Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2025, Том 12, № s4 / 2025, Vol. 12, Iss. s4 https://resources.today/issue-s4-2025.html

URL статьи: https://resources.today/PDF/22FAOR425.pdf

DOI: 10.15862/22FAOR425 (https://doi.org/10.15862/22FAOR425)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Бестаев, Г. Б. Сценарное моделирование экономических рисков при внедрении открытых API в российский контур кибербезопасности / Г. Б. Бестаев // Отходы и ресурсы. — 2025. — Т. 12. — № s4. — URL: https://resources.today/PDF/22FAOR425.pdf. DOI: 10.15862/22FAOR425.

For citation:
Bestaev G.B. Scenario modeling of economic risks during the implementation of open APIs in the Russian cybersecurity framework. *Russian Journal of Resources, Conservation and Recycling*. 2025; 12(s4): 22FAOR425. Available at: https://resources.today/PDF/22FAOR425.pdf. DOI: 10.15862/22FAOR425. (In Russ., abstract in Eng.).

УДК 338.24:004.056

Бестаев Георгий Бадриевич
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: 224944@edu.fa.ru

Сценарное моделирование экономических рисков при внедрении открытых API в российский контур кибербезопасности

Аннотация. Ускоренная цифровизация финансового сектора и расширение межинституциональных цифровых взаимодействий формируют потребность в исследовании устойчивости национальной финансовой инфраструктуры к новым категориям технологических угроз. В условиях перехода российского финансового рынка к модели открытого банкинга, предполагающей обязательное использование стандартизированных программных интерфейсов (API) крупнейшими участниками отрасли, возникает объективная необходимость оценки системных рисков, сопряжённых с расширением периметра информационного обмена между банками, финтех-компаниями и сторонними поставщиками услуг. Настоящее исследование направлено на разработку сценарного подхода к моделированию системных рисков, возникающих в процессе интеграции открытых API в российский контур кибербезопасности, с учётом отраслевых особенностей финансового сектора и современного ландшафта киберугроз. В работе автором систематизированы ключевые категории уязвимостей, характерных для API-архитектуры финансовых организаций, проанализированы регуляторные механизмы управления рисками, предложена авторская матрица сценарного моделирования, позволяющая дифференцировать уровни системных угроз в зависимости от масштаба внедрения открытых интерфейсов. Результаты исследования свидетельствуют о том, что наибольшую угрозу для финансовой устойчивости представляют каскадные сценарии, при которых компрометация одного API-шлюза распространяется по цепочке связанных участников экосистемы, а существующие механизмы пруденциального надзора требуют дополнения инструментами риск-ориентированного мониторинга технологических цепочек. Практическая значимость работы состоит в формировании рекомендаций для регулятора и участников финансового рынка по выстраиванию многоуровневой системы управления рисками открытого банкинга.

Ключевые слова: открытый банкинг; открытые API (англ. Open API); системные риски; кибербезопасность; финансовая инфраструктура; сценарное моделирование; Банк России; финтех; пруденциальный надзор; цифровая трансформация

Введение

Актуальность настоящего исследования определяется тем, что несмотря на перенос сроков обязательного внедрения открытых API для финансового рынка на период после 2026 года, Банк России утвердил и опубликовал десять стандартов Открытых API в декабре 2025 года, а 20 банков и финтех-компаний уже тестируют единые стандарты на платформе Ассоциации ФинТех.[1] Необходимо подчеркнуть, что данный процесс протекает в условиях усиления киберугроз и ужесточения требований к безопасности критической информационной инфраструктуры, закреплённых Федеральным законом от 7 апреля 2025 г. № 58-ФЗ.[2] Следует отметить, что по данным Grand View Research глобальный рынок технологий открытого банкинга оценивался в 31,61 млрд долларов в 2024 году и прогнозируется на уровне 135,17 млрд долларов к 2030 году при среднегодовом темпе роста 27,6 %[3], что свидетельствует о глобальном характере процесса и его неизбежности для национальных финансовых систем.

Вместе с тем расширение межинституционального информационного обмена посредством API неизбежно сопровождается увеличением поверхности кибератак и формированием новых каналов распространения системных рисков. Особого внимания заслуживает тот факт, что в 2024 году 67 % кибератак в финансовой отрасли пришлись на API-шлюзы необанков.[4] Показательно, что финансовая отрасль продолжает оставаться в пятёрке наиболее атакуемых секторов экономики, на которую приходилось 7 % всех успешных кибератак в России за период 2024 года и первого квартала 2025 года.[5] Вместе с тем адаптация сценарного инструментария моделирования к специфике российского контура кибербезопасности остаётся недостаточно исследованной.

Объектом исследования выступает финансовая инфраструктура Российской Федерации в условиях перехода к модели открытого банкинга.

Предметом исследования являются системные риски кибербезопасности, возникающие при внедрении открытых API, и механизмы их сценарного моделирования.

Целью исследования является разработка сценарного подхода к оценке системных рисков, сопряжённых с интеграцией открытых API в российский контур кибербезопасности финансовой системы.

Для достижения поставленной цели решаются следующие задачи.

1. Систематизировать категории уязвимостей и факторы системного риска API-инфраструктуры финансового сектора.

---

[1] РБК Компании. Что происходит с Открытыми API Банка России сейчас. — [Электронный ресурс] Режим доступа: URL: https://companies.rbc.ru/news/RxpB7vyqU0/chto-proishodit-s-otkryityimi-api-banka-rossii-sejchas/ (дата обращения 23.04.2026).

[2] Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»». — [Электронный ресурс] Режим доступа: URL: https://www.garant.ru/products/ipo/prime/doc/411724730/ (дата обращения 23.04.2026).

[3] Grand View Research. Open Banking Market Size & Share, Industry Report 2030. — [Электронный ресурс] Режим доступа: URL: https://www.grandviewresearch.com/industry-analysis/open-banking-systems-market (дата обращения 23.04.2026).

[4] ComNews. Открытые API станут привычным явлением для российских банков. — [Электронный ресурс] Режим доступа: URL: https://www.comnews.ru/content/238853/2025-04-17/2025-w16/1008/otkrytye-api-stanut-privychnym-yavleniem-dlya-rossiyskikh-bankov (дата обращения 23.04.2026).

[5] Positive Technologies. Киберугрозы финансовой отрасли. Прогноз на 2025–2026 г. — [Электронный ресурс] Режим доступа: URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения 23.04.2026).

2. Проанализировать регуляторные механизмы управления рисками открытого банкинга в российском и международном контексте.
3. Разработать матрицу сценарного моделирования системных рисков при различных масштабах внедрения открытых API.

Научная новизна исследования состоит в формировании авторской классификации сценариев системных рисков открытого банкинга с учётом российской специфики регулирования и ландшафта киберугроз, а также в разработке матрицы оценки каскадных эффектов компрометации API-шлюзов.

Практическая значимость определяется возможностью использования предложенного инструментария регулятором и участниками финансового рынка для превентивного управления рисками в процессе масштабирования открытых API.

1. Материалы и методы

Методологическую основу исследования составляют системный и институциональный подходы, позволяющие рассматривать финансовую инфраструктуру как целостную экосистему, устойчивость которой зависит от надёжности каждого элемента информационного обмена. Сравнительный метод применён для сопоставления регуляторных подходов к управлению рисками открытого банкинга в Российской Федерации, Европейском Союзе и Великобритании. Метод сценарного моделирования использован для формирования дифференцированных прогнозов развития системных угроз в зависимости от масштаба и скорости интеграции открытых API.

Информационную базу составили нормативные документы Банка России, стандарты Ассоциации ФинТех, аналитические отчёты Positive Technologies, «Лаборатории Касперского», ФинЦЕРТ, TAdviser, а также научные публикации, представленные в базах eLibrary и CyberLeninka. Дополнительно использовались методы контент-анализа и синтеза, позволяющие обобщить результаты и сформулировать рекомендации.

2. Результаты и обсуждение

Теоретический фундамент настоящего исследования опирается на концептуальные положения о системном характере рисков в финансовой инфраструктуре, сформулированные в трудах А.М. Карминского и М.И. Столбова, обосновавших подходы к оценке взаимосвязи финансовой устойчивости и системного риска кредитных организаций на основе канонического корреляционного анализа [1]. Равным образом существенным является вклад С.А. Петренко и С.В. Симонова в разработку методологии анализа и оценки рисков информационной безопасности банковских систем, заложивших основы экономически обоснованного подхода к управлению информационными рисками [2]. Немаловажное значение имеют результаты зарубежных исследований. В частности, работа, опубликованная в журнале Entropy, предложила интегрированную модель управления рисками открытого банкинга на основе системной динамики, агентного моделирования и симуляции Монте-Карло, демонстрирующую снижение операционных хвостовых потерь на 20–30 % при ужесточении контроля API [3]. Формализованный анализ безопасности протоколов API операций и транзакций (англ. Account and Transaction API), выполненный с применением верификатора ProVerif, выявил ряд потенциальных уязвимостей в стандартных спецификациях открытого банкинга [4]. Наряду с этим исследование Д.А. Дроздова систематизировало влияние технологии открытых API на трансформацию рынка финансовых услуг в российских условиях [5].

Стоит обратить внимание на то, что категории уязвимостей API-инфраструктуры финансовых организаций существенно отличаются от традиционных рисков информационной безопасности банковского сектора. Анализ, проведённый исследователями Trend Micro, показал, что финтех-компании, получающие доступ к банковским данным через API, как правило имеют ограниченный штат специалистов по безопасности, активно используют облачную инфраструктуру и сторонние SDK, что формирует принципиально иной профиль уязвимости. [6] Принципиально важным представляется понимание того, что в условиях открытого банкинга угроза может реализоваться не через прямое проникновение в банковскую инфраструктуру, а через компрометацию стороннего участника экосистемы, обладающего легитимным API-доступом. Исследование киберрисков как нового класса операционных рисков банков подтверждает принадлежность таких угроз к «тяжелохвостым» распределениям, характеризующимся высокой корреляцией событий и потенциалом каскадных нарушений [6].

Систематизация ключевых категорий уязвимостей API-инфраструктуры финансового сектора представлена в таблице 1.

Таблица 1

Категории уязвимостей API-инфраструктуры финансового сектора и их характеристика

Категория уязвимости	Механизм реализации	Потенциальный масштаб ущерба	Частота фиксации (по данным 2024–2025 гг.)
Компрометация учётных данных API-ключей	Перехват, фишинг, утечка через репозитории кода	Доступ ко всем операциям, авторизованным через скомпрометированный ключ	54 % инцидентов связаны с компрометацией учётных данных (ФинЦЕРТ, 2025)
DDoS-атаки на API-эндпоинты	Генерация аномально высокого числа запросов к конкретным точкам API	Отказ в обслуживании, каскадные сбои в связанных системах	Удвоение DDoS-атак на API в IV квартале 2024 г., 70 % на ритейл и банки
Эксплуатация уязвимостей авторизации (BOLA/BFLA)	Обход механизмов контроля доступа через манипуляции с параметрами запросов	Несанкционированный доступ к данным клиентов, инициирование платежей	Входит в OWASP API Security Top-10 как ведущая уязвимость
Атаки через цепочку поставщиков (англ. Supply Chain)	Внедрение вредоносного кода в обновления ПО подрядчиков	Одновременная компрометация множества организаций	До 50 % успешных компрометаций (Singleton Security, 2025)

Составлено автором на основе анализа материалов[7]

Данные таблицы 1 свидетельствуют о многовекторном характере угроз, направленных на API-инфраструктуру, и подтверждают тезис о том, что расширение открытого банкинга объективно увеличивает поверхность атаки. Уместно заметить, что по данным «Лаборатории Касперского» количество кибератак на финансовый сектор России в первом полугодии 2025 года увеличилось на 13 % по сравнению с аналогичным периодом 2024 года, при этом число атак с применением вредоносного ПО для кражи средств через онлайн-доступ к

[6] Trend Micro. Ready or Not for PSD2: The Risks of Open Banking. — 2019. —[Электронный ресурс] Режим доступа: URL: https://habr.com/ru/companies/trendmicro/articles/472078/ (дата обращения 23.04.2026).

[7] Positive Technologies. Киберугрозы финансовой отрасли. Прогноз на 2025–2026 г. — [Электронный ресурс] Режим доступа: URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения 23.04.2026).

ФинЦЕРТ. Отчёт центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере за 2025 год. — [Электронный ресурс] Режим доступа: URL: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения 23.04.2026).

Банковское обозрение. API и подрядчики станут главными угрозами для банков в 2026 году. — [Электронный ресурс] Режим доступа: URL: https://ib-bank.ru/bisjournal/post/2600 (дата обращения 23.04.2026).

банковским счётам возросло в 2,4 раза.[8] В 2025 году мошенники похитили у банков 29,3 млрд рублей, причём вернуть удалось лишь 1,7 млрд (5,9 %), тогда как банки сумели предотвратить хищения на общую сумму 13,9 трлн рублей.[9]

В развитие данного положения необходимо проанализировать регуляторный контекст, в котором происходит внедрение открытого банкинга в Российской Федерации. Следует отметить, что Банк России избрал гибридную модель внедрения открытых API, сочетающую элементы регуляторного давления и рыночной инициативы. Первоначально обязательное использование открытых API планировалось с 2026 года для крупнейших банков, брокеров и страховых компаний, однако в октябре 2025 года сроки были перенесены до принятия соответствующего федерального закона.[10] Наряду с этим в декабре 2025 года были утверждены десять стандартов, разработанных Ассоциацией ФинТех совместно с участниками рынка и учитывающих результаты пилотных сервисов с реальными клиентами.[11] Исследование вопросов гармонизации стандартов открытого банкинга в контексте директивы PSD2 и рамочных стандартов кибербезопасности, проведённое в Европейском Союзе [7], подтверждает значимость формирования единых профилей безопасности API для снижения системных рисков, что представляется в равной мере применимым к российской практике.

Таблица 2

Сравнительный анализ регуляторных подходов к управлению рисками открытого банкинга

Параметр сравнения	Российская Федерация	Европейский Союз (PSD2/PSD3)	Великобритания
Тип регулирования	Гибридный (регуляторная инициатива с участием рынка)	Директивный (обязательная имплементация PSD2)	Директивный (регулятор CMA, OBIE)
Статус внедрения на 2026 г.	Пилотное тестирование, 20 организаций, обязательное внедрение отложено	Полная имплементация PSD2, разработка PSD3	15 млн пользователей Open Banking
Стандарты безопасности API	ФАПИ.СЕК, отечественная криптография, 10 стандартов АФТ	OpenID FAPI, eIDAS, SCA	UK OBIE Security Profile, FAPI
Оператор инфраструктуры	Не определён, обсуждается	Национальные компетентные органы	Open Banking Implementation Entity
Механизм аккредитации участников	В разработке (Платформа коммерческих согласий на «Госуслугах»)	Реестр NCA, паспортный режим	FCA Register

Составлено автором на основе анализа материалов[12]

[8] InvestFuture. Кибератаки на финансы России выросли на 13 %. — [Электронный ресурс] Режим доступа: URL: https://investfuture.ru/articles/kiberataki-na-finansy-rossii-vyrosli-na-13-analiz-i-statistika-2025-goda-1168188500 (дата обращения 23.04.2026).

[9] AltaPress. Мошенники украли у банков 29,3 млрд рублей в 2025 году. — [Электронный ресурс] Режим доступа: URL: https://altapress.ru/story/ne-tolko-radi-deneg-moshenniki-stali-atakovat-finansoviy-sektor-chtobi-prosto-navredit-381378 (дата обращения 23.04.2026).

[10] Банковское обозрение. Банк России перенёс сроки обязательного внедрения Open API. — [Электронный ресурс] Режим доступа: URL: https://bosfera.ru/press-release/bank-rossii-perenes-sroki-obyazatelnogo-vnedreniya-open-api (дата обращения 23.04.2026).

[11] Ведомости. ЦБ обновил комплекс стандартов открытых API. 24.12.2025. — [Электронный ресурс] Режим доступа: URL: https://www.vedomosti.ru/finance/news/2025/12/24/1165941-tsb-obnovil-kompleks (дата обращения 23.04.2026).

[12] РБК Компании. Россия и глобальные стандарты Open Banking. — [Электронный ресурс] Режим доступа: URL: https://companies.rbc.ru/news/GvzEApsahM/rossiya-i-globalnyie-standartyi-open-banking-idem-svoim-putem/ (дата обращения 23.04.2026).

Ассоциация ФинТех. Стандарты безопасности Открытых API, разработанные АФТ и ИнфоТеКС, опубликованы Банком России. — [Электронный ресурс] Режим доступа: URL: https://www.fintechru.org/press-center/news/standarty-bezopasnosti-otkrytykh-api-razrabotannye-aft-i-infoteks-opublikovany-bankom-rossii/ (дата обращения 23.04.2026).

Существенное значение приобретает сопоставление российского подхода с международным опытом регулирования рисков открытого банкинга. Сравнительный анализ регуляторных моделей представлен в таблице 2.

Анализ представленной в таблице 2 информации демонстрирует, что российская модель существенно отличается от зарубежных аналогов по ряду параметров. В дополнение к изложенному следует подчеркнуть, что отсутствие централизованного оператора инфраструктуры и незавершённость законодательной базы создают дополнительные риски неоднородности стандартов безопасности между участниками экосистемы. В свою очередь, стандарты безопасности API, разработанные АФТ и компанией «ИнфоТеКС», базируются на отечественной криптографии и предполагают встраивание информационной безопасности непосредственно в архитектуру решений.[13] Как отмечает К.В. Макаркина, открытые API становятся каналом, позволяющим взаимодействовать между различными элементами финансовой экосистемы, однако одновременно порождают необходимость совершенствования методов борьбы с угрозами на государственном уровне [8].

Помимо указанного, принципиально значимым для понимания системных рисков является анализ каскадных эффектов компрометации API-инфраструктуры. Особого внимания заслуживает тот факт, что согласно отчёту Банка России о кибератаках в финансовой сфере за 2024 год компрометация подрядных организаций стала самым частым способом получения первоначального доступа к финансовым организациям страны.[14] Данное обстоятельство приобретает критическое значение в контексте открытого банкинга, где число «доверенных» третьих сторон с легитимным API-доступом многократно возрастает. По оценке аналитиков Singleton Security на инциденты в цепочках поставок уже приходится до 50 % успешных компрометаций со средним ущербом в 6,2 млн долларов.[15] Как показывают исследования в области экспертного формального анализа безопасности API финансового уровня (англ. Financial-grade API), даже верифицированные спецификации могут содержать уязвимости, обусловленные нарушением целостности потока авторизации между компонентами экосистемы [9].

На основе проведённого анализа автором разработана матрица сценарного моделирования системных рисков при внедрении открытых API, учитывающая три уровня масштабирования и три категории угроз. Матрица представлена в таблице 3.

Результаты, отражённые в таблице 3, позволяют сделать вывод о нелинейном характере нарастания системных рисков по мере масштабирования открытого банкинга. Примечательно, что при переходе от пилотного к универсальному масштабу критичность сценариев возрастает не пропорционально числу участников, а экспоненциально за счёт эффекта сетевой связанности. Следует отметить, что именно сценарий В (атака через цепочку поставщиков ПО) представляет наибольшую угрозу с точки зрения системной устойчивости, поскольку в условиях универсального внедрения открытых API единый вредоносный компонент способен одновременно поразить десятки и сотни организаций. Как подчёркивают С.В. Афанасьева, Е.С. Черепанова и Н.В. Шехова, инновационные методы предотвращения киберугроз должны

[13] ComNews. Центробанк опубликовал обновлённые стандарты безопасности открытых API. — [Электронный ресурс] Режим доступа: URL: https://www.comnews.ru/content/236863/2024-12-16/2024-w51/1008/centrobank-opublikoval-obnovlennye-standarty-bezopasnosti-otkrytykh-api (дата обращения 23.04.2026).

[14] Positive Technologies. Киберугрозы финансовой отрасли. Прогноз на 2025–2026 г. — [Электронный ресурс] Режим доступа: URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения 23.04.2026).

[15] Банковское обозрение. API и подрядчики станут главными угрозами для банков в 2026 году. — [Электронный ресурс] Режим доступа: URL: https://ib-bank.ru/bisjournal/post/2600 (дата обращения 23.04.2026).

рассматриваться в неразрывной связи с задачами обеспечения экономической безопасности организации [10].

Таблица 3

Матрица сценарного моделирования системных рисков открытого банкинга

Сценарий / Масштаб	Пилотный (до 20 участников)	Масштабный (крупнейшие банки, брокеры, страховщики)	Универсальный (включая МФО, депозитарии, финплатформы)
Сценарий А. Компрометация единичного API-шлюза	Низкий системный риск. Локальная утечка данных клиентов одного участника. Ущерб ограничен	Средний системный риск. Возможна компрометация данных клиентов нескольких связанных организаций	Высокий системный риск. Каскадный эффект на широкий круг участников через единый API-хаб
Сценарий Б. Массированная DDoS-атака на API-инфраструктуру	Низкий. Затронуты отдельные пилотные сервисы	Высокий. Нарушение функционирования платёжной инфраструктуры крупнейших игроков	Критический. Угроза для национальной платёжной системы, сопоставимая с атакой на КИИ
Сценарий В. Внедрение вредоносного кода через обновление ПО подрядчика	Средний. Компрометация нескольких участников пилота	Критический. Одновременное поражение множества организаций с потерей доверия	Катастрофический. Системный кризис финансовой инфраструктуры, требующий вмешательства регулятора

Составлено автором на основе анализа материалов[16]

Наряду с этим необходимо подчеркнуть роль регуляторного фактора в управлении выявленными рисками. Вступление в силу Федерального закона от 07.04.2025 № 58-ФЗ с 1 сентября 2025 года, направленного на усиление технологической независимости КИИ и обязывающего субъектов КИИ использовать отечественное программное обеспечение, создаёт дополнительный контур защиты для API-инфраструктуры финансового сектора.[17] Вместе с тем объём российского рынка информационной безопасности достиг 299 млрд рублей в 2024 году, увеличившись на 23 % по сравнению с 2023 годом, а по прогнозам TAdviser в 2025 году он превысит 400 млрд рублей [18], что свидетельствует об активном наращивании отраслевых инвестиций в защиту. По данным издания CIPR Россия вошла в первую десятку стран мира по расходам на кибербезопасность.[19]

Существенным элементом анализа является оценка готовности финансового сектора к управлению рисками открытого банкинга. Согласно данным компании F6 средняя оценка уровня кибербезопасности российских компаний составила 5,2 балла из 10, при этом финансовый сектор получил наивысший средний балл в 5,8, что, как отмечают эксперты, является показателем скорее умеренной зрелости, чем высокой защищённости.[20] В свою

[16] Positive Technologies. CODE RED 2026. Актуальные киберугрозы для российских организаций. — [Электронный ресурс] Режим доступа: URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (дата обращения 23.04.2026).

TAdviser. Российский рынок ИБ 2025. Обзор. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Российский_рынок_ИБ_2025._Обзор_TAdviser (дата обращения 23.04.2026).

[17] Б1. Изменения в сфере регулирования безопасности критической информационной инфраструктуры (КИИ). — [Электронный ресурс] Режим доступа: URL: https://b1.ru/insights/law-messenger/security-of-critical-information-activities-20-october-2025/ (дата обращения 23.04.2026).

[18] TAdviser. Российский рынок ИБ 2025. Обзор. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Российский_рынок_ИБ_2025._Обзор_TAdviser (дата обращения 23.04.2026).

[19] CIPR. Россия вошла в топ-10 по расходам на кибербезопасность. — [Электронный ресурс] Режим доступа: URL: https://cipr.ru/izdanie-2025/rossiya-voshla-v-top-10-po-rashodam-na-kiberbezopasnost/ (дата обращения 23.04.2026).

[20] ComNews. Финансовый сектор в России оказался самым защищённым от кибермошенников. — [Электронный ресурс] Режим доступа: URL: https://www.comnews.ru/content/239372/2025-05-26/2025-w22/1008/finansovyy-sektor-rossii-okazalsya-samym-zaschischennym-kibermoshennikov (дата обращения 23.04.2026).

очередь, по данным ГК «Солар» в среднем на одну компанию из финансово-страховой отрасли в 2025 году пришлось 6 048 кибератак, при этом 30 % инцидентов были связаны с нарушением сотрудниками политик информационной безопасности.[21] Как справедливо отмечает М. К. Водопьянова, правовые коллизии защиты критической инфраструктуры в условиях нарастания киберугроз требуют пересмотра конституционных гарантий приватности с учётом новых технологических реалий [11].

В развитие данного анализа автором предложена таблица рекомендуемых мер по управлению системными рисками открытого банкинга, дифференцированных по уровням защиты (табл. 4).

Таблица 4

Рекомендуемые меры по управлению системными рисками открытого банкинга (по уровням защиты)

Уровень защиты	Рекомендуемые меры	Ответственный субъект	Ожидаемый эффект
Регуляторный	Принятие федерального закона об открытом банкинге, определение оператора инфраструктуры, обязательная аккредитация третьих сторон	Банк России, Минцифры, Государственная Дума	Унификация правил, снижение регуляторного арбитража
Инфраструктурный	Внедрение единого стандарта ФАПИ.СЕК с отечественной криптографией, создание централизованного API-хаба с мониторингом	АФТ, финансовые организации	Стандартизация безопасности, снижение поверхности атаки
Операционный	Внедрение ограничений частоты API-запросов (англ. rate limiting), поведенческая аналитика API-трафика, регулярное тестирование на проникновение	Каждый участник экосистемы	Выявление аномалий на ранней стадии, снижение времени реагирования
Процессный	Управление рисками третьих сторон (англ. Third-Party Risk Management), аудит безопасности SDK, практики безопасной разработки (англ. DevSecOps)	Финансовые организации, финтех-компании	Снижение риска атак через цепочку поставщиков

Составлено автором на основе анализа материалов[22]

Данные таблицы 4 свидетельствуют о необходимости многоуровневого подхода к управлению рисками, в котором регуляторные, инфраструктурные, операционные и процессные меры дополняют друг друга, формируя целостный контур защиты. Вместе с тем реализация подобного подхода требует значительных инвестиций и координации усилий всех участников экосистемы.

Принципиально важным представляется вопрос о перспективах развития системы управления рисками открытого банкинга в среднесрочной перспективе. По прогнозам вице-президента Сбербанка по кибербезопасности С. Лебедя до 75 % кибератак в 2025 году будут базироваться на разработках с искусственным интеллектом[23], что ставит перед участниками экосистемы открытого банкинга задачу интеграции ИИ-компонентов как в системы защиты, так и в механизмы мониторинга API-трафика. Более 1 700 организаций являются участниками информационного обмена с ФинЦЕРТ, включая все российские банки[24], что формирует

[21] TAdviser. Информационная безопасность в банках. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/ (дата обращения 23.04.2026).

[22] Ассоциация ФинТех. Банк России опубликовал стандарты Открытых API. — [Электронный ресурс] Режим доступа: URL: https://www.fintechru.org/press-center/news/bank-rossii-opublikoval-standarty-otkrytykh-api-razrabotannye-na-ploshchadke-assotsiatsii-fintekh/ (дата обращения 23.04.2026).

[23] TAdviser. Информационная безопасность в банках. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_банках (дата обращения 23.04.2026).

[24] Банк России. Информационная безопасность. — [Электронный ресурс] Режим доступа: URL: https://www.cbr.ru/information_security/ (дата обращения 23.04.2026).

институциональную основу для построения централизованной системы раннего предупреждения об угрозах в API-среде. Как подчёркивают Н.Э. Соколинская и О.М. Маркова, рынок финтех-услуг развивается с темпами, опережающими готовность регуляторных механизмов, что формирует дополнительные риски для устойчивости банковского сектора [12].

Выводы

Анализ категорий уязвимостей и факторов системного риска API-инфраструктуры финансового сектора показал, что расширение открытого банкинга качественно трансформирует ландшафт киберугроз, перемещая вектор атаки с прямого проникновения в банковский периметр на эксплуатацию межинституциональных API-каналов и компрометацию сторонних участников экосистемы. Установлено, что в 2024 году 67 % кибератак на финансовые организации были направлены на API-шлюзы, а компрометация подрядных организаций стала основным способом получения первоначального доступа к инфраструктуре банков. Особую угрозу представляют атаки через цепочки поставщиков, на которые приходится до 50 % успешных компрометаций.

Сравнительный анализ регуляторных механизмов управления рисками открытого банкинга продемонстрировал, что российская модель находится на начальной стадии формирования и существенно отличается от зарубежных аналогов отсутствием централизованного оператора, незавершённостью законодательной базы и рекомендательным характером стандартов безопасности. Вместе с тем утверждение десяти стандартов Открытых API Банком России в декабре 2025 года и разработка стандартов безопасности на основе отечественной криптографии формируют необходимую нормативную базу для последующего масштабирования.

Разработанная автором матрица сценарного моделирования системных рисков выявила нелинейный характер нарастания угроз по мере расширения экосистемы открытого банкинга. Установлено, что наибольшую опасность представляют каскадные сценарии компрометации через обновления ПО подрядчиков при универсальном масштабе внедрения, когда единый вредоносный компонент способен одновременно поразить десятки организаций. Предложенная система четырёхуровневых мер защиты (регуляторный, инфраструктурный, операционный, процессный уровни) позволяет выстроить целостный контур управления системными рисками, адаптированный к специфике российского финансового рынка и современного ландшафта киберугроз.

ЛИТЕРАТУРА

1. Карминский, А.М. Оценка взаимосвязи финансовой устойчивости и системного риска крупнейших российских банков / А.М. Карминский, М.И. Столбов // Корпоративные финансы. — 2016. — Т. 10, № 1(37). — С. 77–87. — EDN XAAJYD.
2. Петренко, С.А. Управление информационными рисками: Экон. оправд. безопасность: Информ. технологии для инженеров / С.А. Петренко, С.В. Симонов — Москва: Акад. АйТи, 2004. — 383 с. — EDN QQESJB.
3. Ojehomon, O.G. Cyber Risk Management of API-Enabled Financial Crime in Open Banking Services / O.G. Ojehomon, J. Cichorska, J. Michnik // Entropy. — 2026. — Т. 28, № 2. — С. 163.
4. Security analysis of the open banking account and transaction API protocol / P. Modesti, L. Freitas, Q. Shotomiwa, A. Almehrej — DOI 10.1016/j.csa.2025.100097. // Cyber Security and Applications. — 2025. — Т. 3. — С. 100097 — EDN PUWRAI.

5. Дроздов, Д.А. Влияние технологии открытых API на развитие рынка финансовых услуг / Д.А. Дроздов — DOI 10.18101/2304-4446-2024-2-57-65. // Вестник Бурятского государственного университета. Экономика и менеджмент. — 2024. — № 2. — С. 57–65 — EDN EKKPZO.

6. 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. — EDN QSKHXS.

7. Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards / M. Gounari, G. Stergiopoulos, K. Pipyros, D. Gritzalis — DOI 10.1365/s43439-023-00108-8. // International Cybersecurity Law Review. — 2024. — Т. 5, № 1. — С. 79–120 — EDN IWUFTW.

8. Макаркина, К.В. Цифровизация банковского сектора в России / К.В. Макаркина, Ю.С. Попонкина — DOI 10.24411/2658-6932-2022-6-18-25. // Контентус. — 2022. — № 6(119). — С. 18–25 — EDN RYWCCL.

9. Fett D., Hosseyni P., Küsters R. An Extensive Formal Security Analysis of the OpenID Financial-grade API // arXiv preprint arXiv:1901.11520. — 2019. —URL: https://arxiv.org/pdf/1901.11520 (дата обращения 23.04.2026).

10. Афанасьева, С.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации / С.В. Афанасьева, Е.С. Черепанова, Н.В. Шехова — DOI 10.18287/2542-0461-2023-14-2-7-16. // Вестник Самарского университета. Экономика и управление. — 2023. — Т. 14, № 2. — С. 7–16 — EDN WGCCZC.

11. Водопьянова, М.К. Конституционные гарантии приватности и киберугрозы: правовые коллизии защиты критической инфраструктуры / М.К. Водопьянова // Вопросы российской юстиции. — 2025. — № 36. — С. 31–40. — EDN UGTPZK.

12. Соколинская, Н.Э. Рынок финтех услуг: состояние и тенденции развития / Н.Э. Соколинская, О.М. Маркова // Финансовые рынки и банки. — 2023. — № 6. — С. 117–124. — EDN ZZYHAC.

Bestaev Georgy Badrievich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: 224944@edu.fa.ru

Scenario modeling of economic risks during the implementation of open APIs in the Russian cybersecurity framework

Abstract. The accelerated digitalization of the financial sector and the expansion of inter-institutional digital interactions create a need to study the resilience of the national financial infrastructure to new categories of technological threats. As the Russian financial market transitions to an open banking model, which requires the mandatory use of standardized application programming interfaces (APIs) by major industry participants, there is an objective need to assess the systemic risks associated with the expansion of the perimeter of information exchange between banks, fintech companies, and third-party service providers. This study aims to develop a scenario-based approach to modeling systemic risks arising from the integration of open APIs into the Russian cybersecurity framework, taking into account the industry-specific characteristics of the financial sector and the current cyberthreat landscape. In this paper, the author systematizes key categories of vulnerabilities characteristic of the API architecture of financial institutions, analyzes regulatory risk management mechanisms, and proposes a scenario modeling matrix that differentiates systemic threat levels depending on the scale of open interface implementation. The study's results indicate that cascading scenarios, in which the compromise of a single API gateway spreads through a chain of related ecosystem participants, pose the greatest threat to financial stability. Existing prudential oversight mechanisms require supplementing with risk-based monitoring tools for process chains. The practical significance of this study lies in the development of recommendations for regulators and financial market participants on building a multi-tiered risk management system for open banking.

Keywords: open banking; open APIs; systemic risks; cybersecurity; financial infrastructure; scenario modeling; Bank of Russia; fintech; prudential supervision; digital transformation