DOI: 10.34773/EU.2026.1.13

Роль искусственного интеллекта в выявлении и предотвращении финансовых угроз хозяйствующих субъектов*

The Role of Artificial Intelligence in Identifying and Preventing Financial Threats to Business Entities

Г. АХТАМОВА, Д. РАФИКОВ

Ахтамова Гульнара Авхадиевна, канд. экон. наук, доцент кафедры экономического анализа и статистики Уфимского государственного нефтяного технического университета (УГНТУ)
Рафиков Данил Талгатович, магистрант программы 38.04.01 «Экономическая безопасность» УГНТУ. E-mail: rafikov.danil@mail.ru

Аннотация. *Актуальность исследования. В статье рассматривается роль искусственного интеллекта (ИИ) в сфере информационной безопасности, охватывая его использование для обнаружения и предотвращения кибератак, анализа и классификации вредоносного программного обеспечения, а также прогнозирования будущих угроз. Освещаются преимущества, возможности и перспективы применения ИИ, включая повышение эффективности защиты информационных систем и адаптацию к эволюционирующему ландшафту угроз. Однако статья также подчеркивает существующие риски и проблемы, связанные с приватностью, этическими вопросами и потенциалом злоупотреблений.*
Ключевые слова*: искусственный интеллект, кибербезопасность, кибератака, информационная угроза.*
Abstract. *This article examines the role of artificial intelligence (AI) in information security, covering its use in detecting and preventing cyberattacks, analyzing and classifying malware, and predicting future threats. The benefits, capabilities, and prospects for using AI are highlighted, including improving the effectiveness of information system security and adapting to the evolving threat landscape. However, the article also highlights existing risks and concerns related to privacy, ethical issues, and the potential for abuse.*
Keywords*: artificial intelligence, cybersecurity, cyberattack, information threat.*

Введение

На сегодняшний день ИИ активно используется участниками российского финансового рынка в различных сферах бизнеса: для работы с клиентами, управления рисками, аналитики, мониторинга и выполнения транзакций и прочего. При этом существует значительный потенциал для расширения применения ИИ в финансовых организациях. Использование ИИ способствует повышению эффективности этих организаций и улучшению качества их услуг. В то же время стремительное развитие технологий, особенно в области генеративного ИИ, не только открывает новые возможности, но и приносит определенные вызовы и риски. Поэтому важно создать условия для развития этой технологии и одновременно выработать стратегию регулирования её применения.

Методы

В современной научной литературе ИИ принято классифицировать по уровню его когнитивных возможностей, выделяя три фундаментальные категории: узкоспециализированный интеллект, интеллект общего типа и сверхинтеллект. Такая градация позволяет разграничить текущие технологические достижения и теоретические модели.

Узкоспециализированный ИИ, обозначаемый как Artificial Narrow Intelligence (ANI), представляет собой совокупность алгоритмических систем, предназначенных для выполнения конкретных, строго ограниченных задач. Его ключевая характеристика заключается в высокой

* *Ссылка на статью*: Ахтамова Г.А., Рафиков Д.Т. Роль искусственного интеллекта в выявлении и предотвращении финансовых угроз хозяйствующих субъектов // Экономика и управление: научно-практический журнал. 2026. № 1. С. 70–74. DOI: 10.34773/EU.2026.1.13.

эффективности в пределах выбранной области при невозможности выходить за её рамки. Внутри этой категории нередко выделяют несколько направлений. Традиционные алгоритмические системы имитируют элементы логического рассуждения и позволяют осуществлять прогнозирование и интерпретацию данных, что делает их востребованными, например, в финансовых организациях при оценке кредитных рисков, выявлении мошеннических операций и совершенствовании процедур управления рисками. Адаптивные системы способны модифицировать собственные модели функционирования под воздействием поступающих данных, оперативно реагируя на изменения среды. Отдельное место занимает генеративный ИИ, ориентированный на формирование новых объектов данных – текстовых, визуальных, аудио- или видеоматериалов. Его отличительной особенностью является способность создавать содержательный контент, выходящий за рамки предопределённых шаблонов, что рассматривается исследователями как промежуточный этап на пути к созданию более универсальных интеллектуальных систем.

Искусственный интеллект общего уровня, или Artificial General Intelligence (AGI), трактуется как теоретически возможная система, способная решать широкий круг задач на сопоставимом с человеком уровне. Предполагается, что такой интеллект будет способен к самостоятельной постановке целей, формированию сложных причинно-следственных связей, рациональному планированию и действию в условиях высокой неопределённости. На сегодняшний день подобных систем не существует, однако концепция AGI позволяет обозначить долгосрочные ориентиры исследований, связанных с моделированием универсальных когнитивных способностей. Концепция сверхинтеллекта (Artificial Superintelligence, ASI) описывает перспективу создания искусственных систем, превосходящих человека практически по всем мыслительным характеристикам.

Наиболее динамично развивающимся направлением исследований и коммерческого внедрения в ближайшие годы считается генеративный ИИ. Согласно аналитическим оценкам, его глобальный рынок продемонстрирует многократный рост в течение текущего десятилетия, что объясняется широким спектром практических приложений генеративных моделей. К ним относятся персонализация клиентского опыта, автоматизация коммуникаций, повышение эффективности внутренних процессов организаций и оптимизация разработки программных продуктов. Существенное внимание к данному направлению обусловлено тем, что генеративные модели позволяют существенно расширить возможности автоматизации интеллектуальных функций, ранее доступных исключительно человеку. По мнению международных консалтинговых компаний, использование генеративных технологий способно приносить мировой экономике эффекты, оцениваемые в триллионы долларов/евро, особенно в областях маркетинга, обслуживания клиентов, анализа данных и программной инженерии. Финансовая индустрия, в силу характера своей деятельности, получает значительные преимущества от внедрения таких технологий: повышается точность принятия решений, оптимизируются операционные процессы, существенно возрастает скорость обработки клиентских запросов.

Особое значение ИИ приобретает в сфере обеспечения информационной безопасности. Современные системы защиты используют алгоритмы машинного обучения для анализа больших массивов данных, отражающих закономерности функционирования информационной инфраструктуры предприятия. К таким данным относятся характеристики рабочих процессов сотрудников, частотность и направленность сетевых взаимодействий, использование сервисов и приложений, а также структурные особенности рабочей среды. На основе выявленных закономерностей формируются модели нормального поведения, которые позволяют автоматически фиксировать отклонения, указывающие на потенциальные риски. При этом все процессы анализа могут быть организованы таким образом, чтобы конфиденциальная информация не покидала внутреннего контура предприятия. Генеративные алгоритмы, применяемые в области безопасности, также способны формировать аналитические описания выявленных угроз, моделировать возможности их развития и повышать эффективность реагирования за счёт более точного понимания природы обнаруженных аномалий.

Важным аспектом современных систем ИБ является способность интеллектуальных

алгоритмов самостоятельно адаптироваться к новым видам атак, которые ранее не встречались. Благодаря этому ИИ формирует динамическую модель обороны, которая становится всё более устойчивой по мере накопления знаний о ранее встреченных угрозах. Это создаёт предпосылки для постепенного перехода от традиционных статичных средств защиты к гибким архитектурам, способным эволюционировать синхронно с изменениями цифровой среды.

В силы вышеизложенного, ИИ, независимо от уровня его развития – от узкоспециализированных систем до гипотетических моделей общего и сверхинтеллекта, – формирует основу технологического прогресса и трансформирует представления о возможностях автоматизации мыслительных процессов. Современные тенденции свидетельствуют о том, что генеративные и адаптивные системы станут ключевыми компонентами цифровой экономики, включая финансовый сектор, информационную безопасность и множество иных сфер, где требуется обработка больших объёмов данных, идентификация закономерностей и оперативное принятие решений [2; 6].

Результаты

Несмотря на то, что ключевое значение в системе корпоративной безопасности попрежнему принадлежит человеку, роль интеллектуальных технологий в обеспечении устойчивости цифровой инфраструктуры постоянно возрастает. Применение систем искусственного интеллекта становится особенно актуальным в условиях стремительного увеличения числа кибератак на российские организации. Данные за второй квартал 2024 года указывают на фиксацию порядка 381 тысяч инцидентов в сфере информационной безопасности, что существенно – примерно на 17 % – превышает показатели предыдущего квартала. Подобная динамика отражает усиливающееся давление со стороны злоумышленников и демонстрирует структурный рост угроз в цифровой среде. Дополнительным подтверждением негативной тенденции является общее увеличение числа атак на 20 % с конца 2023 года, что свидетельствует о попытках киберпреступников причинить максимальный ущерб инфраструктуре российских компаний.

При этом согласно исследованию, компании становятся более подготовленными к предотвращению угроз. Статистика по количеству инцидентов представлена в таблице.

Диапазон	1 кв. 2023	1 кв. 2024	2 кв. 2023	2 кв. 2024	6 мес. 2023	6 мес. 2024
Кол-во инцидентов	290	294	325	381	615	675

Интеллектуальные системы уже сегодня обладают возможностью проводить автоматизированный анализ инцидентов, формировать предварительные выводы, поддерживать расследование действий и обеспечивать оперативное реагирование на возникающие угрозы. Их применение в области информационной безопасности приобретает особое значение на фоне дефицита квалифицированных специалистов, что является хронической проблемой российского и мирового рынков труда. Спрос на компетенции в сфере защиты информации многократно превышает предложение, что вынуждает разработчиков создавать программно-аппаратные решения, позволяющие частично компенсировать нехватку экспертов. ИИ способен обрабатывать большие массивы разнородных данных, выявлять закономерности, характерные для вредоносной активности, а также автоматически устранять часть инцидентов, освобождая специалистов для решения более сложных задач, связанных с системным анализом, стратегическим планированием защиты и расследованием сложных атак [5].

В области экономической безопасности применение интеллектуальных технологий обеспечивает ряд значимых преимуществ. Прежде всего оно проявляется в способности ИИ к быстрому выявлению отклонений как внешнего, так и внутреннего характера. Системы анализируют большое количество факторов, устанавливают корреляции между множеством событий и способны выделять потенциально опасные процессы, даже если каждое отдельное действие кажется рядовым. Существенную роль играет и возможность выявления уязвимостей, связанных с использованием небезопасных устройств, устаревших операционных систем, уязвимых

приложений или незащищённых данных. Аналитические алгоритмы также оказываются эффективными при распознавании действий квалифицированных злоумышленников, которые стремятся скрыть следы активности путём изменения технических параметров инфраструктуры. За счёт последовательного анализа больших объёмов информации интеллектуальные системы способны выделять наиболее значимые аномалии, требующие оперативного вмешательства специалистов [4].

Однако развитие и внедрение подобных технологий в России сталкивается с объективными внешними ограничениями. Санкционная политика существенно усложняет доступ к зарубежным инструментам, используемым для построения систем машинного обучения и интеллектуального анализа данных. По результатам опросов профессионального сообщества, значительная часть российских компаний выражает обеспокоенность нехваткой отечественных решений в области ИИ. Такая ситуация осложняет реализацию проектов, так как стоимость разработки программного обеспечения и цифровых платформ на базе ИИ в стране существенно возросла, достигнув прироста порядка 30-40 % в 2022 году. В этих условиях формирование устойчивой отечественной технологической базы становится одним из приоритетных направлений развития российской экономики. Создание национальных информационно-коммуникационных систем не только укрепляет технологический суверенитет, но и позволяет финансовым организациям и другим хозяйствующим субъектам оперативно адаптировать инструменты и методы защиты к особенностям внутреннего рынка. Развитие собственных решений способствует повышению устойчивости национальной цифровой инфраструктуры и сокращает зависимость от внешних поставщиков в критически важной сфере обеспечения информационной безопасности.

Обсуждение

Использование технологий ИИ в современном контуре информационной безопасности уже не ограничивается задачами детектирования и аналитической интерпретации инцидентов. Существенно более значимым направлением становится прогнозирование потенциальных кибератак, основанное на способности интеллектуальных систем выявлять долгосрочные тенденции, скрытые зависимости и характерные паттерны поведения в цифровом пространстве. Такой подход позволяет сформировать упреждающие защитные меры ещё до того, как вредоносная активность приобретёт конкретное воплощение и начнёт оказывать воздействие на инфраструктуру организации.

Прогностические компоненты систем информационной безопасности, созданные на базе алгоритмов машинного обучения и технологий анализа больших данных, считаются одним из наиболее перспективных направлений развития современной киберзащиты. Их принципиальное преимущество заключается в возможности моделирования вероятных сценариев действий злоумышленников. Интеллектуальные алгоритмы способны не только фиксировать уже совершённые попытки несанкционированного доступа, но и выявлять ранние маркеры, предшествующие реализации атаки, что принципиально повышает готовность компаний к противодействию сложным угрозам. Большие массивы данных, аккумулируемые в ходе мониторинга цифровой среды, используются для построения математических моделей, которые отражают закономерности функционирования информационных систем и позволяют распознавать даже минимальные отклонения от нормы.

Процесс прогнозирования формируется на основе анализа широкого спектра информации. Интеллектуальные системы исследуют журналы событий, сетевые пакеты, динамику интернет-трафика, данные о ранее зарегистрированных инцидентах, содержимое тематических сообществ, изменения в активности участников теневых цифровых площадок, а также сведения о произошедших утечках данных. Одновременное изучение таких разнородных источников даёт возможность выявлять взаимосвязи и причинно-следственные структуры, которые зачастую остаются невидимыми при традиционном ручном анализе. В результате формируются комплексные профили угроз, отражающие не только специфику атакующих методов, но и потенциальные закономерности, по которым злоумышленники выбирают свои цели [3; 7].

Заключение

Предварительное моделирование киберугроз на основе алгоритмов ИИ формирует новый вектор развития информационной безопасности, позволяя преобразовать защитные механизмы из реактивных в проактивные. Интеллектуальные системы, анализирующие большие объёмы разнородных данных, обеспечивают раннее выявление потенциальных атак и создают условия для упреждающего укрепления корпоративной инфраструктуры, что существенно повышает уровень устойчивости организаций к современным киберрискам.

Литература

1. Алпеева О.И., Бушуева А.В. Применение цифровых технологий и искусственного разума при предупреждении преступности // Вестник Пензенского государственного университета. 2021. № 3. С. 54–62.

2. Герасимова Е.Б., Басенко И.К. Анализ перспектив использования искусственного интеллекта для обнаружения и предотвращения экономических преступлений // Экономические науки. 2024. № 5(234). С. 158–165. DOI: 10.14451/1.234.158.

3. Гозгешев Э.А. Искусственный интеллект в банковском секторе: возможности и риски // Вестник евразийской науки. 2024. Т. 16, № S6. С. 49.

4. Мамателашвили О.В. Риски и угрозы экономической безопасности организации / О.В. Мамателашвили, Э.Ф. Мухамадиева, Р.Ф. Хисамутдинова // Экономика и управление: научно-практический журнал. 2023. № 3(171). С. 43–46. DOI: 10.34773/EU.2023.3.8.

5. Перевертун Д.Р. Роль искусственного интеллекта в информационной безопасности // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9, № 5(43). С. 92–97.

6. Применение искусственного интеллекта на финансовом рынке. Доклад для общественных консультаций / Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/156061/Consultation_Paper_03112023.pdf

7. Юрченко А.И., Мамателашвили О.В. Концепция мониторинга эффективности системы экономической безопасности на предприятии // Экономика и управление: научно-практический журнал. 2023. № 5(173). С. 124–129. DOI: 10.34773/EU.2023.5.23.