



Научная статья

УДК 339 (075)

<https://doi.org/10.24412/2687-0185-2025-4-199-203>

EDN: <https://elibrary.ru/ACEIRH>

НИОН: 2007-0083-4/25-749

MOSURED: 77/27-005-2025-04-949

Роль искусственного интеллекта в повышении экономической безопасности предприятий в условиях автоматизации производственных процессов

Кирилл Игоревич Антоненков

Московский авиационный институт (национальный исследовательский университет), Москва, Россия, kikipkf@mail.ru

Аннотация. Раскрывается роль искусственного интеллекта (ИИ) в повышении экономической безопасности предприятий при автоматизации производственных процессов. Подчеркивается, что ИИ становится ключевым инструментом для мониторинга финансовых операций, управления рисками, защиты интеллектуальной собственности, оптимизации закупок, управления дебиторской задолженностью и обеспечения кибербезопасности. Акцентируется внимание на необходимости комплексного подхода к внедрению ИИ, включая обеспечение качественных данных.

Ключевые слова: искусственный интеллект, экономическая безопасность, автоматизация, риски, кибербезопасность

Для цитирования: Антоненков К. И. Роль искусственного интеллекта в повышении экономической безопасности предприятий в условиях автоматизации производственных процессов // Криминологический журнал. 2025. № 4. С. 199–203. <https://doi.org/10.24412/2687-0185-2025-4-199-203>. EDN: ACEIRH.

Original article

The role of artificial intelligence in enhancing the economic security of enterprises in the context of production process automation

Kirill I. Antonenkov

Moscow Aviation Institute (National Research University), Moscow, Russia, kikipkf@mail.ru

Abstract. The role of artificial intelligence (AI) in increasing the economic security of enterprises in automating production processes is revealed. It is emphasized that AI is becoming a key tool for monitoring financial transactions, risk management, intellectual property protection, procurement optimization, accounts receivable management, and cybersecurity. Attention is focused on the need for an integrated approach to the implementation of AI, including providing high-quality data.

Keywords: artificial intelligence, economic security, automation, risks, cybersecurity

For citation: Antonenkov K. I. The role of artificial intelligence in enhancing the economic security of enterprises in the context of production process automation. Criminological Journal. 2025;(4):199–203. (In Russ.). <https://doi.org/10.24412/2687-0185-2025-4-199-203>. EDN: ACEIRH.

В эпоху цифровизации и повсеместной автоматизации производственных процессов вопросы экономической безопасности предприятий приобретают особую актуальность. Интеллектуальные системы, основанные на искусственном интеллекте, становятся ключевым инструментом в обеспечении устойчивого развития и защиты от возникающих угроз. Внедрение ИИ в экономическую безопасность предприятий по-

зволяет значительно повысить эффективность процессов, снизить риски и оптимизировать затраты.

Актуальность исследования роли искусственного интеллекта в повышении экономической безопасности предприятий в условиях автоматизации производственных процессов обусловлена несколькими ключевыми факторами.

Во-первых, цифровизация и автоматизация про-



изводственных процессов хотя и приносят значительные выгоды в виде повышения эффективности, снижения затрат и улучшения качества продукции, в то же время порождают новые и сложные риски для экономической безопасности предприятий. Традиционные методы обеспечения безопасности оказываются недостаточными для противодействия современным угрозам, требуя инновационных подходов, одним из которых и является применение технологий искусственного интеллекта.

Во-вторых, экономическая безопасность предприятий включает в себя широкий спектр направлений, таких, как защита от финансовых махинаций, предотвращение утечки конфиденциальной информации, обеспечение устойчивости к кибератакам, оптимизация управления рисками и соблюдение нормативных требований. Искусственный интеллект обладает потенциалом в каждом из этих направлений. Системы ИИ могут анализировать существенные объемы данных для выявления аномалий и подозрительных операций, предсказывать потенциальные угрозы на основе анализа данных и тенденций, автоматизировать процессы мониторинга и реагирования на инциденты, а также адаптироваться к меняющимся условиям.

В-третьих, в условиях глобальной конкуренции и нестабильности экономической среды защита активов и конкурентных преимуществ становится приоритетной задачей для каждого предприятия. Успешное внедрение ИИ для повышения экономической безопасности не только снижает риски потерь и убытков, но и способствует укреплению доверия со стороны инвесторов, партнеров и клиентов. Более того, компании, активно использующие ИИ для обеспечения безопасности, получают конкурентные преимущества за счет повышения эффективности, инновационности и адаптивности [2, поз. 27].

Рост внедрения ИИ в финансовом секторе (таблица 1) закономерно сопровождается увеличением инвестиций в технологии кибербезопасности и защиты от мошенничества (таблица 2). Это связано с тем, что расширение цифровых финансовых услуг требует более совершенных механизмов защиты данных и транзакций. В таблице 1 раскрыты данные по росту ИИ в реализации бизнес-процессов предприятий.

Так, демонстрируется устойчивый рост рынка ИИ в финтехе, что подчеркивает значимость технологий искусственного интеллекта для финансового сектора. Несмотря на относительно низкий среднегодовой темп роста (2,91 %), прогнозируемое увеличение объема рынка с 42,83 млрд долларов в 2023 г. до 49,43 млрд долларов в 2028 г. свидетельствует о стабильном спросе на ИИ-решения. Это может быть связано с тем, что финансовые учреждения стремятся повысить эффективность процессов, снизить операционные издержки и улучшить качество обслуживания клиентов. Рост

рынка также отражает тенденцию к автоматизации и цифровизации финансовых услуг, что становится неотъемлемой частью современной экономики.

Таблица 1

**Данные по росту ИИ
в реализации бизнес-процессов
предприятий [6, п. 14]**

Год	Объем рынка (млрд долларов)
2021	38.5
2022	41.0
2023	42.83
2024	44.1
2025	45.4
2026	46.7
2027	48.1
2028	49.43
2029	51.0
2030	52.5

Таблица 2

**Инвестиции в системы ИИ
для кибербезопасности и обнаружения
мошенничества [6, п. 18]**

Год	Объем инвестиций (млрд долларов)
2021	5.8
2022	6.5
2023	7.2
2024	7.9
2025	8.6
2026	9.3
2027	10.0
2028	10.8
2029	11.6
2030	12.5

Анализируя вышеозначенное, можно отметить значительное увеличение инвестиций в системы ИИ для кибербезопасности и обнаружения мошенничества. Если в 2022 г. компании направили 6,5 млрд долларов на эти цели, то к 2027 г. этот показатель возрастет до 10 млрд долларов. Такой рост инвестиций объясняется увеличением числа киберугроз и мошеннических атак в условиях роста цифровых транзакций. Финансовые учреждения осознают необходимость внедрения передовых технологий для защиты данных клиентов и предотвращения финансовых потерь. Это также подтверждает значимость ИИ как ключевого инструмента в борьбе с киберпреступностью.

Как видно из данных, объем рынка ИИ в финтехе к 2028 г. достигнет 49,43 млрд долларов, а инвестиции



в ИИ для кибербезопасности за тот же период составят 10,8 млрд долларов. Такая динамика подтверждает, что компании уделяют особое внимание не только автоматизации процессов, но и минимизации рисков, связанных с цифровизацией.

Более высокие темпы роста инвестиций в безопасность (CAGR ~8,4 % против 2,91 % в общем рынке финтех-ИИ) показывают, что защита активов становится критически важным направлением развития технологий искусственного интеллекта [6, п. 27].

Сравнение данных из двух таблиц позволяет сделать вывод о том, что кибербезопасность и обнаружение мошенничества являются одними из приоритетных направлений использования ИИ в финтехе. Значительная доля инвестиций в эти технологии (более 10 млрд долларов к 2027 г.) указывает на их высокую актуальность. В то же время, общий рост рынка ИИ в финтехе (до 49,43 млрд долларов) говорит о том, что другие направления, такие, как кредитный скоринг, чат-боты и количественное управление активами, также продолжают развиваться.

Внедрение ИИ радикально меняет подходы к выполнению широкого набора задач, что оказывает глубокое воздействие на динамику развития финансовой отрасли. Под влиянием цифровизации ИИ приобретает качество необходимого элемента для формирования устойчивых конкурентных преимуществ и становится неотъемлемым компонентом стратегического планирования предприятий в современной экономике.

Особое значение приобретает использование ИИ в автоматизированных системах мониторинга и оценки финансовых транзакций. При том что традиционные средства контроля, подразумевающие участие человека, оказываются недостаточно эффективными при значительном потоке информации и стремительных изменениях операций, интеллектуальные платформы демонстрируют способность мгновенно обнаруживать нетипичные события, выявлять попытки мошенничества и реагировать на потенциальные угрозы до возникновения ощутимых убытков. За счет подобных возможностей ИИ реализует функции проактивного реагирования, минимизируя риски и финансовые издержки.

Значимым аспектом становится применение аналитических механизмов ИИ для управления неопределенностью и оценки потенциальных кризисов. Комплексный анализ разнородных массивов данных, включающих как статистическую финансовую отчетность и параметры рынка, так и информацию из новостных ресурсов и социальных медиаплатформ, позволяет алгоритмам искусственного интеллекта выявлять тонкие структурные связи и скрытые тренды. В результате предприятия получают инструментарий для выявления сложных причинно-следственных отношений, своевременного прогнозирования неблагоприятных событий и разработки превентивных стра-

тегий. В условиях нестабильности внешней среды именно такие интегрированные интеллектуальные решения становятся определяющими в обеспечении устойчивости бизнеса [3, с. 7].

Применение искусственного интеллекта в механизмах охраны конфиденциальных сведений и интеллектуальных активов выражается, прежде всего, в комплексном отслеживании цифровых коммуникаций, диагностике несанкционированных попыток доступа и систематическом выявлении возможных каналов утечки критически значимых данных. Специализированные платформы, функционирующие на ИИ-алгоритмах анализа пользовательских моделей взаимодействия, обеспечивают эффективную идентификацию атипичных паттернов поведения работников, что позволяет своевременно предупредить инциденты, обусловленные человеческой небрежностью или злоумышленными действиями.

Благодаря внедрению передовых технологий машинного обучения, анализ закупочных процедур и контрактных соглашений приобретает дополнительный уровень прозрачности. Искусственный интеллект, обрабатывая массивы информации о поставщиках, условиях сделок, исторической динамике цен, способен фиксировать нетипичные отклонения в транзакциях, что служит индикатором потенциальных коррупционных механизмов либо проявлений недобросовестной конкуренции. В результате повышается открытость процессов снабжения, а потенциал возникновения рисков при взаимодействии с недобросовестными субъектами значительно минимизируется [4, с. 268].

В контексте управления дебиторской задолженностью применение интеллектуальных вычислительных систем позволяет смоделировать вероятность дефолта, выявлять клиентов с наибольшей степенью кредитного риска и формулировать инструменты возврата долговых обязательств. С помощью автоматизированных платформ кредитного скоринга, использующих анализ больших данных, организации способны значительно повысить точность оценки финансовой благонадежности контрагентов и применять обоснованные подходы к предоставлению кредитных лимитов.

Актуализация задач защиты информации возрастает вместе с усилением технологической автоматизации производственных цепочек. С применением искусственного интеллекта возможно строить барьеры для несанкционированных попыток проникновения в индустриальные управляющие комплексы, а также выявлять вредоносные программы на ранней стадии и препятствовать вторжению в жизненно важные компоненты инфраструктуры. Алгоритмы ИИ, интегрированные в средства мониторинга сетевой активности, способны детектировать нестандартные процессы и подозрительные действия, что существенно повышает скорость реагирования на поступающие



угрозы кибербезопасности и минимизирует риски возникновения производственных перебоев.

Реализация искусственного интеллекта в задачи обеспечения экономической защищенности корпоративных структур требует всестороннего анализа специфики бизнеса и продуманного проектирования соответствующих механизмов. Ключевое значение приобретает корректное формулирование целевых ориентиров, грамотный подбор технологических решений и создание комплексных процедур внедрения, подстроенных под индивидуальные особенности предприятия. Немаловажно организовать систематическую подготовку сотрудников и наладить инфраструктуру поддержки для полноценного раскрытия потенциала интеллектуальных систем.

Приоритетным условием результативности считается обеспечение качественной эмпирической базы, поскольку функционирование ИИ построено на работе с большими массивами данных. Для этого компаниям необходимо наладить процессы аккумулирования, обработки и хранения информации с соблюдением стандартов безопасности и строгой конфиденциальности.

Этические соображения, связанные с применением искусственного интеллекта, требуют детального рассмотрения, поскольку только размещение акцентов на обеспечении отчетности и ясности работы алгоритмических моделей способно предотвратить появление и закрепление предвзятых суждений либо несправедливых различий. Перспективный вектор внедрения ИИ в систему обеспечения экономической безопасности предприятий способен не просто трансформировать традиционные процедуры и минимизировать возможные угрозы, но и выступить инструментом для ощутимого повышения эффективности, а также рационализации издержек. Тем не менее, практический успех таких инноваций во многом обусловлен точной адаптацией под специфику хозяйственной деятельности организации, организацией доступа к верифицированным и релевантным массивам данных, а также неукоснительным соблюдением норм этического кодекса [5, с. 81].

Применение искусственного интеллекта в авиационной транспортной сфере становится критическим инструментом для поддержания экономической устойчивости: он интегрируется в процессы управления данными, совершенствует системы логистического планирования, а также отвечает за предотвращение киберинцидентов и обеспечение защиты информации. Благодаря ИИ оптимизируются затраты, снижается вероятность финансовых потерь, и повышается надежность полетных операций, что позволяет снизить совокупные риски авиакомпаний в условиях постоянной угрозы как со стороны цифровых нарушителей, так и в аспекте эксплуатационной безопасности.

1. В целях минимизации риска мошеннических

действий при продаже авиабилетов ведущие перевозчики внедряют искусственный интеллект для скрупулезной проверки транзакционных данных и оперативного определения аномалий, связанных с подозрительными сценариями покупок, такими, как, скажем, повторяющиеся групповые бронирования с последующим их аннулированием или использование компрометированных платежных инструментов. Так, British Airways реализовала продвинутую интеллектуальную платформу, нацеленную на автоматическое подавление потенциально мошеннических финансовых операций, что позволило добиться 30-процентного сокращения финансовых потерь за счет осуществления мгновенной блокировки транзакций, несущих признаки обмана.

2. В последние годы возрастающее число инцидентов киберугроз направлено на авиационные структуры: хакеры все чаще выбирают в качестве целей как авиаперевозчиков, так и инфраструктуру аэропортов, нацеливаясь, в частности, на системы бронирования или платформы, управляющие воздушным движением. Инновационный подход продемонстрировали Dubai Airports, где в 2023 г. внедрили автоматизированные ИИ-системы для анализа сетевого трафика и комплексного наблюдения за цифровой средой. Благодаря интеграции этих интеллектуальных алгоритмов удалось своевременно заблокировать и предотвратить свыше двух сотен попыток несанкционированного проникновения в корпоративные цифровые ресурсы за год.

3. ИИ-технологии, анализируя погодные условия, трафик в аэропортах, а также параметры маршрутов, позволяют существенно минимизировать издержки, связанные с потреблением топлива авиационными компаниями. Так, динамическая маршрутизация, интегрированная в процессы Lufthansa, позволила добиться снижения расходов на горючее до пяти процентов на каждом рейсе, благодаря внедрению интеллектуальной платформы, способной адаптивно перестраивать траекторию полета на основе оперативной информации о загрузке аэродромов и метеофакторах.

4. Авиаперевозчики осуществляют обработку масштабных массивов сведений личного характера, включающих идентификационные данные путешественников, а также биометрические показатели. Например, внедрение искусственного интеллекта в компании Delta Airlines позволяет не только реализовывать криптографические протоколы при работе с данными, но и эффективно отслеживать потенциальные инциденты информационной безопасности. Подобная практика отвечает стандартам GDPR, обеспечивая соответствие корпоративных процедур нормативным предписаниям и минимизируя вероятность применения санкций со стороны регулирующих органов.



5. С применением алгоритмов искусственного интеллекта авиаперевозчики получили возможность значительно минимизировать финансовые потери, возникающие вследствие частичной загрузки рейсов, посредством адаптивного управления стоимостью билетов и прогностического анализа покупательского поведения. Например, компания Air France-KLM посредством внедрения интеллектуальных систем прогнозирования рыночной активности и актуализации тарифов в оперативном режиме смогла добиться увеличения валовой выручки на 7 %.

Как и в финтехе, отрасль авиаперевозок демонстрирует, что инвестиции в ИИ для экономической безопасности (киберзащита, например) и операционной эффективности (логистика, ценообразование) напрямую влияют на прибыль и устойчивость бизнеса. Компании, которые внедряют эти технологии, не только снижают риски, но и получают значительное конкурентное преимущество в условиях цифровизации.

В заключение стоит отметить, что ИИ – это инструмент, который может быть эффективным только при правильном применении. Поэтому предприятиям необходимо тщательно планировать и контролировать процесс внедрения ИИ, чтобы получить максимальную отдачу от инвестиций.

Стратегическое использование ИИ в экономической безопасности позволяет предприятиям не только защититься от угроз, но и получить конкурентные преимущества за счет оптимизации процессов, снижения затрат и повышения эффективности.

Таким образом, предприятия, которые активно внедряют ИИ в свою деятельность, будут иметь значительное преимущество перед конкурентами в условиях цифровой экономики.

Список источников

1. Петрова И. В., Чернухина Р. В. Автоматизация технологических процессов и производств. Н.: Новосибирский государственный технический университет, 2020.
2. Национальный портал в сфере искусственного интеллекта (2024): В «Сбере» 40 % решений по выдаче кредитов корпоративным клиен-

там принимает ИИ // URL: <https://ai.gov.ru/mediacenter/v-sbere-40-resheniy-po-vy-dache-kreditov-korporativnym-klientam-prinimaet-ii/?pageStart=23&lastGrand=1>

3. Винокурова С. ИИ в помощь: как МТС Банк оценивает заемщиков с помощью новых технологий // URL: <https://www.forbes.ru/special/newreality/ii-v-pomoshch>
4. Шишов О. В. Современные средства АСУ ТП. М. : Инфра-Инженерия, 2021.
5. Щетинина Н. Ю. Индустрия 4.0: практические аспекты реализации в российских условиях // Модели, системы, сети в экономике, технике, природе и обществе. 2017. С. 75–84.
6. Mordor Intelligence. AI in Fintech Market (2022–2027) // URL: <https://www.mordorintelligence.com/industry-reports/ai-in-fintech-market-size#:~:text=The%20AI%20>

References

1. Petrova I. V., Chernukhina R. V. Automation of technological processes and production. N. : Novosibirsk State University of technology, 2020.
2. National portal in the field of artificial intelligence (2024): AI makes 40% of decisions on granting loans to corporate clients in Sberbank // URL: <https://ai.gov.ru/mediacenter/v-sbere-40-resheniy-po-vy-dache-kreditov-korporativnym-klientam-prinimaet-ii/?pageStart=23&lastGrand=1>
3. Vinokurova S. AI to help: how MTS Bank evaluates borrowers using new technologies // URL: <https://www.forbes.ru/special/newreality/ii-v-pomoshch>
4. Shishov O. V. Modern automated process control systems. M. : Infra-Engineering, 2021.
5. Shtetynina N. Yu. Industry 4.0: practical aspects of implementation in Russian conditions // Models, systems, and networks in economics, technology, nature, and society. 2017. P. 75–84.
6. Mordor Intelligence. AI in Fintech Market (2022–2027) // URL: <https://www.mordorintelligence.com/industry-reports/ai-in-fintech-market-size#:~:text=The%20AI%20>

Информация об авторе

К. И. Антоненков – аспирант Московского авиационного института (национального исследовательского университета).

Information about the author

K. I. Antonenkov – Graduate student of the Moscow Aviation Institute (National Research University).

Статья поступила в редакцию 01.07.2025; одобрена после рецензирования 10.07.2025; принята к публикации 17.07.2025.

The article was submitted 01.07.2025; approved after reviewing 10.07.2025; accepted for publication 17.07.2025.