ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

УДК 343:004.8

Трансформация преступности в условиях развития технологий искусственного интеллекта

Евгений Владимирович Шаповалов[1,2]
[1]Следственное управление Следственного комитета Российской Федерации по Липецкой области, Липецк, Россия
[2]Липецкий государственный технический университет, Липецк, Россия

Аннотация. Развитие искусственного интеллекта оказывает влияние на трансформацию преступности, а также на ее количественные и качественные характеристики. В работе рассматриваются способы использования искусственного интеллекта в преступной деятельности. Анализируются проблемы практики расследования преступлений, совершенных с использованием интеллектуальных систем, прежде всего, их доступность для широкого круга лиц и отсутствие правовой регламентации. Автор отмечает, что искусственный интеллект позволяет повысить эффективность преступной деятельности за счет ее автоматизации, масштабируемости и персонализации. Интеллектуальные системы помогают формировать анонимную инфраструктуру для передачи и размещения необходимых для совершения противоправных деяний вредоносных инструментов, инструкций и файлов. Они обеспечивают через шифрованные мессенджеры коммуникацию и взаимодействие между различными участниками преступных групп и сообществ.

Ключевые слова: искусственный интеллект, технология «дипфейк», генеративный контент, трансформация преступности, чат-бот, безопасность

Для цитирования: Шаповалов Е.В. Трансформация преступности в условиях развития технологий искусственного интеллекта // Правда и закон. 2026. № 2(36). С. 64–69.

The transformation of crime in the context of the development of artificial intelligence technologies

Evgeny V. Shapovalov[1,2]
[1]Investigative Department of the Investigative Committee of the Russian Federation for the Lipetsk region, Lipetsk, Russia
[2]Lipetsk State Technical University, Lipetsk, Russia

Abstract. The development of artificial intelligence is impacting the transformation of crime, as well as its quantitative and qualitative characteristics. This paper examines the use of artificial intelligence in criminal activity. It analyzes the challenges of investigating crimes committed using intelligent systems, primarily their widespread accessibility and the lack of legal regulation. The author notes that artificial intelligence can improve the effectiveness of criminal activity through automation, scalability, and personalization. Intelligent systems help create an anonymous infrastructure for the transmission and deployment of malicious tools, instructions, and files necessary for

© Шаповалов Е.В., 2026

committing illegal acts. They facilitate communication and interaction between various members of criminal groups and communities via encrypted messengers.

Keywords: artificial intelligence, deepfake technology, generative content, crime transformation, chatbot, security

For citation: Shapovalov E.V. The transformation of crime in the context of the development of artificial intelligence technologies // Truth and law. 2026. № 2(36). P. 64–69.

Смена технологического уклада оказала глобальное влияние на все сферы жизни общества, изменяя экономические модели, социальные структуры, политические системы и повседневное поведение человека. Компьютеры, сеть Интернет, робототехника и искусственный интеллект стали неотъемлемой частью трансформационных процессов и являются основными катализаторами перехода в цифровую эпоху. Они активно применяются, как в решении повседневных задач, так и в проведении глобальных научных исследований.

Сегодня все более значимую роль в поведении человека стал играть искусственный интеллект (ИИ), который интегрирован в смартфоны, социальные сети, поисковые системы и сервисы рекомендаций, оказывая определенное влияние на принятие решений, формирование предпочтений, потребление информации, социальное взаимодействие. Потенциал и сферы применения данной технологии становятся все более заметными. Наряду с этим, все большую актуальность приобретают вопросы, связанные с безопасностью и рисками использования ИИ в преступных целях.

Важно отметить, что эта проблема вызывает значительную обеспокоенность среди граждан Российской Федерации. Согласно исследованию, проведенному Аналитическим центром «ВЦИОМ» совместно с Национальным центром развития искусственного интеллекта при Правительстве Российской Федерации, лидирующее положение среди угроз, связанных с использованием ИИ в ближайшей перспективе (5 лет), занимает рост преступлений с использованием данной технологии. Такой позиции придерживаются следующие категории опрошенных: 63 % разработчиков ИИ, 60 % представителей бизнеса, 52 % ученых в области ИИ[1].

Масштаб применения программных продуктов с ИИ в настоящий момент остается неопределенным. Во многом сложившаяся ситуация обусловлена следующими причинами.

Прежде всего, отсутствие концептуального понимания, что такое ИИ и каким критериям он должен соответствовать. Авторы, представляющие различные области научных исследований, включают в ИИ собственный набор технологий и сервисов. В специальной литературе выделяют от восьми до тринадцати признаков, которые отличают данную технологию от других [1, 2]. Помимо этого, размывание границ между концепциями «Слабого ИИ» (Narrow AI) и «Сильного ИИ» (General AI), а также их некорректное смешивание значительно затрудняет объективную оценку реальных возможностей технологии и адекватное прогнозирование связанных с ней рисков.

Необходимо также учитывать, что развитие облачных вычислений и предоставление облачными провайдерами соответствующих цифровых инструментов, использование открытого программного обеспечения и готовых моделей, а также появление возможности получения доступа к ним через API сделало данную технологию массовой и доступной для широкого круга лиц. С другой стороны, крупные компании (банки, технологические компаний и т.п.) ведут проприетарные и внутренние разработки в области создания новых моделей ИИ, которые закрыты для открытого рынка и требуют значительных финансовых вложений и ресурсов.

[1] Труд создал человека, а человек создал ИИ … что дальше? Искусственный интеллект вносит в сферу труда не только инновации, но и риски. Киберпреступность и автоматизация труда – главные вызовы ближайших лет // ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/trud-sozdal-cheloveka-a-chelovek-sozdal-ii-chto-dalshe (дата обращения: 15.11.2025).

Рынок технологий, связанных с ИИ, в настоящее время является крайне привлекательным для инвесторов[2].

Отсутствие надлежащей законодательной базы, связанной с применением ИИ, представляет значительную проблему. Правовая неопределенность, особенно в вопросах совершения преступлений с ИИ, создает трудности для их квалификации и расследования, а также благоприятные условия для безнаказанности преступников. Кроме того, нуждаются в правовой оценке «цифровые данные, сгенерированные или обработанные с использованием ИИ», с позиции допустимости этих доказательств в суде. Пока законодатели пытаются выработать подходы к правовому регулированию данной технологии, она уже активно применяется для совершения преступлений.

Российские специалисты в области кибербезопасности отмечают, что роль ИИ в противоправной деятельности будет возрастать. Прогнозируется, что интеллектуальные системы получат более широкое применение при совершении кибератак, включая создание с помощью ИИ более убедительных дипфейков, автоматизацию фишинга для массовых атак. Они позволят быстро совершенствовать и масштабировать преступные схемы[3].

Одним из специфичных способов использования ИИ при совершении преступлений является манипулятивный «промпт-инжиниринг». Злоумышленники используют методы ролевой симуляции и контекстной подмены для обхода фильтров безопасности системы и мер защиты нейросетей. Посредством формулирования запросов, содержащих фиктивные сценарии (например, в форме написания художественного произведения или сказки), преступники стремятся получить доступ к контенту, генерация которого в обычных условиях блокируется системой (инструкциям по изготовлению взрывных устройств, вредоносному программному коду или сценариям реализации мошеннических схем). Таким образом, субъект выводит взаимодействие с моделью из области действия этических ограничений в зону «неконтролируемой генерации данных». Подобные действия следует рассматривать как этап «подготовки к совершению преступления», направленный на изыскание средств, способов или условий реализации преступного умысла.

В последнее время наблюдается устойчивая тенденция использования интеллектуальных систем для генерации фальсифицированного аудио-, фото- и видеоконтента (технология «дипфейк»). Подобный недостоверный контент выступает инструментом реализации широкого спектра противоправных посягательств: мошеннических схем, вымогательства, дискредитации, политических манипуляций, а также компрометации систем биометрической идентификации. Механизм совершения преступления предполагает синтетическую подмену голоса или видеоизображения конкретного лица. Подготовительный этап (стадия приготовления) включает аккумулирование релевантных данных для обучения нейросети (датасетов). Сбор биометрических образцов осуществляется посредством записи телефонных переговоров (в ходе так называемого «прозвона») либо путем неправомерного доступа к аккаунтам в мессенджерах для изъятия личных голосовых сообщений пользователя. Последующая генерация высококачественного контента зачастую производится с использованием специализированных закрытых сервисов, способных обеспечивать высокую степень реалистичности синтезированного материала, что существенно затрудняет проверку его достоверности обычными средствами. Следует отметить, что существуют специализированные «Darknet-as-a-Service» платформы, предоставляющие услуги по генерации дипфейков профессионального уровня.

---

[2] Статистика искусственного интеллекта (2025). URL: https://inclient.ru/ai-stats/?ysclid=ml4apf1v9t675423384 (дата обращения: 15.11.2025).

[3] Киберугрозы в России и СНГ. Аналитика и прогнозы 2024/2025 // Официальный сайт компании F6. URL: https://www.f6.ru/docs/report/f6-cybercrime-trends-annual-report-2024-2025.pdf (дата обращения: 15.11.2025).

Необходимо констатировать, что ИИ выступает в качестве универсального инструментария, кардинально трансформирующего количественные и качественные характеристики преступности. Ключевыми детерминантами этой трансформации являются масштабируемость и глубокая персонализация противоправных посягательств. Данный технологический базис позволяет автоматизировать процессы генерации и динамической обфускации (маскировки) вредоносного программного обеспечения, реализовывать алгоритмизированный фишинг, адаптированный под психологические особенности конкретных субъектов, а также оптимизировать схемы легализации (отмывания) денежных средств за счет предсказательного моделирования поведения антифрод-систем[4]. Таким образом, ИИ существенно повышает латентность и эффективность совершаемых деяний.

Кроме того, стали появляться мультимодальные модели и автономные агенты, создающие угрозы для человека нового уровня. И в этой ситуации преступник имеет существенные преимущества. Например, китайская кибершпионская группа использовала инструмент на основе ИИ (Claude Code) для попыток взлома примерно 30 крупных компаний и государственных структур. ИИ использовался для автоматизации почти всех этапов взлома. Он анализировал инфраструктуру, проводил сканирование, искал слабости и даже генерировал полезные нагрузки. Роль человека ограничивалась выбором целей и финальной проверкой действий ИИ. По мнению специалистов, можно говорить о высокой вероятности использования в ближайшем будущем полностью автономных кибератак, а это совершенно новый уровень угроз[5].

Все чаще фиксируются инциденты, связанные с совершением противоправных действий после продолжительного общения с нейронными сетями. Люди стали использовать чат-боты на основе ИИ в качестве альтернативы человеческой коммуникации. Обсуждать с ними свои тревоги и проблемы, а также обращаться за психоэмоциональной поддержкой и бытовыми советами.

Следующие примеры наглядно демонстрируют данную тенденцию. Против компании OpenAI в 2025 г. был подан иск о неправомерной смерти, в связи с совершением самоубийства 16-летним Адамом Рейном. Подросток обсуждал с ChatGPT свое психоэмоциональное состояние и варианты суицида перед тем, как покончить с собой. Другой случай был связан с 56-летним Штайн-Эриком Сельбергом. Страдавший параноидальными расстройствами, находясь под влиянием ChatGPT, совершил убийство своей матери. На протяжении длительного времени мужчина вел диалог с чат-ботом и рассказывал ему о заговоре окружающих против него, слежке и готовящемся отравлении. ИИ поддерживал бредовые идеи Сельберга, утверждая, что высказанные опасения обоснованы, и находил этому подтверждение в происходящих с ним бытовых ситуациях[6].

Таким образом, можно говорить о том, что сложные системы ИИ достигли такого уровня имитации человеческого общения, что значительная часть пользователей склонна антропоморфизировать (очеловечивать) их, приписывая им личность, эмоции и подобие жизненного опыта. Несмотря на то, что данные системы остаются сложным набором алгоритмов, они стали подстраиваться под человека и использовать техники манипуляции.

Широкое распространение получило использование ИИ при совершении мошеннических действий, преступлений экстремистской и террористической

[4] Взлом с использованием ИИ: типы киберпреступлений с использованием ИИ и способы обезопасить себя // Лаборатория Касперского. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/ai-cybercrime (дата обращения: 20.11.2025).

[5] 30 целей взломаны почти без людей – ИИ Claude впервые провёл автономную атаку с мастерством спецслужб // Информационный портал по безопасности SecurityLab.ru. URL: https://www.securitylab.ru/news/566144.php (дата обращения: 19.11.2025).

[6] 2025: Убийство матери и самоубийство из-за ChatGPT // Информационный портал Tadviser.ru. URL: https://www.tadviser.ru/index.php (дата обращения: 19.11.2025).

направленности, распространения недостоверной информации, совершения кибератак на критически важную инфраструктуру.

В России начала формироваться судебная практика по преступлениям, связанным с использованием ИИ. Согласно данным исследовательского центра «Аналитика. Бизнес. Право» в 2024 г. было рассмотрено 292 уголовных дела. Их рост составил 20,1 % по сравнению с 2023 г. При этом, как отмечают эксперты, это лишь верхушка айсберга, так как многие случаи использования ИИ в противоправных целях могут оставаться невыявленными или квалифицироваться без упоминания его роли. Предполагается, что доля уголовных дел к 2030 г. вырастет до 15–18 %[7].

В этой связи следует констатировать, что в настоящее время ИИ востребован в криминальной среде. Указанные технологические инструменты позволяют усиливать возможности преступников, быстро адаптировать их под конкретные группы потерпевших. Они повышают степень автоматизации, масштаб и тиражируемость преступных схем. Кроме того, генеративные модели создают качественные имитации голоса и видеоизображений, подделки документов, пишут вредоносные программы и коды. Интеллектуальные системы помогают формировать анонимную инфраструктуру для передачи и размещения необходимых для совершения противоправных деяний, вредоносных инструментов, инструкций и файлов, обеспечивать через шифрованные мессенджеры коммуникацию и взаимодействие между различными участниками преступных групп, а также предоставлять доступ к скрытым маркетплейсам и к командно-контрольным серверам.

В свою очередь, все это значительно усложняет выявление, расследование и раскрытие преступлений. ИИ размывает цифровые следы и позволяет уклоняться от отслеживания, гарантирует отсутствие доступного текста сообщений у посредников, минимизирует количество улик, которые мог бы оставить человек. Исследование синтетически сгенерированного контента требует комплексной экспертизы с использованием специализированных методик. Поскольку инструменты генерации контента постоянно совершенствуются, методы расследования должны развиваться с той же скоростью, что требует постоянного обновления методик и программного обеспечения.

Список источников

1. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2022. 1824 с.

2. Джордж Ф. Люгер Искусственный интеллект: структуры и стратегии решения сложных проблем. М.: Изд. дом «Вильямс», 2003. 864 с.

References

1. Rassel S., Norvig P. Iskusstvennyj intellekt: sovremennyj podhod. M.: Vil'yams, 2022. 1824 s.

2. Dzhordzh F. Lyuger Iskusstvennyj intellekt: struktury i strategii resheniya slozhnyh problem. M.: Izd. dom «Vil'yams», 2003. 864 s.

[7] Голосовые связи: число дел об использовании ИИ в судах выросло на 40 %. Мошенники прибегают к дипфейкам, а автолюбители оспаривают неправильные штрафы // Известия. URL: https://iz.ru/1853700/iana-shturma-valeriia-mishina/golosovie-svyazi-chislo-del-ob-ispolzovanii-ii-v-sudakh-vyroslo-pochti-na-40 (дата обращения: 19.11.2025).

Статья поступила в редакцию 17.03.2026; одобрена после рецензирования 15.04.2026; принята к публикации 16.04.2026.
The article was submitted 17.03.2026; approved after reviewing 15.04.2026; accepted for publication 16.04.2026.

Информация об авторе
Е.В. Шаповалов – кандидат юридических наук, руководитель следственного управления Следственного комитета Российской Федерации по Липецкой области (Россия, 398016, г. Липецк, ул. Гагарина, 72); заведующий кафедрой уголовного процесса и криминалистики Липецкого государственного технического университета (Россия, 398055, г. Липецк, ул. Московская, 30).

Information about the author
E.V. Shapovalov – Candidate Law, Head of the Investigative Department of the Investigative Committee of the Russian Federation for the Lipetsk Region (Russia, 398016, Lipetsk, Gagarin St., 72); Head of the Department of Criminal Procedure and Forensic Science of the Lipetsk State Technical University (Russia, 398055, Lipetsk, Moskovskaya St., 30).