КРИМИНОЛОГИЧЕСКИЕ РИСКИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ТЕОРЕТИЧЕСКИЙ АНАЛИЗ И ПУТИ МИНИМИЗАЦИИ

Яковчик Д.В.,
преподаватель кафедры общеюридических и уголовно-правовых дисциплин факультета повышения квалификации и переподготовки кадров учреждения образования «Могилевский институт Министерства внутренних дел Республики Беларусь», магистр юридических наук

Стремительное развитие технологий искусственного интеллекта (ИИ) и их интеграция во все сферы общественной жизни объективно влекут за собой не только позитивные экономические и социальные трансформации, но и порождают новые, ранее неизвестные криминальные угрозы. На современном этапе искусственный интеллект перестает быть исключительно инструментом научно-технического прогресса; он все активнее эксплуатируется криминальным сообществом, трансформируя традиционные формы преступной деятельности и создавая почву для возникновения качественно новых видов общественно опасных деяний [1; 2]. Данное обстоятельство позволяет рассматривать ИИ не просто как технологический феномен, а как значимый криминогенный фактор, влияющий на состояние, структуру и динамику современной преступности.

Понятие искусственного интеллекта, несмотря на его широкое употребление в научной и нормативной лексике, до настоящего времени не получило единого легального закрепления. Вместе с тем отметим, что под данным понятием можно понимать область информатики, которая занимается разработкой интеллектуальных компьютерных систем, то есть систем, обладающих возможностями, которые традиционно связываются с человеческим разумом, – понимание языка, обучение, способность рассуждать, решать проблемы и т.д. [3, с. 19]. Все технологии искусственного интеллекта можно разделить на две большие группы: модели машинного обучения (использует результаты обучения на наборах данных для создания моделей, способных выполнять сложные задачи) и генеративные модели (уже имеющие базу данных / доступ к Интернету для решения задач) [4, с. 213].

В зарубежной и отечественной криминологической науке предпринимаются попытки систематизации угроз, связанных с криминальным использованием ИИ. Наиболее авторитетной и методологически обоснованной представляется трехэлементная классификация, предложенная К. Хейвордом и М. Маасом, которая выделяет преступления, совершаемые с использованием ИИ (crimes with AI), преступления против систем

ИИ (crimes against AI) и преступления, совершаемые самим ИИ (crimes by AI) [5, p. 214–217]. Данная типология позволяет охватить все ключевые аспекты взаимодействия технологий ИИ с преступностью и служит теоретическим фундаментом для дальнейшего криминологического анализа.

Crimes with AI (преступления с ИИ). В рамках данной категории искусственный интеллект рассматривается как высокотехнологичное орудие совершения общественно опасных деяний, значительно расширяющее арсенал средств преступника. Наибольшую тревогу в этом контексте вызывает стремительное распространение дипфейк-технологий (deepfake) – синтетический мультимедийный контент, созданный с помощью технологий искусственного интеллекта для неосознаваемой аудиторией подмены на итоговом видео / аудио биометрических или аудиальных характеристик реального человека на иные, фейковые [6, с. 32]. ИИ существенно усиливают возможности мошенников по созданию персонализированных атак и автоматизированных схем социальной инженерии. Масштаб угрозы подтверждается также и сотрудниками правоохранительных органов – количество схем и случаев использование дипфейков увеличивается постоянно [7].

Помимо дипфейков, технологии ИИ активно используются для автоматизации фишинговых атак (генерация персонализированных сообщений с помощью языковых моделей), создания вредоносного программного обеспечения без глубоких познаний в программировании, синтезирования фейковой информации, а также для посягательств посредством автоматизированных автономных систем и ботов. Отличительной особенностью преступлений данной категории является их масштабируемость: ИИ позволяет преступнику одновременно атаковать тысячи потенциальных жертв, что качественно отличает современную цифровую преступность от традиционных форм.

Crimes against AI (преступления против ИИ). Вторую группу криминологических рисков образуют посягательства на сами системы искусственного интеллекта, выступающие в качестве объекта преступных действий. Как отмечают Р. Дремлюга и А. Коробеев, система ИИ представляет собой исполняемый программный код или коэффициенты модели, которые при вводе определенных данных приводят к получению результата; как и любая иная компьютерная информация, система ИИ может стать объектом преступных посягательств [8]. Особую опасность в этом контексте представляют так называемые «состязателные атаки» (adversarial attacks) – действия, при которых злоумышленник, зная особенности разработки и функционирования системы ИИ, намеренно подает на ее вход данные, приводящие к некорректной работе алгоритма. К данной категории также относится «отравление данных»

(data poisoning) – внесение искаженной информации в обучающие выборки на этапе разработки модели, что приводит к системным сбоям в ее последующем функционировании. Исследователи подчеркивают, что подобные методы вмешательства могут не содержать формальных признаков составов преступлений, предусмотренных действующим российским уголовным законодательством, однако обладают высокой степенью общественной опасности, достаточной для их криминализации.

Crimes by AI (преступления, совершаемые ИИ). Третья, наиболее дискуссионная категория, связана с потенциальной возможностью совершения преступления автономной системой искусственного интеллекта без непосредственного участия человека. Ключевая проблема заключается в том, что технологии ИИ способны к самообучению и самостоятельным действиям без прямого вмешательства и контроля со стороны человека [9]. В этой связи в научной литературе активно обсуждается вопрос о возможности признания искусственного интеллекта и роботов субъектами уголовной ответственности в контексте их когнитивных способностей и автономии [10; 11].

Таким образом, проведенный анализ демонстрирует, что искусственный интеллект представляет собой комплексный криминогенный фактор, воздействие которого на преступность проявляется в трех взаимосвязанных направлениях. Данная классификация создает теоретическую основу для дальнейшего исследования механизма влияния ИИ на преступное поведение и виктимность, а также для разработки адекватных мер уголовно-правового и криминологического реагирования.

Закономерным и практически значимым продолжением является поиск адекватных и эффективных мер противодействия этим угрозам. Масштаб и специфика преступлений, сопряженных с использованием ИИ, диктуют необходимость формирования комплексной системы реагирования. Как показывает анализ текущей ситуации, изолированных, разрозненных действий в этой сфере недостаточно. Эффективная стратегия должна объединять три ключевых направления: совершенствование правовой базы, внедрение передовых технологических решений и развитие международной кооперации.

Совершенствование уголовного законодательства является краеугольным камнем противодействия преступности в цифровую эпоху. Ключевым вектором этого совершенствования должен стать сам факт признания применения технологий искусственного интеллекта обстоятельством, отягчающим наказание. Образцом для совершенствования может стать опыт Российской Федерации, где предлагается считать дипфейки отягчающим обстоятельством [12].

Уголовно-правовое реагирование, при всей его значимости, не способно в полной мере решить проблему противодействия

преступности, связанной с ИИ, без комплексной системы криминологической профилактики. В целях предупреждения преступлений, связанных с использованием искусственного интеллекта, необходимо проанализировать криминологические риски его развития и выработать систему мер криминологического предупреждения. Принципиально важным компонентом профилактической деятельности является повышение цифровой и финансовой грамотности населения. С виктимологической точки зрения, эффективная профилактика преступлений, связанных с ИИ, невозможна без учета специфики механизмов виктимизации в цифровой среде. Представляется, что данное направление нуждается в дальнейшей теоретической разработке и практической реализации в рамках государственной политики противодействия киберпреступности.

Специфика преступлений, совершаемых с использованием ИИ, обусловливает необходимость применения адекватных технологических средств противодействия. Ключевыми направлениями технологического противодействия могут выступать развитие антифрод-систем, внедрение механизмов многоуровневой аутентификации, а также интеграция обучающих материалов в популярные онлайн-платформы.

Помимо этого, трансграничный характер преступлений, совершаемых с использованием технологий искусственного интеллекта, обусловливает необходимость развития международного сотрудничества в данной сфере. Таким образом, искусственный интеллект, будучи продуктом технологического прогресса, одновременно порождает принципиально новые криминологические вызовы, адекватный ответ на которые требует консолидации усилий законодателя, правоприменителя, научного сообщества и институтов гражданского общества. Дальнейшие исследования в данной области должны быть направлены на углубленное изучение механизмов виктимизации в цифровой среде, разработку методик криминологического прогнозирования развития угроз, связанных с ИИ, а также на формирование научно обоснованных рекомендаций по минимизации криминогенного потенциала технологий искусственного интеллекта.

Список использованных источников:

1. Мошенники используют ИИ. Более 3 тыс. киберпреступлений зарегистрировано в Беларуси с начала года // news.by. – URL: https://news.by/news/obshchestvo/mosheniki-ispolzuyut-ii-bolee-3-tys-kiberprestupleniy-zaregistrirovano-v-belarusi-s-nachala-goda (дата обращения: 11.04.2026).

2. В 2026 году удельный вес киберпреступлений в структуре преступности составляет почти 40 процентов // SB.BY. Беларусь сегодня. – URL: https://www.sb.by/articles/v-2026-godu-udelnyy-ves-kiberprestupleniy-v-strukture-prestupnosti-sostavlyaet-pochti-40-protsentov.html (дата обращения: 11.04.2026).

3. Вислова, А. Д. Современные тенденции развития искусственного интеллекта / А. Д. Вислова // Известия Кабардино-Балкарского научного центра РАН. – 2020. – №. 2 (94). – С. 14-30.

4. Яковчик, Д. В. Методологические аспекты применения генеративного искусственного интеллекта для психологического портретирования / Д. В. Яковчик // Актуальные вопросы социогуманитарного знания в правоохранительной деятельности: материалы Междунар. науч.-практ. конф. (20 нояб. 2025 г.) / Краснодар. ун-т МВД России; редкол.: Г. А. Гюрджян (пред.) [и др.]. – Краснодар, 2025. – С. 210-216.

5. Hayward, K. J., Artificial intelligence and crime: A primer for criminologists / K. J. Hayward, M. M. Maas // Crime, Media, Culture. – 2021. – Т. 17. – №. 2. – С. 209-233.

6. Воронин, И. А. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы / И. А. Воронин, Д. П. Гавра // Российская школа связей с общественностью. – 2024. – №. 33. – С. 28-47.

7. Фишинг, дипфейки и «Антикино»: СК о самых распространенных видах мошенничества // БелТА – URL: https://belta.by/society/view/fishing-dipfejki-i-antikino-sk-o-samyh-rasprostranennyh-vidah-moshennichestva-741623-2025/ (дата обращения: 11.04.2026).

8. Дремлюга, Р. И. Преступные посягательства на системы искусственного интеллекта: уголовно-правовая характеристика / Р. И. Дремлюга, А. И. Коробеев // Всероссийский криминологический журнал. – 2023. – Т. 17. – №. 1. – С. 5-12.

9. Садикова, М. А. Самообучение искусственного интеллекта. базовые принципы работы искусственного интеллект на простом примере / М.А. Садикова, Н.К. Авазова // Al-Farg'oniy avlodlari. – 2023. – Т. 1. – №. 4. – С. 246-250.

10. Мосечкин, И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления / И. Н. Мосечкин // Вестник Санкт-Петербургского университета. Право. – 2019. – Т. 10. – №. 3. – С. 461-476.

11. Карташов, И. И. Искусственный интеллект как субъект уголовной ответственности: настоящее и перспективы / И. И. Карташов, И. И. Карташов // Право: история и современность. – 2021. – №. 2(15). – С. 68-78.

12. Дипфейк может стать отягчающим обстоятельством // Ceur.ru. – URL: https://ceur.ru/news/zakony_sudy/dipfejk-mozhet-stat-otyagchayushhim-obstoyatelstvom/ (дата обращения: 11.04.2026).