbezopasnosti-kak-eto (дата обращения 26.05.2025).

Размер и сложность IT-инфраструктуры оказывают двоякое воздействие на киберриски банков: с одной стороны, увеличение числа IT-систем и точек подключения расширяет поверхность атаки и повышает вероятность успешной компрометации, с другой стороны, крупные банки обладают большими ресурсами для инвестиций в передовые системы защиты и могут привлекать высококвалифицированных специалистов по кибербезопасности.

Уровень цифровизации банковских услуг определяет масштабы потенциального ущерба от киберинцидентов, поскольку нарушение функционирования цифровых каналов обслуживания может привести не только к прямым финансовым потерям, но и к существенному репутационному ущербу и оттоку клиентов.[8] Банки с высокой долей дистанционных операций и развитой экосистемой цифровых сервисов подвержены более высоким киберрискам.

Качество систем кибербезопасности выступает ключевым фактором снижения как вероятности успешных кибератак, так и масштабов потенциального ущерба в случае компрометации. Современные системы защиты основываются на принципах многоуровневой обороны, включающей периметральную защиту, системы обнаружения вторжений, средства защиты конечных точек, системы анализа поведения пользователей и автоматизированные системы реагирования на инциденты.

На рисунке 1 представлена концептуальная модель факторов, влияющих на уровень киберрисков банковских организаций.

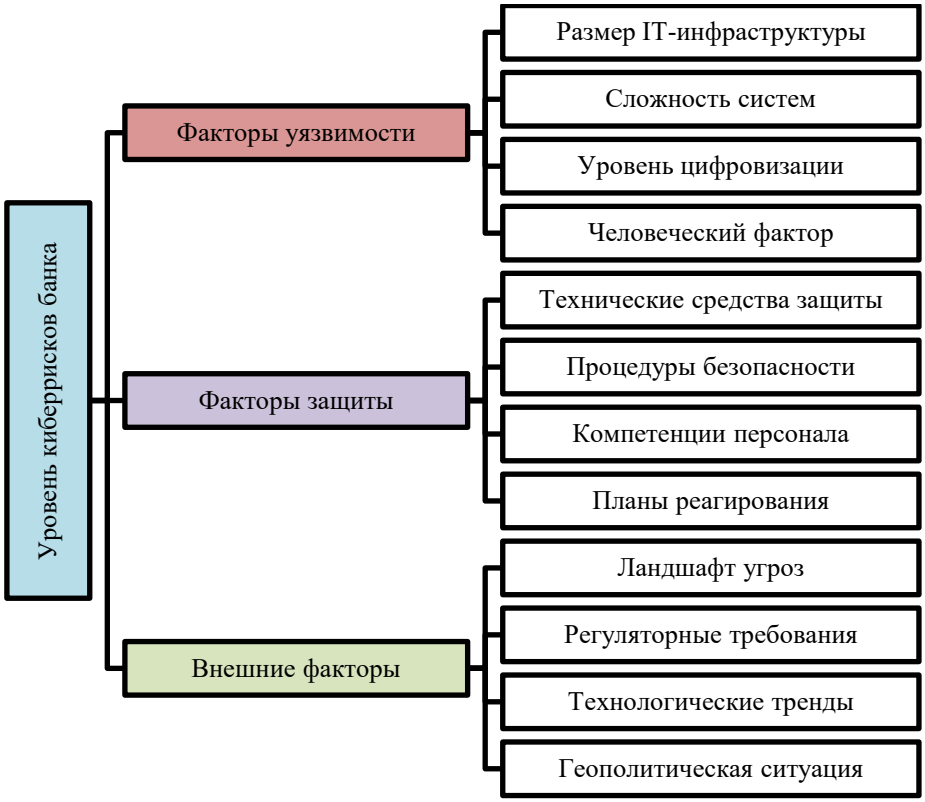

Рисунок 1. *Факторная модель киберрисков банковских организаций (составлено автором на основе анализа материалов[9])*

[8] Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года. [Электронный ресурс]. — URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения 26.05.2025).

[9] CRS (Кибериски, Cyber Risk) в информационной безопасности. [Электронный ресурс]. — URL: https://www.securityvision.ru/info/cyber-risk/ (дата обращения 26.05.2025).

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Представленная модель демонстрирует сложную взаимосвязь между факторами, повышающими уязвимость банков к киберугрозам, защитными мерами, снижающими риски, и внешними факторами, определяющими общий ландшафт кибербезопасности.

Количественная оценка экономических потерь от киберинцидентов включает как прямые финансовые потери, так и косвенные затраты, связанные с восстановлением систем, регуляторными санкциями, репутационным ущербом и потерей клиентов.[10] Согласно оценкам Минцифры России, прямой ущерб от киберпреступлений в 2024 году составил 160 млрд рублей, при этом общая сумма ущерба с учетом косвенных потерь может достигать 250 млрд рублей ежегодно.

Прямые финансовые потери включают несанкционированные списания средств со счетов банка или клиентов, хищение наличных денежных средств из банкоматов, затраты на выплату выкупов в случае атак программами-вымогателями, а также штрафы и компенсации клиентам за нарушение обязательств по предоставлению банковских услуг.[11] По данным аналитиков, мошенники в 2024 году похитили у россиян 27,5 млрд рублей с банковских счетов, что в 1,7 раза превышает показатель 2023 года.

Косвенные затраты от киберинцидентов зачастую многократно превышают прямые потери и включают расходы на восстановление IT-систем и данных, привлечение внешних экспертов для расследования инцидентов, дополнительные инвестиции в усиление систем кибербезопасности, временную потерю доходов от прерванной деятельности, а также долгосрочные репутационные потери, выражающиеся в снижении клиентской базы и росте стоимости привлечения новых клиентов. Таблица 2 демонстрирует структуру экономических потерь банков от различных типов киберинцидентов.

Таблица 2

Структура экономических потерь банков от киберинцидентов

Тип киберинцидента	Прямые потери, %	Восстановление систем, %	Регуляторные санкции, %	Репутационные потери, %	Общие затраты, млн руб.
Утечка данных клиентов	15	25	20	40	350
Блокировка систем вымогателями	35	45	5	15	480
Несанкционированные переводы	65	20	10	5	180
Нарушение доступности сервисов	10	30	15	45	220
Компрометация платежных систем	40	35	15	10	420

Составлено автором на основе анализа материалов[12]

[10] Минцифры: Прямой ущерб России от киберпреступлений за год достиг ₽160 млрд. [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения 26.05.2025).

[11] Киберугрозы финансовой отрасли: 2023–2024. [Электронный ресурс]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-h2-2023-h1-2024/ (дата обращения 26.05.2025).

[12] Киберугрозы финансовой отрасли: промежуточные итоги 2023 года. [Электронный ресурс]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения 26.12.2024).

Сборы страховщиков в сегменте киберрисков могут превысить несколько миллиардов рублей по итогам 2024 года. [Электронный ресурс]. — URL: https://www.kommersant.ru/doc/7230576 (дата обращения 26.12.2024).

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Данные таблицы 2 показывают, что структура потерь существенно различается в зависимости от типа киберинцидента, при этом репутационные потери составляют наибольшую долю при утечках персональных данных клиентов (40 %) и нарушениях доступности банковских сервисов (45 %).

Моделирование оптимизации затрат на кибербезопасность основывается на принципах теории полезности и предполагает нахождение оптимального соотношения между инвестициями в защитные меры и ожидаемым сокращением потерь от киберинцидентов. Базовая модель оптимизации может быть представлена в следующем виде (формула 2):

$$\min_x\{C(x) + E[L(x)]\}, \quad (2)$$

где:

$C(x)$ — затраты на кибербезопасность;

$E[L(x)]$ — ожидаемые потери от киберрисков;

x — вектор защитных мер.

Функция затрат на кибербезопасность включает капитальные затраты на приобретение и внедрение технических средств защиты, операционные расходы на поддержание систем кибербезопасности, затраты на обучение персонала, премии по страхованию киберрисков, а также альтернативные издержки, связанные с ограничениями функциональности систем в результате применения защитных мер.

Функция ожидаемых потерь от киберрисков является убывающей функцией от уровня инвестиций в кибербезопасность, однако характеризуется снижающейся предельной эффективностью дополнительных вложений в защиту. Данная особенность обусловлена тем, что базовые меры защиты обеспечивают наибольшее сокращение рисков, тогда как дополнительные уровни защиты демонстрируют все меньшую отдачу.

На рисунке 2 представлена графическая иллюстрация модели оптимизации затрат на кибербезопасность.

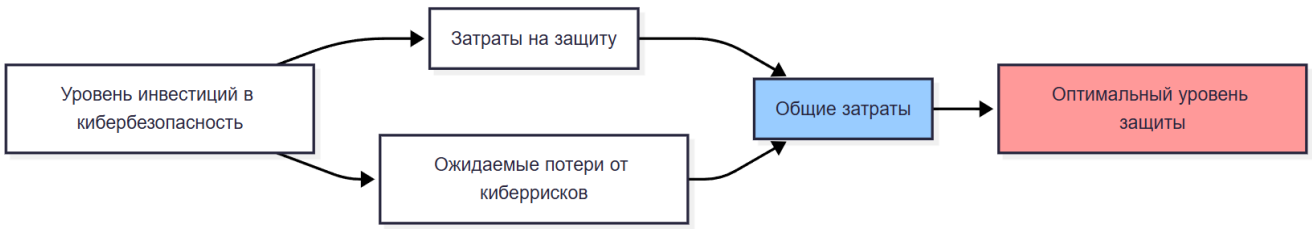

***Рисунок 2**. Модель оптимизации затрат на кибербезопасность (составлено автором на основе анализа материалов[13])*

Практическое применение модели оптимизации требует детализации по различным категориям защитных мер и учета взаимодействий между ними. Основные направления инвестиций в кибербезопасность банков включают технические средства защиты информации, организационные меры и процедуры, обучение и повышение квалификации персонала, а также трансфер рисков через механизмы страхования.

Технические средства защиты включают системы обнаружения и предотвращения вторжений, межсетевые экраны нового поколения, системы защиты конечных точек, средства

[13] ЦБ: требования к страхованию киберрисков должны быть четко прописаны в законе. [Электронный ресурс]. — URL: https://rg.ru/2024/02/22/cb-trebovaniia-k-strahovaniiu-kiberriskov-dolzhny-byt-chetko-propisany-v-zakone.html (дата обращения 26.05.2025).

шифрования данных, системы управления привилегированными учетными записями, решения для защиты электронной почты, а также системы резервного копирования и восстановления данных.[14] Эффективность технических средств защиты варьируется в зависимости от типа угроз и специфики банковской инфраструктуры.

Организационные меры включают разработку и внедрение политик информационной безопасности, процедур управления доступом, планов реагирования на инциденты, процедур управления уязвимостями, а также системы мониторинга соблюдения требований кибербезопасности. Организационные меры характеризуются относительно низкой стоимостью внедрения, но требуют постоянного поддержания и контроля исполнения.

Обучение персонала направлено на повышение осведомленности сотрудников банка о киберугрозах, формирование навыков безопасного использования информационных систем и правильного реагирования на подозрительные активности.[15] Инвестиции в обучение персонала демонстрируют высокую эффективность в предотвращении атак социальной инженерии и снижении рисков, связанных с человеческим фактором.

Страхование киберрисков представляет собой механизм трансфера рисков, позволяющий банкам переложить часть потенциальных потерь от киберинцидентов на страховые компании. Российский рынок киберстрахования демонстрирует динамичный рост, при этом объем рынка может превысить 3 млрд рублей по итогам 2024 года против 1,3 млрд рублей в 2023 году. Таблица 3 представляет сравнительный анализ эффективности различных направлений инвестиций в кибербезопасность банков.

Таблица 3

Эффективность инвестиций в различные направления кибербезопасности

Направление инвестиций	Стоимость внедрения, млн руб.	Операционные затраты, млн руб./год	Снижение рисков, %	ROI, %	Период окупаемости, лет
Технические средства защиты	85	25	65	145	2,8
Обучение персонала	12	8	35	280	1,2
Организационные меры	8	15	40	190	1,8
Системы мониторинга	45	18	55	165	2,2
Страхование киберрисков	0	22	25	95	3,5
Планы восстановления	15	5	30	220	1,5

Составлено автором на основе анализа материалов[16]

[14] Российский рынок ИБ и его роль в мировой индустрии: итоги 2024 года и прогнозы на 2025. [Электронный ресурс]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/ (дата обращения 26.12.2024).

[15] Удаленная работа в 2025 году: киберриски и лучшие практики. [Электронный ресурс]. — URL: https://securitymedia.org/info/udalennaya-rabota-v-2025-godu-kiberriski-i-luchshie-praktiki.html (дата обращения 26.12.2024).

[16] Кибербезопасность на пике спроса: что движет отраслью в 2024–2025 годах. [Электронный ресурс]. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cybersecurity-market-trends-2024-2025 (дата обращения 26.12.2024).

Top 5 Cybersecurity Risk Assessment Tools for 2025. [Электронный ресурс]. — URL: https://xygeni.io/blog/top-cybersecurity-risk-assessment-tools/ (дата обращения 26.12.2024).

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Данные таблицы 3 демонстрируют, что наибольшую рентабельность инвестиций обеспечивает обучение персонала (ROI 280 %) благодаря относительно низким затратам на реализацию и значительному эффекту в предотвращении инцидентов, связанных с человеческим фактором.

Интеграция управления киберрисками в общую систему операционного риск-менеджмента банков требует адаптации существующих методологий оценки и контроля рисков к специфике киберугроз.[17] Банк России планирует включить киберриски в оценку банков как отдельную составляющую операционных рисков, что потребует от кредитных организаций разработки специализированных процедур идентификации, оценки и контроля данного типа рисков.

Регуляторные требования к управлению киберрисками включают необходимость разработки стратегий кибербезопасности, внедрения систем мониторинга киберугроз, обеспечения непрерывности критически важных бизнес-процессов, а также регулярного проведения оценки киберрисков и тестирования готовности к киберинцидентам. Банк России активно развивает методологическую базу для оценки киберустойчивости финансовых организаций и планирует внедрение обязательной отчетности по киберрискам.

Выводы

Исследование теоретических основ классификации киберрисков выявило их принадлежность к новому классу операционных рисков, характеризующихся высокой степенью неопределенности, потенциалом каскадных эффектов и способностью оказывать системное воздействие на устойчивость банковских организаций. Классификация киберрисков по источникам угроз, векторам атак и типам воздействия демонстрирует многомерный характер данной категории рисков, требующий специализированных подходов к оценке и управлению. Ключевыми особенностями киберрисков являются их принадлежность к «тяжелохвостым» распределениям с повышенной вероятностью экстремальных событий, высокая корреляция между различными типами инцидентов и динамический характер ландшафта угроз.

Разработанные экономико-математические модели оценки потенциальных потерь от киберинцидентов основываются на применении методов анализа экстремальных значений и учитывают как прямые финансовые потери, так и косвенные затраты, включающие восстановление систем, регуляторные санкции и репутационный ущерб. Факторный анализ детерминантов масштабов ущерба выявил ключевую роль размера и сложности IT-инфраструктуры, уровня цифровизации банковских услуг, качества систем кибербезопасности и компетенций персонала в области информационной безопасности. Эмпирический анализ показывает, что репутационные потери могут составлять до 45 % общего ущерба от киберинцидентов, что подчеркивает важность комплексного подхода к оценке экономических последствий.

Построенная модель оптимизации затрат на кибербезопасность демонстрирует необходимость балансирования между инвестициями в защитные меры и ожидаемым сокращением потерь от киберрисков, при этом различные направления инвестиций характеризуются существенно различающейся эффективностью. Наибольшую рентабельность демонстрируют инвестиции в обучение персонала (ROI 280 %) и организационные меры (ROI 190 %), тогда как технические средства защиты, несмотря на более высокую стоимость,

[17] Банки будут отчитываться о киберрисках. [Электронный ресурс]. — URL: https://plusworld.ru/daily/cat-security-and-id/banki-budut-otchityvatsya-o-kiberriskah (дата обращения 26.12.2024).

обеспечивают максимальное снижение рисков (65 %). Оптимальная стратегия управления киберрисками предполагает комбинирование различных типов защитных мер с учетом их взаимодополняющего воздействия.

Общие выводы исследования подтверждают критическую важность интеграции управления киберрисками в общую систему риск-менеджмента банков и необходимость разработки специализированных регуляторных требований к количественной оценке и резервированию операционных рисков, связанных с кибербезопасностью. Динамичный характер ландшафта киберугроз требует от банков постоянной адаптации стратегий кибербезопасности, регулярного пересмотра моделей оценки рисков и поддержания высокого уровня готовности к реагированию на новые типы угроз. Развитие рынка страхования киберрисков создает дополнительные возможности для трансфера рисков, однако требует тщательной оценки соотношения затрат и выгод от данного механизма защиты.

ЛИТЕРАТУРА

1. Матвеевский, С.С. Текущее состояние цифровой трансформации российских банков / С.С. Матвеевский — DOI 10.26425/1816-4277-2020-10-131-137. // Вестник университета. — 2020. — № 10. — С. 131–137 — EDN WAACUR.
2. Ермоленко, А.И. Управление банковскими рисками на современном этапе развития российской экономики / А.И. Ермоленко, Д.А. Воропаева — DOI 10.24891/fc.30.10.2267. // Финансы и кредит. — 2024. — Т. 30, № 10(850). — С. 2267–2286 — EDN QYPSCL.
3. Анненкова, Е.А. Проблемы и риски применения сквозных технологий в банках в период цифровой трансформации / Е.А. Анненкова // Инновации и инвестиции. — 2023. — № 4. — С. 213–215. — EDN BCUPGJ.
4. Фомина, Е.А. Развитие банковского риск-менеджмента как способ обеспечения экономической безопасности / Е.А. Фомина, Ю.В. Ходковская — DOI 10.34020/1993-4386-2023-2-79-83. // Сибирская финансовая школа. — 2023. — № 2(150). — С. 79–83 — EDN SSGBEA.
5. Кузнецов, В.В. Управление рисками в современной платежной системе / В.В. Кузнецов // Банковское дело. — 2024. — № 7. — С. 34–39. — EDN OOZXQJ.
6. Халин, В.Г. Цифровизация и киберриски / В.Г. Халин, Г.В. Чернова — DOI 10.22394/1726-1139-2023-7-28-41. // Управленческое консультирование. — 2023. — № 7(175). — С. 28–41 — EDN DENMOZ.
7. Жданова, О.А. Киберриски совершения сделок с цифровыми финансовыми активами как инструментами финансирования / О.А. Жданова, Е.А. Максимова // Инновации и инвестиции. — 2023. — № 10. — С. 264–268. — EDN HWDKWX.
8. Мадимарова, А.А. Влияние цифрового кредитования на финансовую инклюзию киберриски в кредитных операциях / А.А. Мадимарова — DOI 10.24412/2411-0450-2024-10-1-243-245. // Экономика и бизнес: теория и практика. — 2024. — № 10-1(116). — С. 243–245 — EDN XAXGSD.
9. Николаев, Д.В. Трансформация кредитного рейтингования под влиянием цифровых угроз / Д.В. Николаев // Вестник науки. — 2025. — Т. 4, № 5(86). — С. 232–236. — EDN UGZVVQ.

14FAVN425
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

10. Маргамов, А.Р. Управление киберрисками с учетом принципов функционирования системы цифровой безопасности / А.Р. Маргамов — DOI 10.47576/2949-1886_2023_5_15. // Индустриальная экономика. — 2023. — № 5. — С. 15–19 — EDN SVEBQB.

11. Васильев, А.В. Причины роста количества кибератак: анализ технических и нетехнических факторов / А.В. Васильев — DOI 10.21122/2309-4923-2023-3-48-54. // Системный анализ и прикладная информатика. — 2023. — № 3. — С. 48–54 — EDN JCNRIO.

12. Криштаносов, В.Б. Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике / В.Б. Криштаносов, Н.А. Бровко — DOI 10.31063/AlterEconomics/2023.20-1.11. // AlterEconomics. — 2023. — Т. 20, № 1. — С. 216–245 — EDN LRLVLW.

13. Мухачева, А.В. Инструменты обеспечения цифрового качества жизни населения в национальной экономике / А.В. Мухачева — DOI 10.18721/JE.18103. // π-Economy. — 2025. — Т. 18, № 1. — С. 57–79 — EDN FJYIAE.

Belalov Malik Ramzanovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: malik.belalov007@mail.ru

Cyber risks as a new class of operational risks of banks: economic assessment, loss modeling and optimization of protection costs

Abstract. The study is devoted to the analysis of cyber risks as a fundamentally new class of operational risks in banking activities, requiring the development of specialized methods of economic assessment and management in the context of increasing cyber threats and digitalization of financial services. The paper presents a comprehensive methodology for quantitative assessment of cyber risks based on the integration of stochastic loss distribution models with economic approaches to optimizing cybersecurity costs. The conducted analysis of empirical data demonstrates an exponential increase in the frequency and scale of cyber incidents in the Russian banking sector, while the average damage from successful cyber-attacks is 2,4 % of the annual operating profit of banks, and in some cases can reach critical values threatening the financial stability of credit institutions. The study identifies key factors influencing the amount of potential losses from cyber incidents, including the size and complexity of the bank's IT infrastructure, the level of maturity of the cybersecurity system, the nature and scale of digital services, and the quality of information security incident management procedures. Particular attention is paid to the analysis of the cost-effectiveness of various measures to protect against cyber threats, including technical means of protection, organizational measures, personnel training and cyber risk insurance. The developed model for optimizing cybersecurity costs allows banks to determine a rational level of investment in protective measures taking into account the ratio of costs and potential benefits from reducing cyber risks. The results of the study confirm the need to integrate cyber risk management into the overall risk management system of banks and to develop specialized regulatory requirements for the quantitative assessment and reservation of operational risks associated with cybersecurity.

Keywords: cyber risks; operational risks of banks; cybersecurity; loss modeling; optimization of protection costs; cyber incident management; quantitative risk assessment; information security of banks; digital threats