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

2025, Том 12, № s3 / 2025, Vol. 12, Iss. s3 https://resources.today/issue-s1-2026.html

URL статьи: https://resources.today/PDF/03FAOR325.pdf

DOI: 10.15862/03FAOR325 (https://doi.org/10.15862/03FAOR325)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Бестаев, Г. Б. Применение методов машинного обучения для прогнозирования киберугроз в финансовых экосистемах / Г. Б. Бестаев // Отходы и ресурсы. — 2025. — Т. 12. — № s3. — URL: https://resources.today/PDF/03FAOR325.pdf. DOI: 10.15862/03FAOR325.

For citation:
Bestaev G.B. Application of machine learning methods to predict cyber threats in financial ecosystems. *Russian Journal of Resources, Conservation and Recycling*. 2025; 12(s3): 03FAOR325. Available at: https://resources.today/PDF/03FAOR325.pdf. DOI: 10.15862/03FAOR325. (In Russ., abstract in Eng.).

УДК 004.056:336.7

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

Применение методов машинного обучения для прогнозирования киберугроз в финансовых экосистемах

Аннотация. Нарастающая сложность ландшафта киберугроз и усиление целенаправленных атак на финансовый сектор обусловливают потребность в переходе от реактивной модели обеспечения информационной безопасности к проактивной, основанной на прогнозировании вероятных сценариев развития инцидентов. Методы машинного обучения предоставляют финансовым экосистемам инструментарий для анализа массивов транзакционных, сетевых и поведенческих данных, выявления нетривиальных закономерностей и формирования моделей вероятности киберриска. Целью настоящего исследования является определение особенностей применения методов машинного обучения для прогнозирования киберугроз в финансовых экосистемах, раскрытие их функциональных возможностей и оценка ключевых ограничений практического внедрения. В работе систематизированы основные направления прогнозирования киберугроз средствами машинного обучения, проведён сравнительный анализ классов алгоритмов (обучение с учителем, обучение без учителя, глубокое обучение) по критериям применимости к финансовым данным, предложена авторская классификация ограничений внедрения интеллектуальных моделей, дифференцированная по природе барьера. Результаты свидетельствуют о том, что наибольшую эффективность обеспечивает комплексное применение нескольких классов моделей, встроенных в общую архитектуру управления киберрисками, при условии сочетания технологической зрелости организации, достаточной полноты данных и наличия регламентов, определяющих место интеллектуальных решений в системе принятия решений. Научная новизна состоит в разработке авторской классификации ограничений внедрения ML-моделей в финансовый сектор, дифференцированной по природе барьера, и в систематизации направлений прогнозирования с учётом российской специфики ландшафта киберугроз 2025–2026 годов. Практическая значимость определяется возможностью использования полученных выводов финансовыми организациями при формировании стратегии внедрения интеллектуальных систем обнаружения угроз и при выстраивании регламентов, определяющих место ML-моделей в контуре принятия решений.

Ключевые слова: машинное обучение; киберугрозы; финансовые экосистемы; кибербезопасность; прогнозирование; обучение с учителем; обучение без учителя; глубокое обучение; антифрод; интеллектуальный анализ данных

Введение

Актуальность настоящего исследования определяется устойчивым ростом интенсивности и сложности кибератак на финансовый сектор Российской Федерации. По данным «Лаборатории Касперского» количество кибератак на финансовые организации в первом полугодии 2025 года увеличилось на 13 % по сравнению с аналогичным периодом 2024 года, число атак с применением вредоносного ПО для кражи средств через онлайн-доступ к банковским счётам возросло в 2,4 раза, а количество атак с использованием онлайн-ресурсов увеличилось на 81 %[1]. По данным CNews в 2025 году число кибератак на финансовые учреждения выросло на 43 %, при этом 83 % финансовых организаций столкнулись с угрозами в корпоративной электронной почте[2].

Вместе с тем традиционные средства защиты, основанные на статических правилах и сигнатурном обнаружении, уже не обеспечивают необходимого уровня противодействия быстро меняющимся сценариям атак. Особого внимания заслуживает прогноз вице-президента Сбербанка по кибербезопасности С. Лебедя о том, что до 75 % кибератак в 2025 году будут базироваться на разработках с искусственным интеллектом[3], что свидетельствует о необходимости применения аналогичных технологий для защиты. По оценкам Servicepipe в 2025 году порядка 30 % всех DDoS-атак создавалось с использованием ИИ, а в 2026 году их доля может вырасти минимум вдвое[4].

Объектом исследования выступают финансовые экосистемы Российской Федерации в условиях нарастания киберугроз.

Предметом исследования являются методы машинного обучения, применяемые для прогнозирования и раннего обнаружения киберугроз в финансовом секторе.

Целью исследования является определение функциональных возможностей и ограничений методов машинного обучения для прогнозирования киберугроз в финансовых экосистемах.

Для достижения поставленной цели решаются следующие задачи.

1. Систематизировать основные направления прогнозирования киберугроз в финансовых экосистемах средствами машинного обучения.

[1] 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).

[2] CNews. В 2025 г. число кибератак на финансовые учреждения выросло на 43%. — [Электронный ресурс] Режим доступа: URL: https://safe.cnews.ru/news/line/2026-02-18_v_2025_gchislo_kiberatak_na#:~:text=Финансовая%20отрасль%20остается%20одной%20из,сообщили%20представители%20«Лаборатории%20Касперского»Е%С2%ВВ. (дата обращения 23.04.2026).

[3] 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).

[4] Anti-Malware. Прогноз киберугроз и средств защиты в России на 2026 год. — [Электронный ресурс] Режим доступа: URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026 (дата обращения 23.04.2026).

2. Провести сравнительный анализ классов алгоритмов по критериям применимости к задачам финансовой кибербезопасности.
3. Разработать классификацию ограничений внедрения интеллектуальных моделей в контур обеспечения информационной безопасности.

Научная новизна состоит в разработке авторской классификации ограничений внедрения ML-моделей в финансовый сектор, дифференцированной по природе барьера, а также в систематизации направлений прогнозирования с учётом российской специфики ландшафта киберугроз 2025–2026 годов.

Практическая значимость определяется возможностью использования результатов финансовыми организациями для формирования стратегии внедрения интеллектуальных систем обнаружения угроз.

1. Материалы и методы

Методологическую основу исследования составляют системный и сравнительный подходы. Системный подход позволяет рассматривать финансовую экосистему как взаимосвязанную среду, в которой уязвимость одного элемента способна повлиять на устойчивость всей цепочки цифровых сервисов. Сравнительный метод применён для сопоставления различных классов алгоритмов машинного обучения по критериям точности, скорости реакции, устойчивости к шуму и пригодности для обработки в реальном времени.

Информационную базу составили аналитические отчёты Positive Technologies, «Лаборатории Касперского», ФинЦЕРТ, F6, TAdviser, Gartner, а также научные публикации в области применения машинного обучения для задач кибербезопасности.

2. Результаты и обсуждение

Теоретический фундамент настоящего исследования опирается на положения о многоуровневой архитектуре киберзащиты финансовых экосистем, в рамках которой методы машинного обучения выступают не изолированным инструментом, а компонентом целостной системы управления киберрисками. Финансовые экосистемы функционируют в условиях постоянного обмена данными между внутренними банковскими платформами, мобильными приложениями, внешними API, платёжными шлюзами и облачными сервисами, что создаёт среду, в которой угроза может проявляться как совокупность слабых сигналов, распределённых по различным сегментам инфраструктуры [1]. Как подчёркивает Х. Умаров, трансформация финансовых сервисов через применение искусственного интеллекта требует вдумчивого, поэтапного стратегического подхода, следующего правовым, юридическим и экономическим нормам [2].

Систематизация основных направлений прогнозирования киберугроз средствами машинного обучения в финансовых экосистемах представлена в таблице 1.

Таблица 1

Основные направления прогнозирования киберугроз средствами машинного обучения в финансовых экосистемах

Направление прогнозирования	Задачи ML-модели	Источники данных	Критичность для финансового сектора
Выявление мошеннических транзакций	Оценка риска каждой транзакции в реальном времени, блокировка подозрительных операций	Транзакционные данные, профили клиентов, метаданные устройств	Высокая (прямые финансовые потери)

Прогнозирование фишинговых атак	Анализ структуры сообщений, признаков доменов, поведенческих характеристик переходов	Почтовый трафик, данные о доменах, поведенческая аналитика	Высокая (начальная стадия крупных инцидентов)
Анализ сетевого трафика и телеметрии	Поиск отклонений в частоте соединений, маршрутах обращения, размере пакетов, длительности сессий	Журналы событий ИБ, сетевая телеметрия, SIEM-данные	Средняя (обнаружение вторжения на ранней стадии)
Выявление инсайдерских угроз	Оценка поведенческих отклонений сотрудников от установившегося профиля деятельности	Данные о сессиях пользователей, объём доступа к данным, временны́е профили	Высокая (30 % инцидентов связаны с нарушением политик ИБ сотрудниками)

Составлено автором на основе анализа материалов [3; 4][5]

Данные таблицы 1 свидетельствуют о многоплановом характере задач прогнозирования киберугроз, для решения которых требуются различные классы алгоритмов машинного обучения. Уместно заметить, что 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, что подтверждает критическую значимость направления выявления инсайдерских угроз[6].

В развитие данного положения необходимо провести сравнительный анализ классов алгоритмов машинного обучения по критериям применимости к задачам финансовой кибербезопасности. Сравнительный анализ представлен в таблице 2.

Таблица 2

Сравнительный анализ классов алгоритмов машинного обучения для задач финансовой кибербезопасности

Класс алгоритмов	Характерные методы	Преимущества для финансового сектора	Ограничения	Области наибольшей эффективности
Обучение с учителем (англ. Supervised Learning)	Градиентный бустинг, случайный лес, логистическая регрессия	Высокая точность при наличии размеченных данных, интерпретируемость	Зависимость от качества и полноты разметки, быстрое устаревание шаблонов	Классификация транзакций, оценка кредитного риска
Обучение без учителя (англ. Unsupervised Learning)	Кластерный анализ, автокодировщики, метод изоляционного леса	Способность обнаруживать неизвестные ранее аномалии, отсутствие требования к разметке	Высокий уровень ложных срабатываний, сложность интерпретации	Выявление новых типов атак, обнаружение отклонений от нормы
Глубокое обучение (англ. Deep Learning)	Рекуррентные сети, трансформеры, графовые нейронные сети	Способность выявлять сложные многоуровневые зависимости в потоках данных	Высокие требования к вычислительным ресурсам, низкая интерпретируемость	Анализ последовательных данных, сетевой трафик, NLP

Составлено автором на основе анализа материалов [5][7]

[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).

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).

[6] 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).

[7] SecurityVision. Кибербезопасность ИИ. Нейросети и машинное обучение. — [Электронный ресурс] Режим доступа: URL: https://www.securityvision.ru/blog/kiberbezopasnost-ii-chast-1-neyroseti-i-mashinnoe-obuchenie/ (дата обращения 23.04.2026).

Анализ представленной в таблице 2 информации демонстрирует, что каждый класс алгоритмов обладает специфическими преимуществами и ограничениями, что обосновывает целесообразность их комплексного применения. Следует отметить, что методы обучения с учителем остаются фундаментом антифрод-систем крупнейших банков, однако их эффективность снижается в условиях появления новых типов атак, не представленных в обучающей выборке. Методы обучения без учителя компенсируют данное ограничение, обеспечивая обнаружение аномалий, не воспроизводящих ранее наблюдавшиеся формы поведения [6]. Глубокое обучение позволяет перейти от анализа отдельных признаков к выявлению сложных многоуровневых зависимостей, что особенно актуально при обработке потоков данных высокой интенсивности [7]. Как отмечает «Лаборатория Касперского», прогноз о росте числа кибератак с применением машинного обучения на 2025 год полностью оправдался[8].

На основе проведённого анализа автором разработана классификация ограничений внедрения ML-моделей в контур обеспечения информационной безопасности финансовых экосистем. Классификация представлена в таблице 3.

Таблица 3

Классификация ограничений внедрения ML-моделей в финансовый сектор по природе барьера

Природа ограничения	Содержание барьера	Проявление в финансовом секторе	Рекомендуемые меры преодоления
Дата-ориентированные	Недостаточное качество обучающих выборок, несбалансированность классов, устаревание данных	Редкие критически опасные инциденты недостаточно представлены в данных	Аугментация данных, синтетическая генерация миноритарных классов, регулярное переобучение
Методологические	Низкая интерпретируемость моделей, сложность объяснения решений	Регуляторные требования к обоснованию каждого решения об отклонении операции	Применение объяснимого ИИ (англ. XAI, Explainable AI), гибридные модели с экспертными правилами
Инфраструктурные	Высокие требования к вычислительным ресурсам, необходимость обработки в реальном времени	Задержки в принятии решений критичны для блокировки мошеннических транзакций	Оптимизация архитектуры, распределённые вычисления, облачные ML-платформы
Адаптационные	Возможность адаптации злоумышленников к используемым моделям (состязательные атаки)	Мошенники изменяют паттерны поведения для обхода автоматизированных фильтров	Непрерывное переобучение, мониторинг дрейфа данных, состязательная тренировка моделей

Составлено автором на основе анализа материалов [8–10][9]

Результаты, отражённые в таблице 3, позволяют сделать вывод о комплексном характере ограничений, препятствующих широкому внедрению ML-моделей в финансовый сектор. Примечательно, что адаптационные ограничения приобретают нарастающую значимость в условиях использования злоумышленниками искусственного интеллекта для генерации атак. По данным Positive Technologies финансовая отрасль входит в пятёрку наиболее атакуемых

[8] Securelist. Прогноз по финансовым киберугрозам и crimeware на 2025 год. — [Электронный ресурс] Режим доступа: URL: https://securelist.ru/ksb-financial-and-crimeware-predictions-2025/111084/ (дата обращения 23.04.2026).

[9] F6. Новые риски кибератак в России и СНГ. — [Электронный ресурс] Режим доступа: URL: https://www.f6.ru/cybercrime-trends-annual-report-2024-2025/ (дата обращения 23.04.2026).

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).

секторов, и в 67 % успешных кибератак злоумышленники похищали данные и шантажировали жертву их уничтожением или раскрытием[10].

Помимо указанного, необходимо подчеркнуть перспективы развития интеллектуальных моделей в контексте финансовой кибербезопасности. Наиболее перспективным направлением представляется интеграция ML-моделей в единые центры мониторинга безопасности (англ. SOC, Security Operations Center), где результаты анализа транзакций, сетевых событий, пользовательского поведения и внешней киберразведки объединяются в общую систему раннего предупреждения [11]. Существенную роль может сыграть развитие гибридных подходов, сочетающих вероятностные модели, экспертные правила и поведенческую аналитику [12]. Объём российского рынка информационной безопасности достиг 299 млрд рублей в 2024 году и прогнозируется на уровне свыше 400 млрд рублей в 2025 году[11], что создаёт экономические предпосылки для масштабного внедрения интеллектуальных систем защиты. Средняя оценка уровня кибербезопасности финансового сектора России составляет 5,8 балла из 10[12], что свидетельствует о необходимости дальнейшего наращивания защитного потенциала, в том числе за счёт интеллектуальных решений.

Стоит обратить внимание на то, что в антифрод-центре Сбербанка уже функционируют более 100 моделей искусственного интеллекта, а более 1 700 организаций являются участниками информационного обмена с ФинЦЕРТ[13], что формирует инфраструктурный каркас для построения межбанковских предиктивных систем. Как подчёркивают аналитики Gartner, выделяя ключевые тренды кибербезопасности на 2025–2026 годы, всё более широкое использование технологий машинного обучения и систем искусственного интеллекта в защитных решениях позволяет компенсировать недостаток квалифицированных специалистов и ускорить реагирование на угрозы[14].

Выводы

Систематизация основных направлений прогнозирования киберугроз средствами машинного обучения выявила четыре ключевые области применения в финансовых экосистемах, наиболее критичными из которых являются выявление мошеннических транзакций и обнаружение инсайдерских угроз. Установлено, что в 2025 году 30 % инцидентов в финансово-страховой отрасли были связаны с нарушением сотрудниками политик информационной безопасности, что подтверждает необходимость поведенческой аналитики на основе ML-моделей.

[10] 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).

[11] 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).

[12] 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).

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

[14] TAdviser. Главные тенденции в защите информации. — [Электронный ресурс] Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (дата обращения 23.04.2026).

Сравнительный анализ классов алгоритмов продемонстрировал, что методы обучения с учителем, обучения без учителя и глубокого обучения обладают взаимодополняющими возможностями, и наибольшая эффективность достигается при их комплексном применении в рамках единой архитектуры управления киберрисками. Установлено, что изолированное использование одного класса алгоритмов не позволяет адекватно противостоять адаптивным угрозам, характеризующимся маскировкой под легитимную активность.

Разработанная классификация ограничений внедрения ML-моделей выявила четыре категории барьеров (дата-ориентированные, методологические, инфраструктурные, адаптационные), среди которых нарастающую значимость приобретают адаптационные ограничения, связанные с использованием злоумышленниками искусственного интеллекта для генерации атак. Практическое внедрение интеллектуальных систем возможно только при условии сочетания технологической зрелости организации, достаточной полноты данных, организационной готовности специалистов и наличия регламентов, определяющих место ML-моделей в контуре принятия решений.

ЛИТЕРАТУРА

1. 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.
2. Умаров, Х. С. Трансформация российских финансовых и банковских сервисов через применение искусственного интеллекта: текущие тенденции и стратегические перспективы / Х. С. Умаров — DOI 10.31432/1994-2443.2025.17. // Информация и инновации. — 2025. — Т. 20, № 4. — С. 5-24 — EDN XZHNWZ.
3. Петренко, С. А. Управление информационными рисками: Экон. оправд. безопасность: Информ. технологии для инженеров / С. А. Петренко, С. В. Симонов; Петренко С. А., Симонов С. В.. — Москва: Акад. АйТи, 2004. — 383 с. — (Информационные технологии для инженеров). — ISBN 5-98453-001-5. — EDN QQESJB.
4. Обнаружение аномальных транзакций криптовалюты с помощью нейронных сетей и онтологий / И. В. Котенко, Д. С. Левшун, К. Н. Жернова, А. А. Чечулин — DOI 10.18287/2223-9537-2025-15-3-334-350. // Онтология проектирования. — 2025. — Т. 15, № 3(57). — С. 334-350 — EDN IVCFZU.
5. Генкин, А. С. Управление рисками в сфере искусственного интеллекта: основные подходы к регулированию / А. С. Генкин // Управление риском. — 2025. — № 3(115). — С. 44-52. — EDN GPSWFM.
6. Нейросетевая технология обнаружения аномального сетевого трафика / В. А. Частикова, С. А. Жерлицын, Я. И. Воля, В. В. Сотников — DOI 10.21672/2074-1707.2020.49.4.020-032. // Прикаспийский журнал: управление и высокие технологии. — 2020. — № 1(49). — С. 20-32 — EDN WUCDII.
7. Hamilton W. Inductive representation learning on large graphs / W. Hamilton, Z. Ying, J. Leskovec // Advances in neural information processing systems. — 2017. — URL: https://www.researchgate.net/publication/317399572_Inductive_Representation_Learning_on_Large_Graphs

8. Дядюнов, Д. А. Машинное обучение для риск-менеджмента в банке: возможности и вызовы / Д. А. Дядюнов // Вестник науки. — 2025. — Т. 1, № 1(82). — С. 265-273. — EDN OJWRUL.

9. Ильгамович, К. К. Интеллектуальный анализ данных и обработка Big Data с применением ML-технологий для эконометрического и финансового моделирования / К. К. Ильгамович, М. М. Супрунов, Е. С. Крючков // Вестник евразийской науки. — 2025. — Т. 17, № S2. — EDN WHRSRI.

10. Гутник, С. А. Применение методов интеллектуального анализа данных и машинного обучения для повышения эффективности управления в менеджменте / С. А. Гутник, М. М. Звягинцев — DOI 10.24833/2949-639X-2025-3-13-74-95. // Международный бизнес. — 2025. — № 3(13). — С. 74-95 — EDN KFVPMM.

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. 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.

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

Application of machine learning methods to predict cyber threats in financial ecosystems

Abstract. The growing complexity of the cyber threat landscape and the intensification of targeted attacks on the financial sector necessitate a transition from a reactive to a proactive information security model based on predicting probable incident scenarios. Machine learning methods provide financial ecosystems with tools for analyzing transactional, network, and behavioral data sets, identifying nontrivial patterns, and generating cyber risk probability models. The purpose of this study is to identify the specifics of applying machine learning methods to predict cyber threats in financial ecosystems, explore their capabilities, and assess the key limitations of their practical implementation. This paper systematizes the main approaches to cyberthreat forecasting using machine learning. It also conducts a comparative analysis of algorithm classes (supervised learning, unsupervised learning, and deep learning) based on their applicability to financial data. It also proposes a classification of limitations to the implementation of intelligent models, differentiated by the nature of the barrier. The results demonstrate that the greatest effectiveness is achieved through the integrated use of several classes of models integrated into the overall cyber risk management architecture, provided that the organization has a combination of technological maturity, sufficient data completeness, and the existence of regulations defining the role of intelligent solutions in the decision-making system. The scientific novelty lies in the development of a classification of limitations to the implementation of ML models in the financial sector, differentiated by the nature of the barrier, and in the systematization of forecasting approaches, taking into account the specifics of the Russian cyber threat landscape for 2025–2026. The practical significance lies in the potential for financial institutions to use the findings when formulating strategies for implementing intelligent threat detection systems and developing regulations governing the role of ML models in decision-making.

Keywords: machine learning; cyberthreats; financial ecosystems; cybersecurity; forecasting; supervised learning; unsupervised learning; deep learning; antifraud; data mining