УДК 342

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА И ВЫЗОВЫ ДЛЯ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

К. А. ОДИНЦОВ
(Представлено: В. С. Гриневич)

В статье исследуются современные тенденции преступности в Республике Беларусь в условиях цифровизации и внедрения систем искусственного интеллекта. Дается уголовно-правовая характеристика преступлений, совершаемых с использованием указанных технологий, а также рассматриваются основные проблемы, которые существуют в данной сфере на современном этапе. Проводится изучение зарубежного опыта регулирования и предлагаются меры по изменению отдельных норм Уголовного *кодекса.*

Сегодня в связи с динамичным развитием информационных технологий и широким распространением систем искусственного интеллекта (далее – ИИ) во всех сферах общественной жизни произошли некоторые изменения в структуре современной преступности в Республике Беларусь. На данный момент в условиях цифровой трансформации общества ИИ стал не только средством достижения результатов в научной и других сферах, но и опасным инструментом для совершения общественно опасных деяний. Криминализация данной сферы способствует возникновению принципиально новых вызовов, как для правоохранительных органов, так и для общества и государства в целом, и в связи с этим требует особого внимания.

В октябре 2026 года на совместном заседании Палаты представителей и Совета Республики Национального собрания Генеральный прокурор Республики Беларусь сообщил, что за истекший период 2026 года удельный вес киберпреступлений в общей структуре преступности составил 30 % (против 27 % в 2025 году). Кроме того, отдельно было отмечено, что при совершении таких преступлений активно используются технологии ИИ [1]. Это говорит о том, что данной проблеме в нашем государстве уделяется внимание на самом высоком уровне.

При этом, если в начальном этапе цифровизации злоумышленники использовали классические вредоносные программы, то к 2025–2026 годам на первый план вышли генеративные нейросети и технологии цифровой симуляции личности (т.н. дипфейки). С учетом этого, в нынешних реалиях ИИ превратился в универсальное средство автоматизации и масштабирования преступной деятельности, которое может использоваться для совершения крайне широкого круга преступлений, предусмотренных Уголовным кодексом Республики Беларусь (далее – УК) [2].

Искусственный интеллект представляет собой систему, имитирующую когнитивные функции человека, включая обучение, анализ данных и принятие решений на основе алгоритмов машинного обучения. На данный момент в уголовном праве ИИ не может выступать субъектом преступления, а рассматривается лишь как орудие или средство его совершения, поскольку у него отсутствует воля и, соответственно, какой-либо умысел. На уровне доктрины выделяется т.н. «слабый» ИИ (алгоритмы и нейросети, предназначенные для решения конкретных прикладных задач, таких, как генерация текстов, распознавание лиц, анализ массивов данных) и «сильный» ИИ (он может выходить за рамки ранее заданного алгоритма задач и самостоятельно принимать решения) [1]. ИИ ставит перед уголовным правом две основные задачи: защитить охраняемые интересы от новых форм посягательств, а также выработать адекватные режимы ответственности там, где ИИ становится инструментом или посредником преступной деятельности [3].

Понятие противоправности ИИ определяется нарушением охраняемых благ: имущества, информационной безопасности, жизни и здоровья [4]. На данный момент можно выделить следующие виды преступлений, совершаемые с использованием ИИ.

Первая и самая распространенная группа – преступления против собственности. Среди них наиболее распространены:

1) мошенничество (ст. 209 УК) – ИИ используется для создания фишинговых ссылок, сайтов-двойников, а также позволяет всего за несколько минут создавать убедительные копии изображений, аудио- и видеоматериалы, которые в связи с быстрым развитием указанных технологий становится все сложнее отличить от реальных;

2) хищение имущества путем модификации компьютерной информации (ст. 212 УК) – ИИ используется непосредственно для выполнения объективной стороны данного преступления. Он позволяет изменять компьютерные данные в автоматическом режиме со скоростью, недоступной человеку, анализирует профиль потенциального потерпевшего в Интернете и в последующем генерирует индивидуально подобранный текст сообщения и т.п;

3) ИИ применяется также в ходе совершения т.н. «традиционных» форм хищения, таких как, кража (ст. 205 УК), разбой (ст. 207 УК) и вымогательство (ст. 208 УК). В этих составах ИИ выступает в качестве

средства подготовки, автоматизации или непосредственного использования в процессе выполнения объективной стороны преступления. Например, для получения физического доступа к каким-либо помещениям или сейфам могут разрабатываться различные устройства с элементами машинного обучения, которые способны по звуку работы механизма замка или другим способом подбирать ключи и коды значительно быстрее, чем с использованием стандартных орудий и средств. Также с помощью ИИ могут создаваться определенные фото- или видеоматериалы, которые в последующем могут использоваться для вымогательства под угрозой их распространения среди коллег, родственников и т.п.

Вторая группа – это преступления против безопасности движения и эксплуатации транспорта (глава 28 УК). В частности, сюда можно отнести нарушение правил дорожного движения, повлекшее телесные повреждения либо смерть человека (ст. 317). Автономный транспорт, управляемый ИИ может, например, неверно распознавать силуэты людей или препятствий на дороге либо в результате иной алгоритмической ошибки провоцировать дорожно-транспортные происшествия. Особенно актуальной данная проблема станет в недалеком будущем, когда подобные транспортные средства получат распространение в Беларуси.

Третья группа – преступления против общественной безопасности, общественного порядка и общественной нравственности и государства (главы 27, 30, 32 УК). В рамках данных преступлений ИИ может использоваться для:

1) террористической и диверсионной деятельности: ИИ путем алгоритмического планирования и автономного исполнения облегчает подготовку и осуществления действий, образующих объективную сторону данных преступлений: взрыва; поджога; совершения производственных аварий, крушений транспортных средств; разрушения средств коммуникации; использования ядерного, радиологического, химического оружия или иных действий, создающих опасность гибели людей, причинения им телесных повреждений, причинения ущерба в крупном размере или наступления иных тяжких последствий;

2) выявления и вовлечения в автоматическом режиме с помощью ИИ-инструментов в различных социальных сетях (в частности в Telegram-каналах и чатах) лиц в террористические либо экстремистские организации. В частности, такие инструменты способны подбирать соответствующих лиц по различным критериям, таким как уровень их радикализации, наличие у них финансовых проблем, протестных настроений и т.п.

Исходя из вышеизложенного видно, что противоправное использование ИИ вносит в уже казалось бы привычные виды преступлений крайне серьезные изменения, требующие своевременной адаптации уголовного права Республики Беларусь.

На данный момент в правовом регулировании ИИ остаются большие пробелы, что является важной задачей для всех государств. Однако, международная практика демонстрирует понимание важности создания особых правовых механизмов, регламентирующих санкции за преступления, совершенные с использованием ИИ-технологий [6].

Например, Итальянская Республика осуществила прямую материально-правовую криминализацию деликтов, связанных с нарушением безопасности ИИ. Так, в конце сентября 2026 года вступил в силу Законодательный декрет 160/2026, которым была введена новая статья 437-bis в Уголовный кодекс Италии «Несоблюдение мер безопасности в системах искусственного интеллекта и незаконное вмешательство в такие системы», которая устанавливает ответственность за:

1) умышленное несоблюдение мер безопасности или контроля в отношении систем искусственного интеллекта;

2) незаконное вмешательство в системы искусственного интеллекта [7]. Данный подход направлен на защиту архитектуры безопасности ИИ. Кроме того, в Италии мошенническое использование ИИ признается отягчающим обстоятельством, ужесточая наказание за выдачу себя за другое лицо, мошенничество, кражу личных данных, «отмывание» денег и финансовое мошенничество.

Рассмотренные проблемы, а также анализ зарубежного опыта (на примере Итальянской Республики), показывает, что главными направлениями регулирования ИИ в уголовно-правовой сфере должны стать внесение изменений базовые институты уголовного права, а также введение новых составов преступлений. В связи с этим видится возможным осуществление следующих мер.

1. Дополнение ст. 64 УК (обстоятельства, отягчающие ответственность) новым пунктом, признающим совершение преступления с использованием технологий ИИ, нейросетей или цифровой симуляции личности обстоятельством, отягчающим ответственность. Данная мера связана с повышенной общественной опасностью таких деяний, в частности с их транснациональным характером, способностью автоматизировать преступную деятельность и масштабировать ее преступный результат, создает дополнительные препятствия правоохранительным органам в противодействии указанным преступлениям.

2. Введение нового квалифицирующего признака «совершенное с использованием технологий искусственного интеллекта» в ряд составов (мошенничество, хищение имущества путем модификации компьютерной информации) по аналогии с признаками «повторно» или «группой лиц». Это будет способствовать индивидуализации ответственности и даст возможность назначать более строгие наказания лицам, использующим ИИ в целях обмана и фальсификации.

3. Введение нового состава в главу 31 УК (преступления против компьютерной безопасности), который бы предусматривал ответственность за создание и распространение «вредоносного» ИИ. В данной главе уже есть ст. 354, устанавливающая ответственность за разработку, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств. Но в данной статье речь идет о компьютерной программе или специальном программном или аппаратном средстве, которые заведомо предназначены для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя. При этом современные нейросети, используемые для совершения указанных действий не подпадают под данную статью, так как они в целом не являются т.н. «вирусами», а представляют собой законный по своей сути программный код, обученный на совершение преступлений.

ЛИТЕРАТУРА

1. Целюк, А. Гора: удельный вес киберпреступлений в общей структуре преступности составил 30 % / А. Целюк // СБ. Беларусь сегодня [Электронный ресурс]. – 2026. – 7 окт. – Режим доступа: https://www.sb.by/articles/gora-udelnyy-ves-kiberprestupleniy-v-obshchey-strukture-prestupnosti-sostavil-30.html. – Дата доступа: 08.10.2026.
2. Уголовный кодекс Республики Беларусь : Кодекс Респ. Беларусь от 9 июля 1999 г. № 275-З : в ред. Закона Респ. Беларусь от 20.10.2025 г. № 101-З // ЭТАЛОН-ONLINE [Электронный ресурс] / Нац. центр законодательства и правовой информации Респ. Беларусь. – Минск, 2026. – Режим доступа: https://etalonline.by/document/?regnum=hk9900275&q_id=6466161. – Дата доступа: 10.10.2026.
3. Шмяткова, Н.В. Искусственный интеллект: субъект или способ совершения преступления? / Н.В. Шмяткова // Государственная служба и кадры. – 2023. – № 5. – С. 276–279.
4. Сорокин, А.И. Искусственный интеллект как объект и средство совершения преступления: уголовно-правовые риски и пределы ответственности / А.И. Сорокин // Образование. Наука. Научные кадры. – 2026. – № 1. – С. 162–167.
5. Корбут, Н.В. Противоправное использование искусственного интеллекта: уголовно-правовая оценка / Н.В. Корбут // Universum: экономика и юриспруденция. – 2026. – № 1 (135). – С. 121–125.
6. Шагапов, И.Р. К вопросу определения субъекта совершения преступления с использованием искусственного интеллекта / И.Р. Шагапов // Российский научный вестник. – 2026. – № 4. – С. 414–420.
7. Morgese, G. Artificial Intelligence: Legislative Decree 160/2026 Enters into Force on 30 September / G. Morgese, P. E. Liedholm, C. Mammola // LCA Studio Legale [Электронный ресурс]. – 2026. – 29 Sept. – Режим доступа: lcalex.it. – Дата доступа: 10.10.2026.