УДК 336.71

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Телесова Дарья Александровна
студент специалитета
Российская академия народного хозяйства и государственной службы при Президенте РФ
Сибирский институт управления
Новосибирск, Россия

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К УПРАВЛЕНИЮ КИБЕРРИСКАМИ В АРХИТЕКТУРЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО БАНКА

Аннотация

Проводится систематизация и сравнительный анализ пяти ключевых методологических подходов к управлению киберрисками: нормативно-комплаенсного, риск-ориентированного, угрозо-ориентированного, архитектурно-резильентного и поведенческо-предиктивного. Выявлены их концептуальные ограничения и зоны взаимодополняемости. Предложена интегрированная методическая конструкция, объединяющая принципы нулевого доверия, киберразведку, моделирование атак и автоматизированное реагирование в единый цикл управления, встроенный в модель трёх линий защиты. Результаты исследования формируют научно-методическую основу для перехода банков от изолированной ИТ-защиты к системной киберустойчивости, интегрированной в архитектуру экономической безопасности.

Ключевые слова: киберриск, экономическая безопасность, коммерческий банк

Цифровая трансформация банковского сектора, масштабирование экосистемных сервисов и переход к распределённым облачным инфраструктурам кардинально изменили профиль угроз информационной безопасности. Киберриски более не рассматриваются исключительно как техническая задача подразделений ИБ: они напрямую влияют на непрерывность бизнес-процессов, ликвидность, репутацию и, в конечном счёте, на экономическую безопасность кредитной организации [1]. Регуляторные документы Банка России, включая Положения № 716-П и № 814-П, а также международные стандарты (NIST CSF, ISO/IEC 27001) подчёркивают необходимость перехода от пассивной защиты периметра к проактивному управлению киберустойчивостью.

Научная проблема заключается в отсутствии унифицированной методологии, способной гармонично интегрировать разрозненные подходы к кибербезопасности в контур риск-менеджмента первого и второго уровней. На практике банки часто используют комплаенс-чеклисты или изолированные системы мониторинга, которые не обеспечивают сквозной видимости угрозового ландшафта, не валидируют эффективность контролей в условиях реальных атак и не адаптируются к изменяющимся тактикам противников [2].

Цель статьи – систематизировать и сравнительно проанализировать современные методологические подходы к управлению киберрисками в коммерческих банках, выявить их ограничения и предложить интегрированную методическую конструкцию, обеспечивающую переход от реактивного контроля к проактивной киберустойчивости. Научная новизна состоит в синтезе принципов угрозо-ориентированного тестирования, архитектурной резильентности и поведенческой аналитики в единый цикл управления, встроенный в модель трёх линий защиты.

Исторически управление киберрисками в кредитных организациях прошло несколько этапов методологического развития, каждый из которых отражал изменения в угрозовом ландшафте и регуляторных ожиданиях.

Первое поколение (периметровая защита и комплаенс). Фокус на технических средствах (FW, IPS/IDS, антивирусы) и соблюдении отраслевых стандартов. Методология носила контрольно-аудиторский характер: наличие политик, проведённые пентесты, сертификаты соответствия. Ограничение: статичность, ориентация на формальное соответствие, отсутствие привязки к бизнес-процессам [3].

Второе поколение (риск-ориентированный подход). Смещение фокуса на активы, оценку вероятности и воздействия, ведение реестров рисков. Методология опирается на матрицы рисков, сценарный анализ и качественные оценки. Ограничение: высокая субъективность экспертных оценок, сложность учёта каскадных и системных угроз, разрыв между ИТ-рисками и стратегическими целями бизнеса [1].

Третье поколение (угрозо-ориентированное и резильентное). Принцип «assume breach» (предполагать взлом), киберразведка (CTI), красные команды, моделирование реальных тактик противников (MITRE ATT&CK). Ограничение: высокая ресурсоёмкость, требование экспертных компетенций, сложность масштабирования на все подразделения банка [4].

Четвёртое поколение (предиктивное и архитектурное). Архитектура нулевого доверия (Zero Trust), поведенческая аналитика (UEBA), автоматизация реагирования (SOAR), машинное обучение для выявления аномалий. Ограничение: зависимость от качества данных, проблемы интерпретируемости моделей, необходимость кросс-функциональной трансформации процессов [2].

Современная практика показывает, что ни один из подходов в изоляции не обеспечивает достаточного уровня киберустойчивости. Эффективность достигается

через методологическую гибридизацию, адаптированную под зрелость организации и регуляторный контекст.

Для формирования обоснованной архитектуры управления киберрисками целесообразно сопоставить ключевые подходы по методологическим признакам (табл. 1).

Таблица 1 – Ключевые подходы по методологическим признакам

Подход	Методология	Преимущества	Ограничения
Нормативно-комплаенсный	Соответствие стандартам и регуляторным требованиям	Прозрачность для регулятора, структурированность	Реактивность, отставание от угрозовой динамики, формализация без валидации эффективности
Риск-ориентированный	Оценка вероятности и воздействия на активы	Приоритизация ресурсов, бизнес-ориентированность	Субъективность оценок, сложность учёта неизвестных угроз, статичность
Угрозо-ориентированный	Моделирование реальных тактик противников	Валидация контролей в реальных условиях, выявление слепых зон	Высокая стоимость, требование экспертных компетенций
Архитектурно-резильентный	Снижение радиуса поражения и ускорение восстановления	Ограничение lateral movement, адаптивность	Сложность миграции, культурные барьеры, необходимость перестройки IAM
Поведенческо-предиктивный	Выявление аномалий до реализации инцидента	Раннее предупреждение, работа с неизвестными паттернами	Ложные срабатывания, зависимость от чистоты данных

Анализ показывает данных таблицы 1, что подходы не конкурируют, а дополняют друг друга на разных этапах жизненного цикла киберриска: от проектирования и оценки до обнаружения, реагирования и восстановления. Ключевой методологический пробел заключается в отсутствии сквозной связности между этими этапами в рамках единого управленческого контура [3].

На основе сравнительного анализа предлагается многоуровневая методическая конструкция, которая может быть внедрена в архитектуру экономической безопасности коммерческого банка.

Уровень фундамента: Непрерывный комплаенс + Zero Trust. Методология заменяет периодические аудиты на автоматизированную валидацию соответствия. Политики безопасности трансформируются в исполняемые правила. Архитектура

нулевого доверия внедряется как принцип: явная верификация, минимальные привилегии, сегментация по бизнес-контексту. Это создаёт устойчивую основу, не зависящую от периметра [4].

Уровень обнаружения: Кибербразведка + Поведенческая аналитика. Вместо изолированного мониторинга событий предлагается корреляция внешних индикаторов компрометации с внутренними поведенческими паттернами сотрудников, приложений и сессий. Методология опирается на непрерывное обучение моделей на размеченных данных, снижение порога детекции аномалий и приоритизацию инцидентов по бизнес-критичности [2].

Уровень валидации: Угрозо-ориентированное тестирование (TLPT). Регулярное моделирование атак на критичные бизнес-процессы под руководством реальной угрозовой разведки. Методология TLPT позволяет проверить не только технические контролы, но и процессы эскалации, коммуникации и принятия решений в условиях инцидента, выявляя разрывы между первой и второй линиями защиты [5].

Уровень реагирования и восстановления: SOAR + Резильентность. Автоматизация типовых сценариев реагирования с обязательным включением бизнес-контекста: какие сервисы затронуты, каков приоритет восстановления, какие регуляторные обязательства активируются. Параллельно внедряются упражнения на киберустойчивость, моделирующие не только ИТ-восстановление, но и операционную адаптацию бизнес-подразделений в условиях длительного простоя [6].

Интеграция в модель трёх линий защиты. Предложенная конструкция обогащает классическую модель: первая линия отвечает за встроенные контролы и первичное реагирование; вторая линия калибрует риск-аппетит, валидирует эффективность через TLPT, управляет кибербразведкой; третья линия оценивает зрелость процессов валидации и культуру киберустойчивости [1].

Предложенная конструкция методологически универсальна, однако её успешная реализация зависит от ряда факторов. Культурная трансформация остаётся главным барьером: переход от «защиты периметра» к «управлению последствиями» требует изменения менталитета руководства и бизнес-лидеров. Киберриск должен обсуждаться на уровне совета директоров наравне с кредитным и рыночным риском [3].

Качество данных и интерпретируемость ИИ также критичны: поведенческие модели эффективны только при наличии структурированных логов, корректной

разметки инцидентов и понятных механизмов объяснения решений. Без этого возрастает риск «алертовой усталости» и ложных эскалаций [2]. Регуляторная фрагментация требует выстраивания маппинга требований, чтобы избежать дублирования контролей. Наконец, человеческий фактор остаётся уязвимым звеном даже при совершенной архитектуре, что делает необходимым непрерывное обучение и симуляции социальной инженерии, интегрированные в KPI руководителей подразделений [4].

Перспективы развития включают стандартизацию метрик киберустойчивости, разработку этических рамок применения ИИ в кибербезопасности и адаптацию методологии к требованиям регуляторов разных юрисдикций.

Управление киберрисками в коммерческих банках вышло за рамки технической функции и стало стратегическим элементом экономической безопасности. Сравнительный анализ методологических подходов показывает, что ни один из них в изоляции не обеспечивает достаточной проактивности и устойчивости. Предложенная интегрированная конструкция объединяет принципы непрерывного комплаенса, архитектуры нулевого доверия, киберразведки, поведенческой аналитики и угрозо-ориентированного тестирования в единый управленческий цикл, встроенный в модель трёх линий защиты.

Методологическая ценность подхода заключается в переходе от статичной оценки соответствия к динамической валидации эффективности контролей, от реактивного мониторинга к предиктивной корреляции угроз, от ИТ-восстановления к бизнес-резильентности. Практическая реализация требует поэтапной трансформации процессов, инвестиций в компетенции и изменения культуры управления рисками на уровне высшего руководства. Дальнейшие исследования могут быть направлены на стандартизацию метрик киберустойчивости и разработку этических рамок применения ИИ в системах предиктивной аналитики угроз.

Список использованных источников

1. Малыхина С. И. Система управления рисками в банковском холдинге: современные вызовы // Экономика и банки. – 2024. – № 2. – EDN: FSYQHZ

2. NIST Cybersecurity Framework (CSF) 2.0. – National Institute of Standards and Technology, 2024.

3. Веретин М. С. Повышение экономической безопасности коммерческих банков на основе внутреннего контроля операционного риска // Вестник РУДН. Серия: Экономика. – 2023. – № 1. – DOI: 10.22363/2313-2329-2023-31-1-107-119. – EDN: REWLKX

4. Кирилюк И. Л. Модельные риски в финансовой сфере в условиях использования ИИ и машинного обучения // Russian Journal of Economics and Law. – 2022. – № 1. – DOI: 10.21202/2782-2923.2022.1.40-50. – EDN: XEFPBE

5. MITRE ATT&CK Framework for Financial Services. – MITRE Corporation, 2025.

6. ENISA Threat Landscape for the Financial Sector 2025. – European Union Agency for Cybersecurity, 2025.

7. Шаик К. А., Сриниваса Рао С. Г. Predictive Modeling for HR Decision-Making: A Study // Journal of Marketing & Social Research. – 2025. – Vol. 02.