



М.Е. Касымхан^{1*} , А.А. Алексенко² , Е.Н. Грек³ 

¹ магистр юридических наук, сеньор-лектор Высшей школы права «Әділет» Каспийского общественного университета, (г. Алматы, Казахстан)

ORCID ID: 0009-0009-8389-0232, e-mail: mkasymxanova@inbox.ru

² магистр юридических наук, сеньор-лектор Высшей школы права «Әділет» Каспийского общественного университета (г. Алматы, Казахстан) ORCID ID: 0009-0004-2335-4060; e-mail: a.zairova@cu.edu.kz

³ Phd, юристконсультант Алматинской городской палаты юридических консультантов «Эгида» (Алматы, Казахстан) e-mail: e.grek@cu.edu.kz

ТРАНСФОРМАЦИЯ ПРИНЦИПОВ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ В УСЛОВИЯХ АВТОНОМНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ

Аннотация. Статья посвящена теоретико-правовому анализу трансформации фундаментальных принципов юридической ответственности под воздействием автономных систем искусственного интеллекта. Актуальность исследования обусловлена качественным изменением социальной реальности, в которой алгоритмические системы всё чаще выступают не пассивным инструментом, а активным элементом правоотношений, способным самостоятельно принимать решения в условиях неопределённости. В работе обосновывается, что сохранение антропоцентрической модели ответственности при фактической автономности алгоритмов порождает системное противоречие: классические институты вины, причинной связи и субъекта правонарушения перестают адекватно описывать механизм причинения вреда. Автор выделяет три уровня трансформации правовой конструкции ответственности: 1) изменение структуры субъектного состава (появление «алгоритмического посредничества»); 2) деформация причинно-следственной связи (многоуровневый, вероятностный и непрозрачный характер алгоритмических решений); 3) размывание критериев вины (неопределённость границ между умыслом, неосторожностью и «технологически неизбежной ошибкой»). Сформулированы предложения по эволюционной адаптации института юридической ответственности к реалиям цифровой эпохи, включая внедрение принципа технологической нейтральности, закрепление стандартов прозрачности алгоритмов и введение дифференцированных режимов ответственности в зависимости от степени автономности системы. Автор приходит к выводу, что технологическое развитие не отменяет необходимости правовой ответственности как таковой, но требует её концептуального переосмысления: ответственность остаётся категорией человеческой, однако механизмы её реализации должны быть адекватны новой технологической реальности.

Ключевые слова: юридическая ответственность, искусственный интеллект, автономные системы, субъект правоотношения, причинно-следственная связь, вина, алгоритмическая непрозрачность, принципы права, цифровая трансформация права.

Введение

Стремительная интеграция систем искусственного интеллекта (ИИ) в государственное управление, финансовый сектор и промышленность знаменует переход к качественно новому технологическому

укладу. Наряду с автоматизацией и оптимизацией процессов, цифровизация генерирует обратный эффект – формирует новые риски для правопорядка. Современные алгоритмы, способные генерировать контент, имитировать личность и прогнозировать

* Corresponding author: mkasymxanova@inbox.ru



поведение, становятся доступным инструментом криминальной деятельности.

В научной литературе и правоприменительной практике остро обозначился разрыв между технологическими возможностями ИИ и существующими уголовно-правовыми механизмами. Возникают фундаментальные вопросы: как квалифицировать деяния, если традиционные способы преступлений (мошенничество, вымогательство) цифровизируются? Как устанавливать субъект и вину в условиях автономности алгоритма и трансграничности цифровых следов?

Цель настоящей работы заключается в комплексном анализе уголовно-правовых и уголовно-процессуальных проблем противодействия преступлениям, совершаемым с использованием ИИ, а также в выработке предложений по адаптации законодательства Республики Казахстан к вызовам цифровой эпохи. Достижение цели предполагает решение задач:

- а) анализ трансформации способа совершения преступления под воздействием ИИ;
- б) выявление особенностей доказывания и расследования;
- в) оценка судебных перспектив и процессуальных гарантий.

Методы и материалы

Нормативно-эмпирическую базу исследования составили систематизированные источники трёх уровней: материально-правовые и процессуальные нормы (Уголовный кодекс Республики Казахстан, Уголовно-процессуальный кодекс Республики Казахстан, Закон «О персональных данных и их защите», стратегические документы в сфере цифровизации); правоприменительные материалы (обзоры судебной практики Верховного Суда РК по делам о киберпреступлениях, отдельные приговоры и определения судов первой и апелляционной инстанций, связанные с использованием генеративных нейросетей и дипфейк-технологий); а также доктринальные источники – труды казахстанских и зарубежных учёных в области уголовного

права, цифровой криминалистики и алгоритмической этики, включая аналитические отчёты международных организаций (Совет Европы, ООН) и рекомендации в рамках Будапештской конвенции о киберпреступности.

Методологический инструментарий работы построен на сочетании общенаучных и специально-юридических методов познания. Диалектический и системно-структурный методы позволили рассмотреть искусственный интеллект как динамически развивающееся явление в системе общественных отношений, а формально-юридический и сравнительно-правовой – осуществить толкование действующих норм и сопоставить казахстанские подходы с международными стандартами. Метод анализа правоприменительной практики и юридическая герменевтика использованы для выявления устойчивых судебных позиций по вопросам допустимости цифровых доказательств и установления формы вины; элементы криминалистического анализа – при изучении механизмов фиксации электронных носителей, лог-файлов и хеш-сумм в досудебном производстве. Исследование проведено поэтапно: от нормативного и доктринального обзора – к идентификации правовых пробелов и формулированию предложений по эволюционной адаптации уголовного и процессуального законодательства к технологическим реалиям цифровой эпохи.

Результаты и обсуждение

Современное развитие цифровых технологий обусловило необходимость правового осмысления феномена искусственного интеллекта (далее – ИИ) в контексте уголовного судопроизводства. В законодательстве Республики Казахстан на сегодняшний день отсутствует единое легальное определение искусственного интеллекта в уголовно-правовом смысле, однако в стратегических и программных документах ИИ рассматривается как совокупность технологий машинного обучения, обработки больших данных и автоматизированного принятия решений [1].

С точки зрения уголовного права ИИ не



является субъектом преступления, поскольку согласно ст. 15 Уголовного кодекса Республики Казахстан (далее – УК РК) субъектом преступления признаётся физическое вменяемое лицо, достигшее установленного законом возраста.¹ Следовательно, искусственный интеллект может рассматриваться исключительно как средство совершения преступления либо как инструмент реализации преступного умысла [2].

В этом контексте особо значение приобретают факультативные признаки объективной стороны, в которых способ совершения уголовных правонарушений традиционно понимается как приемы и методы, используемые при совершении общественно опасных деяний.

Применение ИИ существенно трансформирует содержание способа совершения уголовных правонарушений. Если ранее технические средства играли лишь вспомогательную роль, то в нынешних реалиях интеллектуальные системы способны к анализу информации, моделированию поведения жертвы, адаптации сценариев воздействия и автоматизации противоправных процессов. Это придает способу преступления новые характеристики: интеллектуализированность, масштабируемость, персонализацию и высокую латентность.

Одним из наиболее распространённых направлений криминального использования ИИ является автоматизированная рассылка сообщений, направленных на получение персональных и конфиденциальных данных. Генеративные модели позволяют создавать фишинговые письма, сообщения в мессенджерах и социальных сетях, имитирующие стиль банков, государственных органов или конкретных должностных лиц. Такие действия при признаках хищения могут образовывать состав мошенничества (ст.190 УК РК), поскольку направлены на завладение чужим имуществом путем обмана или злоупотребления доверием. Использование ИИ в данном случае усложняет способ

совершения преступления, поскольку включает предварительный анализ цифрового профиля потерпевшего и персонализацию обмана [3].

Незаконное собирание и обработка персональных данных с применением алгоритмов машинного обучения могут подпадать под признаки ст. 147 УК РК (Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите), а также ст. 205 УК РК (Неправомерный доступ к информации), ст. 206 УК РК (Неправомерное уничтожение или модификация информации), ст. 210 УК РК (Создание, использование или распространение вредоносных компьютерных программ и программных продуктов).

Особую общественную опасность представляют технологии создания дипфейков – реалистичных аудио- и видеоматериалов, сформированных с использованием нейросетей. Их использование возможно при совершении мошенничества (ст. 190 УК РК), вымогательства (ст. 194 УК РК), оскорбления (ст. 131 УК РК). В данном случае способ совершения уголовных правонарушений приобретает качественно иную форму: обман или угроза реализуются посредством визуальной – аудиальной имитации реальности, что усиливает психологическое воздействие на потерпевшего и затрудняет выявление фальсификации.

ИИ также может использоваться при создании и модификации вредоносных программ, предназначенных для обхода систем информационной безопасности. Такие действия могут квалифицироваться по ст. 206 УК РК (Неправомерное уничтожение или модификация информации), ст. 210 УК РК (Создание, использование или распространение вредоносных компьютерных программ и программных продуктов).² Характерной особенностью способа совершения преступления в данном случае является его адаптивность: алгоритмы способны автоматически изменять код в

¹ Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. URL: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 19.05.2026).

² Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК.



зависимости от параметров атакуемой системы, что повышает устойчивость к обнаружению.

С теоритической точки зрения применение ИИ свидетельствует о высоком уровне предварительной подготовки и интеллектуализации преступной деятельности.

Алгоритмическое моделирование, прогнозирование поведения жертвы, анализ уязвимостей информационных систем указывают на целенаправленный и продуманный характер действий виновного лица, что имеет значение для установления формы вины и оценки степени общественной опасности. Таким образом, ИИ не изменяет конструкцию состава преступления, однако существенно трансформирует способ его совершения, усиливая его технологическую сложность и масштаб.

В уголовном процессе ключевым является установление обстоятельств, подлежащих доказыванию. В соответствии со ст. 113 Уголовно-процессуального кодекса Республики Казахстан (далее – УПК РК) подлежат доказыванию событие преступления, виновность лица, форма вины, мотивы, характер и размер вреда.³ При использовании ИИ возникает усложнённая модель причинно-следственной связи между действиями лица и наступившими последствиями.

Таким образом, доказательная деятельность по делам, связанным с использованием ИИ, предполагает установление:

1. факта использования ИИ;
2. характера вмешательства человека в работу системы;
3. степени автономности алгоритма;
4. наличия умысла либо неосторожности у лица.

Особенность предмета доказывания заключается в необходимости установления технологического механизма совершения преступления. Например, при совершении мошенничества с использованием алгоритмов генеративного ИИ (создание поддельных голосов, видео – deepfake) следствие обязано

доказать не только факт обмана, но и то, что обвиняемый осознавал применение ИИ как инструмента воздействия на потерпевшего.

В соответствии со ст. 111 УПК РК доказательствами являются любые фактические данные, на основе которых суд, прокурор, следователь устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию. В делах данной категории такими доказательствами чаще всего выступают:

- цифровые лог-файлы;
- серверные журналы;
- результаты компьютерно-технической экспертизы;
- заключения специалистов в области машинного обучения;
- данные телекоммуникационных соединений.

Проблема заключается в допустимости и относимости таких доказательств. Согласно ст. 112 УПК РК доказательства признаются допустимыми, если получены в соответствии с требованиями закона. Нарушение порядка изъятия цифровых носителей либо отсутствие санкции суда на доступ к данным может повлечь признание доказательств недопустимыми.

Кроме того, специфика ИИ предполагает наличие так называемой «алгоритмической непрозрачности» (black box problem), когда невозможно полностью объяснить логику принятия решений системой. Это ставит под сомнение полноту установления причинно-следственной связи и требует привлечения экспертов.

Цифровые доказательства в делах, связанных с ИИ, занимают центральное место. УПК РК не содержит отдельного института «цифровых доказательств», однако нормы о вещественных доказательствах (ст. 118 УПК РК) применимы к электронным носителям информации.

Судебная практика Республики Казахстан демонстрирует, что электронные данные (переписка, логи, IP-адреса) признаются допустимыми доказательствами при условии соблюдения процедуры их фиксации и изъятия. В делах о

³ Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V. URL:

<https://adilet.zan.kz/rus/docs/K1400000231> (дата обращения: 19.05.2026).



киберпреступлениях органы следствия активно используют компьютерно-технические экспертизы.

Особенность доказывания по делам с ИИ заключается в необходимости:

- установления подлинности цифровых данных;
- подтверждения отсутствия их изменения;
- фиксации времени и последовательности операций.

Для этого применяется цифровая криминалистика (digital forensics), обеспечивающая сохранение цепочки хранения доказательств (chain of custody).

Ключевой уголовно-правовой проблемой является установление формы вины. Согласно ст. 19 УК РК лицо подлежит уголовной ответственности только за те общественно опасные деяния, в отношении которых установлена его вина⁴.

Если преступление совершено с использованием автономной системы, необходимо доказать:

- имел ли обвиняемый умысел на использование ИИ для преступных целей;
- осознавал ли он общественную опасность последствий;
- мог ли предвидеть результат функционирования алгоритма.

Например, если разработчик создал ИИ-систему, впоследствии использованную третьими лицами для незаконного доступа к информации, возникает вопрос о пределах ответственности разработчика.

Суд должен разграничить:

- 1.умышленное использование ИИ;
- 2.преступную небрежность;
- 3.отсутствие вины вследствие непредвиденности результата.

В судебной практике Республики Казахстан по делам о киберпреступлениях (ст. 205-213 УК РК) уже выработаны подходы к оценке цифровых доказательств. Однако дела, где ИИ выступает активным инструментом преступления (генерация поддельных данных, автоматизированный фишинг), требуют дальнейшей методологической разработки.

Суд, руководствуясь ст. 125 УПК РК, оценивает доказательства, по внутреннему убеждению⁵. При этом необходима:

- всесторонность исследования;
- сопоставление экспертных заключений;
- проверка альтернативных версий.

Особую роль играет состязательность сторон: защита вправе ходатайствовать о повторной или дополнительной экспертизе.

Республика Казахстан участвует в международном сотрудничестве в сфере борьбы с киберпреступностью. Подходы к доказыванию цифровых преступлений формируются с учётом международных рекомендаций, включая положения Будапештской конвенции о киберпреступности⁶.

Международная практика подчёркивает необходимость:

- технологической нейтральности законодательства;
- сохранения баланса между эффективностью расследования и защитой прав человека;
- прозрачности алгоритмических решений.

Доказывание по делам о преступлениях, совершённых с использованием ИИ, характеризуется высокой степенью технологической сложности и требует адаптации традиционных процессуальных механизмов. Основные проблемы связаны с установлением причинно-следственной связи, формы вины и допустимости цифровых доказательств. Совершенствование законодательства Республики Казахстан должно учитывать особенности алгоритмических систем и развитие цифровой криминалистики.

Расследование преступлений, совершённых с применением искусственного интеллекта, характеризуется высокой технологической сложностью и необходимостью сочетания уголовно-процессуальных норм с цифровой криминалистикой [4]. В соответствии со ст. 24 УПК РК суд, прокурор, следователь обязаны

⁴ Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК.

⁵ Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V.

⁶ Конвенция о киберпреступности (Будапешт, 23 ноября 2001 года). URL: https://prg.kz/document/?doc_id=30170556 (дата обращения: 19.05.2026).



принять все предусмотренные законом меры для всестороннего, полного и объективного исследования обстоятельств дела ⁷.

Использование ИИ как средства совершения преступления усложняет установление:

- механизма преступления;
- роли конкретных лиц;
- характера взаимодействия человека и алгоритма;
- места совершения преступления (особенно при трансграничном характере деяния).

В делах данной категории следствие сталкивается с тем, что алгоритмические системы могут функционировать автономно, используя распределённые вычислительные мощности и облачные инфраструктуры, размещённые за пределами Республики Казахстан.

Основанием для начала досудебного расследования является наличие достаточных данных, указывающих на признаки уголовного правонарушения (ст. 179 УПК РК). При использовании ИИ первичная информация может поступать:

- от потерпевших (например, жертвы deepfake-мошенничества);
- от финансовых организаций;
- от подразделений по борьбе с киберпреступностью;
- в рамках оперативно-розыскной деятельности.

Квалификация преступления осуществляется по соответствующим статьям УК РК. В зависимости от характера деяния это могут быть:

- мошенничество (ст. 190 УК РК);
- незаконный доступ к информации (ст. 205 УК РК);
- создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК);
- Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите (ст. 147 УК РК) ⁸.

Особенность квалификации заключается

в том, что ИИ не образует самостоятельного состава преступления, а выступает способом или средством его совершения. Следователь обязан установить форму вины лица (ст. 19 УК РК) и доказать, что использование ИИ носило осознанный характер.

Согласно ст. 221-232 УПК РК осмотр места происшествия, обыск и выемка проводятся с соблюдением процессуальных гарантий. При расследовании преступлений с применением ИИ ключевым объектом изъятия становятся: серверы, жёсткие диски, мобильные устройства, облачные аккаунты, исходный код программ.

Особенность заключается в необходимости сохранения целостности цифровых данных. Нарушение процедуры изъятия может привести к признанию доказательств недопустимыми (ст. 112 УПК РК).

Следователь обязан обеспечить:

- фиксацию времени изъятия;
- создание копий с применением хеш-сумм;
- документирование состояния носителей.

В соответствии с УПК РК доступ к информации, содержащейся в информационных системах, допускается на основании санкции следственного судьи. Это особенно актуально при работе с облачными ИИ-сервисами.

Проблема возникает в случае размещения серверов за пределами Казахстана. В таких ситуациях применяется механизм международной правовой помощи в соответствии с гл. 59 УПК РК.

В делах с использованием ИИ судебная экспертиза приобретает ключевое значение. Согласно ст. 272 УПК РК экспертиза назначается, если для установления обстоятельств дела необходимы специальные знания.

На практике назначаются:

- компьютерно-техническая экспертиза;
- телекоммуникационная экспертиза;
- автороведческая экспертиза (при анализе текстов, созданных ИИ);
- фоноскопическая экспертиза (при

⁷ Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V.

⁸ Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК.



deepfake-аудио).

Эксперт устанавливает:

- использовались ли алгоритмы машинного обучения;
- имело ли место вмешательство человека;
- возможно ли было прогнозирование результата.

Особую сложность представляет оценка «автономности» алгоритма. Следствие должно доказать, что лицо либо запрограммировало ИИ на противоправные действия, либо сознательно допустило их совершение.

В расследовании преступлений данной категории активно используются меры негласного следствия (глава 30 УПК РК):

- снятие информации с каналов связи;
- мониторинг сетевой активности;
- контроль электронных сообщений.

При этом необходимо соблюдать принцип соразмерности и недопустимости вмешательства в частную жизнь сверх необходимого⁹.

Использование ИИ нередко предполагает трансграничный характер преступлений. Республика Казахстан взаимодействует с другими государствами в рамках договоров о правовой помощи.

Согласно ст. 557 УПК РК органы Казахстана исполняют международные поручения о производстве следственных действий. В делах, связанных с ИИ, это особенно важно при:

- получении данных от иностранных IT-компаний;
- установлении IP-адресов;
- изъятии серверных логов.

Основные проблемы:

1. Недостаточная техническая подготовка следователей.
2. Отсутствие унифицированных методик расследования преступлений с применением ИИ.
3. Сложности доказывания умысла.
4. Алгоритмическая непрозрачность (black box).

В целях совершенствования предлагается:

- разработка методических рекомендаций Генеральной прокуратуры РК;
- создание специализированных подразделений по расследованию преступлений с применением ИИ;
- повышение квалификации следователей;
- законодательное закрепление понятия цифровых доказательств.

Расследование преступлений с применением ИИ требует комплексного подхода, сочетающего нормы УПК РК, положения УК РК и достижения цифровой криминалистики. Особое значение имеют процессуальные гарантии законности получения цифровых доказательств, международное сотрудничество и судебная экспертиза. Без адаптации процессуальных механизмов к реалиям цифровой эпохи эффективное противодействие таким преступлениям невозможно.

Судебное разбирательство по делам о преступлениях, совершённых с использованием искусственного интеллекта, осуществляется на основе общих принципов уголовного процесса Республики Казахстан. В соответствии со ст. 11 УПК РК правосудие по уголовным делам осуществляется только судом.

При этом сохраняют своё значение фундаментальные принципы:

- законность (ст. 10 УПК РК);
- состязательность и равноправие сторон (ст. 23 УПК РК);
- презумпция невиновности (ст. 19 УПК РК);
- обеспечение права на защиту (ст. 26 УПК РК).

Использование ИИ как средства совершения преступления не изменяет сущности судебного разбирательства, однако существенно усложняет процесс оценки доказательств и реализацию процессуальных гарантий.

В соответствии со ст. 125 УПК РК суд оценивает доказательства по своему внутреннему убеждению на основе всестороннего, полного и объективного исследования всех обстоятельств дела.

⁹ Конституция Республики Казахстан принята на республиканском референдуме 30 августа 1995 года. URL:

https://adilet.zan.kz/rus/docs/K950001000_ (дата обращения: 19.05.2026).



В делах, связанных с применением ИИ, суду приходится исследовать:

- цифровые логи;
- алгоритмические модели;
- экспертные заключения;
- данные облачных сервисов;
- результаты компьютерно-технической экспертизы.

Особую сложность представляет проблема «алгоритмической непрозрачности» – невозможности полного объяснения механизма принятия решений ИИ. Суд не вправе основывать обвинительный приговор на предположениях (ст. 19 УПК РК), поэтому заключение эксперта должно быть ясным, мотивированным и поддающимся проверке.

В судебной практике по делам о киберпреступлениях Верховный Суд Республики Казахстан указывает на необходимость тщательной проверки допустимости цифровых доказательств и соблюдения процессуального порядка их получения¹⁰.

Судебная экспертиза в делах с применением ИИ приобретает ключевое значение. Согласно ст. 287 УПК РК суд вправе назначить дополнительную или повторную экспертизу, если заключение эксперта является неполным или вызывает сомнения.

Защита вправе:

- заявлять ходатайства о назначении альтернативной экспертизы;
- допрашивать эксперта в судебном заседании;
- представлять заключения специалистов.

Таким образом, обеспечивается принцип состязательности сторон.

Особое значение имеет квалификация эксперта. В условиях сложных алгоритмических систем суд должен убедиться в компетентности эксперта в области машинного обучения и цифровой криминалистики.

Право на защиту гарантируется ст. 13 Конституции Республики Казахстан и ст. 26 УПК РК. В делах, связанных с ИИ, реализация данного права осложняется технической

сложностью доказательственной базы.

Для обеспечения эффективной защиты необходимо:

1. Предоставление стороне защиты полного доступа к цифровым материалам дела.

2. Обеспечение возможности привлечения независимых специалистов.

3. Разъяснение обвиняемому сути предъявленных ему цифровых доказательств.

Если обвиняемый не обладает специальными знаниями, суд обязан обеспечить перевод сложной технической информации в доступную форму, иначе нарушается принцип справедливого судебного разбирательства.

Согласно ст. 77 Конституции Республики Казахстан лицо считается невиновным, пока его вина не будет доказана в предусмотренном законом порядке и установлена вступившим в законную силу приговором суда¹¹.

В делах о преступлениях с использованием ИИ существует риск «технологического детерминизма», когда сам факт использования сложной системы воспринимается как доказательство виновности. Однако обязанность доказывания лежит на стороне обвинения.

Суд не вправе перекладывать на обвиняемого обязанность доказывать отсутствие контроля над алгоритмом или невозможность предвидения его действий.

Использование ИИ часто связано с обработкой больших массивов персональных данных. Согласно ст. 18 Конституции РК каждый имеет право на неприкосновенность частной жизни.

Закон Республики Казахстан «О персональных данных и их защите» предусматривает необходимость соблюдения режима конфиденциальности при сборе и использовании информации¹².

В судебном процессе это означает:

- ограничение разглашения персональных данных;
- проведение закрытых судебных заседаний при наличии оснований (ст. 29 УПК

¹⁰ Изменения по вопросам кибербезопасности, информационных систем и документооборота в судах. URL: https://prg.kz/document/?doc_id=34024140&pos=0;0 (дата обращения: 19.05.2026).

¹¹ Конституция Республики Казахстан принята на республиканском референдуме 30 августа 1995 года.

¹² Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года.



РК);

– обеспечение баланса между публичностью процесса и защитой частной жизни.

Республика Казахстан признаёт международные стандарты в сфере прав человека. Ст. 4 Конституции РК закрепляет приоритет международных договоров над национальным законодательством.

Международная практика подчёркивает необходимость прозрачности алгоритмических систем, используемых в уголовном процессе, и запрета принятия решений исключительно на основе автоматизированной обработки данных.

В условиях цифровизации судебная система должна исключить возможность использования ИИ как самостоятельного «судьи». Технологии могут выступать вспомогательным инструментом, но окончательное решение всегда принимает человек – судья.

В целях совершенствования судебного разбирательства по делам данной категории целесообразно:

- разработать методические рекомендации для судей по оценке цифровых доказательств;
- предусмотреть специализированное обучение судей в области ИИ;
- закрепить в УПК РК понятие цифровых доказательств;
- установить стандарты прозрачности алгоритмических систем.

Развитие правоприменительной практики должно идти по пути усиления гарантий личности при одновременном повышении эффективности правосудия.

Судебное разбирательство по делам о преступлениях, совершённых с использованием искусственного интеллекта, требует адаптации традиционных процессуальных механизмов к цифровым реалиям. При этом базовые принципы уголовного судопроизводства Республики Казахстан сохраняют свою фундаментальную роль.

Главной задачей суда является обеспечение баланса между эффективностью правосудия и защитой прав личности, исключение автоматизированного правосудия и недопустимость обвинительного уклона,

основанного на технологической сложности дела.

Стремительное развитие технологий искусственного интеллекта радикально трансформирует социальную реальность, формируя новые формы общественных отношений, цифровые модели взаимодействия и принципиально иные способы осуществления как законной, так и противоправной деятельности. Искусственный интеллект перестал быть исключительно инструментом автоматизации процессов и превратился в самостоятельный технологический фактор, способный оказывать значительное влияние на принятие решений, обработку информации и моделирование поведения. В этой связи закономерно возникает вопрос о его роли в механизме преступления и о пределах уголовной ответственности при использовании ИИ в противоправных целях.

В первой части статьи, выполненной с позиции уголовного права, было обосновано, что искусственный интеллект не может рассматриваться в качестве самостоятельного субъекта преступления в рамках действующего законодательства Республики Казахстан. В соответствии с УК РК субъектом уголовной ответственности признаётся физическое вменяемое лицо, достигшее установленного законом возраста. Следовательно, ИИ в современных правовых условиях выступает исключительно как средство совершения преступления либо как инструмент реализации преступного умысла человека. Материально-правовой анализ показал, что основная проблема заключается не в признании ИИ субъектом права, а в правильной квалификации деяния, установлении формы вины, разграничении умысла и неосторожности, а также определении границ ответственности разработчиков, операторов и пользователей алгоритмических систем.

Однако уголовно-правовое регулирование не может быть эффективным без адекватного процессуального механизма его реализации. Именно поэтому вторая часть исследования была посвящена уголовно-процессуальным аспектам — доказыванию, расследованию и судебному разбирательству по делам о преступлениях, совершённых с



использованием искусственного интеллекта.

Проведённый процессуальный анализ позволяет сделать вывод о том, что внедрение ИИ в сферу преступной деятельности не разрушает фундаментальных принципов уголовного судопроизводства Республики Казахстан, но существенно усложняет их практическую реализацию. Принципы законности, презумпции невиновности, состязательности сторон, обеспечения права на защиту и недопустимости доказательств, полученных с нарушением закона, сохраняют свою абсолютную ценность. Вместе с тем их применение в условиях цифровизации требует новых методологических подходов.

Во-первых, специфика преступлений с использованием ИИ трансформирует структуру предмета доказывания. Если в традиционных преступлениях причинно-следственная связь прослеживается относительно непосредственно, то при использовании автономных алгоритмов возникает многоуровневая модель взаимодействия человека и технологии. Следствию и суду необходимо установить не только факт противоправного результата, но и характер программирования, степень вмешательства человека, возможность предвидения последствий, а также уровень автономности системы. Тем самым процесс доказывания приобретает технически насыщенный характер, требующий глубоких специальных знаний.

Во-вторых, ключевую роль в таких делах приобретают цифровые доказательства. Их объём, сложность и уязвимость создают риск процессуальных нарушений. Неправильное изъятие носителей информации, нарушение целостности данных, отсутствие фиксации хеш-сумм или санкции следственного судьи на доступ к информации способны привести к признанию доказательств недопустимыми. Это усиливает значение процессуальной дисциплины и цифровой криминалистики. Законодательство Республики Казахстан уже содержит механизмы получения доступа к информации в информационных системах, проведения экспертиз и международного сотрудничества, однако развитие технологий ИИ объективно опережает формирование детальных процессуальных регламентов.

В-третьих, особую сложность

представляет установление вины. В условиях так называемой алгоритмической непрозрачности (black box problem) защита вправе ставить под сомнение предсказуемость поведения системы и возможность контроля со стороны обвиняемого. В этой связи усиливается значение судебной экспертизы и состязательности сторон. Суд не вправе основывать обвинительный приговор на предположениях либо на авторитете технологической сложности. Стандарт доказывания остаётся неизменным: вина должна быть установлена вне разумных сомнений, а все неустранимые сомнения толкуются в пользу обвиняемого.

В-четвёртых, судебное разбирательство по данной категории дел требует особого внимания к процессуальным гарантиям личности. Техническая сложность доказательственной базы не должна превращаться в инструмент обвинительного уклона. Обвиняемый имеет право понимать существо предъявленных ему доказательств, оспаривать заключения экспертов, привлекать независимых специалистов и получать полноценную юридическую помощь. В противном случае нарушается принцип справедливого судебного разбирательства и равенства сторон.

Таким образом, сопоставление уголовно-правового и уголовно-процессуального анализа позволяет сформулировать комплексный вывод: проблема ответственности за преступления, совершённые с использованием искусственного интеллекта, лежит не в плоскости «очеловечивания» алгоритмов, а в сфере корректного распределения ответственности между людьми, задействованными в создании, внедрении и эксплуатации ИИ-систем. Материальное право определяет пределы уголовной ответственности, а процессуальное право обеспечивает механизм её справедливой реализации.

Вместе с тем проведённое исследование выявило ряд системных вызовов для правоприменительной практики Республики Казахстан:

1.Отсутствие легального определения цифровых доказательств в УПК РК и унифицированных стандартов их фиксации.



2. Недостаточная методическая регламентация расследования преступлений с применением ИИ.

3. Необходимость специализированной подготовки следователей, прокуроров и судей в области алгоритмических технологий.

4. Риск нарушения баланса между эффективностью расследования и защитой права на неприкосновенность частной жизни.

5. Сложность доказывания субъективной стороны преступления при автономном функционировании алгоритмов.

В целях совершенствования правового регулирования представляется целесообразным:

- закрепить на законодательном уровне понятие цифровых доказательств и минимальные стандарты их сохранности;

- разработать методические рекомендации по расследованию преступлений с применением ИИ;

- усилить международное сотрудничество в сфере трансграничных киберпреступлений;

- обеспечить регулярное повышение квалификации судей и следователей;

- внедрить стандарты прозрачности алгоритмов при использовании ИИ в доказательственном процессе.

Важно подчеркнуть, что технологическое развитие не отменяет базовых правовых ценностей. Искусственный интеллект может быть инструментом как прогресса, так и преступления, однако ответственность всегда остаётся категорией человеческой. Уголовное право не наказывает алгоритм – оно реагирует на общественно опасное поведение лица. Уголовный процесс, в свою очередь, обязан обеспечить, чтобы такая реакция была законной, справедливой и основанной на доказательствах, полученных с соблюдением всех процессуальных гарантий.

Тем самым взаимодействие материально-правового и процессуального подходов позволяет сформировать целостную концепцию противодействия преступлениям с использованием искусственного интеллекта. Только при гармоничном сочетании уголовно-правовых конструкций и эффективных процессуальных механизмов возможно достижение баланса между интересами общества в обеспечении безопасности и

обязанностью государства защищать права и свободы личности.

Заключение

Проведенное исследование подтверждает, что искусственный интеллект в механизме преступления выступает не в качестве субъекта, а в качестве высокотехнологичного средства, модифицирующего традиционные составы уголовных правонарушений. Установлено, что ключевая уголовно-правовая проблема смещается из плоскости квалификации в плоскость доказывания субъективной стороны: определение формы вины (умысел или неосторожность) в условиях алгоритмической «непрозрачности» требует принципиально иных экспертных подходов.

Системными вызовами для уголовного процесса РК остаются: отсутствие легальной дефиниции и процедур работы с цифровыми доказательствами; пробелы в методиках расследования автономных действий алгоритмов; а также риск нарушения баланса между эффективностью следствия и правом на неприкосновенность частной жизни. В этой связи обоснована необходимость не революционной ломки УК и УПК, а их эволюционной адаптации через:

- 1) законодательное закрепление стандартов фиксации цифровых улик;

- 2) специализацию судей и следователей в сфере machine learning;

- 3) внедрение принципа технологической нейтральности, позволяющего применять нормы к любым алгоритмическим системам без привязки к конкретным программным решениям.

Резюмируя, подчеркнем: внедрение ИИ не отменяет антропоцентричности уголовной ответственности. Однако правовая система обязана обеспечить, чтобы техническая сложность дела не становилась непреодолимым барьером для правосудия. Стратегическая задача уголовной политики Казахстана в эпоху цифровизации – сохранить приоритет человеческой ответственности, одновременно наделив правоприменителя инструментарием, адекватным современным технологическим реалиям.



Список литературы

89. 1 Бабанов Т.Т. Цифровые доказательства в уголовном процессе Республики Казахстан. – Алматы, 2021. – С. 89.
2 Нургалиев Р.К. Уголовный процесс Республики Казахстан. – Алматы, 2022, – С. 112.
3 Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. –Polity Press, 2007. – 276 p.
4 Бабанов Т.Т. Расследование киберпреступлений в Республике Казахстан. – Алматы, 2022. – Р. 119.

References

- 1 Bapanov T.T. Tsifrovyye dokazatel'stva v ugovnom protsesse Respubliki Kazakhstan. – Almaty, 2021. – S. 89.
2 Nurgaliyev R.K. Ugolovnyy protsess Respubliki Kazakhstan. – Almaty, 2022, – S. 112.
3 Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. –Polity Press, 2007. – 276 p.
4 Bapanov T.T. Rassledovaniye kiberprestupleniy v Respublike Kazakhstan. – Almaty, 2022. – P. 119.

М.Е. Қасымхан ¹, А.А. Алексенко ², Е.Н. Грек ³

¹ з.ғ.м., Каспий қоғамдық университетінің «Әділет» Жоғары заң мектебінің сеньор-лекторы (Алматы қ., Қазақстан) ORCID ID: 0009-0009-8389-0232, e-mail: mkasymxanova@inbox.ru

² з.ғ.м., Каспий қоғамдық университетінің «Әділет» Жоғары заң мектебінің сеньор-лекторы (Алматы қ., Қазақстан) ORCID ID: 0009-0004-2335-4060; e-mail: a.zairova@cu.edu.kz

³ PhD, «Эгида» Алматы қалалық заң кеңесшілері палатасының заң кеңесшісі (Алматы қ., Қазақстан) e-mail: e.grek@cu.edu.kz

АВТОНОМДЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖАҒДАЙЫНДА ҚҰҚЫҚТЫҚ ЖАУАПКЕРШІЛІК ҚАҒИДАТТАРЫНЫҢ ТРАНСФОРМАЦИЯСЫ: ТЕОРИЯЛЫҚ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Аңдатпа. Мақала автономды жасанды интеллект жүйелерінің әсерінен құқықтық жауапкершіліктің іргелі қағидаттарының трансформациясын теориялық-құқықтық тұрғыдан талдауға арналған. Зерттеудің өзектілігі алгоритмдік жүйелердің әлеуметтік шынайылықты сапалық тұрғыдан өзгертуімен негізделеді, мұнда олар барған сайын тек пассивті құрал ретінде емес, құқықтық қатынастардың белсенді элементі ретінде көрініс тауып, белгісіздік жағдайында дербес шешім қабылдау қабілетіне ие болумен ерекшеленеді. Жұмыста алгоритмдердің нақты автономдылығы жағдайында жауапкершіліктің антропоцентристік моделін сақтап қалу жүйелік қайшылық туындататыны негізделеді: кінә, себептік байланыс және құқық бұзушылық субъектісі сияқты классикалық құқықтық институттар зиян келтіру механизмін барабар сипаттаудан қалады. Автор құқықтық жауапкершілік конструкциясының трансформациясының үш деңгейін айқындайды: субъектілік құрам құрылымының өзгеруі («алгоритмдік делдалдықтың» пайда болуы); себеп-салдар байланысының деформациясы (алгоритмдік шешімдердің көпдеңгейлі, ықтималдық және мөлдір емес сипаты); кінә өлшемдерінің айқын болмауы (қасақаналық, абайсыздық және «технологиялық тұрғыдан сөзсіз қателік» арасындағы шекаралардың анық еместігі). Құқықтық жауапкершілік институтын цифрлық дәуір шыныдығына бейімдеудің эволюциялық бағыттары ұсынылды, соның ішінде технологиялық бейтараптық қағидатын енгізу, алгоритмдердің ашықтығы стандарттарын бекіту және жүйенің автономдылық дәрежесіне байланысты сараланған жауапкершілік режимдерін қалыптастыру қарастырылады. Автор технологиялық даму құқықтық жауапкершіліктің өзін жоққа шығармайтынын, алайда оны тұжырымдамалық тұрғыдан қайта пайымдауды талап ететінін қорытындылайды: жауапкершілік өз мәні бойынша адами категория болып қала береді, бірақ оны іске асыру тетіктері жаңа технологиялық шынайылыққа сәйкес болуы тиіс.

Тірек сөздер: субъектісі, себеп-салдар байланысы, кінә, алгоритмдік мөлдір еместік, құқық қағидаттары, құқықтың цифрлық трансформациясы.

M.E. Kasymkhan ¹, A.A. Alekseenko ², E.N. Grek ³

¹ M.I.s., Senior Lecturer, Adilet Higher School of Law, Caspian Public University (Almaty, Kazakhstan) ORCID ID: 0009-0009-8389-0232, e-mail: mkasymxanova@inbox.ru



² M.I.s., Senior Lecturer, Adilet Higher School of Law, Caspian Public University
(Almaty, Kazakhstan) ORCID ID: 0009-0004-2335-4060; e-mail: a.zairova@cu.edu.kz

³ PhD, Legal Counsel, Almaty City Chamber of Legal Consultants “Egida”
(Almaty, Kazakhstan) e-mail: e.grek@cu.edu.kz

TRANSFORMATION OF THE PRINCIPLES OF LEGAL RESPONSIBILITY IN THE CONTEXT OF AUTONOMOUS ARTIFICIAL INTELLIGENCE: A THEORETICAL AND LEGAL ANALYSIS

Abstract. *The article is devoted to a theoretical and legal analysis of the transformation of the fundamental principles of legal responsibility under the influence of autonomous artificial intelligence systems. The relevance of the study is обусловлена a qualitative transformation of social reality, in which algorithmic systems increasingly act not merely as passive tools but as active elements of legal relations, capable of independently making decisions under conditions of uncertainty. The paper substantiates that the preservation of an anthropocentric model of responsibility in the context of the de facto autonomy of algorithms gives rise to a systemic contradiction: classical legal institutions of fault, causation, and the subject of an offense cease to adequately describe the mechanism of harm causation. The author identifies three levels of transformation of the legal construct of responsibility: (1) a change in the structure of the subject composition (the emergence of “algorithmic intermediation”); (2) a deformation of the causal link (the multi-layered, probabilistic, and opaque nature of algorithmic decision-making); (3) a blurring of the criteria of fault (the uncertainty of the boundaries between intent, negligence, and a “technologically inevitable error”). Proposals are formulated for the evolutionary adaptation of the institution of legal responsibility to the realities of the digital age, including the introduction of the principle of technological neutrality, the establishment of standards for algorithmic transparency, and the implementation of differentiated liability regimes depending on the degree of system autonomy. The author concludes that technological development does not eliminate the need for legal responsibility as such, but requires its conceptual rethinking: responsibility remains inherently human in nature; however, the mechanisms of its implementation must be adequate to the new technological reality.*

Keywords: *legal responsibility, artificial intelligence, autonomous systems, subject of legal relations, causation, fault, algorithmic opacity, principles of law, digital transformation of law.*