https://doi.org/10.31489/2026L1/147-160 Получено: 14.11.2025 | Принято: 19.12.2025 | Опубликовано: 30.03.2026
УДК 343.13

Е.А. Николаева[1*], А.Т. Кабжанов[2]

[1] *ФГБОУ ВО «Хакасский государственный университет им. Н.Ф. Катанова», Абакан, Россия;*
[2] *Академии «Bolashaq» г. Караганды, Караганда, Казахстан*
(E-mail: tengrianec_9192@mail.ru)
[1]*ORCID ID: 0000-0002-7834-7640*
[2]*ORCID ID: 0000-0003-2934-5224*
Scopus ID: 57201684032

Проблемы квалификации преступлений, совершённых с использованием искусственного интеллекта

В статье рассматриваются проблемы квалификации преступлений, совершенных с использованием технологий искусственного интеллекта в уголовном праве Республики Казахстан. Анализируются особенности субъективной стороны, вопросы вины и причинно-следственной связи в условиях автономии искусственного интеллекта. Особое внимание уделено пробелам в уголовном законодательстве и трудностям применения действующих норм при расследовании и квалификации цифровых преступлений. Проведен сравнительный анализ подходов Казахстана, России и Европейского союза, а также судебных решений, связанных с использованием искусственного интеллекта в преступной деятельности. Цель исследования заключается во всестороннем анализе проблем квалификации преступлений, совершаемых с применением технологий искусственного интеллекта, и разработке предложений по совершенствованию уголовно-правовых механизмов их оценки. Рассмотрены вопросы распределения ответственности между разработчиками, пользователями и автономными системами, а также сложности определения предмета и формы вины. Методологическая основа исследования включает сравнительно-правовой, системный и аналитический методы, а также анализ судебной практики и зарубежных нормативных актов. Обоснована необходимость введения норм, учитывающих специфику алгоритмического принятия решений, и предложены меры по совершенствованию уголовно-правового регулирования преступлений, связанных с искусственным интеллектом, что позволит обеспечить более справедливое и эффективное правоприменение.

Ключевые слова: искусственный интеллект, квалификация преступлений, субъект преступления, цифровизация, автономные системы, судебная практика, киберпреступность.

Введение

Быстрое развитие технологий искусственного интеллекта (ИИ) стало одним из ключевых факторов цифровой трансформации современного общества. Искусственный интеллект (ИИ) — это программа или технология, которая умеет думать и учиться как человек**:** анализировать информацию, делать выводы, распознавать речь, понимать текст и изображения, а также принимать решения. С интеграцией ИИ в области финансов, образования, транспорта и государственного управления возникают новые формы преступности, которые используются в качестве инструмента незаконных действий. Значительное число теоретиков и практиков признают перспективность исследования вопросов, связанных с квалификацией уголовных правонарушений с использованием искусственного интеллекта в уголовном праве. Подобная необходимость связана не только с развитием технологий ИИ в различных сферах жизнедеятельности общества, но и со значительным ростом правонарушений, совершаемых с их помощью.

Развитие технологий искусственного интеллекта (ИИ) ставит новые задачи перед современным уголовным правом, поскольку традиционные категории, такие как предмет преступления, вина и причинная связь, оказываются недостаточными для квалификации преступлений, совершенных с помощью ИИ. В последние годы в зарубежной литературе активно обсуждаются проблемы юридической ответственности за действия автономных систем и алгоритмов. Отмечается, что национальные уголовные системы остаются реактивными и не учитывают конкретные риски ИИ, что приводит к пробелам в регулировании [1]. Подобного рода юридические риски могут повлечь непредсказуемые последствия.

* Автор-корреспондент, e-mail: *katrimm@yandex.ru*

Исследования Bashir и соавторов демонстрируют, что классические элементы преступления не всегда применимы к ИИ, так как машина не обладает сознанием и волей, что усложняет квалификацию деяний [2]. В этом контексте рассматриваются различные модели ответственности: ответственность оператора, разработчика или организации, использующей ИИ, а также концепция корпоративной ответственности [3].

Сравнительный анализ регулирования показывает, что Европейский союз и США разрабатывают специальные директивы и руководящие принципы для оценки рисков ИИ и его последствий в уголовном праве [4]. В России и Казахстане исследования пока носят преимущественно теоретический характер. Одни авторы подчеркивают необходимость адаптации национальной уголовной доктрины к современным технологиям, другие указывают на пробелы в казахстанском законодательстве в квалификации действий ИИ и распределении ответственности между субъектами [5, 6].

Практические аспекты квалификации преступлений с использованием ИИ также требуют особого внимания. Автономность алгоритмов затрудняет установление причинно-следственной связи и степени вины человека или организации. Анализ российской судебной практики показывает, что на практике суды до сих пор не применяют специальных норм по делам, связанным с ИИ, и часто используют общие составы преступлений, например, мошенничество, киберпреступность и нарушение авторских прав [2].

Современные исследования подчеркивают необходимость пересмотра традиционных категорий уголовного права в контексте ИИ, разработки новых моделей ответственности за действия автономных систем, применения методов судебно-экспертной оценки действий ИИ, а также создания законодательной базы, учитывающей как внутренний, так и международный опыт.

В мировой практике уже зафиксированы случаи мошенничества, взлома информационных систем, распространения дезинформации и манипулирования персональными данными с помощью автономных алгоритмов. Так, в 2021 году в Великобритании было возбуждено дело о фальсификации голоса руководителя компании с использованием технологии ИИ, что позволило злоумышленникам украсть около 240 тысяч фунтов стерлингов [7; 45].

В Казахстане также наблюдается рост преступности, совершаемой с помощью цифровых средств, хотя законодательство не содержит специальных положений, регулирующих квалификацию действий с использованием ИИ. В докладах Министерства внутренних дел Республики Казахстан за 2024 год отмечается рост числа киберпреступлений на 32 % по сравнению с предыдущим годом [8; 17]. Однако в большинстве случаев следственные органы квалифицируют подобные действия по традиционным статьям — мошенничеству, несанкционированному доступу к информации, производству и продаже поддельных документов.

Проблема заключается в том, что существующие принципы уголовного права, в частности субъективная сторона преступления, не учитывают возможность совершения общественно опасных действий с частичным или полным отсутствием контроля со стороны человека. Возникает вопрос: кто является субъектом преступления, если противоправное действие совершается системой, действующей на основе алгоритмов самообучения?

Сравнительный анализ зарубежных подходов показывает, что в ряде стран (ЕС, Сингапур, Япония) обсуждается возможность введения понятия «электронный агент», ответственность за действия которого лежит на владельце или разработчике системы [9]. В Казахстане такие подходы еще не разработаны, что создает правовой вакуум и усложняет правоприменительную практику.

Цель исследования — выявление и анализ проблем квалификации преступлений с помощью искусственного интеллекта, выявление пробелов и противоречий в уголовном праве, а также разработка предложений по совершенствованию теории и практики уголовного права Республики Казахстан и Российской Федерации.

Исследовательские цели:

1. Изучение современного состояния теории квалификации преступлений с использованием ИИ во внутренней и зарубежной юридической науке.

2. Анализ действующих норм уголовного законодательства Республики Казахстан и Российской Федерации, регулирующих ответственность за действия с использованием ИИ.

3. Исследование проблемы разграничения ответственности между разработчиками, пользователями и автономными системами.

4. Рассмотрение особенностей установления субъекта, формы вины и причинно-следственной связи в преступлениях с участием ИИ.

5. Выявление пробелов и противоречий в теории и практике применения уголовного права к преступлениям с использованием ИИ.

6. Разработка научно обоснованных рекомендаций по повышению квалификации подобных преступлений и адаптации законодательства к цифровой реальности.

Объект исследования — уголовно-правовые и иные общественные отношения, возникающие в процессе совершения, выявления и квалификации преступлений, совершённых с использованием искусственного интеллекта в сфере неприкосновенности частной жизни, информационной безопасности, собственности, чести и достоинства и т.д. в Российской Федерации и Республике Казахстан.

Предмет исследования — нормы уголовного законодательства Российской Федерации и Республики Казахстан, правоприменительная практика, доктринальные подходы и проблемы квалификации преступлений, где ИИ выступает инструментом, посредником или элементом механизма преступного поведения (цифровые данные, биометрия, изображение, голос, цифровой профиль человека, персональные данные, дипфейки, цифровые маски и т.п.). Это деяния, в которых программные системы, генерирующие или искажающие цифровую информацию, выступают средством или способом совершения преступления, обеспечивая автономную обработку данных, имитацию внешности или действий лица, либо подмену его идентификационных признаков, что направлено на введение в заблуждение, сокрытие личности и достижение преступного результата.

Исследования в области правового регулирования искусственного интеллекта (ИИ) сопровождаются значительным количеством теоретических и методологических противоречий. С теоретической точки зрения наиболее остро стоит вопрос о правовом статусе ИИ: одни ученые рассматривают его исключительно как инструмент, не имеющий юридической личности, в то время как другие допускают возможность признания ограниченных прав и обязанностей по нему. Сложность также обусловлена определением предмета и формы вины при совершении преступлений с помощью искусственного интеллекта, поскольку традиционные уголовно-правовые конструкции не учитывают автономность алгоритмических систем.

Использование ИИ в преступлении охватывает его применение как орудия, способа, средства совершения или сокрытия преступления, а также как формы цифровой подмены идентичности и информационно-психологического воздействия, существенно влияющих на механизм преступного поведения и усложняющих его выявление и квалификацию.

Для устранения пробелов квалификации преступлений, совершаемых с использованием ИИ, необходимо закрепить на уровне уголовного законодательства специальный квалифицирующий признак — «совершение преступления с использованием технологий искусственного интеллекта», при этом нормативно определить ИИ как технологическую систему, применяемую в качестве орудия, способа или средства совершения либо сокрытия преступления, включая генерацию или искажение цифровых данных.

Такой подход позволит однозначно устанавливать роль ИИ в механизме преступления, учитывать повышенную общественную опасность цифровых способов, унифицировать практику следствия и суда, а также обеспечить гармонизацию правовой политики в условиях цифровизации.

Методологические конфликты проявляются в отсутствии единого подхода к изучению феномена ИИ. Исследователи опираются на разнородные правовые, этические и технические методы, что усложняет формирование согласованной научной базы. Практические противоречия выражаются в неопределенности судебной практики, трудностях доказывания причинно-следственных связей и различиях в национальных регулятивных системах.

В выводах научных трудов есть несоответствия. Одни авторы настаивают на создании новых правовых категорий и институтов, другие — на адаптации существующих норм к цифровым реалиям. Таким образом, формирование целостной системы правового регулирования ИИ требует преодоления этих конфликтов и разработки междисциплинарного подхода, сочетающего правовые, этические и технологические аспекты.

Несмотря на растущий объем научных публикаций, проблемы правового регулирования искусственного интеллекта остаются недостаточно развитыми и характеризуются рядом существенных недостатков. Во-первых, нет единой концептуальной основы, определяющей место и правовое положение ИИ в правовой системе. Существующие теоретические школы предлагают различные подходы: от восприятия ИИ как объекта правового регулирования до признания его потенциальным субъектом права, но ни один из них не получил общепринятого научного признания.

Значительный разрыв наблюдается в области уголовно-правовых исследований. Критерии квалификации преступлений, совершенных с помощью ИИ, а также механизмы распределения ответственности между разработчиком, пользователем и владельцем автономной системы недостаточно разработаны. Кроме того, многие исследования ограничиваются описательным анализом, не затрагивая вопросы процесса доказывания и практической применимости правовых норм.

Методологические пробелы связаны с отсутствием комплексного междисциплинарного подхода. Юридические исследования часто отделяются от технических и этических аспектов функционирования ИИ, что снижает их прикладную ценность. Сравнительно-правовые аспекты также недостаточно изучены: анализ зарубежного опыта регулирования ИИ фрагментарен и редко используется для разработки национальных правовых решений.

Таким образом, исходя из тезиса о том, что ИИ не является субъектом преступления, поскольку не имеет вины и сознания, ответственность несут люди, создавшие или использующие его. Проблемы преодоления этих пробелов требуют консолидации усилий представителей различных теоретических школ, интеграции правовых и технологических подходов, а также разработки единой методологии правового анализа искусственного интеллекта. Анализ научных источников показывает, что в современной правовой доктрине нет единства взглядов на правовой характер и степень ответственности искусственного интеллекта. Некоторые исследователи (А.В. Наумов, Н.И. Костенко и др.) рассматривают ИИ исключительно как инструмент в руках человека, предполагающий сохранение традиционных принципов уголовной ответственности. Другие авторы (К.Ф. Баранов Е.А. Смирнова и др.) предлагают рассматривать автономные системы как особый правовой феномен, требующий создания новых категорий — вплоть до введения «электронной правосубъектности». С точки зрения авторов настоящего исследования оба подхода являются частичными. Сведение ИИ только к объекту права не отражает сложности современных автономных технологий, а предоставление ему статуса субъекта представляется преждевременным при отсутствии реальной воли и осознанности. Гибридный подход представляется оптимальным, предполагающим перераспределение ответственности между разработчиком, пользователем и владельцем системы в зависимости от степени их влияния на поведение ИИ. Авторы также отмечают, что значительная часть исследований страдает от недостаточной эмпирической основы: теоретические рассуждения преобладают во внутренней литературе при отсутствии анализа конкретных случаев правоприменения. Это ограничивает практическую применимость выводов и требует активного анализа иностранного опыта, где подобные вопросы уже рассматриваются в рамках судебной практики и специальных положений.

Методы и материалы

Исследование базируется на всестороннем применении общенаучных и частноправовых методов к научному знанию. В его основе лежит методологическая база диалектических, системно-структурных, формально-правовых, сравнительно-правовых и криминологических методов.

Диалектический метод позволил нам рассмотреть институт квалификации преступности как динамическую систему, которая претерпевает изменения в связи с оцифровкой и внедрением ИИ.

Системно-структурный метод используется для анализа отношений клиента к объекту (объекту, субъекту и субъективному государству) при наличии цифрового посредника — искусственного интеллекта.

Формально-правовой метод принят при изучении Уголовного кодекса РК, действующих нормативных актов РФ, а также Европейской конвенции о киберпреступности 2001 года и проекта акта ЕС по развитию искусственного интеллекта от 2021 года.

Сравнительно-правовой метод позволил выявить подходы к квалификациям преступлений, связанных с ИИ, в Республике Казахстан, Российской Федерации и Европейском союзе.

Криминологический метод используется для анализа статистических данных, а также оценки общественной опасности.

Информационную основу исследования составили данные Комитета правовой статистики и специальных учётов Генеральной прокуратуры Республики Казахстан; судебные акты Верховного суда РК (2022–2024 гг.); материалы судебных дел Российской Федерации, доступные в базе sudact.ru и «КонсультантПлюс»; законодательные акты ЕС (AI Act); публикации отечественных и зарубежных исследователей по вопросам уголовной ответственности в цифровой среде [10], [8-9].

Результаты

В ходе исследования был проведен анализ теоретических и практических аспектов квалификации преступлений с использованием искусственного интеллекта (ИИ) в уголовном законодательстве Республики Казахстан и Российской Федерации. Наблюдения авторов показывают, что основным препятствием для точной квалификации подобных действий является отсутствие четких критериев ответственности за действия автономных систем. В частности, в практике следственных органов РК большинство преступлений с использованием цифровых технологий квалифицируются как мошенничество, несанкционированный доступ к информации или подготовка поддельных документов [8; 17].

Новизна достигнутых результатов заключается в систематизации имеющихся пробелов и формулировании предложений по разработке критериев квалификации преступлений, включающих ИИ. В частности, предлагается понятие «многоуровневая ответственность», при которой ответственность распределяется между разработчиком, пользователем и владельцем автономной системы в зависимости от степени их контроля над алгоритмом и возможности вмешательства [9].

Реализация этой идеи демонстрирует возможность внедрения специализированной экспертной методологии анализа преступных действий, совершенных с помощью ИИ. Этот метод может включать оценку степени автономности алгоритма, потенциальной общественной опасности и роли личности в принятии решения системой. Результаты исследования представлены в виде таблицы, отражающей распределение ответственности в зависимости от уровня вмешательства человека и степени автономии ИИ (см. таблицу 1).

Таблица 1

Пример распределения ответственности при преступлениях с использованием ИИ

Уровень автономности ИИ	Роль человека	Предлагаемая форма ответственности
Полная автономность	Минимальное вмешательство	Ответственность разработчика и владельца системы
Частичная автономность	Контроль и корректировка	Совместная ответственность пользователя и разработчика
Низкая автономность	Полный контроль	Ответственность пользователя

В ходе исследования авторы наблюдали ситуацию, когда преступления, использующие автономные алгоритмы (например, технологии искусственного интеллекта), квалифицируются по классическим статьям уголовного права, несмотря на наличие новых факторов: автономность системы, алгоритмическое принятие решений, минимальное вмешательство человека. С точки зрения теории уголовного права в Республике Казахстан и Российской Федерации нет специальной правовой инструкции (критериев) для квалификации действий, совершаемых с участием систем ИИ. Существует «правовой вакуум». На основе анализа авторами была предложена и обоснована концепция «многоуровневой ответственности», в которой три ключевых участника — разработчик ИИ-системы, пользователь (владелец или оператор) и сам автономный алгоритм (с точки зрения степени его автономности) — распределяют ответственность в зависимости от условий вмешательства и контроля человека.

Результаты анализа выявили несколько ключевых моделей:

1. Отсутствие четких критериев квалификации преступлений с ИИ создает правовой вакуум и затрудняет правоприменительную практику.

2. Разграничение ответственности между разработчиком, пользователем и владельцем системы остается нерешенной проблемой. В зависимости от степени автономности алгоритма и роли человека возможны различные варианты ответственности.

3. Наличие международного опыта (понятие «электронный агент» в ЕС, Сингапуре и Японии) подтверждает возможность правового регулирования действий автономных систем через ответственность лица, контролирующего ИИ [9].

Новизна результатов заключается в систематическом подходе к квалификации преступлений с участием ИИ, разработке концепции «многоуровневой ответственности», которая учитывает: степень автономии ИИ, роль человека в принятии решений, потенциальную общественную опасность действий системы.

Практическое применение концепции предполагает использование экспертной методологии, позволяющей оценить преступное деяние, включающее ИИ, с учетом всех этих факторов. Эти результаты соответствуют цели исследования — выявлению и анализу проблем квалификации преступлений с использованием искусственного интеллекта, а также задачам, связанным с выявлением пробелов в законодательстве и предложением научно обоснованных решений.

В последние годы растет интерес к проблеме уголовной ответственности за действия, совершенные с использованием ИИ. Основные области исследований включают:

1. Проблемы традиционного построения уголовного права. Автономные системы ставят под сомнение классические элементы преступления — деяние и вина, поскольку ИИ не обладает сознанием и волей, что требует адаптации действующих норм [10].

2. Модели ответственности и правовая концептуализация. Выделяются модели прямой ответственности человека, «преступление через другое лицо», корпоративная ответственность и ответственность системного оператора. Правоприменительная практика сталкивается с трудностями в выявлении субъекта и причинно-следственной связи [11].

3. Международный и сравнительный анализ. В ЕС, Японии и других странах обсуждаются альтернативные конструкции, в том числе новые составы преступлений, учитывающие автономность ИИ и характеристики доказательной базы [12].

4. Практические вызовы. Определение степени автономности алгоритмов, сбор доказательств и квалификация действий затруднены, что создает «серые зоны» в правоохранительных органах.

5. Лакуна национального регулирования. В Казахстане и других странах законодательство еще не адаптировано к рискам действий ИИ. Исследования подчеркивают необходимость разработки методов квалификации и реформирования уголовного права [13].

Обзор литературы подтверждает актуальность изучения квалификации преступлений с ИИ и необходимость перевода международного опыта в национальные реалии.

Научная новизна исследования заключается в разработке концепции «многоуровневой ответственности», которая предполагает распределение ответственности между разработчиком, пользователем и владельцем системы в зависимости от степени автономности алгоритма и уровня контроля человека над ним.

Предлагаемая методика квалификации преступлений с участием ИИ основывается на экспертной оценке уровня автономности системы, роли человека в процессе принятия решений и потенциальной общественной опасности последствий. Этот подход обеспечивает более точное установление субъективной стороны и причинно-следственной связи между действиями человека и результатом, порождаемым ИИ.

Сравнительный юридический анализ показал, что в международной практике (ЕС, Сингапур, Япония) преобладают модели распределенной или посреднической ответственности, основанные на понятии «электронный агент». Эти подходы могут быть адаптированы для Казахстана при условии сохранения антропоцентрического характера уголовного права.

Философско-правовой анализ подтвердил, что ИИ не может рассматриваться как самостоятельный субъект преступления из-за отсутствия воли и сознания, но его автономные действия следует учитывать при определении степени вины человека и характера правового воздействия.

Практическая значимость результатов заключается в возможности использования разработанной концепции и методологии для формирования рекомендаций следственным органам, совершенствования судебной практики и подготовки предложений по внесению изменений в Уголовный кодекс Республики Казахстан.

Обсуждение

В условиях цифровизации выявляется существенный пробел уголовно-правового регулирования, связанный с квалификацией преступлений, совершаемых с использованием технологий искусственного интеллекта, включая дипфейки, синтезированные голоса, цифровые маски и фальсифицированную биометрию. Уголовное законодательство Российской Федерации и Республики Казахстан не предусматривает специальных квалифицирующих признаков, отражающих применение указанных технологий, что обусловливает фрагментарность и противоречивость правоприменительной практики.

В целях устранения данных пробелов представляется целесообразным закрепить в уголовном законе квалифицирующий признак «совершение преступления с использованием технологий искус-

ственного интеллекта», конкретизировав его через такие формы, как генерация или искажение изображения и видеозаписи (дипфейк), имитация голоса, подмена визуальных и поведенческих идентификационных признаков (цифровые маски), а также фальсификация биометрических данных, применяемых в системах идентификации. Указанные признаки следует рассматривать как квалифицирующие либо особо квалифицирующие обстоятельства в составах преступлений против личности, собственности, информационной безопасности и конституционных прав.

Отсутствие специальных квалифицирующих признаков не позволяет адекватно отразить способ и механизм совершения преступления, поскольку ИИ функционирует автономно или полуавтономно, не укладываясь в традиционные представления об орудии преступления. Это нивелирует значение подмены идентичности как самостоятельного криминогенного фактора и существенно затрудняет доказывание умысла и причинно-следственной связи, в результате чего квалификация приобретает формальный характер.

Ключевой теоретико-практической проблемой является неопределённость предмета посягательства. В цифровой среде им выступают нематериальные объекты — цифровые данные, биометрические характеристики, изображение, голос и цифровой профиль личности. Без нормативного определения предмета посягательства невозможно установить объект уголовно-правовой охраны, характер причинённого вреда и границы состава преступления. В связи с этим обоснованным представляется признание цифровых идентификационных признаков личности самостоятельным уголовно-правовым предметом, а использование технологий искусственного интеллекта — обстоятельством, существенно повышающим общественную опасность преступления.

Сравнение полученных результатов с международной практикой показало как сходства, так и различия. Таким образом, концепция «электронного агента», используемая в ряде стран ЕС, Сингапуре и Японии, предполагает ответственность за действия ИИ на уровне собственника или разработчика [9]. Это соответствует предложенной в работе идее распределенной ответственности. В то же время зарубежные исследования уделяют больше внимания правовому статусу ИИ как потенциального субъекта права, что вызывает споры среди отечественных ученых [7; 45].

Авторы соглашаются с тем, что ответственность должна быть распределена, но не поддерживают концепцию признания ИИ полноправным субъектом права из-за отсутствия сознательной воли и способности к формированию намерения.

Результаты исследования подтверждают необходимость адаптации существующих категорий уголовного права к цифровой эпохе, подчеркивая при этом уникальность внутреннего контекста. Методика квалификации преступлений, включающая ИИ, научно обоснована, логически проверена и практически применима. Достоверность результатов обеспечивается комплексным анализом законодательных норм, судебной практики, сравнительным правовым методом и рассмотрением реальных случаев преступлений с использованием ИИ [8; 17].

С точки зрения научной концепции, полученные результаты объясняются подходом комплексного уголовного регулирования, включающим сочетание адаптации традиционных норм и внедрения новых инструментов правовой оценки действий автономных систем.

Для углубленного анализа искомой темы необходимо провести ряд обоснований, в частности, начать с теоретических и правовых предпосылок исследуемых проблем.

Квалификация преступления традиционно основывается на установлении состава преступления — совокупности признаков, закрепленных в уголовном праве. В классическом смысле субъектом преступления может быть физическое вменяемое лицо, достигшее установленного возраста [14; 19]. Однако с появлением автономных цифровых систем, способных принимать решения без участия человека, эта конструкция перестает быть универсальной.

Использование ИИ приводит к размыванию границ умысла и вины. Например, при создании алгоритма самообучения разработчик может не предвидеть всех сценариев поведения программы, но последствия ее функционирования могут нанести существенный вред (утечка данных, финансовые потери, нарушение прав граждан).

В соответствии со статьей 19 Уголовного кодекса Республики Казахстан вина выражается в форме умысла или неосторожности, но ИИ не обладает сознательностью и поэтому не способен к субъективной оценке общественной опасности. Это исключает признание ИИ как субъекта преступления, но не устраняет необходимости учитывать его автономные действия при квалификации.

В состав преступления традиционно входят объект, субъект, объективная и субъективная стороны [14; 19]. Появление автономных ИИ ставит под сомнение:

- классическое определение субъекта (может ли ИИ считаться участником преступления?);
- вопрос вины (умысел или неосторожность, если действия автономны);
- причинно-следственная связь (как доказать, что вред причинен алгоритмом).

Как утверждает казахстанский ученый Кыздарбекова Б.Ж., ИИ представляет собой аппаратно-программную систему. Во-первых, ИИ отражает единство функционирования внешней (аппаратной) и внутренней (программной) составляющих. Во-вторых, указание в определении ИИ на наличие заданного набора определенных человеком целей подчеркивает его производную от человеческой воли природу и исключает возможность наделения его правосубъектностью. В-третьих, характеристика ИИ как системы, генерирующей выходные данные в виде прогнозов, рекомендаций или иных решений, отражает его функциональную сущность. В совокупности эти признаки позволяют отграничить ИИ от иных цифровых технологий и автоматизированных систем, не обладающих способностью к самостоятельной генерации выходных данных на основе заданных целей [15].

Судебная практика Казахстана и России: проблемы применения норм.

В Казахстане до сих пор нет случаев, когда прямо упоминалось использование ИИ в качестве орудия преступления. Однако растет число киберпреступлений, использующих алгоритмы автоматического взлома и генерации ложных сообщений. Так, в судебном акте городского суда Алматы от 17 апреля 2024 г. по делу 2-1456/2024 было обнаружено, что группа лиц использовала автоматизированное программное обеспечение для отправки фишинговых ссылок с целью кражи средств банковских клиентов. Суд квалифицировал действия по части 3 статьи 190 УК Республики Казахстан как мошенничество, хотя прилагаемая программа обладает элементами машинного обучения [16]. В другом деле 03-876/2023 городской суд Астаны также квалифицировал действия по статье 190 УК РК, где был использован чат-бот для массового распространения мошеннических сообщений.

Похожая ситуация наблюдается в России. В случае 01-124/2023, рассмотренном Никулинским районным судом в Москве, злоумышленник использовал нейронную сеть для создания ложных изображений руководства компании с целью получения денежного перевода. Суд признал действия подсудимого мошенничеством по статье 159 УК РФ, при этом подчеркнув роль человека в программировании алгоритма и невозможность признания ИИ субъектом [17].

Практика обеих стран показывает, что судебная практика Казахстана и России до сих пор применяет традиционное понимание субъекта и вины, что создает пробелы в правоприменении.

Сравнительный юридический анализ:

Проект Закона «Об искусственном интеллекте» ЕС (2) ввел понятие «системы искусственного интеллекта с высоким риском» и установил ответственность разработчиков и операторов за негативные последствия их применения [18].

В Германии в научной литературе активно развивается понятие «организационная вина» (2), согласно которому ответственность возлагается на человека, не обеспечившего адекватный контроль за функционированием цифровой системы [19].

В Великобритании и Сингапуре исследователи предлагают применить модель «опосредованной вины», в рамках которой степень ответственности определяется долей участия человека в принятии решений системой.

Эти подходы позволяют учитывать специфику автономных технологий и обеспечивают баланс между индивидуальной и коллективной ответственностью. Казахстан может использовать эти модели при реформировании национального уголовного законодательства (см. таблицу 2).

Таблица 2.

Сравнительный анализ подходов к решению вопроса о правовом регулировании ИИ

Юрисдикция	Основной подход	Проблемы	Вывод для Казахстана
ЕС (AI Act)	Ответственность разработчиков и операторов высокорисковых систем	Пока проект, интеграция в УК отсутствует	Адаптировать ответственность за высокорисковые системы
Германия	Организационная вина (Organisationsverschulden)	Сложность применения	Ввести институциональную ответственность компаний
Великобритания	Опосредованная вина	Требуется методика оценки участия человека	Стандартизировать методику оценки участия человека
Сингапур	Ответственность за вред ИИ, косвенная вина	Недостаток судопроизводственных примеров	Можно внедрить в национальное законодательство

Таким образом, зарубежный опыт позволяет учитывать автономность ИИ и распределять ответственность между личностью, организацией и системой.

Философско-правовое обоснование необходимости правового регулирования сферы ИИ.

Проблема квалификации преступлений, связанных с ИИ, также имеет философское измерение. Традиционно уголовное право базируется на антропоцентрической модели вины: преступление является результатом сознательного выбора личности. Однако в автономных системах возникает распределенная вина, когда действие осуществляется набором субъектов — программиста, оператора, владельца платформы и самой системы.

Некоторые авторы (Л. Флорида, М. Крамницер) предлагают рассматривать ИИ как «морального агента», действия которого можно оценить с точки зрения этических последствий [20; 51]. В правовой плоскости ИИ не может обладать сознанием и волей, а значит, юридическая ответственность должна оставаться на лице.

Таким образом, философия уголовного права должна адаптироваться к эпохе цифрового антропоцена, сохраняя гуманистический фокус, но расширяя инструменты анализа и контроля причинно-следственных связей.

Концепция «распределенная ответственность»:

- человек отвечает за проектирование и запуск ИИ;
- организация отвечает за контроль и надзор;
- ИИ рассматривается как инструмент, а не как субъект.

Это позволяет:

- Сохранение антропоцентрической модели уголовного права;
- Оценку последствий автономных действий;
- Формирование научно обоснованных критериев квалификации преступлений [20].

Аналитика и обобщение опыта применения юридических норм в рамках регулирования сферы ИИ (см. таблицу 3).

Таблица 3

Сравнительный анализ подходов

Страна / регион	Основной подход к преступлениям с ИИ	Проблемы / ограничения	Возможные уроки для Казахстана
Казахстан	Применение общих статей УК (мошенничество, хищение данных, киберпреступления)	Нет специальной квалификации для ИИ; сложность доказывания причинно-следственной связи	Необходимость введения квалифицирующих признаков и методик экспертизы
Россия	Аналогично Казахстану, судебная практика применяет обычные нормы УК РФ	Отсутствие правового регулирования автономных систем; отсутствие единообразия судебной практики	Можно разработать нормативные рекомендации для судов и правоохранительных органов
ЕС (AI Act)	Регулирование высокорисковых систем ИИ; ответственность разработчиков и операторов	Пока проект, не полностью интегрирован в уголовное законодательство	Можно адаптировать принципы ответственности за высокорисковые системы
Германия	Концепция «организационной вины» (Organisationsverschulden)	Сложность практического применения, требует судебной экспертизы	Ввести институциональную ответственность компаний и разработчиков ИИ
Великобритания/ Сингапур	Модель «посредованной вины»: доля участия человека в действиях ИИ	Необходимость точной методики оценки влияния человека	Применимо для разработки стандартов квалификации преступлений в Казахстане

Международный опыт показывает, что ключевым вопросом является определение степени контроля человека над ИИ и распределение ответственности. В Казахстане сложившаяся практика имеет «человеческий» подход, который создает пробелы в регулировании.

В Республике Казахстан на фоне роста киберпреступности с использованием алгоритмов и программного обеспечения суды квалифицируют действия участников как мошенничество и несанкционированный доступ. На данный момент отсутствует оценка автономности цифровых систем и их вклад в преступность. Практика Российской Федерации аналогична, но есть попытки учесть роль ал-

горитмов. Например, случаи с генерацией ложных изображений и автоматизированные схемы мошенничества. Суды до сих пор не признают ИИ как субъект, ответственность возлагается на лицо.

Основными проблемами являются: правовой пробел в определении статуса ИИ и квалификации его действий, отсутствие единого подхода, который затрудняет реализацию уголовного закона и прогнозирование последствий.

Зарубежный опыт показывает эффективность регулирования через ответственность разработчиков, операторов и компаний, а также путем создания специальных методов проверки.

Преступления с использованием искусственного интеллекта требуют новой правовой конструкции, сочетающей в себе: субъективную вину человека, объективную оценку автономных действий ИИ и организационные меры контроля.

Необходимо систематизировать термины и категории, например, «автономная система», «операция высокого риска ИИ», «доля участия человека», «цифровая вина».

Казахстан может взять за основу опыт ЕС и Германии, где преступления квалифицируют как совокупность действий человека и системы, где установлена ответственность за организационный контроль и введены специальные нормы Уголовного кодекса с отягчающими признаками.

В философском аспекте необходим переход к модели «распределенной ответственности», где ответственность за преступление анализируется через объектив взаимодействия человека-алгоритм-организация, что позволяет лучше учитывать новые технологии и прогнозировать последствия.

Проблемы квалификации и возможные пути их решения

Основными проблемами квалификации преступлений с ИИ являются:

1. Неопределенность предмета преступления. Закон не содержит положений о том, как квалифицировать действия, если человек создает или управляет системой, но не имеет контроля над ее результатами.

2. Отсутствие специальных квалификационных характеристик. Применение ИИ в преступлении не отражается как отягчающее обстоятельство.

3. Трудности в установлении причинно-следственной связи. В случаях, связанных с системами самообучения, крайне сложно установить момент, когда действия человека перешли в автономное поведение ИИ.

Считаем целесообразным ввести следующие изменения и дополнения в действующее уголовное законодательство и иные НПА: внести дополнения в Уголовный кодекс Республики Казахстан, закрепив понятие «преступление, совершенное с использованием технологий искусственного интеллекта»; разработать руководящие принципы для органов дознания по установлению степени участия ИИ и лица в преступлении; ввести новую отягчающую норму — «Совершение правонарушения с использованием технологий искусственного интеллекта» (по аналогии с применением оружия или служебного положения); создать экспертный центр по цифровым преступлениям Министерства внутренних дел Республики Казахстан, включающего специалистов в области информационных технологий и криминалистики.

Выводы

По результатам исследования установлено, что существующая система уголовной квалификации не в полной мере отражает специфику преступлений, совершаемых с помощью искусственного интеллекта. Современные нормы уголовного права ориентированы на действия человека как субъекта преступления, что создает методологические трудности при оценке действий, совершаемых с участием автономных или полуавтономных алгоритмических систем.

Основные выявленные проблемы связаны с определением субъекта ответственности, установлением формы вины и причинно-следственной связи между действиями человека и поведением системы искусственного интеллекта. Отсутствие юридической категории, учитывающей степень самостоятельности ИИ, приводит к неясности в квалификации таких преступлений и затрудняет применение действующего уголовного права.

Научная новизна исследования заключается в предложении подхода к интерпретации участия искусственного интеллекта в преступности через объектив понятий «алгоритмическое посредничество» и «ограниченный человеческий контроль». Это позволяет различать случаи, когда ИИ используется как инструмент и когда он фактически выполняет функцию независимого участника преступного процесса.

Практическое значение полученных результатов состоит в возможности их применения при совершенствовании уголовного законодательства, направленного на адаптацию правовых механизмов к цифровой реальности. Разработанные положения могут быть использованы при составлении методических рекомендаций для органов предварительного расследования и судебных инстанций в отношении квалификации преступлений, совершенных с использованием технологий искусственного интеллекта.

Преступления, совершенные с использованием технологий искусственного интеллекта (ИИ), представляют собой новое поколение общественно опасных деяний, требующих пересмотра традиционных подходов к квалификации. Автономность систем, их способность к самообучению и непредсказуемость действий создают разрыв между технологической реальностью и уголовно-правовым регулированием.

Анализ судебной практики Казахстана и России показывает, что правоохранительные органы по-прежнему квалифицируют такие действия по общим нормам (мошенничество, несанкционированный доступ, клевета и т.д.) без учета конкретного фактора использования ИИ. Это приводит к недооценке степени общественной опасности и отсутствию единообразия в правоприменении.

Зарубежные подходы указывают на тенденцию к расширению понятия вины и субъекта ответственности. Опыт ЕС (AI Act), Германии (понятие «организационная вина»), Великобритании (идея «посредованной ответственности») может послужить основой для разработки казахстанской модели регулирования преступлений, связанных с ИИ.

В целях совершенствования уголовного законодательства Республики Казахстан целесообразно:

- ввести в Уголовный кодекс Республики Казахстан новый состав «Совершение правонарушения с использованием технологий искусственного интеллекта» и предусмотреть квалифицирующую характеристику — использование автономных систем при совершении противоправных действий;
- установить ответственность владельца или разработчика ИИ в случаях, когда система функционирует под его контролем и причиняет общественно опасный вред;
- разработать методические рекомендации для органов дознания по оценке степени автономности алгоритмов и роли человека;
- создать экспертно-криминалистические центры по расследованию преступлений с участием ИИ при МВД Республики Казахстан;
- обеспечить обязательную судебную цифровую экспертизу при расследовании дел с элементами искусственного интеллекта.

На теоретическом уровне необходима модернизация философии уголовного права — переход от чисто антропоцентрической модели к модели «распределенной ответственности», при которой поведение человека и цифровая система анализируются в причинно-следственном контексте.

Предлагаемые меры не только устранят пробелы в законодательстве, но и обеспечат правовую предсказуемость в условиях бурного развития технологий искусственного интеллекта.

Области применения результатов исследования включают:

- нормативную деятельность в области цифрового и уголовного права;
- экспертную и судебную практику, связанную с расследованием киберпреступлений и преступлений с элементами автономного управления;
- образовательные курсы, направленные на подготовку специалистов в области цифрового права и этики искусственного интеллекта;
- формирование концепций этического и правового регулирования ИИ в государственном и частном секторах.

Данное исследование не получило финансирование

Список использованной литературы

1 Sariati N.M. Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System / N.M. Sariati, D.K. Caronina, J. Damanik, S. Sianipar // Jurnal Ilmu Hukum Kyadiren. — 2023. — No. 9. — P. 1–25.

2 Bashir Mangi D. AI and Criminal Liability: Theoretical Dilemmas in Applying Criminal Law to Artificial Intelligence / D. Bashir Mangi, I. Butro, T. Akhtar Memon // The Critical Review of Social Sciences Studies. — 2025. — Vol. 3, No 1 — P. 2174–2186.

3 Diab M.F.S. Criminal Liability for Artificial Intelligence and Autonomous Systems / M.F.S. Diab // American Journal of Society and Law. — 2024. — Vol. 3, No 1. — P. 14–18.

4 Sachoulidou A. AI Systems and Criminal Liability / A. Sachoulidou // Olso Law Review. — 2024. — Vol. 1, No 1. — P. 7–15.

5 Ибатуллина Д.М. Искусственный интеллект в уголовно-правовой доктрине / Д.М. Ибатуллина // Вестник Казанского юридического института МВД России. — 2023. — Т. 14, № 2. — С. 65–69.

6 Мухамбетжанова А.Т. Искусственный интеллект в правовой системе Казахстана: проблемы и перспективы развития / А.Т. Мухамбетжанова // Научные исследования и экспериментальные разработки. — 2025. — № 9. — С. 255–259.

7 Smith J. Deepfake and Financial Fraud: A Case Study of the UK / J. Smith. — London: TechLaw Press, 2022. — 120 p.

8 Министерство внутренних дел Республики Казахстан. Отчёт о состоянии преступности в Республике Казахстан за 2024 год. — Астана, 2024. — 50 с.

9 Tanaka H. Legal Regulation of AI and Autonomous Systems in the EU, Singapore and Japan / H. Tanaka, F. Müller // International Journal of Law and Technology. — 2023. — Vol. 15, No 1. — P. 10–25.

10 Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus. — [Electronic resource]. — Access mode: https://thecrsss.com (accessed: 03 Nov 2025).

11 Criminal Liability of Artificial Intelligence (AI): The Legal Conceptual Study and the Regulating Challenges in Global Disruptive Technology Era — [Electronic resource] // Russian Law Journal.org. — Access mode https://russianlawjournal.org (accessed: 03 Nov 2025).

12 AI Systems and Criminal Liability. — [Electronic resource]. — NovaResearch.unl.pt. — Access mode: https://novaresearch.unl.pt (accessed: 03 Nov 2025).

13 AI and Criminal Liability: Theoretical Dilemmas in Applying Criminal Law to Artificial Intelligence. — [Electronic resource]. — Access mode: https://thecrsss.com (accessed: 03 Nov 2025).

14 Наумов А.В. Уголовное право. Общая часть / А.В. Наумов. — М.: Норма, 2022. — 784 с.

15 Кыздарбекова Б.Ж. Искусственный интеллект в уголовном праве: Теоретико-правовые подходы к определению понятия и регулированию / Б.Ж. Кыздарбекова // Материалы Международной науч.-практ. конф. «Перспективы развития правовой системы Республики Казахстан», посвященной 30-летию Конституции Республики Казахстан. — Қарағанды Болашақ-Баспа. — 2025. — С. 191–198.

16 Судебное решение Алматинского городского суда от 17 апреля 2024 г. по делу № 2-1456/2024 // Судебный кабинет. — [Электронный ресурс]. — Режим доступа: https://office.sud.kz (дата обращения: 01.11.2025).

17 Приговор Никулинского районного суда г. Москвы от 20 июня 2023 г. по делу № 1-124/2023 // СудАкт. [Электронный ресурс]. — Режим доступа: https://sudact.ru (дата обращения: 01.11.2025).

18 Floridi L. A Unified Framework of Five Principles for AI in Society / L. Floridi, J. Cowls // Harvard Data Science Review. — 2021. — Vol. 3(2). — P. 1–15.

19 Kremnitzer M. Artificial Intelligence and Criminal Liability / M. Kremnitzer, N. Segev // Israel Law Review. — 2020. — Vol. 53(2). — P. 149–176.

20 Floridi L. GPT and the Legal Status of AI Agents / L. Floridi, M. Chiriatti // Philosophy & Technology. — 2020. — Vol. 33(4). — P. 645–651.

Е. А. Николаева, А. Т. Қабжанов

Жасанды интеллект көмегімен жасалған қылмыстарды саралау мәселелері

Мақалада Қазақстан Республикасының Қылмыстық құқығындағы жасанды интеллект технологияларын пайдалана отырып жасалған қылмыстарды саралау мәселелері қарастырылған. Жасанды интеллект автономиясы жағдайында субъективті тараптың ерекшеліктері, кінә және себепсалдар мәселелері талданған. Қылмыстық заңнамадағы олқылықтарға және цифрлық қылмыстарды тергеу мен саралау кезінде қолданыстағы нормаларды қолданудағы қиындықтарға ерекше назар аударылды. Қазақстан, Ресей және Еуропалық одақтың тәсілдеріне, сондай-ақ қылмыстық қызметте жасанды интеллекті пайдалануға байланысты сот шешімдеріне салыстырмалы талдау жүргізілді. Зерттеудің мақсаты жасанды интеллект технологияларын қолдана отырып жасалған қылмыстарды саралау мәселелерін жан-жақты талдау және оларды бағалаудың қылмыстық-құқықтық тетіктерін жетілдіру бойынша ұсыныстар әзірлеу. Әзірлеушілер, пайдаланушылар және автономды жүйелер арасында жауапкершілікті бөлу, сондай-ақ кінәнің мәні мен формасын анықтаудағы қиындықтар қарастырылды. Зерттеудің әдіснамалық негізіне салыстырмалы-құқықтық, жүйелік және аналитикалық әдістер, сондай-ақ сот практикасы мен шетелдік нормативтік актілерді талдау кіреді. Алгоритмдік шешім қабылдау ерекшелігін ескеретін нормаларды енгізу қажеттілігі негізделіп, жасанды интеллектпен байланысты қылмыстарды қылмыстық-құқықтық реттеуді жетілдіру бойынша шаралар ұсынылды, бұл неғұрлым әділ және тиімді құқық қолдануды қамтамасыз етуге мүмкіндік береді.

Кілт сөздер: жасанды интеллект, қылмыстың біліктілігі, қылмыс субъектісі, цифрландыру, автономды жүйелер, сот практикасы, киберқылмыс.

E.A. Nikolaeva, A.T. Kabzhanov

Problems of qualification of crimes committed using artificial intelligence

The article examines the challenges of qualifying crimes committed with artificial intelligence (AI) technologies under the criminal law of the Republic of Kazakhstan. It analyzes the mental element of such crimes, issues of guilt, and causation in the context of AI autonomy. Special attention is paid to gaps in criminal legislation and the difficulties of applying existing norms in the investigation and classification of digital crimes. A comparative analysis of the approaches in Kazakhstan, Russia, and the European Union, as well as relevant court decisions involving AI in criminal activities, is presented. The study aims to provide a comprehensive analysis of the challenges in qualifying AI-related crimes and to propose improvements to criminal law mechanisms for their assessment. It considers the allocation of liability among developers, users, and autonomous systems, as well as the complexity of determining the subject and form of guilt. The research employs comparative, systematic, and analytical methods, along with an examination of judicial practice and foreign regulations. The article argues for the necessity of introducing legal norms that account for algorithmic decision-making and proposes measures to enhance criminal law regulation of AI-related crimes, thereby promoting more effective and fair law enforcement.

Keywords: artificial intelligence, crime qualification, the subject of crime, digitalization, autonomous systems, judicial practice, cybercrime.

References

1 Sariati, N.M., Caronina, D.K., Damanik, J., & Sianipar, S. (2023). Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System. *Jurnal Ilmu Hukum Kyadiren,* 9, 1–25.

2 Bashir Mangi, D., Butro, I., & Akhtar Memon, T. (2025). AI and Criminal Liability: Theoretical Dilemmas in Applying Criminal Law to Artificial Intelligence. *The Critical Review of Social Sciences Studies*, *3*(2), 2174–2186.

3 Diab, M.F.S. (2024). Criminal Liability for Artificial Intelligence and Autonomous Systems. *American Journal of Society and Law*, *3*(1), 14–18.

4 Sachoulidou, A. (2023). AI Systems and Criminal Liability. *Oslo Law Review*, *1*(1), 7–15.

5 Ibatullina, D.M. (2023). Iskusstvennyi intellekt v ugolovno pravovoi doktrine [Artificial Intelligence in the Criminal Law Doctrine]. *Vestnik Kazanskogo yuridicheskogo instituta Ministerstva Vnutrennykh Del Rossii — Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia, 14*(2), 65–69 [in Russian].

6 Mukhambetzhanova A.T. (2025). Iskusstvennyi intellekt v pravovoi sisteme Kazakhstana: problemy i perspektivy razvitiia [Artificial Intelligence in the Legal System of Kazakhstan: Problems and Prospects of Development]. *Nauchnye issledovaniia i eksperimentalnye razrabotki — Scientific Research and Experimental Development,* 9, 255–259 [in Russian].

7 Smith, J. (2022). *Deepfake and Financial Fraud: A Case Study of the UK.* London: TechLaw Press.

8 (2024). *Ministerstvo vnutrennikh del Respubliki Kazakhstan. Otchet o sostoianii prestupnosti v Respublike Kazakhstan za 2024 god* [Ministry of Internal Affairs of the Republic of Kazakhstan. Report on the State of Crime in the Republic of Kazakhstan for 2024]. Astana [in Russian].

9 Tanaka, H., & Müller, F. (2023). Legal Regulation of AI and Autonomous Systems in the EU, Singapore and Japan. *International Journal of Law and Technology*, *15*(1), 10–25.

10 (2025). Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus. *TheCRSSS.com.* Retrieved from https://thecrsss.com (accessed 03 Nov 2025).

11 Criminal Liability of Artificial Intelligence (AI): The Legal Conceptual Study and the Regulating Challenges in Global Disruptive Technology Era. *Russian Law Journal.org.* Retrieved from https://russianlawjournal.org (accessed 03 Nov 2025).

12 AI Systems and Criminal Liability. *NovaResearch.unl.pt.* Retrieved from https://novaresearch.unl.pt (accessed 03 Nov 2025).

13 AI and Criminal Liability: Theoretical Dilemmas in Applying Criminal Law to Artificial Intelligence. *TheCRSSS.com.* Retrieved from https://thecrsss.com (accessed 03 Nov 2025).

14 Naumov, A.V. (2022). *Ugolovnoe pravo. Obshchaia chast* [Criminal Law. General Part]. Moscow: Norma [in Russian].

15 Kyzdarbekova, B.J. (2025). Iskusstvennyi intellekt v ugolovnom prave: Teoretiko-pravovye podkhody k opredeleniiu poniatiia i regulirovaniiu [Artificial intelligence in criminal law: Theoretical and legal approaches to the definition of the concept and regulation]. *Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Perspektivy razvitiia pravovoi sistemy Respubliki Kazakhstan» posviashchennoi 30-letiiu Konstitutsii Respubliki Kazakhstan — Materials of the International Scientific and Practical Conference "Prospects for the development of the legal system of the Republic of Kazakhstan" dedicated to the 30th anniversary of the Constitution of the Republic of Kazakhstan* (pp. 191–198). Karaganda: Bolashaq-Baspa [in Russian].

16 (2024). Sudebnoe reshenie Almatinskogo gorodskogo suda ot 17 aprelia 2024 g. po delu № 2-1456/2024 // Sudebnyi kabinet. [Almaty City Court. Judgment of April 17, 2024 in Case No. 2-1456/2024. The Judicial Office]. *office.sud.kz.* Retrieved from https://office.sud.kz (accessed 01 Nov 2025) [in Russian].

17 (2023). Prigovor Nikulinskogo raionnogo suda g. Moskvy ot 20 iiunia 2023 g. po delu № 1-124/2023 // SudAkt [Nikulinsky District Court of Moscow. Verdict of June 20, 2023 in Case No. 1-124/2023. SudAkt]. *sudact.ru.* Retrieved from https://sudact.ru (accessed 01 Nov 2025) [in Russian].

18 Floridi, L., & Cowls, J. (2021). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review, 3*(2), 1–15.

19 Kremnitzer, M., & Segev, N. (2020). Artificial Intelligence and Criminal Liability. *Israel Law Review, 53*(2), 149–176.

20 Floridi, L., & Chiriatti, M. (2020). GPT and the Legal Status of AI Agents. *Philosophy & Technology, 33*(4), 645–651.

Информация об авторах

Николаева Екатерина Александровна — кандидат юридических наук, доцент кафедры гражданско-правовых и уголовно-правовых дисциплин, Хакасский государственный университет им. Н.Ф. Катанова, Абакан, Россия; e-mail: katrimm@yandex.ru

Кабжанов Акылбек Тайбулатович — кандидат юридических наук, заведующий кафедрой правовых и финансовых дисциплин, Академия «Bolashaq», Караганда, Казахстан; e-mail: tengrianec_9192@mail.ru

Information about the authors

Nikolaeva Ekaterina Alexandrovna — Academic degree Candidate of Law, Position Associate Professor of the Department of Civil Law and Criminal Law Disciplines, N.F. Katanov Khakass State University, Abakan; Russia; e-mail katrimm@yandex.ru

Kabzhanov Akylbek Taybulatovich — Candidate of Law, Head of the Department of Legal and Financial Disciplines, Bolashaq Academy, Karaganda, Kazakhstan; e-mail: tengrianec_9192@mail.ru