

Научная статья
УДК 343.97
DOI: 10.47475/2311-696X-2024-43-4-148-153

С.148–153

РИСКИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА КАК ОРУДИЯ И СРЕДСТВА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ПРОТИВОДЕЙСТВИЯ

Татьяна Валентиновна Пинкевич¹, Денис Андреевич Конев²


¹ Академия управления МВД России, Москва, Россия

pinkevich@yandex.ru

 <https://orcid.org/0000-0002-5481-0338>

² Территориальная генерирующая компания № 1, Санкт-Петербург, Россия

marwel8@mail.ru

 <https://orcid.org/0009-0005-7813-8979>

Аннотация. Развитие цифровых технологий и их активное внедрение во все сферы жизни общества и государства привели к появлению новых видов преступлений, связанных с использованием искусственного интеллекта. При изучении искусственного интеллекта рассматривают как область информатики, занимающейся созданием систем, способных выполнять задачи, требующие интеллектуальных способностей человека. В статье представлены результаты исследования рисков использования искусственного интеллекта, в том числе в качестве орудия и средства совершения преступлений, которые могут причинить существенный вред личности, обществу и государству. Особое внимание в статье уделено анализу рисков использования искусственного интеллекта, проблемам его правового регулирования и использованию данной технологии в преступных целях.

В ходе исследования авторы приходят к выводу о необходимости разработки комплекса мер по противодействию преступлениям, совершённым с использованием искусственного интеллекта.

Ключевые слова: искусственный интеллект, персональные данные, законодательство, преступления, цифровые права, интеллектуальная собственность, противодействие, правовое регулирование

Для цитирования: Пинкевич Т. В., Конев Д. А. Риски использования искусственного интеллекта как орудия и средства совершения преступлений: проблемы правового регулирования и противодействия // Правопорядок история, теория, практика. 2024. № 4 (43). С. 148–153. DOI: 10.47475/2311-696X-2024-43-4-148-153

Research article

THE RISKS OF USING ARTIFICIAL INTELLIGENCE AS A TOOL AND MEANS OF COMMITTING OFFENCES: PROBLEMS OF LEGAL REGULATION AND WAYS OF COUNTERACTING THEM

Tatyana V. Pinkevich¹, Denis A. Konev²


¹ Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia

pinkevich@yandex.ru

 <https://orcid.org/0000-0002-5481-0338>

² Territorial Generating Company No. 1, St. Petersburg, Russia

marwel8@mail.ru

 <https://orcid.org/0009-0005-7813-8979>

Abstract. The development of digital technologies and their active introduction into all spheres of life of society and the state have led to the emergence of new types of offences related to the use of artificial intelligence. When studying artificial intelligence is considered as a field of computer science dealing with the creation of systems capable of performing tasks that require human intellectual abilities. The article presents the results of the study of the risks of using artificial intelligence, including as a tool and means of committing crimes that can cause significant harm to the individual, society and the state. Special attention in the article is paid to the analysis of the risks of using artificial intelligence, the problems of its legal regulation and the use of this technology for criminal purposes.

In the course of the study, the authors conclude that it is necessary to develop a set of measures to counteract crimes committed with the use of artificial intelligence.

Keywords: artificial intelligence, personal data, legislation, crime, digital rights, intellectual property, counteraction, legal regulation

For citation: Pinkevich TV, Konev DA. The Risks of using artificial intelligence as a tool and means of committing offences: problems of legal regulation and ways of counteracting them. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(4):148-153. (In Russ.) DOI: 10.47475/2311-696X-2024-43-4-148-153

Введение

Искусственный интеллект (далее — ИИ) является одной из самых востребованных технологий в условиях цифровизации в России. Использование ИИ в практической деятельности дает широкие возможности для улучшения качества жизнедеятельности общества. В то же время использование ИИ несет в себе риски, которые чаще всего связаны с доступностью использования ИИ в преступной деятельности. При этом подготовка мер предупредительного характера в этой сфере затруднена, поскольку до настоящего времени отсутствуют единое мнение и понимание сущности ИИ, а также не уточнено какие именно технологии следует рассматривать в качестве ИИ и пр. Особого внимания требует правовая основа развивающихся цифровых технологий в целом, в том числе и ИИ, поскольку отсутствует надлежащий контроль со стороны государства, не подготовлен пакет документов для правового регулирования ИИ, преступные элементы имеют возможность его широко использовать при совершении преступлений и избегать уголовной ответственности. В связи с изложенным, в статье представлены результаты исследования названных проблем, разработан и предложен алгоритм действий для контроля за использованием ИИ, сдерживания и отмечена необходимость ограничения использования ИИ в преступной деятельности. Так, для предотвращения возможных негативных последствий необходимо разработать комплекс мер по противодействию преступлениям, совершённым с использованием ИИ, усилить контроль за его использованием, особенно в тех областях, где он может представлять угрозу для нормально функционирования государства и социума.

Материал и методы

Материалами исследования послужили: законодательная база, составляющая правовую основу внедрения и развития цифровых технологий, в том числе и технологии искусственного интеллекта, а также документы регламентирующие деятельность по защите личности, общества и государства от преступных посягательств, в которых орудием и средством совершения преступления выступает технология искусственный интеллект. В качестве методологического инструментария выступили эмпирический и лингвистический методы познания, научно-аналитический подход, а также специально-юридические методы: формально-юридический и сравнительно-правовой.

Описание исследования

Современное общество уже не представляет жизнь без цифровых технологий, поскольку в повседневной жизни

постоянно пользуются такой продукцией, как Алиса, Google Maps, Siri и др. Социум живет в цифровом мире, но больший интерес вызывает развитие технологии искусственного интеллекта, поскольку «без искусственного интеллекта невозможно повышение конкурентоспособности в мире и национальной безопасности» [1, с. 171]. Действительно, сегодня использование искусственного интеллекта становится обыденным. Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации в 2023 г. провел опрос населения (1600 респондентов), выясняя отношение к технологии ИИ и получил следующие результаты:

«— 47 % за последний год пользовались устройствами или услугами, в которых применяются технологии ИИ несколько раз в неделю и чаще;

— в повседневной жизни сталкивались с технологиями ИИ в сферах онлайн покупок (52 %) и финансовых услуг (40 %);

— чаще в повседневной жизни пользуются технологиями ИИ в составе таких сервисов как навигаторы, умные медиа-рекомендации, онлайн-переводчики и голосовые помощники;

— использование технологий ИИ скажется положительно на качестве жизни людей (64 %) и имидже государства на мировой арене (61 %);

— 82 % согласны с тем, что ИИ сегодня — важен для развития самых разных сфер;

— наиболее часто респонденты ожидают внедрения технологий ИИ в сферах безопасности (31 %), здравоохранения (29 %) и освоения космоса (25 %);

— технологии ИИ приносят людям пользу (78 %), необходимы обществу (73 %) и не представляют опасности (63 %);

— беспокоит возможность роста безработицы (56 %) и риски, связанные с неправомерным использованием технологий ИИ (54 %)»¹.

Как свидетельствуют полученные результаты исследования, интерес к развитию и использованию технологии ИИ не ослабевает, а наоборот, набирает силу — с одной стороны. С другой же стороны видим обеспокоенность населения рисками, которые будут возрастать при неправомерном использовании технологий ИИ. Следует признать, что беспокойство у респондентов

¹ 2023 Доверие к искусственному интеллекту в обществе. Экспресс-анализ социологических опросов 1 квартала 2023 года, НЦРИИ // Национальный портал в сфере Искусственного интеллекта. URL: https://ai.gov.ru/knowledgebase/etika-i-bezopasnost-ii/2023_doverie_k_iskusstvennomu_intellektu_v_obschestve_ekspress-analiz_sociologicheskikh_oprosov_i_kvartala_2023_goda_ncrii/ (дата обращения: 22.10.2024).

вызывает и безработица (56 %). Однако следует понимать, что вопрос при использовании ИИ стоит не о полной замене человека в своей деятельности, это неверный подход. Задача заключается в том, чтобы использовать искусственный интеллект для оказания помощи в любой, например, правоохранительной деятельности, для повышения уровня ее эффективности. Такого мнения придерживается и Т. В. Радченко, указывая при этом, что «основной целью при этом должна стать не попытка заменить человеческий разум компьютерной программой, использующей искусственный интеллект, а оказание помощи правоприменителю в проведении отдельных следственных и процессуальных действий, фиксации материалов расследования в целях оптимизации и повышения эффективности деятельности» [2, с. 182]. Так, например, исследователи Центра математической робототехники и искусственного интеллекта Санкт-Петербургского государственного университета разработали новый метод поиска людей: специалисты сделали упор на акустическую систему, включающую определение в реальном времени человеческого голоса, отсекая лишние шумы — звуки воды, ветра, шум пропеллеров¹. При этом имеются и другие факты использования ИИ в правоприменительной деятельности, например, роботы-адвокаты, составляющие простую, разъяснительную документацию; роботы — помощники судей, проводящие автоматизированный поиск необходимых данных среди множества правовых норм и др.

И действительно, риски названного типа существуют. Развитие и применение ИИ, благодаря подготовленной электронной компонентной базы для использования и применения ИИ, позволило создать ключевые группы технологий ИИ: компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальные системы поддержки принятия решений и перспективные методы в области ИИ.

Использование названных групп технологий и систем ИИ, по мнению А. А. Карцхия, может «осуществляться с определением трех важных аспектов: (1) методов создания искусственного интеллекта (например, машинного обучения); (2) функциональных приложений искусственного интеллекта (обработка речи, компьютерное зрение); (3) приложения технологий искусственного интеллекта (коммуникационные технологии или автономное транспортное средство)» [3, с. 384]. Эти системы способны обучаться на основе различных, получаемых данных, принимать решения, адаптироваться к новой информации и самостоятельно решать сложные задачи². Опасность их применения заключается в том, что ИИ:

а) может имитировать когнитивные функции человека с использованием системы сложных алгоритмов. Эти системы способны обучаться на основе различных получаемых данных, принимать решения, адаптироваться к новой информации и самостоятельно решать сложные задачи³. При этом «глубокие нейронные сети принимают решения не на основе известных алгоритмов, и в ряде случаев проанализировать, как они выбирают решение, невозможно... И в этом кроется опасность тотального использования искусственного интеллекта, потенциально возрастающая» [2, с. 181];

б) его использование в преступной деятельности представляет серьезную угрозу для безопасности личности, общества и государства, а поскольку «ИИ уже сейчас применяется во многих областях, число которых будет расти, можно сделать вывод о том, что и противоправная деятельность потенциально станет осуществляться практически во всех сферах. Если же развитая система искусственного интеллекта будет управлять антропоморфным телом, то не исключается совершение им общественно опасных деяний, предусмотренных любыми статьями Особенной части УК РФ» [4, с. 466].

С каждым годом увеличивается количество отраслей, в том числе и ключевых отраслей экономики, в которые внедрен ИИ, и в которых он может использоваться. С появлением в GPT-4 технологий искусственного интеллекта ИИ переживает второе рождение. Они могут использоваться для «моделирования (прогнозирования) развития определенных событий и процессов экономического, социального и природного плана на основе методов математического моделирования и математической статистики для различных целей, включая моделирование возможных рисков (the probability of adverse consequences) в определенных процессах, основанных на технологии „цифровых двойников“» [3, с. 385]. Это очень важный момент, поскольку результаты прогноза и моделирования позволят проводить профилактику, в том числе и виктимологическую профилактику [7, с. 10] на стадии выявления преступного замысла.

В последние годы значительно возросло количество судебных споров, предметом которых являются вопросы использования ИИ в различных сферах деятельности человека. С марта 2023 по март 2024 гг. российские суды вынесли 406 решений по вопросам применения ИИ — на 60 % больше аналогичного периода прошлого года⁴. Такая тенденция указывает на ускоренное внедрение ИИ в жизнь человека и деятельность государства, что помимо благ для общества, личности и государства, появилось много вопросов, связанных с правовой регламентацией использования ИИ. Действительно, несмотря на значительные достижения в этой области, повсеместное внедрение ИИ в жизнедеятельность общества вызывает серьезные проблемы, связанные с отсутствием его правового регулирования.

¹ Дроны-спасатели: как ИИ помогает находить потерявшихся людей в лесу // Национальный портал в сфере Искусственного интеллекта. URL: <https://ai.gov.ru/mediacenter/drony-spatateli-kak-ii-pomogaet-nakhodit-poteryavshikhsya-lyudey-v-lesu/> (дата обращения: 10.06.2024).

² Искусственный интеллект и программные алгоритмы: границы и отличия // vc.ru. URL: <https://vc.ru/education/1016240-iskusstvennyi-intellekt-i-programmnye-algoritmy-granicy-i-otlichiya> (дата обращения: 03.06.2024).

³ Там же.

⁴ За год число судебных решений в спорах вокруг применения ИИ в РФ увеличилось на 60 % // Хабр. URL: <https://habr.com/ru/news/803895/> (дата обращения: 10.06.2024).

Проблемы правового регулирования ИИ становятся все более актуальными в современном мире. Развитие цифровых технологий и автоматизация процессов ведут к тому, что ИИ начинает играть значительную роль в жизни жителей планеты Земля, что влечёт за собой его внедрение в новые сферы деятельности.

Национальная стратегия развития искусственного интеллекта на период до 2030 года содержит понятие «искусственного интеллекта», «технологии искусственного интеллекта»¹, однако нет единого понимания того, какие именно технологии следует относить к ИИ, а какие нет. Некоторые системы могут быть классифицированы как ИИ, но не все они обладают главными способностями — обучению, самообучению и адаптации. Это создает сложности в определении границ применения ИИ и установлении общих правил его использования, особенно в тех случаях, когда создают ИИ, который самостоятельно производит аналогичный и наделяет его произвольными функциями ИИ². В случае совершения каких-либо неправомерных действий таким, вновь созданным ИИ, будет очень сложно определить конкретные области действующего права и дать юридическую оценку подобному случаю, по причине отсутствия определения понятия самого автора — ИИ. Более того, нет четкого определения в том, как они используются, кто отвечает за их применение, какой и кем осуществляется контроль за их использованием и т. д.

Отсутствие контроля за использованием ИИ способствует использованию его в преступных целях. Примером тому может служить факт обнаружения в Великобритании компании, которая использовала ИИ для изготовления фальшивых удостоверений личности³. В ходе расследования уголовного дела, возбужденного по изложенным обстоятельствам, правоохранительные органы столкнулись с проблемами, связанными с тем фактом, что большую часть заявок на такие документы и изготовление самих документов ИИ проводил самостоятельно, без вмешательства человека.

Отсутствие контроля за противоправным использованием ИИ со стороны государства способствует безнаказанному совершению преступлений. Более того, совместное использование ИИ с иными цифровыми технологиями, например такими как массивы данных (Big Data) или интернет вещей (IoT, Internet of Things) повышают уровень опасности, поскольку ИИ становится более мощным инструментом, который может быть

использован и используется при совершении преступлений, что само по себе несет серьезные риски для безопасности личности, общества и государства. Примером таких рисков может служить его использование при создании сложных мошеннических схем, взломе систем безопасности, создании и использовании вредоносных программ, оружия массового поражения, а возможность его самообучения и отсутствие алгоритма для каких-либо его ограничений вызывает опасение. Вызывает опасение и использование преступниками системы распознавания лиц в преступных целях, например для слежки за людьми без их согласия. В этом случае следует говорить о нарушении прав человека.

При этом, учитывая тот факт, что 66 % граждан России пока еще не готовы доверить свои жизни нейросетям⁴, использование ИИ при совершении преступлений может привести к негативному восприятию этих технологий и отказу от их использования в будущем. В целях предупреждения противоправного использования ИИ необходимо «формирование перечня технологий ИИ, применение которых целесообразно для создания (модернизации) и эксплуатации специальной техники и информационных систем в правоохранительных органах; осуществление стандартизации интеллектуальных технологий в интересах названных органов; формирование и утверждение программы научных исследований и разработок, направленных на создание и внедрение перспективных технологий ИИ» [5, с. 184].

В связи с этим необходимо принятие мер, направленных на ужесточение контроля за противоправным использованием ИИ во всех сферах жизнедеятельности общества. В этом большую помощь могут оказать результаты мониторинга развития и влияния технологий ИИ на жизнедеятельность и общественную безопасность личности, общества и государства, которые позволят определять основные тенденции направления его использования. Следует расширить исследования в этой области с целью дальнейшей разработки современных методов и инструментов для противодействия преступлениям, совершаемым с использованием ИИ, особое внимание уделяя исследованию рисков использования искусственного интеллекта [6].

В этом случае одним из приоритетных направлений деятельности по предупреждению противоправного использования технологии ИИ будет являться необходимость создания правовой основы, которая может снизить уровень названных угроз. Данная работа должна осуществляться во взаимодействии государственных органов, бизнеса и научного сообщества. Это позволит подготовить теоретически обоснованную стратегию правового регулирования ИИ для предоставления, рассмотрения и принятия ее проекта в законодательные органы России. В данном документе должны быть учтены интересы

¹ О развитии искусственного интеллекта в Российской Федерации (вместе с Национальная стратегия развития искусственного интеллекта на период до 2030 года) : Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 20.10.2024).

² Исследователи создали ИИ, который создает ИИ // Хабр. URL: <https://habr.com/ru/news/648151/> (дата обращения: 19.06.2024).

³ Fraudsters are using AI to churn out fake IDs before selling them to under-18s for as little as £12 — and experts say supermarkets, pubs and airports need to be on 'red alert' // Daily Mail Online. URL: <https://www.dailymail.co.uk/sciencetech/article-13252539/Fraudsters-AI-fake-IDs-red-alert.html> (дата обращения: 15.06.2024).

⁴ Бобров Б. Исследование: треть россиян готовы доверить свою жизнь ИИ // Российская газета. URL: <https://rg.ru/2023/10/12/issledovanie-tret-rossiiian-gotovy-doverit-svoiu-zhizn-ii.html?ysclid=m2lrtoux4506518393> (дата обращения 23.10.24)

всех легитимных сторон, но в тоже время его содержание не должно мешать развитию и применению ИИ.

Заключение и вывод

В целях повышения эффективности предупреждения противоправного использования ИИ с учетом результатов, полученных в ходе исследования, необходимо:

— ужесточение контроля над использованием ИИ. В связи с этим важным является подготовка административных регламентов применения, использования технологий ИИ и контроля за их использованием, которые определяют общие правила их использования. Они должны включать в себя определение ответственности за действия ИИ, установление правил его использования и защиту прав потребителей, в том числе и ограничение доступа к ряду функций, которые он в себе несет. Важно разработать единую классификацию технологий ИИ, что позволит разработать более конкретные правила его применения и ограничения в каждой конкретной ситуации;

— совершенствование имеющейся нормативной базы. Законодательство должно быть достаточно гибким, чтобы учитывать быстро развивающиеся технологии ИИ, но в то же время оно должно быть достаточно строгим и жестким, опять же по причине сверхбыстрого развития систем ИИ. Это позволит предотвратить злоупотребления и предупредить наступление негативных последствий за противоправные действия, совершаемые с использованием ИИ;

— осуществление постоянного мониторинга и анализа развития технологий ИИ и их влияния на жизнедеятельность общества, что даст возможность своевременно выявлять новые угрозы и риски, а также во взаимодействии государственных органов, бизнеса и общественности своевременно разрабатывать соответствующие меры противодействия преступлениям, совершаемым с использованием ИИ, и купировать на ранних этапах подготовку к преступной деятельности и выявлять новые преступные схемы;

— необходимо осуществлять обучение и повышение квалификации специалистов в области кибербезопасности и использования ИИ, в том числе проводить совместные регулярные обучающие курсы представителей безопасности коммерческих и специализированных государственных силовых структур, что повысит качество взаимодействия и обмена опытом. Это позволит обучающимся получать своевременную информацию о последних тенденциях и разработках в названной области, а также повысить уровень знаний и выработать новые пути предупреждения преступлений и эффективно им противодействовать.

Предложенные меры являются важными и ориентированы на обеспечение общественной безопасности личности, общества и государства. Разработка нормативных правил и использование искусственного интеллекта в этой области может значительно повысить эффективность предупредительной деятельности.

Список источников

1. Грачева Ю. В., Арямов А. А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15, № 6. С. 169–178. DOI: 10.17803/1994-1471.2020.115.6.169-178
2. Радченко Т. В. Роль искусственного интеллекта в системе уголовно-правовых и уголовно-процессуальных отношений // Цифровые технологии и право : сб. науч. трудов II Международной научно-практической конференции, Казань, 22 сентября 2023 г. Том 2. Казань : Познание, 2022. С. 180–184.
3. Карцхия А. А. Перспективы регулирования искусственного интеллекта в современном контексте цифровых технологий // Цифровые технологии и право : сб. науч. трудов. II Международной научно-практической конференции, Казань, 22 сентября 2023 г. Казань : Познание, 2023. С. 384–386.
4. Мосечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10, № 3. С. 461–476. DOI: 10.21638/spbu14.2019.304
5. Кубасов И. А. Проблемные вопросы применения технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации // Вестник Воронежского института МВД России 2021. № 3. С. 180–186.
6. Bostrom N. Superintelligence: Paths, Dangers, Strategies. Hardcover, Oxford University Press, 2016.
7. Майоров А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11, № 1. С. 7–12. DOI: 10.47475/2411-0590-2024-11-1-7-12

ВКЛАД АВТОРОВ

Пинкевич Т. В. Научное руководство, концепция исследования, развитие методологии, сбор материала, итоговые выводы, доработка текста.

Конев А. Н. Подбор материала, социологическое исследование, сбор и обработка статистических данных, написание исходного текста.

AUTHORS' CONTRIBUTION

Pinkevich T. V. Scientific guidance, research concept, development of methodology, collection of material, final conclusions, finalization of the text.

Konev A. N. Selection of material, sociological research, collection and processing of statistical data, writing the original text.

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 04.11.2024.

Дата рецензирования статьи / Revised: 20.11.2024.

Дата принятия статьи к публикации / Accepted: 05.12.2024.
