ОТРАСЛЕВЫЕ ОСОБЕННОСТИ КИБЕРЗАЩИТЫ ДЛЯ ФИНАНСОВОЙ СФЕРЫ

Ю.А. Косинов[1], *представитель работодателя, участвующего в учебном процессе*
А.Ю. Шарова[2], *доцент*
[1]ООО «АйСиЭл Системные Технологии»
[2]Ивановский государственный политехнический университет
[1](Россия, г. Казань)
[2](Россия, г. Иваново)

DOI:10.24412/2500-1000-2025-10-2-70-74

Аннотация. *В статье анализируются ключевые аспекты кибербезопасности в финансовом секторе России, учитывая специфику отрасли, где высокие риски финансовых потерь от кибератак требуют специализированных подходов. Обсуждаются проблемы тонкой настройки отечественного сетевого и серверного оборудования, методы защиты приложений от DDoS-атак и веб-угроз (Anti-DDOS, WAF, WAAP), антифрод-системы, оценка производительности российских NGFW, качество обнаружения атак в IPS, вызовы интеграции NGFW в SIEM и SOC, меры по защите внутренних разработчиков, подходы к управлению разнородными поставщиками оборудования (NSPM).*

Ключевые слова: *кибербезопасность, финансовая сфера, антифрод-системы, отечественное оборудование, интеграция, защита разработчиков.*

Финансовый сектор России остается одной из наиболее уязвимых отраслей для кибератак, где ущерб от инцидентов может достигать миллиардов рублей. Согласно отчетам Банка России, в 2024 году компрометация подрядных организаций стала ведущим вектором атак, а общий объем предотвращенных мошеннических операций вырос вдвое по сравнению с предыдущим годом. Средний уровень кибербезопасности в финансовых организациях оценивается как высокий (5,2 балла из 10), но специфические отраслевые риски, такие как обработка конфиденциальных данных и высокая зависимость от цифровых сервисов, требуют адаптированных мер защиты. В контексте импортозамещения акцент смещается на отечественные решения.

Исходная задача – разработка и внедрение специализированных мер киберзащиты, учитывающих высокую зависимость от сетевых и серверных систем, необходимость соблюдения строгих регуляторных требований (например, стандартов Банка России и PCI DSS), переход на отечественное оборудование в рамках импортозамещения.

Исходная идея состоит в создании комплексной экосистемы киберзащиты, ориентированной на финансовый сектор, с акцентом на интеграцию отечественных технологий и автоматизацию процессов.

Идея предполагает сотрудничество между регуляторами, банками и IT-компаниями для создания пилотных проектов, что позволит масштабировать решения и повысить общий уровень киберустойчивости финансовой сферы России.

Результаты исследования

В последние годы наблюдается устойчивая эволюция киберугроз, направленных на финансовый сектор. По данным исследований [2-3], в 2024 году доля атак, связанных с социальной инженерией, достигла 64% всех инцидентов, а объем предотвращенных мошеннических операций составил более 20 млрд рублей. Возросла активность злоумышленников, использующих методы компрометации подрядчиков и поставщиков (так называемые supply chain атаки), инструменты искусственного интеллекта для обхода традиционных систем защиты.

Тенденцией стало смещение фокуса атак на мобильные приложения и платежные сервисы, включая систему быстрых платежей (СБП). Более 70 % атак в банковской сфере в 2025 году приходятся на попытки получения доступа к мобильным клиентам, использующим однофакторную аутентификацию. Вектор атак также расширился за счет кибершантажа и использования вредоносных приложений-двойников. Для минимизации подобных

угроз финансовым организациям требуется комплексная защита, охватывающая не только серверную инфраструктуру, но и клиентские устройства.

Помимо прямых атак, усилилось использование искусственного интеллекта злоумышленниками – для создания реалистичных фишинговых писем, имитации голоса сотрудников банков и построения таргетированных сценариев социальной инженерии. Для системного понимания угроз представлена сравнительная таблица 1, демонстрирующая связь между типами атак, последствиями и соответствующими защитными мерами.

Таблица 1. Сравнительная характеристика угроз и методов защиты в финансовой сфере

Тип угрозы	Пример реализации	Последствия	Основные методы защиты
DDoS-атаки	Перегрузка каналов интернет-банка и мобильных API	Недоступность сервисов, потеря клиентов и доходов	Anti-DDoS, балансировка нагрузки, фильтрация L7
Фишинг и соц. инженерия	Поддельные сайты и звонки от «службы безопасности банка»	Кража учетных данных и денежных средств клиентов	DMARC, SPF, обучение персонала, фильтрация трафика
Мошенничество с переводами	Подмена получателя, перехват SMS-кодов	Прямые финансовые потери, компрометация данных	Антифрод-системы, двухфакторная аутентификация
Внутренние утечки	Инсайдеры, копирование исходного кода и баз клиентов	Компрометация критически важных данных	DLP, PAM, аудит действий, разграничение прав
Supply chain атаки	Внедрение вредоносного ПО через подрядчиков	Нарушение целостности и работы инфраструктуры	Сертификация поставщиков, NSPM, постоянный мониторинг

Активное влияние на уровень киберзащиты финансовых организаций оказывают регуляторы – Банк России, ФСТЭК и Роскомнадзор. Банк России выполняет функции методологического и контрольного центра, формируя требования к информационной безопасности участников финансового рынка. Регулирующим документом является стандарт ГОСТ Р 57580, который устанавливает требования к защите персональных и финансовых данных. Также действует Указ Президента РФ № 250 от 2021 года, направленный на повышение устойчивости критической информационной инфраструктуры, включая банковский сектор.

Регулярные проверки со стороны Банка России выявляют типичные проблемы – слабую интеграцию SOC и SIEM, недостаточную сегментацию сетей и несвоевременное обновление отечественных решений. Вместе с тем активно внедряется подход «песочниц» для тестирования решений без риска для производственных систем.

В среднесрочной перспективе (до 2030 г.) можно выделить несколько направлений эволюции кибербезопасности в финансовой отрасли.

Во-первых, возрастает роль искусственного интеллекта в обнаружении аномалий и автоматизации расследований инцидентов. Уже сегодня системы класса AI-SOC позволяют выявлять инциденты по контекстным признакам, прогнозировать угрозы и уменьшать время реакции с часов до минут.

Во-вторых, активное развитие получит архитектура Zero Trust, предполагающая отказ от традиционной модели периметра и проверку каждого запроса независимо от источника. Для финансовых организаций внедрение Zero Trust означает снижение числа инцидентов, связанных с компрометацией внутренних учетных записей.

Третьим направлением станет развитие квантовых и постквантовых криптографических алгоритмов для защиты каналов межбанковского обмена. На базе лабораторий при ведущих вузах уже ведутся пилотные испытания отечественных квантовых систем шифрования.

Существенную роль сыграет создание отечественных WAF/WAAP-платформ нового поколения, поддерживающих защиту API и автоматическую корреляцию событий с данными SOC (табл. 2).

Таблица 2. Прогноз развития технологий киберзащиты до 2030 года

Направление	Текущий уровень внедрения	Перспектива до 2030 г.	Ожидаемый эффект
Архитектура Zero Trust	Низкий	Средний – высокий	Снижение числа внутренних инцидентов на 30%
Отечественные SOC-платформы	Средний	Высокий	Повышение скорости реагирования на инциденты
Квантовая криптография	Низкий	Средний	Повышение стойкости каналов связи
AI-анализ инцидентов	Средний	Очень высокий	Автоматизация расследований, прогнозирование атак
NSPM и автоконфигурация сетей	Средний	Высокий	Снижение операционных затрат и человеческого фактора

Проблемы тонкой настройки отечественного оборудования подразумевает минимизацию уязвимостей путем строгой конфигурации, отключения ненужных сервисов и применения патчей. Однако российские компании сталкиваются с дефицитом компонентов и недостаточной функциональностью оборудования, что приводит к рискам бэкдоров и моральному устареванию. Например, неправильная настройка может вызвать сетевые сбои, а отсутствие собственной базы компонентов требует инвестиций в отечественную электронику. В финансовой сфере это усугубляется необходимостью соблюдения стандартов PCI DSS, где проблемы тонкой настройки включает шифрование данных и контроль доступа [1]. Рекомендуется регулярный аудит конфигураций и использование автоматизированных инструментов для выявления слабых мест, таких как слабые пароли или открытые порты.

При организации защиты финансовых приложений от DDoS-атак и веб-угроз необходим многоуровневый подход. Anti-DDOS решения фильтруют вредоносный трафик на уровнях L3-L7, интегрируясь с другими сервисами.

В сфере кибербезопасности для анализа и фильтрации веб-трафика применяются специальные системы, которые эволюционируют в комплексные платформы для защиты как веб-приложений, программных интерфейсов. В России востребованы облачные сервисы, такие как StormWall, которые интегрируют в себе функции отражения масштабных сетевых атак и фильтрации веб-запросов. Параллельно в банковском секторе действуют антифрод-системы, предназначенные для мониторинга и блокирования мошеннических операций в реальном времени путем анализа поведения клиентов, геолокации и данных телеком-операторов. С помощью указанных систем финансовым учреждениям в 2024 году удалось предотвратить рекордные 72 миллиона попыток краж. Основные рекомендуемые подходы включают машинное обучение для выявления аномалий и интеграцию с SIEM для комплексного анализа [2].

Российские NGFW, такие как UserGate и Solar Dozor, достигают скоростей до 100 Гбит/с в режиме L3/L4, но реальная производительность ниже из-за активации IPS. В рамках проведения метрологических исследований производительности межсетевых экранов нового поколения (МЭСП) осуществляются нагрузочные испытания в соответствии с международными стандартами RFC 2544 и RFC 3511. В ходе данных испытаний производится оценка таких ключевых метрик, как пропускная способность (throughput), задержка передачи пакетов (latency) и коэффициент потерь пакетов (packet loss). По результатам независимого тестирования, решение BI.ZONE NGFW продемонстрировало наивысшие показатели пропускной способности в своем рыночном сегменте [2].

Для организаций финансового сектора особую значимость приобретает интеграция технологий искусственного интеллекта (ИИ) с целью оптимизации сетевого трафика и повышения уровня безопасности. Однако актуальной проблемой остается расхождение между заявленными и фактическими эксплуатационными характеристиками средств защиты информации.

Российские IPS, такие как ViPNet IDS и Континент СОВ, используют сигнатуры и поведенческий анализ для обнаружения вторжений с точностью до 94-98% для SQL-инъекций и сканирования портов. Однако ложные срабатывания остаются проблемой, особенно в высоконагруженных сетях. 52% компаний используют IPS для анализа инци-

дентов, интегрируя с SIEM. В финансовой сфере качество зависит от обновления сигнатур и машинного обучения. Сравнение сигнатурных и поведенческих методов показывает преимущество последних в выявлении новых угроз [3].

Интеграция NGFW в SIEM и SOC сталкивается с проблемами качества логов, несоответствия форматов и пиковых нагрузок на EPS/FPS. Российские NGFW часто имеют ограниченную отчетность, требуя кастомных коннекторов. В SOC данные о запрещенных приложениях и активности пользователей должны передаваться без потерь, но отсутствие интеграции с AD/SIEM усложняет процесс [4].

Защита внутренних разработчиков в финансовой сфере фокусируется на предотвращении утечек кода и доступа к чувствительным данным. Рекомендуется внедрение DLP-систем, шифрование и аудит действий. Угрозы включают социальную инженерию и инсайдерские атаки, поэтому обязательны тренинги и контроль привилегий. В банках используются PAM-решения для мониторинга, обеспечивая соответствие PCI DSS.

NSPM-системы автоматизируют управление политиками безопасности в мультивендорных сетях, анализируя конфигурации и выявляя уязвимости. В России решения вроде НОТА КУПОЛ позволяют централизованный контроль, снижая трудозатраты. Проблемы включают приоритизацию уязвимостей и прогнозирование атак, но NSPM обеспечивает оптимизацию.

В результате проведенного анализа можно сформулировать основные рекомендации для усиления киберзащиты финансовой сферы:

1. Разработка унифицированного фреймворка для hardening оборудования, включающего автоматизированные инструменты аудита и базы знаний по отечественным устройствам, чтобы сократить время настройки и снизить человеческий фактор.

2. Внедрение многоуровневой защиты приложений через комбинацию Anti-DDoS, WAF и WAAP, с использованием ИИ для поведенческого анализа трафика, что позволит адаптироваться к новым угрозам без ручного вмешательства.

3. Построение национальной антифрод-платформы на основе машинного обучения, интегрированной с телеком-операторами и банками, для обмена данными о мошенничестве в реальном времени.

4. Стандартизация измерения производительности NGFW через независимые тесты (по RFC 2544/3511), с созданием открытой базы сравнений российских решений для выбора оптимальных.

5. Улучшение IPS за счет гибридных методов (сигнатурные + поведенческие), с фокусом на снижение ложных срабатываний путем обучения на данных финансовых транзакций.

6. Решение проблем интеграции NGFW в SIEM/SOC через разработку кастомных коннекторов и облачных сервисов, обеспечивающих seamless обмен данными и приоритизацию инцидентов.

7. Защита разработчиков с помощью PAM-систем, DLP и сегментации сетей, дополненных образовательными программами по кибергигиене.

8. Введение NSPM-платформ для централизованного управления поставщиками, с элементами прогнозирования рисков и автоматизированной оптимизацией политик безопасности.

Заключение

Отраслевые особенности киберзащиты в финансовой сфере заключаются в организации баланса между импортозамещением, производительностью и интеграцией решений. Устранение проблем hardening, усиление антифрод и NSPM позволят минимизировать риски. Оптимальные решения в этой области должны содержать технологии ИИ и облачные технологии для повышения устойчивости.

В рамках государственной политики импортозамещения целесообразно разработать национальную программу по киберимпортозамещению, включающую поддержку отечественных разработчиков, сертификацию оборудования и создание централизованных SOC для региональных банков.

Перспективным направлением становится формирование единой базы знаний по инцидентам и уязвимостям, интегрированной с NSPM и GOS-SOC. Ожидается постепенный переход банков на отечественные платформы анализа угроз и автоматической корреляции событий.

Библиографический список

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – [Электронный ресурс]. – Режим доступа: legalacts.ru/doc/FZ-obinformacii-informacionnyh-tehnologijah-i-o-zawite-informacii/.
2. PT Security. Киберугрозы финансовой отрасли: прогноз на 2025-2026 г. – [Электронный ресурс]. – Режим доступа: https://ptsecurity.com/ru-ru/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/.
3. DIS.ru. Политика Банка России в сфере кибербезопасности. – [Электронный ресурс]. – Режим доступа: https://dis.ru/library/706/37907/.
4. Лактюшина О.В., Горбачева Т.А. Киберугрозы в банковской сфере и направления их снижения в российской федерации // Вестник Московского университета имени С.Ю. Витте. Серия 1: Экономика и управление. – 2025. – №1 (52). – С. 27-40.

INDUSTRY-SPECIFIC FEATURES OF CYBER DEFENSE FOR THE FINANCIAL SECTOR

Yu.A. Kosinov[1], *Representative of the employer involved in the educational process*
A.Y. Sharova[2], *Associate Professor*
[1]Limited Liability Company "ICL System Technologies"
[2]Ivanovo State Polytechnic University
[1](Russia, Kazan)
[2](Russia, Ivanovo)

Abstract. *The article analyzes key aspects of cybersecurity in the Russian financial sector, taking into account the specifics of the industry, where high risks of financial losses from cyber-attacks require specialized approaches. The problems of fine-tuning domestic network and server equipment, methods of protecting applications from DDoS attacks and web threats (Anti-DDOS, WAF, WAAP), anti-fraud systems, performance evaluation of Russian NGFWs, quality of attack detection in IPS, challenges of NGFW integration into SIEM and SOC, measures to protect internal developers, approaches to managing heterogeneous equipment suppliers (NSPM).*

Keywords: *cybersecurity, financial sphere, anti-fraud systems, domestic equipment, integration, protection of developers.*