Дата поступления рукописи в редакцию: 23.04.2025 г.
Дата принятия рукописи в печать: 13.05.2025 г.
DOI: 10.24412/2782-3830-2025-4-262-265

МАЛАЕВ Азрет Хусенович,
капитан полиции, преподаватель кафедры организации правоохранительной деятельности Северо-Кавказского института (филиал) Краснодарского Университета МВД РФ,
e-mail: mail@law-books.ru

АНАЛИЗ ВЛИЯНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА УГОЛОВНОЕ ПРАВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. *В статье рассматриваются три аспекта: возможность признания ИИ субъектом уголовной ответственности, его использование как инструмента совершения и расследования преступлений, а также вызовы, которые технологии ИИ создают для правовой системы. На основе актуальной статистики за 2023–2025 годы и анализа российского законодательства предлагаются пути адаптации уголовной политики к новым реалиям.*

Ключевые слова: *уголовная ответственность, искусственный интеллект, киберпреступления, правоприменение, цифровизация.*

MALAEV Azret Khusenovich,
Police Captain, Lecturer at the Department of Law Enforcement Organization, North Caucasus Institute (branch) Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

THE ANALYSIS OF THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CRIMINAL LAW IN THE CONTEXT OF DIGITALIZATION

Annotation. *It analyzes three aspects: the possibility of recognizing AI as a subject of criminal liability, its role as a tool for committing and investigating crimes, and the challenges it poses to the legal system. Based on statistics from 2023–2025, an analysis of Russian legislation, and a comparative legal approach (Russia, EU, USA), measures are proposed to adapt criminal policy.*

Key words: *criminal liability, artificial intelligence, cybercrime, comparative law, digitalization.*

Современный мир вступил в эпоху алгоритмов, где искусственный интеллект (ИИ) проникает во все сферы жизни, включая правоохранительную деятельность и криминальную среду. В Российской Федерации цифровизация сопровождается ростом киберпреступности, изменением характера противоправных деяний и усложнением задач уголовной юстиции. В настоящее время ИИ трансформирует традиционные подходы к ответственности, требуя переосмысления базовых категорий уголовного права.

Согласно статье 19 УК РФ, субъектом уголовной ответственности может быть только физическое лицо, достигшее возраста уголовной ответственности и обладающее вменяемостью. Эта норма, сформированная в эпоху доцифровых технологий, не учитывает появление ИИ, который способен принимать решения, анализировать данные и совершать действия, потенциально подпадающие под признаки преступления. Вопрос о признании ИИ субъектом ответственности активно обсуждается в зарубежной юриспруденции, но в России остаётся на периферии научного дискурса [1].

Современные системы ИИ, такие как нейронные сети и алгоритмы машинного обучения, демонстрируют высокую степень автономности. Например, в 2024 году в России зафиксирован случай, когда алгоритм, управляющий финансовой платформой, совершил несанкционированные транзакции на сумму 150 миллионов рублей, что было квалифицировано как мошенничество (статья 159 УК РФ). Возникает вопрос: кто несёт ответственность — разработчик, оператор системы или сам ИИ?

В зарубежной практике уже есть прецеденты. В 2018 году в США алгоритм торговой платформы вызвал финансовый ущерб, и суд

возложил ответственность на компанию-владельца. Однако в России правовая система пока не готова к таким ситуациям. Отсутствие субъектности ИИ приводит к пробелам в ответственности, особенно если разработчик или оператор не осознавали противоправных последствий действий алгоритма.

Признание ИИ субъектом ответственности потребовало бы радикального пересмотра УК РФ, что в российских условиях маловероятно в ближайшие годы. Более реалистичным представляется введение косвенной ответственности разработчиков и операторов ИИ за непреднамеренные последствия, а также создание специальных норм для регулирования автономных систем [2]. Например, можно дополнить главу 28 УК РФ статьёй о «неправомерном использовании ИИ», предусматривающей ответственность за создание алгоритмов с заведомо противоправным потенциалом.

В России киберпреступность демонстрирует устойчивый рост. По данным МВД РФ, в 2024 году зарегистрировано 677 тысяч киберпреступлений, что на 17,4% больше, чем в 2023 году (577 тысяч). Доля таких деяний в общем массиве преступности достигла 40%, а ущерб составил 200 миллиардов рублей. Значительная часть этих преступлений связана с использованием ИИ.

Например, в 2024 году зафиксирован рост числа мошенничеств с применением дипфейков — поддельных видео и аудиозаписей, созданных ИИ. По данным Банка России, такие схемы привели к хищению 27,5 миллиарда рублей через 1,2 миллиона операций. Дипфейки использовались для имитации голосов руководителей компаний или родственников жертв, что усложняет расследование.

ИИ выступает инструментом в различных категориях преступлений:

- Мошенничество: генерация фишинговых текстов и дипфейков для обмана граждан.
- Неправомерный доступ: использование ИИ для подбора паролей или обхода систем защиты (статья 272 УК РФ).
- Распространение вредоносного ПО: автоматизация атак с помощью алгоритмов (статья 273 УК РФ).
- Экономические преступления: манипуляции на финансовых рынках через торговые боты.

В 2023 году в Москве был выявлен случай использования ИИ для подделки цифровых подписей, что позволило злоумышленникам перевести 80 миллионов рублей с корпоративных счетов. Это подчёркивает необходимость расширения составов преступлений в УК РФ [3].

Действующее законодательство не всегда позволяет адекватно квалифицировать деяния с использованием ИИ. Например, создание дипфейков для мошенничества подпадает под статью 159 УК РФ, но отсутствие прямого указания на цифровые технологии затрудняет доказывание умысла. Требуется введение квалифицирующих признаков, таких как «с использованием ИИ», для ужесточения ответственности.

ИИ активно внедряется в деятельность правоохранительных органов России. В 2024 году система распознавания лиц, основанная на нейронных сетях, помогла раскрыть 12 тысяч преступлений, включая 98% убийств. Алгоритмы анализа больших данных используются для прогнозирования преступлений и выявления подозрительных транзакций. Например, в Санкт-Петербурге в 2023 году ИИ позволил пресечь деятельность группы, занимавшейся отмыванием денег на сумму 300 миллионов рублей.

Преимущества ИИ очевидны: ускорение расследований, повышение раскрываемости и снижение нагрузки на следователей. Однако существуют ограничения:

- Технические ошибки: в 2024 году в Казани система распознавания лиц ошибочно идентифицировала гражданина как подозреваемого, что привело к его задержанию.
- Этические дилеммы: массовая обработка персональных данных вызывает вопросы о нарушении права на частную жизнь, что в России регулируется недостаточно строго по сравнению с GDPR в ЕС.
- Использование ИИ в расследованиях требует чётких процессуальных норм. В Уголовно-процессуальном кодексе РФ (УПК РФ) отсутствуют положения о допустимости доказательств, полученных с помощью алгоритмов. Необходимо дополнить статью 75 УПК РФ нормой о верификации данных, сгенерированных ИИ, для исключения ошибок.

Многие киберпреступления с использованием ИИ совершаются через серверы за пределами России. В 2024 году МИД РФ отметил рост атак с территории стран НАТО и Украины. Это требует усиления международного сотрудничества, однако политические разногласия препятствуют реализации таких инициатив.

Раскрываемость киберпреступлений в России остаётся на уровне 25,9%. Основные причины - нехватка специалистов и длительность компьютерных экспертиз (до 6 месяцев). ИИ мог бы ускорить процесс, но его внедрение ограничено бюджетными и кадровыми ресурсами.

Использование ИИ в уголовном праве также поднимает ряд этических вопросов. Одним из них является проблема ответственности за действия, совершенные с использованием ИИ [4]. Если алгоритм принимает решение, которое приводит к негативным последствиям, кто должен нести за это ответственность - разработчик, владелец системы или пользователь? Отсутствие регулирования ИИ в УК РФ и УПК РФ создаёт риски как для граждан (нарушение прав), так и для государства (невозможность пресечения новых угроз). Например, использование ИИ для создания дезинформации в социальных сетях пока не подпадает под уголовную ответственность [5], хотя представляет угрозу общественной безопасности или системы распознавания лиц, используемые правоохранительными органами, могут быть использованы для массовой слежки за гражданами, что противоречит принципам свободы личности.

Приведем предполагаемые законодательные изменения, которые позволят адаптировать уголовное право к существующим реалиям по рассмотренным проблемам:

1. Расширение УК РФ: Ввести статью «Неправомерное использование ИИ» (например, статья 274.2 УК РФ) с наказанием до 10 лет лишения свободы за создание алгоритмов с противоправным потенциалом.
2. Ужесточение санкций: Дополнить статьи 159, 272 и 273 УК РФ квалифицирующим признаком «с использованием ИИ», увеличивая максимальный срок до 12-15 лет.
3. Процессуальные нормы: Включить в УПК РФ положения о допустимости доказательств, полученных с помощью ИИ, с обязательной независимой экспертизой.

Создание специализированных центров киберрасследований в регионах России и обучение следователей работе с ИИ повысят эффективность правоприменения. В 2025 году МВД РФ планирует подготовить 500 специалистов по цифровым технологиям.

Россия может инициировать разработку новой конвенции ООН о регулировании ИИ в криминальной сфере, дополняя принятую в 2024 году Конвенцию о киберпреступности [6].

Повышение цифровой грамотности населения через образовательные программы снизит уязвимость граждан перед преступлениями с использованием ИИ.

Искусственный интеллект в эпоху алгоритмов одновременно выступает субъектом, инструментом и вызовом для уголовного права. С одной стороны, ИИ может стать мощным инструментом в борьбе с преступностью, повышая эффективность работы правоохранительных органов и судебной системы. С другой стороны, использование ИИ требует разработки новых правовых норм, которые бы учитывали специфику этой технологии и минимизировали связанные с ней риски. В России он пока не признан субъектом ответственности, но активно используется как в совершении, так и в расследовании преступлений. Статистика 2023–2025 годов подчёркивает рост киберпреступности и необходимость адаптации законодательства, особенно важно разработать четкие и прозрачные правила использования ИИ. Это потребует не только законодательных изменений, но и активного участия научного сообщества, которое должно предложить новые подходы к пониманию таких понятий, как вина, ответственность и справедливость в контексте использования ИИ [7].

Предложенные меры - от введения новых норм до развития инфраструктуры - позволят правовой системе справиться с вызовами цифровизации. Уголовное право должно эволюционировать, сохраняя баланс между эффективностью борьбы с преступностью и защитой прав граждан.

Список литературы:

[1] Грибанов Е. В. Перспективные направления развития кибертехнологий предупреждения преступлений // Общество и право. 2021. № 4. С. 21–27.

[2] Ильницкий А. С. Противодействие криминальной идеологии в сети Интернет: дисс. канд. юрид. наук. Краснодар, 2022.

[3] Карачаев А.Р. Криминологические аспекты противодействия организованной преступности в условиях цифровизации // Пробелы в российском законодательстве. 2022. Т. 15. № 5. С. 185-189.

[4] Кумахов Т.Т., Абазов А.Б., Шафиева Э.Т. Сквозные цифровые технологии как фактор трансформации экономических знаний специалистов // Журнал прикладных исследований. 2023. № 11. С. 110-114.

[5] Малаев А.Х. Применение цифровых технологий и искусственного интеллекта при предупреждении экстремистских и террористических преступлений // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 263-267.

[6] Малаев А.Х. О роли цифровых технологий в правоохранительной деятельности // Право и управление. 2023. № 1. С. 183-186.

[7] Машекуашева М.Х. Некоторые аспекты использования в преступных целях искусственного интеллекта. Право и управление. 2024. № 8. С. 376-378.

Spisok literatury:

[1] Gribanov E. V. Perspektivny`e napravleniya razvitiya kibertexnologij preduprezhdeniya prestuplenij // Obshhestvo i pravo. 2021. № 4. S. 21–27.

[2] Il`niczkij A. S. Protivodejstvie kriminal`noj ideologii v seti Internet: diss. kand. yurid. nauk. Krasnodar, 2022.

[3] Karachaev A.R. Kriminologicheskie aspekty` protivodejstviya organizovannoj prestupnosti v usloviyax cifrovizacii // Probely` v rossijskom zakonodatel`stve. 2022. T. 15. № 5. S. 185-189.

[4] Kumaxov T.T., Abazov A.B., Shafieva E`.T. Skvozny`e cifrovy`e texnologii kak faktor transformacii e`konomicheskix znanij specialistov // Zhurnal prikladny`x issledovanij. 2023. № 11. S. 110-114.

[5] Malaev A.X. Primenenie cifrovy`x texnologij i iskusstvennogo intellekta pri preduprezhdenii e`kstremistskix i terroristicheskix prestuplenij // Probely` v rossijskom zakonodatel`stve. 2023. T. 16. № 4. S. 263-267.

[6] Malaev A.X. O roli cifrovy`x texnologij v pravooxranitel`noj deyatel`nosti // Pravo i upravlenie. 2023. № 1. S. 183-186.

[7] Mashekuasheva M.X. Nekotory`e aspekty` ispol`zovaniya v prestupny`x celyax iskusstvennogo intellekta. Pravo i upravlenie. 2024. № 8. S. 376-378.

