

УДК 343.2/.7

Уголовная ответственность за использование искусственного интеллекта в преступных целях

Юрков Сергей Александрович,

кандидат юридических наук, доцент,
исполняющий обязанности заведующий кафедрой судебных экспертиз,
ФГБОУ ВО «Вятский государственный университет». Россия, г. Киров.

E-mail: usr10013@vyatsu.ru

Опалева Софья Алексеевна,

студент, ФГБОУ ВО «Вятский государственный университет». Россия, г. Киров.

E-mail: sofikorpaleva@yandex.ru

Аннотация. В современном мире технологии искусственного интеллекта становятся все более популярными и востребованными. Они применяются в различных областях, от повседневной жизни и образования до бизнеса и государственного управления. Несмотря на его пользу, вместе с этим появляется и новая проблема – возможность использования искусственного интеллекта в преступных целях. В данной статье мы рассмотрим преступления, которые могут быть совершены с использованием искусственного интеллекта, и какие уголовно-правовые меры можно предпринять для борьбы с ними.

Ключевые слова: искусственный интеллект, уголовная ответственность, киберпреступность, уголовное право, информационные технологии.

Искусственный интеллект (далее – ИИ) активно интегрируется в различные сферы жизнедеятельности современного общества, трансформируя как профессиональные, так и повседневные аспекты человеческой жизни. Его применение уже не ограничивается традиционными областями, такими как медицина, научные исследования и бизнес, но также охватывает бытовую сферу, становясь неотъемлемой частью повседневного уклада. Яркими примерами этого являются виртуальные помощники, такие как Яндекс Алиса и технологии «умного дома», которые автоматизируют рутинные процессы, повышают комфорт и оптимизируют использование ресурсов.

Такая широкая интеграция ИИ свидетельствует о его значительном влиянии на формирование новой технологической реальности. Однако она также ставит перед обществом ряд важных вопросов, связанных с безопасностью, этикой и правовым регулированием. Таким образом, ИИ становится инструментом, требующим глубокого анализа и выработки стратегий для его устойчивого и безопасного использования.

Так, в Указе Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» указано: «искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их» [7]. Его можно применять для автоматизации задач, анализа информации и поддержки в принятии решений. Однако те же самые возможности могут быть направлены на совершение противоправных действий, включая: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и многое другое.

Одним из наиболее опасных аспектов использования ИИ является его способность к обучению и адаптации. Это означает, что ИИ может стать более эффективным в совершении преступлений, если он будет использоваться для этого. Кроме того, ИИ может использоваться для создания новых видов преступлений, которые ранее не были известны.

Особенно сейчас, когда государства выделяют большие средства для развития индустрии искусственного интеллекта, возникает все больше опасений о недостаточном контроле ИИ. Например, в Российской Федерации Правительство выделит около 1,2 млрд рублей на поддержку индустрии ИИ [3]. В США же вложат рекордные 500 млрд долларов в его развитие [5].

Применение ИИ для совершения преступных действий в настоящее время поражает своим разнообразием. Использование ИИ можно встретить в случаях мошенничества с помощью подделки голоса, например, вымогатели начали использовать ИИ для подделки голосовых сообщений в Telegram [1]. Используя ИИ, мошенники создают голосовые обращения на основе аудиосообщений владельца аккаунта. Этот способ позволяет злоумышленникам усовершенствовать и сделать более убедительными свои попытки выманить деньги у друзей и знакомых жертвы. Кроме того, нередки случаи использования ИИ при кибератаках: «Сбербанк заявил об использовании хакерами искусственного интеллекта» [4]. Заместитель председателя правления Сбербанка Станислав Кузнецов сообщил, что хакеры начали применять искусственный интеллект при кибератаках на банки. По его словам, атаки стали более сложными и теперь включают элементы ИИ, что позволяет злоумышленникам получать данные о защитных механизмах, архитектуре технологических и операционных систем, а также о системах безопасности банков. В зарубежной практике также существует немало подобных примеров. Так, в ОАЭ мошенники с помощью аудиодипфейка «клонировали» голос директора крупной компании и обманули менеджеров банка, которые перевели на их счет 35 млн долларов [2].

Как известно, в Уголовном Кодексе Российской Федерации отсутствуют нормы, которые бы прямо регулировали использование ИИ и ответственность за его неправомерное применение. Единственное, что может быть косвенно связано с этой темой, – это 28 глава «Преступления в сфере компьютерной информации» [6]. Поэтому в качестве проблем, почему используют искусственный интеллект в преступных целях, можно выделить следующие:

1. Отсутствие четкого законодательства.

Российское уголовное законодательство не учитывает специфику преступлений, совершенных с использованием ИИ. Это создает правовые пробелы, которые могут быть использованы злоумышленниками.

2. Сложность идентификации виновных.

В случаях, когда ИИ используется для совершения преступлений, может быть сложно определить, кто несет ответственность: разработчик, владелец или пользователь системы. Например, если ИИ действовал автономно, кто должен быть привлечен к ответственности?

3. Техническая сложность доказательства вины.

Доказательство того, что ИИ был использован для совершения преступления, требует высокого уровня технической экспертизы. Это может быть затруднительно для правоохранительных органов, которые не всегда обладают необходимыми знаниями и ресурсами.

4. Международный характер преступлений.

Преступления с использованием ИИ часто имеют транснациональный характер, что затрудняет их расследование и преследование. Злоумышленники могут

использовать ИИ для атак на системы в разных странах, что требует международного сотрудничества.

Для решения вышеуказанных проблем и борьбы с использованием ИИ в преступных целях необходимо разработать эффективные уголовно-правовые, организационные, технические механизмы. В качестве путей решения можно привести следующие:

1. Разработка и внедрение специализированного уголовного законодательства.

Создание законов, которые четко определяют уголовную ответственность за использование ИИ в преступных целях. Это должно включать определение ИИ, ролей и ответственности разработчиков, владельцев и пользователей ИИ. Также можно ввести отдельную главу в УК РФ.

2. Ужесточение наказания за совершение преступлений с использованием ИИ.

Это может включать в себя увеличение штрафов, лишение свободы на более длительный срок и другие уголовно-правовые меры.

3. Совершенствование экспертных групп и обучение правоохранительных органов.

Несмотря на то, что в структуре МВД РФ существует Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий и Бюро специальных технических мероприятий, необходимо постоянное их совершенствование, привлечение новых кадров, которые бы специализировались исключительно на работе с ИИ. Также неизбежно регулярное обучение сотрудников техническим аспектам работы с ИИ.

4. Международное сотрудничество.

Укрепление международного сотрудничества в области борьбы с преступлениями, связанными с ИИ. Это может включать создание международных договоров и соглашений, а также обмен информацией и опытом между странами.

5. Разработка технических стандартов и протоколов.

Установление технических стандартов для разработки и использования ИИ, которые минимизируют возможность их использования в преступных целях. Это может включать требования к прозрачности и подотчетности ИИ систем.

6. Повышение осведомленности и образования.

Проведение образовательных программ, тренингов и кампаний для повышения осведомленности общественности и специалистов о рисках и последствиях использования ИИ в преступных целях.

7. Создание механизмов мониторинга и контроля.

Разработка специальных систем мониторинга и контроля за использованием ИИ, которые позволят своевременно выявлять и предотвращать потенциальные угрозы.

Таким образом, использование ИИ в преступных целях негативно сказывается на жизни общества, представляя серьезную опасность. Для решения данной проблемы необходим комплексный подход внесения изменений в уголовное законодательство Российской Федерации, который бы позволил минимизировать риски и обеспечить безопасное использование ИИ в будущем.

Список литературы

1. Вымогатели начали использовать ИИ для подделки голосовых в Telegram // РБК. URL: https://www.rbc.ru/technology_and_media/10/01/2024/659d37899a79473f8a99e35f (дата обращения: 22.02.2025).

2. Знакомый голос: мошенники с помощью дипфейка украли у банка \$35 млн // Газета.Ru. URL:

<https://www.gazeta.ru/tech/2021/10/15/14096293/deepfakethreaten.shtml> (дата обращения: 22.02.2025).

3. Распоряжение Правительства Российской Федерации от 05.10.2023 № 2715-р // Официальный сайт Правительства России. URL: <http://government.ru/docs/49737/> (дата обращения: 20.02.2025).

4. Сбербанк заявил об использовании хакерами ИИ // Коммерсантъ. URL: <https://www.kommersant.ru/doc/3655663> (дата обращения: 22.02.2025).

5. США вложат рекордные 500 млрд долларов в развитие искусственного интеллекта // RG.RU. URL: <https://rg.ru/2025/01/22/ssha-vlozhat-rekordnye-500-mlrd-dollarov-v-razvitie-iskusstvennogo-intellekta.html> (дата обращения: 20.02.2025).

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 01.03.2025) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/ (дата обращения: 24.02.2025).

7. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 // Официальный сайт Президента России. URL: <http://www.kremlin.ru/acts/bank/44731> (дата обращения: 19.02.2025).