Применение искусственного интеллекта для обеспечения кибербезопасности на финансовых рынках
The use of artificial intelligence to ensure cybersecurity in financial markets

Афанасьева Оксана Николаевна
доктор экономических наук,
профессор кафедры финансов и валютно-кредитных отношений
ФГБОУ ВО «Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

Манцкава Диана Вахтанговна
студент специалитета, международно-правовой факультет
ФГБОУ ВО «Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

Аннотация В статье рассмотрено применение искусственного интеллекта для обеспечения кибербезопасности на финансовых рынках. Авторы раскрывают связь цифровизации в финансовых организациях и киберпреступлений, эволюцию и совершенствование киберугроз в зарубежных странах. Изложены стратегии киберзащиты в финансовых учреждениях и прогнозы по применению инструментов искусственного интеллекта для профилактики киберугроз.

Ключевые слова: финансы, искусственный интеллект, кибербезопасность, финансовые рынки, финансовые организации, киберугрозы, финансовый сектор.

Abstract This article examines the use of artificial intelligence to ensure cybersecurity in financial markets. The authors reveal the connection between digitalization in financial organizations and cybercrime, as well as the evolution and improvement of cyber threats in foreign countries. Cyber defense strategies in financial institutions and forecasts for the use of artificial intelligence tools to prevent cyber threats are outlined.

Keywords: finance, artificial intelligence, cybersecurity, financial markets, financial organizations, cyber threats, financial sector.

В XXI веке цифровое пространство превратилось в ключевой компонент национального суверенитета, а значит, применение искусственного интеллекта (ИИ) для защиты финансовых рынков выходит на передний план. Алгоритмы ИИ способны в реальном времени обрабатывать огромные массивы информации, выявляя отклонения и потенциально опасные события, что позволяет быстро реагировать на атаки и

предотвращать финансовые правонарушения. Поскольку фондовые и валютные площадки являются системообразующей частью экономики, их сбои неизбежно подрывают доверие инвесторов и дестабилизируют финансовую систему в целом [1]. Внедрение ИИ не только усиливает киберзащиту, но и содействует формированию устойчивой цифровой инфраструктуры — важного элемента современного суверенитета.

Чем активнее финансовые организации переходят на цифровые технологии и наращивают объём обрабатываемых данных, тем заметнее растёт число кибератак. С точки зрения монетарной политики, основанной на информационной инфраструктуре, надёжная кибербезопасность требуется сегодня как никогда [2]. ИИ-решения рассматриваются в качестве одного из наиболее перспективных инструментов, способных минимизировать риски, связанные с атаками, и обеспечить высокую степень защиты конфиденциальных сведений.

Финансовый сектор остаётся привлекательной целью для киберпреступников. Банки ежедневно сталкиваются с фишингом, DDoS-атаками, вредоносным ПО, эксплуатацией уязвимостей и незаконным доступом к цифровым активам. Фишинговые рассылки позволяют злоумышленникам мошеннически получать данные пользователей, а DDoS-атаки выводят из строя сервисы и парализуют операции. По оценкам IBM Security X-Force, число ударов по финансовым институтам в 2021 году увеличилось на 238 % по сравнению с 2020-м. Средняя ликвидация последствий одной атаки, по данным Accenture, занимает 18,5 дня и ведёт не только к финансовым потерям, но и к репутационному ущербу [3].

Инвестиции в компании, занимающиеся ИИ, в 2020 году достигли примерно 55 млрд долларов, то есть около 18 % общего объёма венчурного капитала, что отражает признание ценности данных технологий [4]. Наглядный пример масштабной кражи — инцидент в Центральном банке Бангладеш (2016 г.), где через уязвимости системы SWIFT мошенники вывели 81 млн долларов. В 2019 году Capital One потерял данные более 100 млн клиентов из-за бреши в облачной инфраструктуре. Подобные истории демонстрируют, что даже крупные игроки уязвимы, а небольшие банки подвергаются атакам ещё чаще, что усиливает необходимость комплексных стратегий защиты [5].

Современные киберугрозы становятся всё более изощрёнными. Исследование IBM за 2022 год показало: на финансовый сектор приходится 23 % всех выявленных атак. Для отражения этих рисков активно развиваются ИИ-системы автоматического

реагирования. Они используют машинное обучение для мгновенной классификации инцидентов и запуска мер противодействия; по оценкам IBM, внедрение таких систем сокращает среднее время ответа на 74 %. Компания Darktrace, например, сообщала, что её решения блокировали свыше 150 тыс. атак ещё на начальной стадии [6].

Успешные примеры применения ИИ видны во многих странах. Так, JPMorgan Chase анализирует транзакции онлайн, что позволило снизить уровень мошенничества почти на треть. HSBC в Великобритании задействует поведенческую аналитику, а сингапурский DBS Bank использует биометрию на базе ИИ для аутентификации клиентов [7]. В Австралии Commonwealth Bank применяет предиктивные модели, предупреждая атаки до их реализации [8]. Сравнение показывает, что по скорости обнаружения угроз и способности работать с «большими данными» ИИ-подходы превосходят традиционные методы [9].

Помимо выявления подозрительных транзакций, ИИ оптимизирует внутренние процессы. Например, система COiN, созданная JPMorgan Chase, за секунды анализирует тысячи договоров, сокращая расходы и избавляя сотрудников от рутины. Отчёты IBM показывают: использование ИИ позволило банкам сократить время обнаружения и реагирования на инциденты на 96 % [10].

Тем не менее внедрение ИИ сопряжено с трудностями. По данным Accenture, 77 % топ-менеджеров финансовых организаций опасаются высоких рисков, связанных с интеграцией ИИ в существующие ИТ-ландшафты. Актуальной задачей остаётся и подготовка персонала. Отчёт Capgemini отмечает, что без ИИ невозможно оперативно отражать атаки: 69 % компаний придерживаются этой точки зрения [11]. Более того, грамотное обучение сотрудников снижает вероятность успешного взлома, что подтверждают исследования IBM за 2022 год.

До 2025 года, по прогнозу Gartner, свыше 60 % организаций будут активно задействовать ИИ для предотвращения и выявления киберугроз. Особое внимание уделяется объяснимому ИИ (Explainable AI), повышающему прозрачность алгоритмов, и объединению ИИ с Интернетом вещей для создания единой системы мониторинга. Комплексное внедрение таких технологий способно значительно повысить устойчивость финансового сектора к угрозам и обеспечить его долгосрочную безопасность [12].

Возросший масштаб цифровых угроз вынуждает финансовые учреждения глубже пересматривать стратегии киберзащиты. Во-первых, это подразумевает широкое

внедрение интеллектуальных платформ, способных круглосуточно анализировать трафик, фиксировать нетипичные аномалии и моментально блокировать вредоносную активность. Такие решения повышают надёжность инфраструктуры, улучшают качество клиентских сервисов и существенно осложняют жизнь мошенникам. Одновременно растёт потребность в регулярном обучении сотрудников: им необходимо понимать логику современных атак — от фишинга и эксплойтов до сложных многоэтапных вторжений. Не менее важно выстраивать многоуровневую модель доступа, минимизируя привилегии к критически важным узлам и усиливая контроль над персональными данными клиентов [13].

Логическим продолжением этой эволюции стала автоматизация реагирования на инциденты (SOAR). Комбинация машинного обучения и обработки больших данных позволяет системе в считанные секунды локализовать источник вторжения, оценить его критичность и активировать заранее прописанный сценарий защиты. По расчётам IBM Security, интеграция ИИ-модулей в такие процессы сокращает среднее время ответа на 74 %, а значит, ограничивает потенциальный ущерб и снижает нагрузку на аналитиков-человек [14].

Практика подтверждает статистику. В 2021 году компания Darktrace сообщила, что её «цифровой иммунитет» в реальном времени остановил более 150 000 попыток взлома, не допустив утечки данных [14]. Подобные примеры иллюстрируют, каким образом автоматизация снимает рутинные задачи со специалистов, давая им возможность сосредоточиться на нестандартных угрозах и стратегическом планировании.

Банковская отрасль по всему миру активно перенимает эти подходы. В США JPMorgan Chase применяет алгоритмы машинного обучения для онлайн-мониторинга транзакций; по данным *Journal of Financial Crime*, уровень выявленного мошенничества сократился примерно на 30 %. В Великобритании HSBC анализирует поведенческие паттерны клиентов в больших массивах данных, а публикация «*Big Data Analytics in Banking*» подчёркивает, что такой подход одновременно усиливает безопасность и повышает точность персонализированных услуг. В Сингапуре DBS Bank внедрил биометрию на базе ИИ (распознавание лиц и отпечатков пальцев) для аутентификации, что, согласно *International Journal of Information Management*, заметно снижает риск несанкционированного доступа [8]. Австралийский Commonwealth Bank использует предсказательную аналитику для выявления атак на ранней стадии; обзор «*Cybersecurity*

in Banking» фиксирует значительное снижение вероятности утечек благодаря таким моделям [9].

Сравнительные исследования неизменно показывают, что традиционные методы проигрывают интеллектуальным системам по скорости обнаружения, адаптивности и способности работать с огромными потоками данных [7]. Поэтому для финансовых организаций переход к ИИ перестал быть конкурентным преимуществом и стал условием выживания. Показателен кейс COiN от JPMorgan Chase: в 2020 году платформа обработала 12 000 контрактов за несколько секунд, практически исключив ошибки человеческого фактора и многократно сократив издержки. Этот пример демонстрирует, как интеграция ИИ одновременно усиливает киберзащиту и оптимизирует бизнес-процессы, задавая новый стандарт безопасности в финансовой сфере.

Мировой опыт подтверждает, что алгоритмы искусственного интеллекта заметно усиливают защиту финансовых систем от цифровых атак. Аналитики IBM установили: после внедрения ИИ-платформ банки сумели почти вчетверо (на 96 %) сократить время, необходимое для обнаружения инцидента и принятия ответных мер. Настолько быстрая реакция минимизирует риск несанкционированных транзакций и утечек данных. К тому же поведенческие модели ИИ способны фиксировать нетипичную активность клиентов или аномальные денежные переводы, останавливая мошеннические схемы ещё до их завершения [15]. Всё это подчёркивает решающую роль ИИ в укреплении надёжности финансовых операций и сохранении доверия клиентов.

Тем не менее интеграция «умных» сервисов в существующие периметры безопасности непроста. В отчёте Accenture говорится, что 77 % руководителей банков воспринимают развёртывание ИИ как зону повышенных рисков: требуется перестройка архитектуры, обновление процессов и перераспределение ответственности за данные. Успех проекта напрямую зависит от грамотного управления этими изменениями.

Несмотря на опасения, преимуществ больше, чем потенциальных угроз. Исследование Capgemini показывает: 69 % компаний убеждены, что без ИИ невозможно противостоять современным атакам в реальном времени. Параллельно растёт спрос на подготовку специалистов: по данным IBM за 2022 год, обучение сотрудников работе с ИИ снижает вероятность успешного взлома в разы, поскольку персонал быстрее распознаёт подозрительные сигналы и корректно реагирует на автоматические оповещения системы.

Эксперты Gartner прогнозируют, что к 2025 году свыше 60 % организаций будут активно пользоваться ИИ-инструментами для профилактики и обнаружения киберугроз. Ключевые направления развития включают самообучающиеся модели, постоянно адаптирующиеся к новым техникам атак, и объяснимый ИИ, повышающий прозрачность решений для регуляторов. Дополняет картину интеграция ИИ с Интернетом вещей: в промышленности, транспорте и энергетике формируются сетевые кластеры датчиков, которые в режиме реального времени собирают и анализируют массивы данных, прогнозируют нагрузки и оптимизируют управление ресурсами. Комплексное применение этих технологий способно радикально повысить киберустойчивость финансового сектора и обеспечить его долгосрочную безопасность и сохранение цифрового суверенитета.

Список литературы

1. Лупоядова Л.Ю. Тенденции и перспективы развития банковской системы в современных экономических условиях. Т.1: материалы II международной научно-практической конференции (17 декабря 2019 года), Брянск: Издательство БГУ им. акад. И.Г. Петровского, 2020. — С. 270

2. Афанасьева О.Н. Развитие теории экономической политики роста: распределение монетарных инструментов по целям и структуре экономики. - Диссертация на соискание ученой степени доктора экономических наук: 5.2.1. экономическая теория. Место выполнения работы: ФГБОУ ВО МГУ имени М.В. Ломоносова. Место защиты: ФГБОУ ВО Санкт-Петербургский государственный университет. - М.: 2024. – С. 145

3. Применение искусственного интеллекта на финансовом рынке. Доклад для общественных консультаций. Центральный банк Российской Федерации, Москва 2023 — С. 11

4. Гуляев Г. Ю. Научные исследования и разработки. Сборник статей III Международной научно-практической конференции. Пенза, 2025. — С. 85

5. Гаврилова Э.Н. Искусственный интеллект в финансовой сфере: эволюция, возможности и перспективы использования // Вестник Московского университета имени С.Ю. Витте. Серия 1. Экономика и управление. — 2024. — № 3 (50). — С. 23–30.

6. Хоперский А.А. Роль искусственного интеллекта в развитии финансовой системы // Международный студенческий научный вестник – 2024. - №4.– С. 3.

7. Wang Y. Kung L.A. & Byrd T.A. Big Data Analytics in Banking: A Review // International Journal of Information Management. 2016. Vol. 36, No. 5. P. 759-772.

8. Zhang Y. Zhao Y. & Xu H. Biometric Authentication in Banking: A Review // International Journal of Information Management. 2019. Vol. 46. P. 1-10.

9. Khan M.A. Alghamdi A. & Alzahrani A. Cybersecurity in Banking: A Review of the Literature // Journal of Cybersecurity and Privacy. 2020. Vol. 1, No. 1. P. 1-20.

10. Ngai E.W.T. Cheng T.C.E. Chiu D.K.W. & Hsu C.W. The application of data mining techniques in financial fraud detection: A classification framework // Journal of Financial Crime. 2011. Vol. 18, No. 2. P. 127-145.

11. Скорикова Е.Н. Приоритеты современной науки: актуальные вопросы, достижения и инновации. В сборнике: Приоритеты современной науки: актуальные

вопросы, достижения и инновации. Сборник научных трудов по материалам V Международной научно-практической конференции. Анапа, 2024. — С. 73

12. Хасиятуллов М.Г. Назарова Ю. А. Латыпов М.Р. Влияние финансовой устойчивости на экономическую безопасность // Научный аспект. - 2024. - № 5. - С. 937

13. Тронин С.А. Правовые аспекты использования блокчейн-технологий в финансовом секторе // Вопросы российского и международного права. - 2023. - Том 13. - № 1А-2А. - С. 286-292.

14. Яковишин А.Д. Развитие алгоритмов ИИ для обнаружения и предотвращения кибератак // Электронный научный журнал «Дневник науки». — 2024. - № 1.– С. 4.

15. Патрикеева Я.О. Ливадина С.П. Инновационные технологии для учета и аудита финансовых результатов. Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный университет им. А.Н. Косыгина (Технологии. Дизайн. Искусство)». Москва, 2023. – С. 309