



О.Ж. Жолдасов¹, Ж.А. Кегембаева²

¹ Академия управления Министерства внутренних дел Республики Казахстан,
г. Астана, Республика Казахстан

² Казахский национальный университет имени аль-Фараби, г. Алматы, Республика Казахстан

АКТУАЛЬНЫЕ ВОПРОСЫ УГОЛОВНОГО ПРАВА В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Статья затрагивает актуальные проблемы уголовно-правового регулирования в контексте быстрого развития и интеграции искусственного интеллекта в различные сферы жизнедеятельности человека. Основное внимание уделяется анализу ответственности за действия, выполненные с использованием искусственного интеллекта, сложностям квалификации таких преступных действий и проблемам со сбором и интерпретацией доказательств при расследовании уголовных дел. Авторами поднимается вопрос о неэффективности традиционных подходов к уголовной ответственности в случаях, когда преступления совершаются с использованием искусственного интеллекта, ведь искусственный интеллект не обладает сознанием или волей, что ставит под вопрос применимость принципов вины и субъективности. Статья также описывает возможные угрозы, такие как использование искусственного интеллекта для военных целей, кибератаки с использованием алгоритмов машинного обучения, преследования людей с помощью алгоритмов распознавания лиц и анализа настроений, а также угрозы безопасности стратегически важных объектов из-за зависимости их инфокоммуникационных сетей обеспечения от интеллектуальных систем. В заключение предлагаются направления для дальнейшего развития законодательства, которые могли бы обеспечить адекватное уголовно-правовое регулирование в условиях продолжающегося внедрения решений искусственного интеллекта в общественную жизнь.

Ключевые слова: искусственный интеллект (ИИ); инфокоммуникационные технологии (ИКТ); кибератака; киберпреступление; машинное обучение; правоохранительный орган; уголовное право; уголовная ответственность.

О.Ж. Жолдасов¹, Ж.А. Кегембаева²

¹ Қазақстан Республикасы Ішкі істер министрлігінің Басқару академиясы,
Астана қ., Қазақстан Республикасы

² Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан Республикасы

ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ДАМУЫ ЖАҒДАЙЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚТЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

Аннотация. Мақала адам өмірінің әртүрлі салаларына жасанды интеллекттің қарқынды дамуы мен интеграциясы тұрғысынан қылмыстық-құқықтық реттеудің өзекті мәселелерін қозғайды. Жасанды интеллект көмегімен жасалған іс-әрекеттер үшін қылмыстық жауаптылықты талдауға, мұндай қылмыстық әрекеттерді саралаудың қиындықтарына және қылмыстық істерді тергеу кезінде дәлелдемелерді жинау мен түсіндіруге қатысты мәселелерге назар аударылады. Авторлар жасанды интеллект көмегімен қылмыстық құқық бұзушылықтар жасалған жағдайларда қылмыстық жауаптылыққа дәстүрлі тәсілдердің тиімсіздігі туралы мәселе көтереді, өйткені жасанды интеллект сана немесе ерік-жігерге ие емес, бұл кінә мен субъективтілік принциптерінің қолданылуына күмән келтіреді. Сондай-ақ, мақалада жасанды интеллектті әскери мақсатта пайдалану, машиналық оқыту алгоритмдерін қолданатын кибершабуылдар, бетті тану және көңіл-күйді талдау алгоритмдері арқылы адамдарды қудалау және ақпараттық-коммуникациялық қамтамасыз ету желілерінің интеллектуалды жүйелерге тәуелділігіне байланысты стратегиялық маңызды объектілердің қауіпсіздігіне ықтимал қауіптер сипатталған. Қорытындылай келе, жасанды интеллект шешімдерін қоғамдық өмірге енгізуді жалғастыру жағдайында тиісті деңгейдегі қылмыстық-құқықтық реттеуді қамтамасыз ете алатын заңнаманы одан әрі дамыту үшін бағыттар ұсынылады.



Түйінді сөздер: жасанды интеллект (ЖИ); инфокоммуникациялық технологиялар (ИКТ); кибершабуыл; киберқылмыс; машиналық оқыту; құқық қорғау органы; қылмыстық құқық; қылмыстық жауаптылық.

O.Zh. Zholdasov¹, Zh.A. Kegembayeva²

*¹Academy of Management of the Ministry of Internal Affairs of the Republic of Kazakhstan,
Astana, the Republic of Kazakhstan*

²Al-Farabi Kazakh National University, Almaty, the Republic of Kazakhstan

CURRENT ISSUES OF CRIMINAL LAW IN THE CONTEXT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract. The article touches upon the actual problems of criminal law regulation in the context of the rapid development and integration of artificial intelligence into various spheres of human activity. The main attention is paid to the analysis of responsibility for actions performed using artificial intelligence, the difficulties of qualifying such criminal actions and problems with the collection and interpretation of evidence in the investigation of criminal cases. The authors raise the issue of the ineffectiveness of traditional approaches to criminal liability in cases where crimes are committed using artificial intelligence, because AI does not have consciousness or will, which calls into question the applicability of the principles of guilt and subjectivity. The article also describes possible threats such as the use of artificial intelligence for military purposes, cyber attacks using machine learning algorithms, harassment of people using facial recognition and mood analysis algorithms, as well as threats to the security of strategically important facilities due to the dependence of their infocommunication support networks on intelligent systems. In conclusion, the directions for further development of legislation are proposed, which could ensure adequate criminal law regulation in the context of the ongoing introduction of artificial intelligence solutions into public life.

Keywords: artificial intelligence (AI); infocommunication technologies (ICT); cyber attack; cybercrime; machine learning; law enforcement agency; criminal law; criminal liability.

DOI: 10.52425/25187252_2025_35_157

Введение. Мы живем в эпоху искусственного интеллекта (далее – ИИ), технологии которого стремительно проникли во все сферы человеческой жизни – от простых бытовых задач до сложных процессов принятия стратегических решений. Однако, за величию технологического прогресса скрываются и невидимые ранее угрозы, которые бросают вызов традиционным правовым отраслям и институтам, в частности, уголовному праву. Этот вызов не только технический, но и философский: как правовая система, созданная людьми и для людей, может эффективно регулировать мир, где решения все чаще принимают машины?

На первый взгляд, ИИ выступает союзником уголовного права, способствуя реализации его принципов и норм. Алгоритмы ИИ способны анализировать данные с точностью, недостижимой для человека, помогая предотвращать уголовные правонарушения, раскрывать и расследовать

их быстрее и объективнее. Однако за этим оптимизмом скрывается другая сторона: алгоритмы ИИ могут быть использованы не только для блага, но и для достижения преступных целей. Как быть с уголовными правонарушениями, совершенными с использованием ИИ? Или, более сложный вопрос: как оценивать автономные действия системы, если ее алгоритмы нарушают закон? Кто понесет ответственность – разработчик или оператор?

Кроме того, развитие ИИ вынуждает задуматься над фундаментальными категориями уголовного права. Например, традиционные понятия вины и умысла становятся недостаточными в контексте автономных технологий. Возможно ли говорить об умысле машины, и, если да, то как это согласуется с традиционными принципами справедливости?

Статья предлагает не только аналитический взгляд на проблему, но и



попытку «заглянуть за горизонт». Авторы исследуют, как взаимодействие права и технологий ИИ меняет само понимание уголовного права, создавая новые подходы и порождая неожиданные дилеммы. В условиях, когда действующие законы сталкиваются с вызовами цифровой эры, перед обществом в целом стоит задача переосмыслить баланс между инновациями и ответственностью, определить тонкую грань между эффективностью и гуманизмом методов, применяемых в уголовном праве.

Материалы и методы. Для исследования актуальных вопросов уголовного права в условиях развития технологий ИИ были использованы междисциплинарные подходы, объединяющие правовой, философский и технологический анализ. Исследование базируется на следующих источниках: нормативные правовые акты, регулирующие сферу применения цифровых технологий, в т.ч. международные конвенции, национальное законодательство; научная литература, посвященная вопросам взаимодействия уголовного права и IT-технологий; а также аналитические материалы, касающиеся различных аспектов функционирования систем ИИ.

Результаты. Проведенное исследование выявило, что современные нормы уголовного права недостаточно адаптированы к вызовам, связанным с развитием технологий ИИ. Традиционные правовые категории, такие как правосубъектность, вина, причинно-следственная связь и т.п., сталкиваются с ограничениями при применении к случаям автономных решений ИИ, что вызывает сложности в определении ответственности. Кроме того, отсутствуют четкие правовые положения, регулирующие использование ИИ, что создает правовую неопределенность и риски злоупотреблений. Вопрос о тенденциях развития уголовно-правовой политики в условиях развития технологий ИИ неизбежно упирается также в морально-этические дилеммы, связанные с поиском баланса между инновационными подходами и гуманизмом, защитой прав человека, включая право на справедливый суд и защиту от дискриминации. Полученные результаты

демонстрируют сложность интеграции новых технологий в традиционные правовые механизмы. Развитие ИИ ставит перед уголовным правом не только задачу адаптации существующих норм, но и требует переосмысления фундаментальных уголовно-правовых принципов. В работе обоснованы предложения по внесению изменений и дополнений в действующий Уголовный кодекс Республики Казахстан (далее – УК РК), в частности, введение четкой дефиниции ИИ, что позволит устранить правовую неопределенность и сформировать базу для регулирования вопросов ответственности. Закрепление дефиниции должно учитывать, как существующие научные подходы, так и потребности правоприменительной практики, включая разграничение понятий «ИИ» и «робот». Кроме того, предложено дополнить УК нормами, регулирующими ответственность за действия автономных систем. Это включает в себя установление критериев для оценки предсказуемости и автономности поведения ИИ, а также четкое распределение ответственности между разработчиками, пользователями и операторами таких систем.

Обсуждение. Технологии ИИ стирают привычные границы между действиями человека и автономными процессами, создавая тем самым «слепые зоны» правового регулирования. Где заканчивается контроль разработчика и начинается автономность системы? Обсуждение этих вызовов неизбежно приводит к необходимости поиска точек равновесия: между эффективным использованием технологий и соблюдением принципов уголовного права.

Темпы развития ИИ таковы, что правовое регулирование, в т.ч. и уголовно-правовое регулирование, просто не успевает за ними. Что можно отметить в числе основных проблем?

Как правило, среди основных угроз, связанных с внедрением ИИ в систему уголовного правосудия, выделяют предвзятость алгоритмов, способную приводить к несправедливым результатам; нарушение конфиденциальности, когда



использование данных угрожает правам и свободам человека; отсутствие четких границ ответственности за решения ИИ, что затрудняет исправление ошибок и предвзятости. Кроме того, существует опасность злонамеренного использования технологий, например, для незаконной слежки или вмешательства в процессы правосудия. Не менее важной угрозой является общественное сопротивление, вызванное непониманием или недоверием к ИИ, что может привести к отрицанию его применения в правоохранительной деятельности [1, 106 стр.].

Соглашаясь с этим перечнем угроз, отметим, что для сферы правоприменения одной из ключевых проблем является определение степени ответственности и ее субъектов при причинении вреда действиями ИИ. Традиционные подходы к уголовной ответственности основываются на принципе вины, что неприменимо к ИИ, не обладающему сознанием или волей. Однако из-за того, что эта технология способна к самообучению и самостоятельным действиям без прямого вмешательства и контроля человека, возникает ряд серьезных вопросов к правовому регулированию отношений, связанных с ИИ, включая вопросы юридической ответственности [2, 117 стр.].

Как подчеркивают исследователи, ИИ недоступны такие категории, как чувство ответственности, самоанализ, моральный самоконтроль и самосуд. Иначе говоря, нравственная оценка уголовного дела доступна исключительно человеку, но не ИИ. В то же время существует противоположная точка зрения, согласно которой прямолинейная логика ИИ, высокая скорость обработки данных, способность анализировать огромные объемы информации и эффективно использовать сетевые источники дают ИИ определенные преимущества перед человеком [3].

Очевидно, что вопросы правосубъектности ИИ не стоят в тех ситуациях, где с применением технологий выполняются

узкие, специализированные задачи, и вся ответственность беспрепятственно может быть возложена на владельца или оператора. В таких ситуациях, хотя сами роботы и ИИ не признаются субъектами юридической ответственности, их создатели или пользователи могут быть привлечены к ответственности за их действия. Если робот причиняет вред, приведший к смерти, это все равно может рассматриваться как убийство, и запрограммировавший его создатель может быть привлечен к ответственности за это преступление. Конечно, создатель не обязательно должен нести уголовную ответственность именно по статье УК об убийстве. В зависимости от таких факторов, как степень халатности при соблюдении мер безопасности, инцидент может быть классифицирован как несчастный случай или привести к обвинению в причинении смерти по неосторожности. По мнению специалистов, здесь действует принцип, похожий на субсидиарную ответственность, когда действия подчиненного субъекта (робота) вменяются в вину ответственному субъекту (создателю). Точно так же, как владелец домашнего животного может быть привлечен к ответственности за действия своей собаки, если он не смог предотвратить причинение вреда, создатели систем ИИ должны внедрять надлежащие функции безопасности для снижения рисков¹.

Однако в отношении автономных систем, выполняющих сложные задачи, которые невозможно заранее полностью контролировать, представляется вполне уместным закрепление их правосубъектности.

В этом аспекте считаем вполне обоснованным мнение зарубежных исследователей, предлагающих введение правовой категории «электронных лиц» для автономных систем, работающих с технологиями ИИ. Это позволило бы систематизировать юридическую ответственность всех вовлеченных сторон (производителей, владельцев, пользователей) и наделить такие системы определенными правами и обязанностями.

¹ Understanding The Criminal Liability of ai [Electronic resource] – Access mode: <https://legalserviceindia.com/legal/article-17007-understanding-the-criminal-liability-of-ai.html> (Access date: 25.02.2025).



«Электронные лица» могли бы регистрироваться в специальном реестре, аналогично юридическим лицам, получая свой правовой статус с момента регистрации. Такой подход целесообразен, например, для ИИ, способного самостоятельно принимать решения или взаимодействовать с людьми, например, заключая контракты [4, 6 стр.].

Объективно оценивая уровень правового регулирования отношений, связанных с ИИ в Казахстане, еще рано говорить о признании самостоятельной категории субъектов права – «электронных лиц», поскольку до сих пор ведутся дискуссии по определениям самых важных терминов. Так, в действующем УК РК вообще не упоминается словосочетание «ИИ».

Более того, дефиниция этого термина не дается и в других законах, которые направлены на правовое регулирование сферы инфокоммуникационных технологий. В Законе РК от 24 ноября 2015 года «Об информатизации» есть определение интеллектуального робота как автоматизированного устройства, способного действовать или бездействовать в зависимости от восприятия внешней среды². Однако это определение, как и в целом подход к ИИ, остается предметом дискуссии, особенно в вопросе разграничения понятий «ИИ» и «робот». Одно очевидно: без четкой нормативной дефиниции любые правовые нормы по регулированию ИИ останутся фрагментарными и, соответственно, неэффективными.

Поэтому в утвержденной постановлением Правительства РК от 24 июля 2024 года Концепции развития искусственного интеллекта на 2024-2029 годы поставлена задача – создание правовой основы для регулирования применения ИИ, включая разработку понятийного аппарата, этических принципов, норм безопасности, ответственности субъектов и механизмов защиты интеллектуальной собственности. Концепция предусматривает предотвращение преступного использования ИИ, упрощение его внедрения, а также маркировку продуктов, созданных с его использо-

ванием. Подзаконные акты будут определять требования к объектам информатизации и классификацию продуктов ИИ³.

Специалистами было предложено множество определений ИИ, которые можно свести к четырем основным подходам: это системы, которые думают, как люди; системы, которые действуют как люди; системы, которые мыслят рационально; и системы, которые действуют рационально [5, 19 стр.]. Эти подходы отражают сложность и многогранность понятия ИИ, которое, несмотря на свою распространенность, до сих пор остается недостаточно четко определенным в правовом поле.

Разработка специальных законодательных актов, регулирующих использование ИИ, является крайне актуальной задачей. В условиях стремительного технологического прогресса необходимо предусмотреть нормативные механизмы, способные охватить все аспекты работы ИИ. Такие акты должны включать четкие определения, которые бы устранили правовую неопределенность, а также регламентировали ответственность за причиненный вред. Это особенно важно для предотвращения злоупотреблений и обеспечения надежной защиты прав и свобод граждан. Как отмечает профессор Г.Р. Рустемова, уголовно-правовое регулирование настоятельно требуется в ситуациях, когда при создании системы ИИ была допущена ошибка, которая впоследствии привела к совершению уголовного правонарушения; когда в систему был осуществлен неправомерный доступ, изменивший функции ИИ; когда ИИ был создан умышленно для совершения преступления [6, 67 стр.]. Кроме того, стандарты разработки и эксплуатации ИИ должны быть четко прописаны, чтобы исключить возможные риски, связанные с непредсказуемым поведением автономных систем.

В УК РК уголовным правонарушением в сфере информатизации и связи посвящена глава 7. В нее входят такие статьи, как неправомерный доступ к информации,

² Об информатизации: закон Республики Казахстан от 24 нояб. 2015 г. № 418-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1500000418> (дата обращения: 17.11.2024).

³ Об утверждении Концепции развития искусственного интеллекта на 2024-2029 годы: постановление Правительства Республики Казахстан от 24 июля 2024 г. № 592 ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/P2400000592> (дата обращения: 18.11.2024).



модификация или уничтожение данных, создание и использование вредоносных программ⁴. Эти нормы могут частично применяться и к ИИ, если рассматривать его как сложную компьютерную программу. Однако без нормативно закреплённого определения самого ИИ применение норм данной главы УК РК остаётся ограниченным.

Для устранения правовой неопределённости и обеспечения надлежащего регулирования предлагаем закрепить дефиниции ИИ непосредственно в тексте главы 7 УК РК. В качестве подходящей нормы для внесения соответствующих изменений и дополнений, наверное, лучше выбрать статью 207 УК РК «Нарушение работы информационной системы или сетей телекоммуникаций». Данная статья прямо касается информационных систем и её расширение за счёт указания, что умышленные посягательства, нарушающие работу, могут касаться и информационных систем с применением ИИ, представляется логичным шагом. Статья 207 УК РК с предлагаемыми изменениями может быть представлена в такой редакции: «1. Умышленные действия (бездействие), направленные на нарушение работы информационной системы, *включая системы с применением искусственного интеллекта, или сетей телекоммуникаций ...*».

Закрепление определения ИИ в качестве примечания к этой статье может быть оформлено следующим образом: «Искусственный интеллект (ИИ) – это программный (программно-аппаратный) элемент информационной системы, интегрированный в её структуру и предназначенный для выполнения задач, связанных с обработкой данных, анализом, прогнозированием, принятием решений, характеризующийся адаптацией к изменениям и взаимодействием с внешней средой, что позволяет автономно выполнять задачи без непосредственного управления человеком на каждом этапе работы». Такое уточнение позволит более точно применять существующие нормы к случаям, связанным с ИИ и не только

укрепит правовую базу, но и создаст условия для последующего внесения изменений в другие статьи УК РК, направленные на регулирование ответственности за действия ИИ, их владельцев и разработчиков.

Очевидно, возможен и другой вариант закрепления определения ИИ, а именно, включение в статью 3 УК РК, в которой изложены дефиниции терминов, используемых в тексте кодекса. Такое нормативное закрепление понятийного аппарата для устранения правовой неопределённости широко распространено и в мировой, и в казахстанской практике. В частности, статья 3 УК РК закрепляет такие определения, как «транспорт», «электронный носитель» и др. Соответственно, предлагаемое определение ИИ будет излагаться в отдельном пункте статьи 3 (Разъяснение некоторых понятий, содержащихся в настоящем Кодексе). При этом новый пункт статьи 3 УК РК будет пронумерован в соответствии с начальной буквой термина согласно алфавита на казахском языке (Ж – жасанды интеллект).

Вне зависимости от способа закрепления дефиниции важен, прежде всего, сам факт внесения соответствующих изменений в УК.

Развитие технологий ИИ порождает новые виды преступлений, такие как несанкционированное использование алгоритмов для манипуляции данными, создание и распространение вредоносного ИИ и пр. В этом аспекте включение дефиниции ИИ станет первым шагом к полноценной адаптации уголовного законодательства к современным вызовам цифровой эпохи.

Что касается дополнения многих других норм Особенной части УК РК, такой прогноз можно сделать на основе того, что ИИ могут разрабатывать специально для совершения тех или иных преступлений, что приведет к причинению более тяжких последствий. Соответственно, введение в некоторые составы такого квалифицирующего признака, как совершение с применением технологии ИИ, также можно считать вопросом времени. Это, например, могут быть такие нормы, как: статьи 190 УК РК «Мошенничество»,

⁴ Уголовный кодекс Республики Казахстан: от 3 июля 2014 г. № 226-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 18.11.2024).



статьи 198 УК РК «Нарушение авторских и (или) смежных прав», статьи 232 УК РК «Изготовление или сбыт поддельных платежных карточек и иных платежных и расчетных документов», статьи 274 УК РК «Распространение заведомо ложной информации» и др., касающиеся самых различных объектов.

Так, одним из направлений, в котором ИИ может повысить эффективность преступной деятельности, является усовершенствование фишинговых атак. Если сегодня подавляющее большинство киберпреступлений начинается с отправки фишинговых писем (91% всех атак), то применение «глубокого» ИИ позволит значительно улучшить персонализацию таких атак. Алгоритмы ИИ смогут автоматически адаптировать сообщения под конкретные демографические группы или отдельные лица, делая их менее уязвимыми для спам-фильтров и существенно повышая вероятность успеха преступников.

В то же время развитие технологий ИИ предоставляет и инструменты для защиты, которые могут взять на вооружение правоохранительные органы. Например, системы, подобные используемые за рубежом ИИ «Панацея», способны не только выявлять мошеннические письма, но и автоматически вступать в коммуникацию с преступниками, используя обработку естественного языка для сбора данных о злоумышленниках и отвлечения их от совершения дальнейших преступлений [7, 215 стр.]. Кроме того, правоохранительные органы могут применять ИИ для анализа больших массивов данных, обнаружения необычного поведения пользователей в сети и прогнозирования потенциальных угроз. Такие инструменты могут быть использованы для предотвращения кибератак, отслеживания незаконных финансовых операций или выявления сети организованных преступлений, поскольку алгоритмы машинного обучения способны выявлять сложные схемы взаимодействий, которые могли бы остаться незамеченными при использовании традиционных методов расследования.

Для эффективного внедрения таких

технологий правоохранительным органам необходимо не только наличие специализированных инструментов, но и соответствующая подготовка кадров, поскольку необходима специализированная подготовка компетентных сотрудников, способных эффективно действовать в условиях быстро меняющейся технологической среды. Это требует, как углубленных знаний в области ИИ, так и компетенций в области права.

В этих условиях особая роль отводится Академии управления Министерства внутренних дел РК, которая призвана формировать профессиональную элиту правоохранительных органов. Сегодня перед руководителями, работающими в системе правопорядка, стоят задачи не только оперативного управления и контроля, но и стратегического планирования в новых технологических реалиях.

Руководители правоохранительных органов должны обладать рядом ключевых компетенций. Прежде всего, это навыки работы с большими данными и базами, включая умение оценивать результаты, полученные с использованием технологий ИИ. Важно понимание алгоритмов машинного обучения и их потенциального применения как для обеспечения безопасности, так и для предотвращения злоупотреблений в этой сфере. Способность адаптировать организационные процессы под новые технологические реалии, оценивать и минимизировать правовые риски, а также эффективно координировать работу в условиях цифровизации деятельности становится обязательным качеством для современных руководителей.

Заключение. Таким образом, в условиях развития технологий ИИ уголовное право неизбежно должно пройти через соответствующую трансформацию: начиная с уточнения понятийного аппарата и закрепления дефиниции ИИ, и заканчивая разработкой норм, определяющих составы уголовных правонарушений, совершаемых с использованием технологий ИИ. Это не только позволит устранить существующую правовую неопределенность и учесть новые способы преступных действий,



ставшие возможными в силу автономности и адаптивности ИИ, но и обеспечить защиту общества от угроз, которые могут стать более серьезными в условиях повсеместной цифровизации.

Первым шагом должно стать закрепление в нормах УК РК дефиниции ИИ. Разработанное нами определение, которое мы предлагаем закрепить в качестве примечания к статье 207 УК РК, отличается своей универсальностью и практичностью. Оно не носит сугубо технический характер, а адаптировано для применения в правовом регулировании широкого спектра общественных отношений, связанных с использованием ИИ. Такое определение ИИ позволяет, на наш взгляд, эффективно применять его в различных аспектах – от уголовного права до гражданских и административно-правовых отношений.

Также обоснована необходимость введения квалифицирующих признаков в ряде

составов уголовных правонарушений (против собственности, против конституционных и иных прав и свобод человека и гражданина и др.), что позволит учитывать применение ИИ в качестве инструмента совершения преступлений.

Актуализирована важность подготовки правоохранительных органов к работе с новыми технологиями, включая обучение сотрудников навыкам работы с системами ИИ, анализом данных и прогнозированием преступлений с использованием технологий.

Предложенные рекомендации и выводы направлены на формирование современной уголовно-правовой политики, способной эффективно реагировать на вызовы цифровой эпохи. Они создают основу для дальнейшего совершенствования законодательства, практики правоприменения, развития научных подходов в этой сфере и предотвращения противоправных действий, связанных с использованием ИИ.

Список использованной литературы:

1. Nurkeeva, D.R. The Usage of Artificial Intelligence to Ensure the Principle of Legality in Criminal Proceedings: Opportunities and Risks / D.R. Nurkeeva, M.B. Sadykov // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 3 (33). – С. 101-108.
2. Sukhodolov, A. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects / A. Sukhodolov, A. Bychkov, A. Bychkova // Journal of Siberian Federal University. Humanities & Social Sciences. – 2020. – № 13. – Pp. 116-122.
3. Литвин, И.И. К вопросу о правосубъектности искусственного интеллекта в уголовном судопроизводстве [Электронный ресурс] / И.И. Литвин // Advances in Law Studies. – 2022. – № 2 (10). – Режим доступа: <https://riorpub.com/ru/nauka/article/50828/view> (дата обращения: 19.11.2024).
4. Nanos, A. Criminal Liability of Artificial Intelligence [Electronic resource] / A. Nanos. – Charles University in Prague, 2023. – 39 p. – Access mode: <http://dx.doi.org/10.2139/ssrn.4623126> (Access date: 12.02.2025).
5. Russell, S. Artificial Intelligence: A Modern Approach (4th ed.) [Electronic resource] / S. Russell, P. Norvig. – Pearson Education Limited, 2022. – 117 p. – Access mode: https://api.pageplace.de/preview/DT0400.9781292401171_A41586057/preview-9781292401171_A41586057.pdf (Access date: 12.02.2025).
6. Рустемова, Г.Р. Искусственный интеллект в медицине и сфере здравоохранения и уголовное право / Г.Р. Рустемова // Ученые труды Алматинской академии МВД Республики Казахстан. – 2023. – № 1 (74). – С. 64-70.
7. Hayward, K.J. Artificial intelligence and crime: A primer for criminologists [Electronic resource] / K.J. Hayward, M.M. Maas // Crime, Media, Culture. – 2021. – № 17 (2). – Pp. 209-233. – Access mode: <https://doi.org/10.1177/1741659020917434> (Access date: 12.02.2025).

References:

1. Nurkeeva, D.R. The Usage of Artificial Intelligence to Ensure the Principle of Legality in Criminal Proceedings: Opportunities and Risks / D.R. Nurkeeva, M.B. Sadykov // Құқық қорғау органдары



akademijasynuң Zharshysy. – 2024. – № 3 (33). – S. 101-108.

2. Sukhodolov, A. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects / A. Sukhodolov, A. Bychkov, A. Bychkova // Journal of Siberian Federal University. Humanities & Social Sciences. – 2020. – № 13. – Pp. 116-122.

3. Litvin, I.I. K voprosu o pravosub#ektnosti iskusstvennogo intellekta v ugovnom sudoproizvodstve [Elektronnyj resurs] / I.I. Litvin // Advances in Law Studies. – 2022. – № 2 (10). – Rezhim dostupa: <https://rriorpub.com/ru/nauka/article/50828/view> (data obrashhenija: 19.11.2024).

4. Nanos, A. Criminal Liability of Artificial Intelligence [Electronic resource] / A. Nanos. – Charles University in Prague, 2023. – 39 p. – Access mode: <http://dx.doi.org/10.2139/ssrn.4623126> (Access date: 12.02.2025).

5. Russell, S. Artificial Intelligence: A Modern Approach (4th ed.) [Electronic resource] / S. Russell, P. Norvig. – Pearson Education Limited, 2022. – 117 p. – Access mode: https://api.pageplace.de/preview/DT0400.9781292401171_A41586057/preview-9781292401171_A41586057.pdf (Access date: 12.02.2025).

6. Rustemova, G.R. Iskusstvennyj intellekt v medicine i sfere zdavoohranenija i ugovnoe pravo / G.R. Rustemova // Uchenye trudy Almatinskoy akademii MVD Respubliki Kazahstan. – 2023. – № 1 (74). – S. 64-70.

7. Hayward, K.J. Artificial intelligence and crime: A primer for criminologists [Electronic resource] / K.J. Hayward, M.M. Maas // Crime, Media, Culture. – 2021. – № 17 (2). – Pp. 209-233. – Access mode: <https://doi.org/10.1177/1741659020917434> (Access date: 12.02.2025).

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Жанар Аманжанқызы Кегембаева – әл-Фараби атындағы Қазақ ұлттық университетінің Мемлекет және құқық теориясы мен тарихы, конституциялық және әкімшілік құқық кафедрасының профессоры, заң ғылымдарының докторы, профессор, e-mail: kegembayevazh@outlook.com.

Кегембаева Жанар Аманжановна – профессор кафедрасы теориясы және тарихының мемлекет және құқық теориясы мен тарихы, конституциялық және әкімшілік құқық кафедрасының профессоры, заң ғылымдарының докторы, профессор, e-mail: kegembayevazh@outlook.com.

Kegembayeva Zhanar Aminzhanovna – Professor of the Department of Theory and History of State and Law, Constitutional and Administrative Law at Al-Farabi Kazakh National University, Doctor of Law, Professor, e-mail: kegembayevazh@outlook.com.

Ораз Жолдасұлы Жолдасов – Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясы бастығының м.а., e-mail: ozholdasov88@mail.ru.

Жолдасов Ораз Жолдасович – и.о. начальника Академии управления Министерства внутренних дел Республики Казахстан, e-mail: ozholdasov88@mail.ru.

Zholdasov Oraz Zholdasovich – Acting Head of the Academy of Management of the Ministry of Internal Affairs of the Republic of Kazakhstan, e-mail: ozholdasov88@mail.ru.