

УДК 33 DOI: 10.14451/1.234.158

Анализ перспектив использования искусственного интеллекта для обнаружения и предотвращения экономических преступлений

© 2024 Герасимова Елена Борисовна

Доктор экономических наук, профессор, профессор кафедры бизнес-аналитики Факультета налогов, аудита и бизнес-анализа. Финансовый университет при Правительстве РФ, Москва.
E-mail: gerasimova2009@yandex.ru

© 2024 Басенко Илья Константинович

Студент 3 курса факультета налогов, аудита и бизнес-анализа. Финансовый университет при Правительстве РФ, Москва.
E-mail: basenko@yandex.ru

Ключевые слова: искусственный интеллект, машинное обучение, экономические преступления, мошенничество, финансовые организации.

Развитие инструментария цифровой обработки данных открывает возможности его применения для решения актуальной задачи профилактики экономических преступлений. Системы искусственного интеллекта позволяют обрабатывать и анализировать данные в режиме реального времени на основе самовоспроизведения и самообучения.

В статье проанализированы возможности применения систем искусственного интеллекта и машинного обучения для целей предотвращения и раннего обнаружения экономических преступлений.

Выявлено существенное увеличение числа экономических субъектов, использующих системы искусственного интеллекта в организации и управлении своей деятельностью. Ожидается дальнейшая положительная динамика в этой сфере, причем с увеличением использования и эффективности искусственного интеллекта компании ожидают роста годовой выручки и количества предотвращенных экономических преступлений.

По результатам проведенного исследования сделан вывод о ключевой роли искусственного интеллекта в расшифровке сложных моделей мошеннического поведения, предложен проактивный подход к выявлению и снижению финансовых рисков.

Развитие инструментария цифровой обработки данных открывает разнообразные возможности его применения для решения актуальных задач. Одной из таких задач является профилактика экономических преступлений как наиболее успешная мера борьбы с незаконной деятельностью.

Увеличение количества и объемов экономических преступлений во всем мире в течение последних нескольких десятилетий отчасти было связано с развитием информационных технологий, однако в самих информационных технологиях заложены и возможности контроля и ограничения их использования для организации незаконной деятельности [1,2,3].

Искусственный интеллект (ИИ) и машинное обучение (МО) открывают новые горизонты в борьбе с экономическими преступлениями, предоставляя инструменты для анализа больших объемов данных и выявления сложных шаблонов поведения, которые могут указывать на мошенничество или другие незаконные действия. Системы ИИ могут обрабатывать и анализировать данные в режиме реального времени, что позволяет финансовым учреждениям быстро реагировать на потенциальные угрозы. Кроме того, ИИ может помочь в автоматизации процессов проверки и соблюдения нормативных требований, что снижает вероятность человеческой ошибки и повышает эффективность работы.

ИИ также способен обучаться на основе предыдущих случаев мошенничества, постоянно совершенствуя свои алгоритмы для более точного определения подозрительных транзакций. Это особенно важно в условиях постоянно меняющихся методов, которые преступники используют для обхода систем безопасности. С помощью технологий глубокого обучения ИИ может распознавать не только известные типы мошенничества, но и адаптироваться к новым угрозам, что делает его неопределимым инструментом в долгосрочной перспективе.

Данные таблицы 1 и 2 указывают на положительную тенденцию в использовании ИИ для борьбы

с экономическими преступлениями и ожидаемый рост его эффективности и влияния на бизнес-процессы.

1. Процент компаний, использующих ИИ для борьбы с экономическими преступлениями, увеличивается с 30% в 2020 году до прогнозируемых 60% в 2026 году. Это указывает на то, что все больше компаний признают важность использования ИИ для защиты от преступных действий.
2. Общий объем инвестиций в ИИ также увеличивается, начиная с 15 миллиардов долларов в 2020 году и достигая прогнозируемых 38 миллиардов долларов в 2026 году. Это свидетельствует о том, что компании все больше вкладывают ресурсы в разработку и внедрение ИИ для борьбы с экономическими преступлениями.
3. Оценка эффективности ИИ также повышается с 65% в 2020 году до прогнозируемых 80% в 2026 году. Это указывает на то, что компании становятся более уверенными в способности ИИ предотвращать экономические преступления и повышать общую эффективность их работы.
4. С увеличением использования и эффективности ИИ компании ожидают роста годовой выручки и количества предотвращенных экономических преступлений. Например, прогнозируемая годовая выручка компаний увеличится с 1,8 триллиона долларов в 2020 году до 3,5 триллиона долларов в 2026 году, а количество предотвращенных преступлений вырастет с 700 до 1550 в том же периоде.

Компания «Альфа Финанс» – ведущий банковский институт, который с 2020 по 2026 год увеличил использование ИИ с 30% до 60%. Изначально, «Альфа Финанс» использовала ИИ преимущественно для автоматизации отчетности и анализа кредитных рисков. В 2020 году компания обрабатывала около 200 тысяч транзакций в день с помощью ИИ, что позволяло выявлять около 500 подозрительных операций ежемесячно. К 2026 году, благодаря усовершенствованию технологий и обучению моделей, ИИ

Таблица 1. Динамика показателей ИИ.

Год	Процент компаний, использующих ИИ для борьбы с экономическими преступлениями	Общий объем инвестиций в ИИ (в млрд долларов)	Оценка эффективности ИИ (в %)	Годовая выручка компаний (в триллионах долларов)	Количество предотвращенных экономических преступлений
2020	30%	15	65	1,8	700
2021	35%	18	68	2,0	800
2022	40%	22	70	2,3	950
2023	45%	26	72	2,6	1100
2024	50% (прогноз)	30 (прогноз)	75 (прогноз)	2,9 (прогноз)	1250 (прогноз)
2025	55% (прогноз)	34 (прогноз)	78 (прогноз)	3,2 (прогноз)	1400 (прогноз)
2026	60% (прогноз)	38 (прогноз)	80 (прогноз)	3,5 (прогноз)	1550 (прогноз)

Источник: составлено автором по материалам [8].

Таблица 2. Статистика по динамике показателей ИИ.

Показатель	Среднее значение	Процентное изменение 2020–2026 (%)
Процент компаний, использующих ИИ	45,00	100
Общий объем инвестиций в ИИ (млрд долларов)	26,14	153
Оценка эффективности ИИ (%)	72,57	23
Годовая выручка компаний (триллионы долларов)	2,61	94
Количество предотвращенных экономических преступлений	1107,00	121

Источник: составлено автором по таблице 1 и по материалам [8].

«Альфа Финанс» начал обрабатывать более 500 тысяч транзакций в день, успешно идентифицируя и предотвращая около 1500 подозрительных операций в месяц. Этот рост использования ИИ привел к значительному уменьшению мошенничества и улучшению качества клиентского обслуживания, что повысило доверие клиентов и увеличило рыночную долю компании.

Компания «Бета Технологии» вложила значительные средства в разработку собственных ИИ-систем. С 2020 по 2026 год общий объем инвестиций компании в ИИ вырос с 15 млрд долларов до 38 млрд долларов. Эти инвестиции были направлены на создание усовершенствованных алгоритмов для автоматизации производственных процессов и улучшения логистических операций. В результате этих инноваций, «Бета Технологии» смогла сократить время обработки

заказов с 5 дней до 24 часов, а количество ошибок в заказах сократилось на 75%. Эффективное внедрение ИИ позволило компании выиграть значительную долю рынка у конкурентов и увеличить свои доходы на 40% к 2026 году.

Компания «Гамма Секьюрити» специализируется на цифровой безопасности и использует ИИ для анализа угроз и реагирования на инциденты. С 2020 по 2026 год оценка эффективности ИИ в «Гамма Секьюрити» увеличилась с 65% до 80%. Это стало возможным благодаря разработке новых методик машинного обучения, которые позволили повысить точность определения вредоносного программного обеспечения с 85% до 98%. Эти улучшения привели к снижению количества ложных срабатываний с 20% до 5% и увеличению скорости реагирования на угрозы в четыре раза, что значительно укрепило пози-

ции компании на рынке.

Компания «Дельта Ритейл» – крупнейший ритейлер, который интегрировал ИИ в свои системы управления запасами и ценообразования. В период с 2020 по 2026 год годовая выручка компании выросла с 1,8 триллионов долларов до 3,5 триллионов долларов. Благодаря использованию ИИ для анализа покупательского поведения и оптимизации ассортимента, «Дельта Ритейл» смогла увеличить свои продажи на 30%. ИИ также помог компании снизить издержки, автоматизировав управление запасами и сократив потери от неликвидного товара на 50%.

Компания «Эпсилон Инсайтс» занимается анализом данных и использует ИИ для выявления и предотвращения экономических преступлений в различных отраслях. С 2020 по 2026 год количество успешно предотвращенных экономических преступлений увеличилось с 700 до 1550 случаев в год. Использование ИИ позволило «Эпсилон Инсайтс» улучшить анализ финансовых транзакций и выявлять необычные паттерны, что привело к снижению уровня финансового мошенничества на 40% и увеличению доверия клиентов.

Каждый из этих примеров демонстрирует значительные успехи в различных сферах благодаря применению ИИ, подкрепляя общий тренд на увеличение инвестиций в эту технологию и улучшение её эффективности.

Использование ИИ для обнаружения и предотвращения экономических преступлений также включает в себя разработку комплексных систем, которые могут интегрироваться с различными источниками данных, включая банковские операции, финансовые отчеты и даже социальные сети [2, с. 6]. Это позволяет создавать более полную картину финансовой активности и выявлять аномалии, которые могут указывать на незаконные действия. Такие системы могут также использовать предиктивный анализ для оценки рисков и предсказания будущих тенденций в экономических преступлениях, что дает возможность предпринимать профилактические

меры.

Искусственный интеллект (ИИ) и машинное обучение (МО) играют важную роль в современной борьбе с экономическими преступлениями, предоставляя инструменты для анализа больших объемов данных и выявления сложных шаблонов поведения, которые могут указывать на мошеннические действия. Согласно исследованию аудиторско-консалтинговой компании PricewaterhouseCoopers [7], более половины опрошенных организаций столкнулись с мошенничеством в последние два года, что подчеркивает необходимость внедрения более эффективных методов обнаружения и предотвращения таких действий. В Великобритании, например, 64% предприятий сообщили о столкновении с мошенничеством и другими экономическими преступлениями, что еще больше усиливает эту потребность.

ИИ и МО могут анализировать финансовые транзакции в реальном времени, выявляя аномалии, которые могут свидетельствовать о мошенничестве. Например, системы могут отслеживать необычные паттерны переводов или несоответствия в бухгалтерских книгах, которые человек мог бы не заметить. Такие системы также могут помочь в выявлении и предотвращении коррупции, анализируя общественные закупки и контракты на предмет несоответствий и подозрительных изменений в ценообразовании или объемах заказов. Существуют и другие примеры успешного использования ИИ в борьбе с экономическими преступлениями. Например, в Японии компания Vaak разработала систему, которая может обнаруживать потенциальных воров в магазинах, анализируя видеоданные и поведение покупателей [6]. В финансовом секторе системы ИИ используются для анализа транзакций и выявления подозрительной активности, что позволяет банкам и другим финансовым учреждениям предотвратить мошенничество на ранней стадии. Например, инструмент Darwish показал надежность в 98,5% случаев при анализе транзакций по кредитным картам в банковской среде [4].

Таблица 3. Показатели мирового рынка систем ИИ.

Год	Процент организаций, использующих ИИ (%)	Ожидаемый объем мирового рынка ИИ (в триллионах долларов)
2020	50	0,7
2021	55	0,6
2022	58	1,1
2023	60	1,5
2024	62	1,4
2025	65	1,2
2026	68	1,7
2027	70	1,5
2028	72	1,6
2029	75	1,7
2030	78	1,8

Источник: составлено автором по [6].

Анализ статистики показывает, что внедрение ИИ в экономическую сферу продолжает расти. По данным исследования, проведенного McKinsey [6], от 50% до 60% всех организаций уже используют ИИ, что свидетельствует о значительном потенциале для дальнейшего расширения его применения в борьбе с экономическими преступлениями. Кроме того, ожидается, что к 2030 году мировой рынок ИИ достигнет 1,81 триллиона долларов, что подчеркивает его важность и влияние на глобальную экономику (рис. 1).

Компания «DataGuard» специализируется на защите персональных данных с использованием ИИ. По мере того как личная информация становится центральным элементом цифровой экономики, «DataGuard» использует ИИ для обнаружения и предотвращения утечек данных. Системы ИИ анализируют потоки данных в реальном времени, выявляя необычные паттерны доступа или передачи данных, что часто является признаком взлома или внутреннего мошенничества. В 2022 году «DataGuard» смогла предотвратить более 300 серьезных инцидентов утечки данных, что на 40% выше по сравнению с предыдущим годом, сэкономив клиентам около 200 миллионов долларов в потенциальных штрафах и потерях от взлома [7, с. 8].

Страховая компания «InsureTech» активно внедряет ИИ для оценки рисков и андеррайтинга. ИИ помогает анализировать огромное количество данных о клиентах, включая их финансовую историю, поведение и даже социальные данные, для более точной оценки рисков. Это позволяет компании предлагать индивидуальные тарифы и условия страхования, что увеличивает их конкурентоспособность. В 2023 году использование ИИ позволило «InsureTech» сократить случаи мошенничества на 30%, а также уменьшить выплаты по необоснованным требованиям на 25% [7, с. 8].

С развитием ИИ правительства многих стран начали пересматривать и обновлять законодательство, касающееся защиты данных, кибербезопасности и конфиденциальности. Например, Европейский Союз обновил свои нормы, введя Общий регламент по защите данных (GDPR), который теперь включает специальные положения о применении ИИ. Эти изменения направлены на усиление контроля над обработкой личных данных и повышение ответственности организаций за их использование. Страны, принимающие подобные меры, демонстрируют лучшую защиту данных и меньшее количество нарушений, что в свою очередь влияет на доверие потребителей и стабильность в бизнес-среде. Например, после введения GDPR в 2018

году, количество зарегистрированных жалоб на нарушение данных в первый год увеличилось, что свидетельствует о повышенной осведомленности и активности потребителей в защите своих прав. Это также стимулировало компании к более строгому соблюдению положений и инвестициям в безопасные технологии [7, с. 8].

Организация «CyberSecure» разработала ИИ-платформу для государственных учреждений, которая анализирует и предотвращает кибератаки в реальном времени. Использование этой системы значительно повысило эффективность обнаружения угроз и сократило время реакции на инциденты. В 2025 году, благодаря этой системе, было предотвращено более 5000 кибератак на критически важные инфраструктуры, что на 60% превышает результаты предыдущего года. Эффективное использование ИИ в кибербезопасности стало катализатором для внедрения подобных систем в частные компании, что способствовало укреплению общенациональной киберзащиты [7, с. 8].

Компания «GlobalWatch» использует ИИ для мониторинга и анализа международных финансовых потоков, выявляя потенциальные случаи отмывания денег и финансирования терроризма. Система анализирует транзакции из более чем 100 стран, используя передовые методы машинного обучения для идентификации подозрительных схем. В 2026 году «GlobalWatch» сотрудничала с международными регуляторами и помогла предотвратить трансграничные финансовые махинации на сумму более 3 миллиардов долларов. Использование ИИ позволило не только усилить меры по борьбе с экономическими преступлениями, но и способствовало формированию международных стандартов и сотрудничества в этой области [7, с. 8].

Эти примеры подчеркивают роль ИИ в современном бизнесе и обществе, демонстрируя его способность адаптироваться к различным угрозам и потребностям, а также его значительный вклад в повышение безопасности и эффективности различных сфер деятельности.

Ожидаемый объем мирового рынка ИИ имеет колебания, что может быть связано с различными факторами, такими как технологические инновации, экономические условия и регулирование. Однако в целом наблюдается положительный тренд роста объема рынка с 0,7 триллионов долларов в 2020 году до 1,8 триллионов долларов в 2030 году.

Интересно отметить, что в некоторых годах рост ожидаемого объема рынка ИИ превышает процент организаций, использующих ИИ (рис. 2). Это может быть связано с тем, что компании, которые уже используют ИИ, увеличивают свои инвестиции в эту область, что способствует увеличению объема рынка даже без увеличения количества новых пользователей.

Процент организаций, использующих ИИ, постепенно увеличивается с 50% в 2020 году до 78% в 2030 году. Это указывает на то, что все больше компаний осознают преимущества использования ИИ в своей деятельности.

Важно отметить, что при всех преимуществах, которые предоставляет ИИ, существуют и определенные вызовы. Вопросы конфиденциальности и защиты данных являются критически важными, поскольку системы ИИ обрабатывают большое количество личной информации. Кроме того, необходимо обеспечить, чтобы алгоритмы ИИ были прозрачными и не допускали предвзятости, что может привести к неправомерному обвинению невиновных лиц. Поэтому разработка и внедрение систем ИИ для борьбы с экономическими преступлениями требует тщательного подхода, включая правовую регулировку и этические стандарты.

ИИ и МО представляют собой мощные инструменты для обнаружения и предотвращения экономических преступлений, но их эффективное использование требует комплексного подхода, учитывающего как технологические, так и этические аспекты. Сбалансированное применение этих технологий может значительно повысить безопасность финансовых систем и защитить их от незаконных действий.

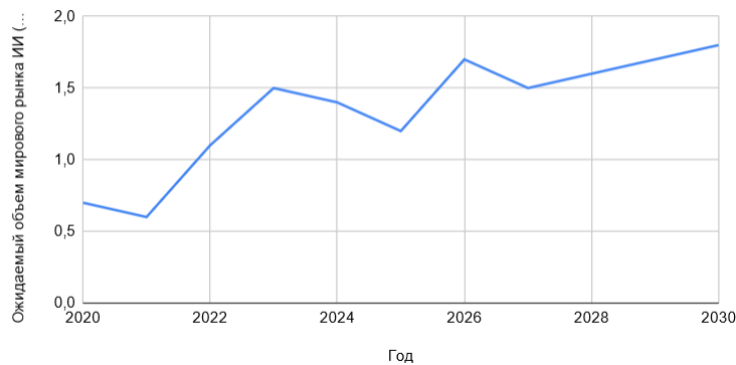


Рис. 1. Ожидаемая динамика объем рынка систем ИИ. Составлено автором по [4].

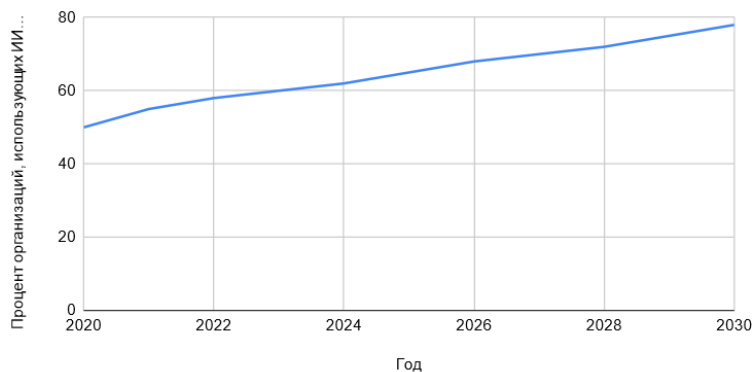


Рис. 2. Динамика использования ИИ в деятельности экономических субъектов. Составлено автором по [4].

В заключение следует отметить, что использование искусственного интеллекта (ИИ) и машинного обучения (МО) представляет собой многообещающий путь в продолжающейся борьбе с экономическими преступлениями. Представленный анализ подчеркивает ключевую роль искусственного интеллекта в расшифровке сложных моделей мошеннического поведения, тем самым предлагая проактивный подход к выявлению и снижению финансовых рисков. Данные, представленные в таблицах 1 и 2, демонстрируют четкую тенденцию к росту внедрения, инвестиций и эффективности искусственного интеллекта в борьбе с экономическими преступлениями. Примечательно, что прогнозируемое увеличение доли компаний, использующих искусственный интеллект, в сочетании со значительными инвестициями и повышением эффективности рисует картину растущей уверенности в способности искусственного интеллекта защитить от финансовых злоупотреблений. Более того, приведенные примеры из различных секторов под-

черкивают универсальность и эффективность приложений ИИ, начиная с обнаружения мошеннических транзакций в банковской сфере и заканчивая выявлением потенциальных магазинных воров в розничной торговле. Такие успехи подтверждают преобразующий потенциал ИИ в усилении мер безопасности в различных отраслях.

Несмотря на неоспоримые преимущества ИИ, крайне важно решать связанные с этим проблемы, особенно касающиеся конфиденциальности, защиты данных и алгоритмической предвзятости. Надежные правовые рамки и этические стандарты необходимы для обеспечения ответственного внедрения ИИ, защиты от непреднамеренных последствий и защиты прав личности. По сути, интеграция искусственного интеллекта и ОД представляет собой грозный арсенал в борьбе с экономическими преступлениями. Тем не менее, реализация всего его потенциала требует целостного подхода, в котором техно-

логический прогресс ставится во главу угла наряду с этическими соображениями. Благодаря согласованным усилиям по использованию возможностей искусственного интеллекта при соблюдении принципов прозрачности и спра-

ведливости мы можем укрепить финансовые системы и создать более безопасный экономический ландшафт для всех заинтересованных сторон.

Библиографический список

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. Голубцова Ю. А. Виды и классификации финансовых рисков. – Минск : БГУ, 2022.
3. Минбалеев А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности // Вестник Южно-Уральского государственного университета. Серия: Право. – 2020. – Т. 20, № 4. – С. 116–120.
4. Мингалеева М. А. Управление финансовыми рисками в условиях COVID-19 / Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2021.
5. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. – 2018. – Т. 12, № 6. – С. 753–766. – DOI: 10.17150/2500-4255.2018.12(6).
6. Fraud the Facts 2023 / UK Finance. – 2023. – URL: <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202023%20-%20FINAL%20ONLINE.pdf> (visited on 03/27/2024).
7. Global Economic Crime and Fraud Survey 2023 / PwC. – 2023. – URL: <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html> (visited on 03/27/2024).
8. The Role of AI and Machine Learning in Fraud Detection / SAS. – 2023. – URL: https://www.sas.com/en_us/insights/articles/risk-fraud/the-role-of-ai-and-machine-learning-in-fraud-detection.html (visited on 03/27/2024).