Криминологические риски развития технологий искусственного интеллекта

Criminological risks of the development of artificial intelligence technologies

Будко Д.В.
Адъюнкт 3 факультета (подготовки научных и научно-педагогических кадров)
Академии управления МВД России
e-mail: danilbudko8@dbudko.ru

Budko D.V.
Adjunct of the 3rd faculty (training of scientific and scientific-pedagogical personnel)
Academy of Management of the Ministry of Internal Affairs of Russia
e-mail: danilbudko8@dbudko.ru

Аннотация
В данной работе обозначена проблема бесконтрольного развития технологий, основанных на функционировании искусственного интеллекта, влекущая за собой криминологические риски их использования в преступной деятельности. Актуальность статьи обоснована запросом от государства на разработку комплекса мер по минимизации негативных рисков развития и внедрения искусственного интеллекта. Технологии искусственного интеллекта, в силу своих специфических признаков, общедоступности и распространенности, предоставляют возможность совершения преступлений лицам, не обладающим техническими знаниями. Обращается внимание, что криминальная практика уже содержит ряд преступных деяний, в которых искусственный интеллект использовался как орудие или средство достижения криминальной цели. В целях предупреждения преступлений, связанных с использованием искусственного интеллекта, необходимо проанализировать криминологические риски его развития, в связи с чем автором предлагается применение мер криминологического предупреждения.
Ключевые слова: искусственный интеллект; цифровые технологии; криминологические риски; бесконтрольное развитие; меры криминологического предупреждения.

Abstract
This paper discusses the problem of unregulated development of technologies based on artificial intelligence, which poses criminological risks in their use for criminal activity. The article's relevance is justified by a government request for a set of measures to mitigate the negative consequences of the development and deployment of artificial intelligence technologies. Due to their specific characteristics, accessibility, and prevalence, artificial intelligence technologies provide an opportunity for individuals without technical expertise to commit crimes. This is evidenced by the fact that existing criminal practices already include a number of crimes in which artificial intelligence has been used as a tool or instrument to achieve a criminal objective. In order to prevent crimes associated with the use of artificial intelligence, it is essential to analyze the criminal risks of its development. In this regard, the author suggests the adoption of preventive measures based on criminology.

Keywords: artificial intelligence; digital technologies; criminological risks; uncontrolled-led development; measures of criminological prevention.

В настоящее время IT-технологии являются одним из наиболее важных и неоспоримых факторов развития общества и государства, несмотря на порождаемые ими негативные последствия в виде цифровой преступности.

Практически на протяжении всего эволюционного процесса человечества, дальнейшее его развитие определялось научно-техническим прогрессом. По мнению А.В. Аносова, поиск и адаптация современных информационных технологий под решение конкретных прикладных задач является существенным ресурсом совершенствования системы сбора, хранения и использования информации [1, с. 212]. Но данная тенденция скрывает в себе большие опасности. С большей степенью укрепления информационно-телекоммуникационных технологий (далее-ИТТ) в обществе, процент совершения преступлений, связанных с данной сферой, возрастал ускоренными темпами, что нельзя сказать о раскрываемости подобных деяний.

Данное положение позволяет сделать вывод, что техническое развитие без должного его «осмысления» и без постепенного введения «новейших» цифровых открытий в общественные процессы, в своей основе, порождает множество различных рисков негативного проявления во всех общественных отношениях, в том числе, в уголовном судопроизводстве. Как справедливо отмечает А.В. Победкин, «…механическое внедрение дистанционных информационно-телекоммуникационных технологий в уголовное судопроизводство чревато порождением в народе недоверия к системе уголовной юстиции и приведением в зыбкое состояние гарантий прав человека, участвующего в следственных действиях» [2, с. 38].

Новой вехой развития цифровых информационных систем являются технологии искусственного интеллекта (далее-ИИ), способные обрабатывать огромный массив информационных данных за короткий промежуток времени и принимать самостоятельные решения.

На VIII конференции по развитию ИИ AIJ «Путешествие в мир искусственного интеллекта» было отмечено, что в основе технологического революционного прорыва в индустрии 5.0 будут лежать технологии ИИ. Практически всеми передовыми странами в области развития ИТТ была дана положительная характеристика данным метатехнологиям, определяя им лидирующую позицию, в частности, в сфере социально-экономического развития. Обладая высоким мультипликативным эффектом, технологии ИИ в будущем могут стать основой для выделения нового показателя экономического развития государства, заменяющего показатели ВВП.

Как отмечают многие специалисты, технологии ИИ уже являются научным драйвером развития мира и вскоре в основе всех других технологических разработок будут представлены именно технологи ИИ. Неслучайно Президентом Российской Федерации В.В. Путиным на вышеупомянутой конференции было отмечено, что «генеративный ИИ – это новая глава существования человечества» [3].

Технологии ИИ молниеносно внедряются во многие общественные процессы, все это обуславливается необходимостью развития социума. Государственная политика также нацелена на их скорейшее использование в своем преобразовании и совершенствовании, но, обращая внимание на пройденный негативный опыт, существует определенная необходимость просчитывать риски их использования. По единодушному признанию специалистов, глобальные процессы технического, технологического и других направлений развития

решительным образом усложнили условия жизни социума и превратили его в мировое общество всеобщего риска, а борьбу с рисками — в одно из условий всеобщего выживания [4, с. 137].

Понятийный аппарат и общие признаки технологии ИИ весьма подробно раскрываются в Указе Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», который утверждает Национальную стратегию развития искусственного интеллекта на период до 2030 г.

Для наиболее лучшего представления о технологиях ИИ необходимо выделить его основные элементы. В частности, ИИ – это комплекс технологических решений, который включает в себя: информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе использующее методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Технологии ИИ раскрываются посредством следующего аппаратно-программного комплекса: компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальная поддержка принятия решений и перспективные методы искусственного интеллекта.

ИИ обладает специфическими характеристиками в сравнении с иными цифровыми продуктами, а именно: позволяет имитировать когнитивные функции человека (большие языковые модели – генеративные искусственные нейросети); при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

Также ИИ позиционируется как «сквозная технология», что означает универсальность, не привязанность к одной из конкретной сфер, его функционирование предполагается во всех областях человеческой жизнедеятельности. В то же время в утвержденной распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г. (далее-Концепция) подчеркивается, что развитие технологий искусственного интеллекта ставит серьезные вызовы перед правовой системой Российской Федерации, системой государственного управления и обществом в целом. Они обусловлены определенной степенью автономности действий систем ИИ в решении поставленных задач и их неспособностью непосредственно воспринимать этические и правовые нормы, учитывать их при осуществлении каких-либо действий» [5].

В данной Концепции государство отражает острый вопрос по развитию и интеграции технологий ИИ, отмечая, что необходима нормативно-правовая регуляция данной области с целью предупреждения коллизий, возникающих в процессе применения подобной системы. Также отмечена необходимость уделения особого внимания тому, что ИИ может функционировать без оператора (управляющего), т.е. обладает большой автономностью, что раскрывает новые грани в его применении, но в то же время, он не обладает этическими и правовыми запретами, что может привести в его использовании к негативным последствиям.

Категория автономности ИИ волнует множество исследователей, изучающих вопросы его развития и применения. Особенно остро идут обсуждения вокруг установления правосубъектности при совершенном преступлении, в котором были задействованы технологии ИИ.

Некоторые российские исследователи предполагают, что алгоритм действий робота полностью определяется человеком, даже если речь идет об искусственном интеллекте и самообучаемых нейронных сетях [6, с. 52]. В этом положении есть верная мысль касаемо того, что комплекс задач и наполнительное содержание запросов перед ИИ ставит непосредственно пользователь. Но сам принцип функционирования ИИ содержит в себе коренную основу независимости проведения цифровых операций

между искусственными нейронными связями, и сами разработчики данной технологии определяют, что на текущий момент невозможно проследить логическую цепочку последовательности действий принимаемых ими решений. Этот аспект имеет название «проблема чёрного ящика».

Другие авторы считают, что необходимо возложить ответственность за последствия функционирования ИИ на создателя (программиста) [7, с. 12]. При этом важнейшим вопросом использования интеллектуальных компьютерных систем является правовая регламентация «вопроса об ошибках при программировании и их последствиях» [8, с. 17]. В защиту этого мнения можно сказать, что действительно, лицо, создающее технологии на основе ИИ, может допустить специально или в силу своего незнания, ошибку, которая приведет к использованию данной цифровой системы в незаконных целях, но будет ли в этом случае уместен вопрос о наличии умысла? По нашему мнению, если у создателя был умысел на дальнейшее использование ИИ в преступных целях, либо он сознательно оставил без внимания таковую возможность, не разрабатывая «барьер» недопущения запросов, повлекших за собой возможность совершения преступных деяний, то имеет смысл говорить об уголовной правосубъектности.

Примером может послужить функционирование ИИ на основе искусственной нейросети, создающей новостные заголовки по запросам пользователя. Отсутствие критериев ценза привело к тому, что любой желающий мог создать новостную повестку, носящую в себе явно экстремистский подтекст [9, с. 282].

Также необходимо сказать, что мировой практике уже известны случаи применения технологий ИИ в механизме совершения преступления, в частности:

- технологии DeepFake по замене человеческого лица и синтеза голоса используются в мошеннических действиях, преступлениях, затрагивающих конституционные права граждан;
- распространение сфальсифицированных агитационных материалов;
- разработка вредоносных компьютерных программ;
- использование автономной робототехники для перевозки запрещенных предметов, дезорганизации критических информационных инфраструктур;
- доведения до самоубийства человека вследствие контакта с искусственной нейросетью, выступавшей в роли психотерапевта;

Кроме того, ИИ используется преступниками для разработки новых преступных методов социальной инженерии, учитывая способность отвечать на сообщения в контексте и использовать специфический стиль общения с целью получения пользовательских паролей и иных личных данных.

По мнению В.С. Овчинского, несмотря на отсутствие сведений о разработках киберпреступников в сфере ИИ, потенциальная возможность такого явления существует: «У киберкриминала есть из чего выбрать для создания собственных мощных платформ ИИ. Практически все разработки ИИ с открытым исходным кодом представляют собой контейнеры. Контейнер-это платформа, на которой при помощи API могут монтироваться любые сторонние программы, сервисы, базы данных и т.п. Если раньше каждый при создании собственной программы или сервиса должен был от начала до конца первоначально разработать алгоритмы, а затем, пользуясь тем или иным языком программирования, перевести их в код, то сегодня возможно создавать продукты и сервисы так же, как строители строят дом-из стандартных, доставленных на стройплощадку деталей». Тем самым подтверждается исключительная особенность, что пользователями разработок на основе ИИ может стать любой человек, не имея специальных знаний в данной области.

Есть действительные основания полагать, что технологии ИИ прочно закрепятся в общественной жизни. В результате этого присутствуют существенные риски всплеска преступности, в которой главным его элементом в механизме

совершения преступления будут выступать подобные метатехнологии. Тем более уже довольно давно и достаточно активно криминальный мир применяет современные технические средства в своем противозаконном промысле. Когда данные прорывные технологии станут общедоступны и понятны не только специалистам, но и «рядовым мошенникам», не имеющим узкой технической специализации, например, связанной с компьютерным программированием, то тогда криминогенная ситуация будет носить массовый характер и обладать высокой степенью риска.

Обоснованную классификацию криминологических рисков предлагает И.Р. Бегишев, определяя 4 категории риска и рассматривая их через парадигму тяжести последствий при причинении вреда: незначительный риск, существенный риск, высокий риск и критический риск. В свою очередь, можно спрогнозировать, что при общей доступности использования технологий, основанных на ИИ, без уделения внимания разработке комплекса мер по недопущению совершения преступлений, связанных с ними, за минимальный промежуток времени уровень криминологического риска будет характеризоваться «высоким» [10, с. 119-122]. Главной особенностью данной категории риска будет являться то, что пользователь программного обеспечения понимает и осознает собственные преступные действия.

Закрывать глаза на проблему рисков неразумно. В первую очередь это может сказаться (и сказывается!) на качестве решения задач предупреждения преступлений: картина криминальной детерминации оказывается неполной, ее оценка неточной и, следовательно, профилактическая система лишается некоторых важных предпосылок повышения эффективности своих практических усилий. Не говоря уже о том, что риски, не взятые под контроль, оставленные на свободе, быстро разрастаются и превращаются в масштабные угрозы безопасности граждан, общества, государства [4, с. 138].

Содержательную сущность дефиниции «риск» в криминологии М.М. Бабаев определяет, как «возможная криминогенная опасность».

Не только учет реального состояния, но и прогностическую оценку будущего, включающую оценку рисков, надо рассматривать как непременную составляющую интеллектуального обеспечения грамотной уголовной политики и, в частности, криминологии [11, с. 104].

Указанные выше положения позволяют говорить, что стадия формирования категории криминогенной опасности достигнута уже на достаточно серьезном уровне. Во-первых, технологии ИИ в силу своей специфичности являются сложными для понимания многих людей, но постепенно они открываются для общества и становятся более «прозрачными», тем самым раскрывая свои возможности не только специалистам, но и обычному пользователю. Во-вторых, мировая криминальная практика уже представляет собой ряд преступных деяний, перечисленных выше, в совершении которых основную позицию занимали технологии ИИ. В-третьих, в силу своих технических преимуществ, например таких как, возможность осуществления большой многозадачности цифровых процессов, множественным выполнением операций за одну единицу измерения, поддерживая при этом на достаточно высоком уровне логико-вычислительные расчеты, общедоступность, беспрепятственное использование как на нормативном уровне, так и техническом и т.п., интерес криминалитета к данным технологиям будет возрастать, явно опережая стадии внедрения ИИ в гражданское общество.

С целью предупреждения преступлений, в основе которых используются технологии генеративного ИИ и установления контроля со стороны правоохранительных органов, для минимизации рисков проявления криминальных возможностей в данной области, целесообразно разработать комплекс криминологических мер по недопущению возникновения угроз общественной безопасности по следующим направлениям:

- общесоциальное предупреждение (реализация ряда нормативно-правовых положений, в частности, Указа Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»; дальнейшее формирование нормативно-правовой базы и регламентов использования ИИ с учетом криминальных угроз);

- специально-криминологическое предупреждение (разработка индикаторов применения ИИ в механизме совершения преступления; осуществление криминологических превентивных мер в сфере использования генеративного ИИ; повышение защищенности объектов критической инфраструктуры и иных ресурсов; подготовка специалистов в области анализа криминогенных факторов использования ИИ и разработка методики криминологической экспертизы внедрения технологий ИИ в деятельность государственных и негосударственных структур);

- индивидуальное предупреждение (выявление особенностей личности преступника, использующего современные технологии ИИ, их типологизация);

- виктимологическая профилактика (разработка рекомендаций для населения по повышению уровня защищенности личных данных с учетом ненадежности ранее считавшихся устойчивыми к подделке биометрических показателей и технических средств защиты, включая криптографию; противодействие социальной инженерии; повышение технической грамотности населения).

Таким образом, выявление рисков на ранней стадии развития социально-негативного явления, в основе которого лежит преступное применение ИИ, позволит заранее выработать комплекс мер по противодействию криминальному миру, тем самым контролируя социально приемлемый уровень преступности, не допуская резкого скачка преступлений в данной сфере. Разработка мер криминологического предупреждения позволит комплексно подойти к решению данной проблемы, исследуя личность преступника и виктимологическое поведение жертвы, учитывая причины и условия совершения преступлений, в которых используются технологии ИИ.

Литература

1. Аносов, А. В. Использование технологии блокчейн в процессе формирования и учета криминологической информации / А. В. Аносов // Вестник Казанского юридического института МВД России. – 2018. – № 2(32). – С. 211-216. – DOI 10.24420/KUI.2018.32.13968. – EDN URZWIM.

2. Победкин, А. В. Процессуальные гарантии объективности уголовного судопроизводства в условиях рисков цифровизации / А. В. Победкин // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации : Сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / Под редакцией Ю.В. Гаврилина, Ю.В. Шпагиной. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2021. – С. 31-40. – EDN DYGCAC.

3. AI Journey 2023 – Международная конференция Сбера по искусственному интеллекту / Сайт «aij.ru» [Электронный ресурс]. URL: https:// aij.ru/?yscklid=ls3jvl458p761321830 (дата обращения: 20.01.2024).

4. Бабаев, М. М. Феномен риска в контексте профилактической политики(криминальная рискология) / М. М. Бабаев, Ю. Е. Пудовочкин // Вестник Санкт-Петербургского университета. Право. – 2019. – Т. 10, № 1. – С. 136-148. – DOI 10.21638/spbu14.2019.110. – EDN PPNJWZ.

5. Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р // Собрание законодательства Российской Федерации. 2020. № 35. Ст. 5593. «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.»
6. Васильев, А. А. Правовое регулирование робототехники и искусственного интеллекта в Европейском Союзе / А. А. Васильев, Ж. И. Ибрагимов // Российско-азиатский правовой журнал. – 2019. – № 1. – С. 50–54.
7. Тирранен, В. А. Преступления с использованием искусственного интеллекта / В. А. Тирранен // Развитие территорий. – 2019. – № 3(17). – С. 10-13. – DOI 10.32324/2412-8945-2019-3-10-13. – EDN FKOQNA.
8. Васильев, А. А. Искусственный интеллект и право: проблемы, перспективы / А. А. Васильев, Ю. В. Печатнова // Российско-азиатский правовой журнал. – 2020. – № 2. – С. 14-18.
9. Калашников, Н. А. Анализ и выявление экстремистских рисков в работе нейросетей / Н. А. Калашников, О. Е. Козлова // Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / Под редакцией И.Р. Бегишева [и др.]. Том 4. – Казань: Издательство "Познание", 2022. – С. 280-284. – EDN DXDSIC.
10. Бегишев, И. Р. Уголовно-правовая охрана общественных отношений, связанных с робототехникой: диссертация на соискание ученой степени доктора юридических наук: специальность 12.00.08 - Уголовное право и криминология; уголовно-исполнительное право - Казань, 2022 - 506 л.
11. Бабаев, М. М. Риски как компонент детерминационного комплекса преступности // Вестник Нижегородской академии МВД России. 2018. № 1 (41). С. 104-110.