ИСПОЛЬЗОВАНИЕ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ВОЗМОЖНОСТИ И РИСКИ

Норов Мирфайз Абдулазизович
магистрант Ташкентского государственного юридического университета.

https://doi.org/10.5281/zenodo.20672285

Аннотация. *В статье рассматриваются теоретико-правовые и практические аспекты применения технологий искусственного интеллекта при расследовании киберпреступлений. На основе анализа национального законодательства Республики Узбекистан, а также опыта Европейского союза, Соединённых Штатов Америки, Китайской Народной Республики и Японии раскрываются основные возможности использования алгоритмов машинного обучения, технологий Big Data и систем цифровой криминалистики в выявлении и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий. Особое внимание уделено правовым, процессуальным, этическим и социальным рискам, возникающим при включении интеллектуальных систем в уголовно-процессуальную деятельность, включая проблему допустимости цифровых доказательств, непрозрачности алгоритмических решений («чёрный ящик»), распределения юридической ответственности за алгоритмические ошибки и защиты персональных данных. По результатам исследования сформулированы предложения по совершенствованию уголовно-процессуального законодательства Республики Узбекистан, направленные на формирование сбалансированной модели применения искусственного интеллекта, обеспечивающей повышение эффективности расследования киберпреступлений при сохранении гарантий прав человека.*

Ключевые слова: *искусственный интеллект, киберпреступность, цифровые доказательства, цифровая криминалистика, Big Data, машинное обучение, уголовный процесс, алгоритмическая прозрачность, защита персональных данных, правоохранительная деятельность.*

Annotation. *This article examines the theoretical, legal and practical aspects of applying artificial intelligence technologies in the investigation of cybercrimes. Drawing on the legislation of the Republic of Uzbekistan, as well as on the experience of the European Union, the United States, the People's Republic of China and Japan, the paper analyses the principal opportunities for using machine learning algorithms, Big Data technologies and digital forensic systems in detecting and investigating crimes committed through information and communication technologies. Particular attention is paid to the legal, procedural, ethical and social risks arising from the integration of intelligent systems into criminal procedure, including the admissibility of digital evidence, the opacity of algorithmic decisions (the 'black box' problem), the allocation of legal liability for algorithmic errors, and personal data protection.*

Based on the findings, proposals are formulated for improving the criminal procedure legislation of the Republic of Uzbekistan aimed at creating a balanced model for the use of artificial intelligence that increases the effectiveness of cybercrime investigation while preserving guarantees of human rights.

Keywords: *artificial intelligence, cybercrime, digital evidence, digital forensics, Big Data, machine learning, criminal procedure, algorithmic transparency, personal data protection, law enforcement.*

Аннотация. *Мазкур мақолада кибержиноятларни тергов қилишда сунъий интеллект технологияларини қўллашнинг назарий-ҳуқуқий ва амалий жиҳатлари кўриб чиқилган. Ўзбекистон Республикаси миллий қонунчилиги, шунингдек Европа Иттифоқи, Америка Қўшма Штатлари, Хитой Халқ Республикаси ва Япония тажрибаси таҳлили асосида машинавий ўқитиш алгоритмлари, Big Data технологиялари ҳамда рақамли криминалистика тизимларидан ахборот-коммуникация технологиялари ёрдамида содир этиладиган жиноятларни аниқлаш ва тергов қилишда фойдаланишнинг асосий имкониятлари ёритиб берилган. Мақолада интеллектуал тизимларни жиноят-процессуал фаолиятга жорий этиш жараёнида юзага келадиган ҳуқуқий, процессуал, ахлоқий ва ижтимоий хавф-хатарларга алоҳида эътибор қаратилган. Жумладан, рақамли далилларнинг мақбуллиги, алгоритмик қарорларнинг шаффоф эмаслиги («қора қути» муаммоси), алгоритм хатолари учун юридик жавобгарликни тақсимлаш ҳамда шахсий маълумотларни ҳимоя қилиш масалалари таҳлил қилинган. Тадқиқот натижаларига кўра, инсон ҳуқуқлари кафолатларини сақлаган ҳолда кибержиноятларни тергов қилиш самарадорлигини оширишга хизмат қилувчи сунъий интеллектдан фойдаланишнинг мувозанатлашган моделини шакллантириш мақсадида Ўзбекистон Республикаси жиноят-процессуал қонунчилигини такомиллаштириш бўйича таклифлар ишлаб чиқилган.*

Калит сўзлар: *сунъий интеллект, кибержиноятчилик, рақамли далиллар, рақамли криминалистика, Big Data, машинавий ўқитиш, жиноят процесси, алгоритмик шаффофлик, шахсий маълумотларни ҳимоя қилиш, ҳуқуқни муҳофаза қилувчи органлар фаолияти.*

ВВЕДЕНИЕ

Глобальная цифровая трансформация общественных отношений сопровождается не только расширением возможностей экономического и социального развития, но и качественным изменением структуры преступности. На смену традиционным формам противоправного поведения приходят деяния, совершаемые в цифровой среде либо с использованием информационно-коммуникационных технологий, которые принято объединять понятием «киберпреступления». Их отличительными чертами выступают высокая латентность, трансграничный характер, техническая сложность и использование технологий анонимизации, что существенно затрудняет применение традиционных криминалистических методов.

Масштаб данной проблемы для Республики Узбекистан подтверждается официальной статистикой Министерства внутренних дел. Если в 2023 году доля киберпреступлений в общей структуре преступности составляла 6,2 процента, то уже в 2024 году этот показатель достиг 44,4 процента, то есть практически каждое второе преступление в стране совершается с использованием информационных технологий. За период 2021–2024 годов в результате киберпреступлений у граждан было похищено свыше 1,9 триллиона сумов, при этом только за 2024 год ущерб составил 603 миллиарда сумов. Подавляющее большинство таких посягательств (порядка 98 процентов) связано с банковскими картами, а около трети случаев сопровождается использованием технологий генерации поддельного видео- и аудиоконтента (deepfake).[1]

[1] Газета.uz. Киберпреступность в Узбекистане: статистика МВД за 2024 год [Электронный ресурс]. URL: https://www.gazeta.uz/ru/2025/11/06/cybersecurity/ (дата обращения: 12.06.2026).

В этих условиях внедрение технологий искусственного интеллекта в деятельность правоохранительных органов перестаёт быть вопросом отдалённой перспективы и приобретает характер насущной практической задачи. Искусственный интеллект, представляющий собой совокупность программно-аппаратных решений, способных выполнять задачи, традиционно требующие интеллектуальной деятельности человека - анализ данных, выявление закономерностей, прогнозирование и принятие решений, - рассматривается современной юридической наукой как один из наиболее перспективных инструментов цифровой криминалистики.[2]

Вместе с тем интеграция алгоритмических систем в уголовно-процессуальную деятельность порождает комплекс правовых, этических и организационных проблем, связанных с допустимостью результатов алгоритмического анализа в качестве доказательств, прозрачностью используемых моделей, распределением юридической ответственности за ошибки автоматизированных систем, а также защитой конституционных прав участников процесса. Действующее законодательство Республики Узбекистан, при наличии отдельных нормативных актов в сфере кибербезопасности и защиты персональных данных, не содержит комплексного регулирования применения искусственного интеллекта в уголовном судопроизводстве, что обусловливает актуальность настоящего исследования.

Целью настоящей статьи является комплексный анализ возможностей и рисков использования искусственного интеллекта при расследовании киберпреступлений с учётом национального законодательства Республики Узбекистан и международного опыта, а также формулирование научно обоснованных предложений по совершенствованию уголовно-процессуального регулирования в данной сфере.

1. Понятие и правовые признаки киберпреступлений как объекта применения искусственного интеллекта

Несмотря на широкое распространение термина «киберпреступление» в научной литературе и правоприменительной практике, легальное определение данного понятия в законодательстве Республики Узбекистан отсутствует, что предполагает обращение к международно-правовым источникам и доктринальным подходам. Ключевым международным актом в данной сфере остаётся Конвенция Совета Европы о киберпреступности 2001 года (Будапештская конвенция), в которой киберпреступления рассматриваются через систему уголовно наказуемых деяний, посягающих на конфиденциальность, целостность и доступность компьютерных данных и систем, а также совершаемых с использованием информационных технологий как средства совершения преступления.[3]

В доктринальном плане киберпреступность характеризуется двойственной природой: информационно-коммуникационные технологии могут выступать одновременно и средством совершения деяния, и непосредственным объектом преступного посягательства. [4] Применительно к национальному правопорядку киберпреступления следует рассматривать как разновидность преступлений в сфере информационных технологий, ответственность за которые предусмотрена Уголовным кодексом Республики Узбекистан, включающим нормы о несанкционированном доступе к

[2] Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - Pearson, 2021.
[3] Convention on Cybercrime (Budapest Convention). - Council of Europe, 2001.
[4] Wall D. Cybercrime: The Transformation of Crime in the Information Age. - Cambridge University Press, 2007.

компьютерной информации, создании и распространении вредоносных программ, а также мошенничестве с использованием цифровых технологий.[5]

Анализ доктринальных подходов и положений действующего законодательства позволяет выделить совокупность признаков, отличающих киберпреступления от традиционных категорий противоправных деяний. Во-первых, это совершение деяния в цифровой среде либо с использованием информационных систем и сетей. Во-вторых, высокий уровень латентности, обусловленный объективной сложностью обнаружения и документирования цифровых следов. По данным исследований Управления ООН по наркотикам и преступности, значительная часть киберпреступлений остаётся невыявленной вследствие технической сложности их фиксации и недостаточной осведомлённости потерпевших. [6] В-третьих, трансграничный характер, при котором деяние, совершённое с территории одного государства, причиняет вред объектам, находящимся в другой юрисдикции, что прямо предполагает развитие механизмов международного сотрудничества, закреплённых, в частности, в Будапештской конвенции.[7] В-четвёртых, высокая техническая сложность, требующая привлечения специалистов в области информационных технологий. В-пятых, выраженная анонимность субъектов, достигаемая посредством использования VPN-сервисов, сетей TOR и криптографических инструментов, что в научной литературе рассматривается как один из ключевых факторов роста киберпреступности.[8]

Перечисленные признаки имеют принципиальное значение для понимания роли искусственного интеллекта в расследовании киберпреступлений. Латентность и техническая сложность обусловливают необходимость автоматизированного анализа значительных объёмов цифровой информации, трансграничность - развитие систем анализа, способных работать с данными из различных юрисдикций, а анонимность субъектов - применение алгоритмов выявления аномалий и реконструкции цифровых следов. Иными словами, специфика киберпреступности как объекта расследования формирует объективный запрос на внедрение интеллектуальных аналитических систем, без которых традиционные методы криминалистики оказываются недостаточно эффективными.

Особое значение для квалификации деяний и определения предмета доказывания приобретает классификация киберпреступлений. В международной практике, в том числе в рамках Будапештской конвенции, выделяются группы преступлений против конфиденциальности, целостности и доступности компьютерных данных, компьютерные преступления, преступления, связанные с содержанием информации, а также нарушения авторских и смежных прав.[9] В доктрине дополнительно применяется классификация по объекту посягательства (информационные системы, персональные данные, имущественные интересы, общественная безопасность), по способу совершения (хакерские атаки, методы социальной инженерии, распространение вредоносного программного обеспечения, использование автоматизированных алгоритмов) и по степени общественной опасности, что находит косвенное отражение в дифференциации уголовной

[5] Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года (с изменениями и дополнениями) // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
[6] UNODC. Comprehensive Study on Cybercrime. - Vienna: United Nations, 2013.
[7] Convention on Cybercrime (Budapest Convention). - Council of Europe, 2001.
[8] Brenner S. Cybercrime and the Law: Challenges, Issues, and Outcomes. - Northeastern University Press, 2010.
[9] Convention on Cybercrime (Budapest Convention). - Council of Europe, 2001.

ответственности по законодательству Республики Узбекистан.[10] Так, статистика МВД Республики Узбекистан показывает, что преобладающая часть киберпреступлений совершается путём распространения вредоносных ссылок и программ (около 60 процентов случаев), путём получения SMS-кодов доступа посредством обмана (порядка 16 процентов), а также через мошенничество на электронных торговых площадках и фиктивные инвестиционные платформы.[11] Каждая из перечисленных групп предполагает свой набор цифровых следов - сетевые журналы, метаданные сообщений, записи телефонных вызовов, истории транзакций, - анализ которых при значительных объёмах данных объективно требует применения интеллектуальных алгоритмов.

2. Искусственный интеллект как объект правового регулирования и инструмент правоприменительной деятельности

Понятие искусственного интеллекта не имеет единого общепринятого определения ни в доктрине, ни в международно-правовых актах, что объясняется междисциплинарным характером данного феномена. В наиболее общем виде под искусственным интеллектом понимается совокупность программно-аппаратных средств, способных выполнять задачи, требующие интеллектуальной деятельности человека, включая анализ данных, обучение на основе опыта, принятие решений и прогнозирование.[12] Функциональный подход к определению искусственного интеллекта закреплён в документах Организации экономического сотрудничества и развития (ОЭСР), согласно которым система искусственного интеллекта - это система, способная для заданного набора целей формировать прогнозы, рекомендации или решения, влияющие на реальные или виртуальные среды.[13]

С технологической точки зрения системы искусственного интеллекта, применяемые в правоохранительной сфере, базируются на трёх взаимосвязанных компонентах. Машинное обучение позволяет алгоритмам самостоятельно выявлять закономерности в данных без явного программирования каждого правила, что особенно значимо при анализе неструктурированных массивов информации, характерных для киберпространства. Нейронные сети, моделирующие принципы функционирования человеческого мозга, применяются для распознавания образов, анализа текстовых данных и выявления аномалий, в том числе при обнаружении фишинговых атак и вредоносного программного обеспечения. Технологии обработки больших данных (Big Data) обеспечивают анализ значительных объёмов информации в режиме, близком к реальному времени, что позволяет оперативно выявлять признаки преступной деятельности.[14]

Правовая природа искусственного интеллекта остаётся предметом продолжающейся научной дискуссии. С одной стороны, искусственный интеллект может рассматриваться как объект гражданско-правовых отношений - программный продукт или комплекс технологий. С другой стороны, он выступает инструментом, используемым субъектами права для достижения определённых целей. Отдельные научные подходы допускают постановку вопроса о признании искусственного интеллекта особым

[10] Уголовный кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
[11] . Газета.uz. Киберпреступность в Узбекистане: статистика МВД за 2024 год [Электронный ресурс]. URL: https://www.gazeta.uz/ru/2025/11/06/cybersecurity/ (дата обращения: 12.06.2026).
[12] Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - Pearson, 2021.
[13] OECD. OECD Principles on Artificial Intelligence. - Paris: OECD Publishing, 2019.
[14] Kitchin R. Big Data, new epistemologies and paradigm shifts // Big Data & Society. - 2014. - Vol. 1, No. 1.

субъектом права, однако подобная концепция на современном этапе не получила нормативного закрепления и вызывает обоснованные сомнения, связанные с отсутствием у алгоритмических систем самостоятельной воли и способности нести юридическую ответственность.[15] Соответственно, в большинстве правовых систем, включая правовую систему Республики Узбекистан, искусственный интеллект рассматривается как объект регулирования, тогда как ответственность за его применение возлагается на разработчиков, операторов и пользователей.

Правовое регулирование искусственного интеллекта в Республике Узбекистан находится на стадии активного формирования. Косвенное регулирование вопросов, связанных с применением алгоритмических систем, осуществляется через законодательство о персональных данных и кибербезопасности. Так, Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 устанавливает требования к обработке информации, включая автоматизированную обработку, что имеет непосредственное значение для функционирования систем искусственного интеллекта.[16] Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 формирует правовую основу защиты информационных систем, в рамках которых могут использоваться интеллектуальные технологии, закрепляя такие категории, как киберпространство, киберинцидент и киберугроза, а также определяя полномочия государственных органов в данной сфере.[17] Постановлением Президента Республики Узбекистан от 30 апреля 2025 года № ПП-153 предусмотрено совершенствование деятельности правоохранительных органов и определение Министерства внутренних дел в качестве уполномоченного органа в сфере противодействия киберпреступности.[18]

Существенным шагом в направлении формирования национальной политики в области искусственного интеллекта стало принятие Постановления Президента Республики Узбекистан от 14 октября 2024 года № ПП-358 «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года», в числе задач которой указаны обеспечение безопасности персональных данных при внедрении и использовании искусственного интеллекта, а также разработка соответствующего нормативно-правового документа на основе передового международного опыта.[19] Дальнейшим развитием данной политики стало принятие Закона Республики Узбекистан от 21 января 2026 года № ЗРУ-1115 «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта».[20] Указанные нормативные акты свидетельствуют о признании государством необходимости системного регулирования искусственного интеллекта, однако специальных норм, регламентирующих применение алгоритмических систем непосредственно в уголовно-процессуальной деятельности,

[15] Bryson J. Artificial Intelligence and Legal Personhood // AI & Society. - 2010. - Vol. 25.
[16] Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
[17] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
[18] Постановление Президента Республики Узбекистан «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий» от 30.04.2025 г. № ПП-153.
[19] Постановление Президента Республики Узбекистан «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» от 14.10.2024 г. № ПП-358.
[20] Постановление Президента Республики Узбекистан «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» от 14.10.2024 г. № ПП-358.

действующее законодательство пока не содержит, что и предопределяет необходимость дальнейшего научного анализа в данной области.

На международном уровне регулирование искусственного интеллекта осуществляется преимущественно в форме рамочных принципов и рекомендаций «мягкого права». Принципы ОЭСР закрепляют требования прозрачности, безопасности и подотчётности алгоритмических систем. [21] Рекомендация ЮНЕСКО по этике искусственного интеллекта 2021 года подчёркивает необходимость соблюдения прав человека, недопущения дискриминации и обеспечения человеческого надзора за автоматизированными системами на всех этапах их жизненного цикла. [22] Европейский союз, в свою очередь, формирует более жёсткую модель регулирования в рамках Акта об искусственном интеллекте (AI Act), предусматривающего дифференциацию требований к системам искусственного интеллекта в зависимости от уровня создаваемого ими риска.[23]

Сопоставление данных моделей - рекомендательной (ОЭСР, ЮНЕСКО), рамочно-стандартизирующей (США) и риск-ориентированной нормативной (ЕС) - представляет значительный интерес для формирования национальной модели регулирования, что подробнее будет рассмотрено в четвёртом разделе настоящей статьи.

3. Возможности применения искусственного интеллекта в выявлении и расследовании киберпреступлений

3.1. Технологии Big Data и выявление цифровых следов

Технологии анализа больших данных (Big Data) представляют собой совокупность методов и инструментов, предназначенных для обработки массивов информации, характеризующихся значительным объёмом, высокой скоростью поступления и разнообразием форматов. Применительно к расследованию киберпреступлений это означает возможность одновременного анализа огромного количества цифровых следов - сетевого трафика, данных пользователей, финансовых транзакций, электронной переписки, журналов активности и иных источников информации. [24] Принципиальное значение имеет способность таких технологий выявлять скрытые закономерности и взаимосвязи между событиями, которые объективно недостижимы при использовании традиционных методов анализа, что особенно актуально при расследовании организованных и много эпизодных киберпреступлений, например, при установлении связей между различными IP-адресами, определении центров координации атак и выявлении временных закономерностей противоправной активности.

Не менее значимым направлением является использование алгоритмов машинного обучения для выявления аномалий и подозрительных паттернов поведения. Подобные алгоритмы анализируют типичные модели поведения пользователей и фиксируют отклонения, которые могут свидетельствовать о противоправной деятельности - нетипичные суммы переводов, изменения геолокации, аномальную частоту операций. В научной литературе подчёркивается, что методы выявления аномалий существенно повышают эффективность обнаружения мошеннических действий и иных видов

[21] OECD. OECD Principles on Artificial Intelligence. - Paris: OECD Publishing, 2019.
[22] UNESCO. Recommendation on the Ethics of Artificial Intelligence. - Paris: UNESCO, 2021.
[23] European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).
[24] Mayer-Schonberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. - Boston: Houghton Mifflin Harcourt, 2013.

киберпреступлений,[25] в том числе позволяют выявлять распределённые атаки типа DDoS посредством анализа резких изменений сетевого трафика, а также обнаруживать вредоносное программное обеспечение на основе анализа поведения программ.

3.2. Международная практика применения искусственного интеллекта: анализ прецедентных кейсов

Практическая значимость рассматриваемых технологий подтверждается рядом резонансных международных расследований, анализ которых имеет существенное значение для формирования национальной методики расследования киберпреступлений.

Так, в 2021 году в результате совместной операции Европола и правоохранительных органов Германии, Нидерландов, США и ряда других государств была ликвидирована одна из крупнейших киберпреступных инфраструктур - ботнет Emotet, использовавшийся для распространения вредоносного программного обеспечения и проведения масштабных фишинговых кампаний. В ходе расследования были применены технологии анализа больших данных и алгоритмы машинного обучения, позволившие обработать информацию о миллионах заражённых устройств, реконструировать структуру сети и установить управляющие серверы.[26]

Сопоставимый по значению пример - расследование атаки на нефтепровод Colonial Pipeline в США в 2021 году, в ходе которого правоохранительные органы применили алгоритмы анализа блокчейн-транзакций для отслеживания движения криптовалютных средств, выплаченных в качестве выкупа. Использование интеллектуальных аналитических систем позволило не только идентифицировать участников преступной группы, но и вернуть значительную часть похищенных средств.[27] Аналогичные методы блокчейн-аналитики были применены при расследовании инцидента Bitfinex (2022), где удалось отследить движение криптовалютных активов на сумму более трёх миллиардов долларов США, что ранее считалось практически невозможным.

Показательным примером эффективности алгоритмического анализа цифровых следов в условиях высокой анонимности субъекта является дело Silk Road, в рамках которого комплексный анализ транзакций и сетевой активности позволил установить личность организатора крупной нелегальной онлайн-платформы, несмотря на использование им технологий анонимизации.[28] При расследовании утечки данных компании Equifax (2017) применение аналитических инструментов позволило установить механизм проникновения злоумышленников и выявить уязвимости информационной системы, тогда как в случае глобальной атаки вредоносного кода WannaCry (2017) автоматизированные системы анализа использовались для отслеживания распространения вредоносного программного обеспечения и выявления его источников.

Анализ перечисленных кейсов позволяет выделить общую закономерность: эффективность применения искусственного интеллекта напрямую зависит от качества организации работы с цифровыми доказательствами - их своевременной фиксации, обеспечения целостности и применения стандартизированных методик анализа.

[25] Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. - 2009. - Vol. 41, No. 3.
[26] Europol. Disruption of Emotet Botnet: Press Release. - The Hague: Europol, 2021.
[27] U.S. Department of Justice. Colonial Pipeline Ransomware Investigation: Press Release. - Washington, D.C.: DOJ, 2021.
[28] United States v. Ulbricht (Silk Road case), 31 F. Supp. 3d 540 (S.D.N.Y. 2014), aff'd 2 Cir. 2017.

В отсутствие данных условий даже самые совершенные алгоритмы не способны обеспечить юридически значимый результат.

3.3. Цифровая криминалистика и интеграция искусственного интеллекта в процессуальную деятельность

Эффективное расследование киберпреступлений объективно невозможно без надлежащего уровня компетентности субъектов расследования в области цифровой криминалистики. Следователь, дознаватель, прокурор и судья, рассматривающие дела данной категории, должны обладать базовыми знаниями об устройстве и функционировании электронных носителей информации - оперативных запоминающих устройств, жёстких дисков, флеш-накопителей, карт памяти, мобильных устройств и облачных хранилищ, поскольку именно на них могут содержаться цифровые следы преступной деятельности. Незнание технических особенностей подобных устройств способно повлечь утрату, повреждение либо ненадлежащую фиксацию цифровой информации, что в дальнейшем может стать основанием для признания соответствующих доказательств недопустимыми.[29]

Международные стандарты, разработанные Национальным институтом стандартов и технологий США (NIST), подчёркивают необходимость обеспечения целостности, достоверности и воспроизводимости цифровых доказательств посредством строгого соблюдения процедур их идентификации, сохранения, анализа и документирования.[30] Искусственный интеллект интегрируется в данные процессы преимущественно на этапе анализа, обеспечивая автоматизированную сортировку информации, выявление релевантных данных и формирование аналитических выводов, что подтверждается, в частности, материалами консалтинговой компании Deloitte, согласно которым внедрение интеллектуальных технологий в цифровую криминалистику позволяет существенно сократить время обработки доказательств и повысить качество расследования за счёт автоматизации первичного анализа.[31]

Существенное значение для практики расследования киберпреступлений имеют специализированные программно-аппаратные комплексы цифровой криминалистики - Magnet AXIOM, EnCase, Belkasoft Evidence Center, AccessData и аналогичные системы, предназначенные для поиска, восстановления и анализа цифровых данных. В сочетании с алгоритмами искусственного интеллекта подобные комплексы позволяют автоматизировать выявление скрытых взаимосвязей между цифровыми объектами и существенно повышают эффективность расследования.[32] Принципиальное значение при этом сохраняет обеспечение целостности цифровых доказательств посредством применения хеш-функций (MD5, SHA-256): изменение хеш-значения свидетельствует о

[29] Астанов И., Хамидов Б. Электрон ёхуд ракамли далилларга оид умумназарий масалалар: муаммо ва ечим // Жамият ва инновациялар - Общество и инновации - Society and Innovations. - 2021. - Special Issue 7. - С. 259-273.

[30] NIST. OSAC Standards Library [Электронный ресурс]. URL: https://www.nist.gov/osac/standards-library (дата обращения: 12.06.2026).

[31] Deloitte. Forensic Investigators Gain an Edge with AI [Электронный ресурс]. URL: https://www.deloitte.com/ch/en/services/consulting-financial/perspectives/forensic-investigators-gain-an-edge-with-ai (дата обращения: 12.06.2026).

[32] Астанов И., Хамидов Б. Электрон ёхуд ракамли далилларга оид умумназарий масалалар: муаммо ва ечим // Жамият ва инновациялар - Общество и инновации - Society and Innovations. - 2021. - Special Issue 7. - С. 259-273.

нарушении целостности информации и может повлечь утрату процессуальной допустимости соответствующего доказательства.

С процессуальной точки зрения расследование киберпреступлений в большинстве правовых систем строится на единой модели, включающей последовательные этапы выявления, сохранения, анализа и документирования цифровых доказательств.

Несоблюдение хотя бы одного из указанных этапов способно повлечь признание доказательств недопустимыми, что подтверждается судебной практикой ряда государств.[33] Искусственный интеллект, таким образом, должен рассматриваться не как самостоятельный источник доказательственной информации, а как элемент единого процессуального механизма работы с цифровыми доказательствами, эффективность которого определяется качеством каждого из перечисленных этапов.

4. Сравнительно-правовой анализ зарубежного опыта регулирования применения искусственного интеллекта в правоохранительной деятельности

Изучение зарубежного опыта правового регулирования применения искусственного интеллекта в уголовном процессе представляет существенный интерес для формирования национальной модели регулирования в Республике Узбекистан. Наиболее показательными в этом отношении являются подходы, сформированные в Соединённых Штатах Америки, Европейском союзе, Китайской Народной Республике и Японии, каждый из которых отражает различные модели баланса между эффективностью применения технологий и обеспечением правовых гарантий.

Подход Соединённых Штатов Америки характеризуется опорой на рамочные стандарты и методические документы, а не на прямое законодательное регулирование. Центральное значение имеет Структура управления рисками искусственного интеллекта (AI Risk Management Framework, AI RMF 1.0), разработанная Национальным институтом стандартов и технологий (NIST) в 2023 году. Указанный документ рассматривает управление рисками искусственного интеллекта как процесс, направленный на снижение вреда для отдельных лиц, организаций и общества, и связывает применение алгоритмических систем с полным жизненным циклом - проектированием, обучением, внедрением, использованием, мониторингом и обновлением.[34] Для целей уголовного процесса подобный подход предполагает необходимость документирования не только итогового результата работы алгоритма, но и условий его получения: источников данных, версии программного обеспечения, параметров модели, действий оператора, даты анализа и сведений о возможной погрешности.

Существенное значение для понимания американского подхода имеют также решения Верховного суда США по делам Riley v. California и Carpenter v. United States, в которых было подчёркнуто, что цифровая информация, содержащаяся на электронных устройствах и в данных операторов связи, требует усиленной конституционной защиты как элемент права на неприкосновенность частной жизни.[35] В научной литературе (О. Керр, Р. Векслер) данная позиция получила развитие в виде требований о применении механизмов избирательного извлечения и предварительного скрининга данных,

[33] NIST. OSAC Standards Library [Электронный ресурс]. URL: https://www.nist.gov/osac/standards-library (дата обращения: 12.06.2026).
[34]NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). - Gaithersburg: National Institute of Standards and Technology, 2023.
[35] Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. ___ (2018).

позволяющих минимизировать вмешательство в права лиц, не связанных с расследуемым деянием.[36]

Европейский союз формирует принципиально иную, нормативно-ориентированную модель регулирования, основанную на дифференциации систем искусственного интеллекта по уровню создаваемого ими риска. Согласно Акту об искусственном интеллекте (AI Act), системы, применяемые в правоохранительной деятельности, в том числе для оценки надёжности доказательств, профилирования лиц в ходе расследования и оценки риска совершения преступлений, относятся к категории высокорисковых и подлежат повышенным требованиям в части контроля качества данных, документирования, прозрачности и обязательного человеческого надзора.[37] Европейская комиссия рассматривает данный акт как первый комплексный правовой механизм регулирования искусственного интеллекта, направленный на обеспечение безопасности, защиту фундаментальных прав и формирование человекоцентричной модели применения технологий.[38]

Подход Китайской Народной Республики представляет интерес как пример интеграции искусственного интеллекта непосредственно в процессуальное законодательство. В соответствии со статьёй 50 Уголовно-процессуального закона КНР (в редакции 2018 года) электронные данные официально признаются самостоятельным видом доказательств в уголовном процессе, а статья 54 закрепляет полномочия суда, прокуратуры и органов общественной безопасности по их сбору и исследованию.[39]

Детальное регулирование содержится в специальном документе - Положениях по отдельным вопросам сбора, извлечения, проверки и оценки электронных данных по уголовным делам (2016 год). В частности, статья 14 указанных Положений предусматривает обязательную фиксацию процесса извлечения электронных данных с указанием времени, места и способа получения информации, составлением соответствующего протокола, указанием хеш-значений и подписями следователя и владельца данных.[40] Статья 16 закрепляет методы исследования цифровых доказательств, включая восстановление удалённых данных, дешифрование и корреляционный анализ,[41] статья 22 устанавливает критерии проверки подлинности электронных доказательств, а статья 24 определяет требования законности их получения, включая обязательное участие не менее двух следователей и соблюдение технических стандартов цифровой криминалистики. [42] Указанный подход демонстрирует возможность детальной процессуальной регламентации работы с цифровыми доказательствами на уровне специального нормативного акта, что представляет практический интерес для совершенствования уголовно-процессуального законодательства Республики Узбекистан.

---

[36] Wexler R. Privacy as Privilege: The Stored Communications Act and Internet Evidence // Stanford Law Review. - 2020. - Vol. 72.

[37] . European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).

[38] European Commission. AI Act: High-Level Summary [Электронный ресурс]. URL: https://artificialintelligenceact.eu/high-level-summary (дата обращения: 12.06.2026).

[39] Criminal Procedure Law of the People's Republic of China, Art. 50 (2018 Revision).

[40] Provisions on Several Issues concerning Collection, Extraction, Review and Judgment of Electronic Data in Criminal Cases (2016), Art. 14.

[41] Provisions on Several Issues concerning Collection, Extraction, Review and Judgment of Electronic Data in Criminal Cases (2016), Art. 16.

[42] Provisions on Several Issues concerning Collection, Extraction, Review and Judgment of Electronic Data in Criminal Cases (2016), Art. 22, 24.

Опыт Японии характеризуется более консервативной моделью, в рамках которой искусственный интеллект рассматривается исключительно как вспомогательный инструмент анализа сетевого трафика, выявления вредоносного программного обеспечения и обработки цифровых доказательств, тогда как итоговое процессуальное решение во всех случаях принимается человеком. Особое внимание уделяется документированию всех этапов расследования и обеспечению воспроизводимости полученных результатов, что в целом соответствует международным стандартам цифровой криминалистики.[43]

Обобщая рассмотренные модели, можно констатировать наличие двух основных ориентиров для совершенствования национального регулирования: риск-ориентированного подхода, реализованного в Европейском союзе и предполагающего дифференцированное регулирование систем искусственного интеллекта в зависимости от степени их влияния на права и свободы личности, и подхода, основанного на стандартизации управления технологическими рисками на протяжении жизненного цикла системы, реализованного в Соединённых Штатах Америки. Опыт Китайской Народной Республики при этом демонстрирует возможность детальной процессуальной регламентации работы с электронными доказательствами на уровне специального нормативного акта, что также представляет интерес для законодательства Республики Узбекистан.

5. Правовые и процессуальные риски применения искусственного интеллекта при расследовании киберпреступлений

Расширение применения искусственного интеллекта в правоохранительной деятельности неизбежно сопровождается формированием комплекса правовых и процессуальных рисков, требующих самостоятельного научного осмысления. В отличие от традиционных криминалистических инструментов, выполняющих заранее определённую функцию, современные алгоритмы машинного обучения способны самостоятельно выявлять закономерности в данных, формировать вероятностные выводы и предлагать следователю или эксперту готовые рекомендации. В.С. Овчинский и Е.С. Ларина, исследуя взаимосвязь искусственного интеллекта, больших данных и преступности, обращают внимание на то, что цифровые технологии меняют не только способы совершения преступлений, но и саму логику криминологического прогнозирования и правоохранительного реагирования, что закономерно повышает значимость вопросов контроля, ответственности и допустимых пределов использования таких технологий.[44] Схожую проблематику развивает П.М. Морхат, анализирующий правовую природу искусственного интеллекта и вопросы ответственности за действия автономных систем; по его мнению, сложность правового регулирования искусственного интеллекта обусловлена его способностью к самообучению и принятию решений, последствия которых не всегда поддаются заблаговременному прогнозированию.[45]

Первым и наиболее существенным риском выступает проблема допустимости доказательств, полученных либо обработанных с использованием искусственного

[43] Астанов И., Хамидов Б. Электрон ёхуд ракамли далилларга оид умумназарий масалалар: муаммо ва ечим // Жамият ва инновациялар - Общество и инновации - Society and Innovations. - 2021. - Special Issue 7. - С. 259-273.
[44] Овчинский В.С., Ларина Е.С. Искусственный интеллект. Большие данные. Преступность. - М.: Книжный мир, 2018.
[45] . Морхат П.М. Искусственный интеллект: правовой взгляд. - М.: Буки Веди, 2017.

интеллекта. В уголовном процессе доказательство приобретает юридическое значение лишь при условии его получения, закрепления, проверки и оценки в порядке, установленном законом, причём для цифровой информации данное требование имеет особую значимость в силу её изменяемости. Процессуальная основа оценки доказательств в Республике Узбекистан закреплена Уголовно-процессуальным кодексом, а дополнительные разъяснения по вопросам допустимости доказательств содержатся в Постановлении Пленума Верховного суда Республики Узбекистан № 24 от 24 августа 2018 года, согласно которому недопустимые доказательства не имеют юридической силы и не могут использоваться для доказывания обстоятельств, предусмотренных уголовно-процессуальным законом.[46] При этом возникает принципиальный вопрос: если алгоритм выявил подозрительную транзакцию, установил связь между IP-адресами или определил вероятность участия лица в кибератаке, является ли подобный результат доказательством, заключением специалиста, ориентирующей информацией либо лишь основанием для дальнейшей проверки? Представляется обоснованным подход, согласно которому результаты алгоритмического анализа должны использоваться не как окончательное доказательство, а как аналитический инструмент, определяющий направление расследования, поскольку уголовный процесс не может основываться на вероятностных выводах, не подтверждённых надлежащими доказательствами.

Второй риск связан с достоверностью и проверяемостью алгоритмических выводов - так называемой проблемой «чёрного ящика» (black box). В традиционной экспертизе методика исследования, действия эксперта и полученный результат могут быть воспроизведены и проверены другим специалистом, тогда как в случае сложных моделей машинного обучения и нейронных сетей подобная проверка существенно затрудняется: система выдаёт результат, но не всегда позволяет объяснить логику его формирования. В уголовном процессе подобная непрозрачность представляет серьёзную опасность, поскольку сторона защиты должна иметь возможность оспаривать доказательства, проверять их происхождение, метод получения и обоснованность выводов. Указанная проблема учитывается в Структуре управления рисками искусственного интеллекта NIST, которая рассматривает управление рисками искусственного интеллекта как процесс, направленный на снижение вреда для отдельных лиц, организаций и общества, и подчёркивает необходимость обеспечения надёжности, безопасности, справедливости, подотчётности и конфиденциальности алгоритмических систем. [47] Для уголовного процесса это означает, что применяемые алгоритмы должны быть не только технически эффективными, но и юридически проверяемыми: следователь, эксперт, прокурор, суд и сторона защиты должны располагать информацией о том, на каких данных обучалась система, какую методику она применяла, какова вероятность ошибки и возможно ли воспроизведение результата.

Третий риск выражается в возможности алгоритмической ошибки, которая может являться следствием неполноты исходных данных, предвзятости обучающей выборки, технического сбоя, неправильной настройки модели либо неверной интерпретации результата оператором.

[46] Постановление Пленума Верховного суда Республики Узбекистан № 24 от 24.08.2018 г. «О некоторых вопросах применения норм уголовно-процессуального закона о допустимости доказательств».
[47] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). - Gaithersburg: National Institute of Standards and Technology, 2023.

В расследовании киберпреступлений данный риск приобретает особое значение в силу фрагментарного характера цифровой информации: IP-адрес может указывать не на конкретное лицо, а на устройство, сеть, прокси-сервер или VPN-сервис, а криптовалютная транзакция может быть связана с несколькими посредниками или биржами. Развитые правовые системы стремятся минимизировать подобные риски посредством стандартизации процедур; в частности, деятельность NIST в области цифровой криминалистики и управления рисками искусственного интеллекта может рассматриваться как пример для Узбекистана при разработке методических стандартов - от порядка изъятия цифровых данных до правил проверки алгоритмического результата.[48]

Четвёртый риск касается распределения юридической ответственности за ошибки алгоритмов и автоматизированных систем. В уголовном процессе ответственность за принятие процессуального решения несёт должностное лицо, а не программа, однако активное использование искусственного интеллекта формирует сложную цепочку участников: разработчик программного обеспечения, поставщик данных, эксперт, оператор системы, следователь, орган дознания, прокурор и суд. Если алгоритм ошибочно определил лицо как подозреваемое либо сформировал неверный вывод о связи цифровых следов, требуется установление конкретного субъекта ответственности за наступившие последствия. Анализ концептуальных подходов к ответственности за действия автономных систем, представленный в работах П.М. Морхата, подтверждает, что наиболее обоснованным является подход, при котором искусственный интеллект не признаётся самостоятельным субъектом ответственности, а соответствующая ответственность распределяется между лицами и организациями, участвующими в создании, внедрении и использовании системы.[49] Подобный подход позволяет сохранить фундаментальный принцип персональной юридической ответственности, не перенося её на техническое средство.

Пятый риск связан с возможным нарушением принципа состязательности и права на защиту. В случае, если сторона обвинения использует сложную систему искусственного интеллекта, а сторона защиты не имеет доступа к информации о методике её функционирования, возникает существенное процессуальное неравенство. Защитник должен иметь возможность проверять цифровые доказательства, ходатайствовать о назначении экспертизы, ставить вопросы специалисту, требовать раскрытия методики анализа в необходимых пределах и оспаривать достоверность алгоритмического вывода; в противном случае искусственный интеллект может стать закрытым инструментом обвинения, что противоречит принципам справедливого судебного разбирательства. Риск-ориентированный подход, реализованный в Акте об искусственном интеллекте Европейского союза, представляет в этом отношении практический интерес: системы, влияющие на оценку доказательств, профилирование лиц или оценку риска совершения преступления, относятся к высокорисковым и подлежат повышенным требованиям прозрачности и контроля.[50]

Шестой риск связан с защитой персональных данных. Расследование киберпреступлений предполагает обработку значительных массивов информации -

[48] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). - Gaithersburg: National Institute of Standards and Technology, 2023.
[49] Морхат П.М. Искусственный интеллект: правовой взгляд. - М.: Буки Веди, 2017.
[50] European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).

переписки, данных о соединениях, геолокации, транзакций, пользовательских профилей, - и применение искусственного интеллекта объективно увеличивает масштаб такого анализа. Закон Республики Узбекистан «О персональных данных» распространяется на отношения, связанные с обработкой и защитой персональных данных независимо от используемых средств обработки, включая информационные технологии,[51] а Закон «О кибербезопасности» требует строгого соблюдения Конституции и иных актов законодательства при обеспечении кибербезопасности.[52] Из этого следует, что правоохранительная цель сама по себе не может оправдывать неконтролируемый сбор данных или применение алгоритмов, результаты которых невозможно проверить.

Седьмой риск состоит в фрагментарности действующего правового регулирования.

Несмотря на принятие Стратегии развития технологий искусственного интеллекта до 2030 года[53] и Закона № ЗРУ-1115 от 21 января 2026 года,[54] специальные нормы о применении искусственного интеллекта при доследственной проверке, проведении следственных действий, назначении экспертизы, оценке цифровых доказательств и осуществлении судебного контроля в уголовно-процессуальном законодательстве Республики Узбекистан пока отсутствуют.

Восьмой риск связан с алгоритмической дискриминацией: система, обученная на неполных или искажённых данных, может воспроизводить содержащиеся в них ошибки и придавать им вид объективного технологического результата, что в контексте расследования киберпреступлений может проявляться в необоснованном повышении «рискового профиля» пользователей определённых платформ, мессенджеров или криптовалютных сервисов, не связанном с конкретными доказательствами.

Девятый риск выражается в формировании эффекта автоматизационного доверия, при котором следователь воспринимает вывод алгоритма как объективную истину, что снижает критическое восприятие альтернативных версий расследования. А.А. Исаков справедливо отмечает, что искусственный интеллект способен автоматизировать анализ угроз и повышать эффективность специалистов, однако должен оставаться вспомогательным инструментом, не заменяющим следователя или эксперта.[55]

Десятый риск связан с трансграничным характером киберпреступлений и вопросами международного сотрудничества: искусственный интеллект способен анализировать данные, находящиеся в различных юрисдикциях, тогда как следственные органы не всегда обладают правом самостоятельно получать или использовать подобные сведения. Будапештская конвенция остаётся наиболее значимым международным договором в данной сфере, а её технологически нейтральный характер позволяет применять её положения к различным цифровым ситуациям,[56] что предполагает

[51] Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.

[52] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.

[53] Постановление Президента Республики Узбекистан «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» от 14.10.2024 г. № ПП-358.

[54] Закон Республики Узбекистан «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта» от 21.01.2026 г. № ЗРУ-1115.

[55] Исаков А.А. Искусственный интеллект и расследование киберпреступлений // Вестник науки. - 2023. - № 5.

[56] Council of Europe. Convention on Cybercrime: Key Facts [Электронный ресурс]. URL: https://www.coe.int/en/web/cybercrime/key-facts (дата обращения: 12.06.2026).

необходимость сочетания развития национального регулирования искусственного интеллекта с укреплением международно-правового сотрудничества по вопросам электронных доказательств.

Наконец, существенное значение имеет проблема судебного контроля за объёмом извлекаемой цифровой информации. Действующее уголовно-процессуальное законодательство Республики Узбекистан не содержит детализированных норм о специальных судебных разрешениях либо ограничениях при доступе к электронным устройствам, аналогичных подходам, сформированным в практике Верховного суда США по делам Riley v. California и Carpenter v. United States, где была подчёркнута необходимость усиленной защиты цифровой информации как элемента права на частную жизнь.[57] При изъятии мобильного устройства следователь может получить доступ не только к сведениям, относящимся к расследуемому деянию, но и к личной переписке, медицинским данным, финансовой информации и иным конфиденциальным сведениям.

Как отмечает О. Керр, неконтролируемое изъятие цифровой информации создаёт условия для чрезмерного вмешательства государства в частную жизнь граждан и повышает риск использования полученных сведений в целях, не связанных с уголовным преследованием,[58] а Р. Векслер обращает внимание на необходимость применения механизмов избирательного извлечения и предварительного скрининга данных, минимизирующих вмешательство в права лиц, не связанных с расследуемым преступлением.[59] Указанные подходы представляются актуальными для совершенствования уголовно-процессуального законодательства Республики Узбекистан в части регламентации порядка получения, фильтрации и исследования цифровых доказательств.

6. Этические и социальные риски применения искусственного интеллекта и пути их минимизации

Помимо собственно правовых и процессуальных рисков, применение искусственного интеллекта при расследовании киберпреступлений порождает комплекс этических и социальных проблем более широкого характера, затрагивающих фундаментальные права человека, доверие общества к правосудию и пределы допустимого государственного контроля за поведением личности.

Центральным этическим риском выступает угроза неприкосновенности частной жизни. Если традиционное расследование, как правило, направлено на установление конкретных доказательств по определённому эпизоду, то искусственный интеллект способен выявлять скрытые связи, реконструировать поведение пользователя и формировать его цифровой профиль, который может содержать сведения, не относящиеся к расследуемому делу - данные о социальных связях, привычках, интересах и перемещениях лица. Л. Флориди и М. Таддео, рассматривая этику данных как самостоятельное направление научного анализа, определяют её как область, изучающую моральные проблемы, связанные с генерацией, сбором, обработкой, хранением, распространением и использованием данных, а также с алгоритмами и практиками их

[57] Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. ___ (2018).
[58] Kerr O. Digital Evidence and the New Criminal Procedure // Columbia Law Review. - 2020. - Vol. 105.
[59] Wexler R. Privacy as Privilege: The Stored Communications Act and Internet Evidence // Stanford Law Review. - 2020. - Vol. 72.

применения.[60] С точки зрения данного подхода расследование киберпреступлений с использованием искусственного интеллекта должно быть ограничено принципом необходимости: обработке подлежат только те данные, которые имеют значение для расследования, а не весь доступный массив цифровой информации о лице. Близкие положения закреплены в Рекомендации ЮНЕСКО по этике искусственного интеллекта 2021 года, согласно которой защита прав человека и человеческого достоинства составляет основу этического регулирования искусственного интеллекта, а ключевыми принципами являются прозрачность, справедливость и человеческий надзор за соответствующими системами.[61]

Существенным риском является алгоритмическая дискриминация. А. Жобин, М. Иенца и Э. Вайена в исследовании глобального ландшафта руководств по этике искусственного интеллекта отмечают, что международные документы в данной сфере демонстрируют сближение вокруг пяти базовых принципов - прозрачности, справедливости, недопущения вреда, ответственности и конфиденциальности, - однако государства и организации существенно различаются в понимании содержания данных принципов и механизмов их практической реализации.[62] Применительно к расследованию киберпреступлений алгоритмическая дискриминация может проявляться не только по классическим социальным признакам, но и по цифровым параметрам: система, обученная на статистике прошлых киберпреступлений, может ошибочно связывать использование определённых мессенджеров, криптовалютных сервисов или VPN-инструментов с противоправной активностью, формируя своего рода «цифровую подозрительность», при которой лицо попадает в сферу внимания правоохранительных органов не на основании конкретных доказательств, а вследствие статистического сходства с ранее выявленными моделями поведения.

Ф. Паскуале в работе «The Black Box Society» описывает проблему закрытых алгоритмических систем, оказывающих существенное влияние на социальную и правовую реальность, оставаясь при этом непрозрачными для лиц, чьи права они затрагивают.[63] В контексте уголовного процесса подобная непрозрачность представляет особую опасность, поскольку сторона защиты должна иметь возможность понять, на основании каких данных был сформирован вывод и можно ли его оспорить.

Значимым социальным риском выступает снижение доверия общества к системе правосудия. Если граждане не понимают, каким образом алгоритмы участвуют в расследовании, на каком основании система определяет те или иные действия как подозрительные и каким образом можно оспорить полученный результат, формируется ощущение закрытости и непредсказуемости правоохранительной деятельности. В этой связи принципиальное значение приобретает требование объяснимости: система искусственного интеллекта должна не только выдавать результат, но и обеспечивать возможность понимания логики его формирования в пределах, достаточных для процессуального контроля.

[60] Floridi L., Taddeo M. What is Data Ethics? // Philosophical Transactions of the Royal Society A. - 2016. - Vol. 374, No. 2083.
[61] UNESCO. Recommendation on the Ethics of Artificial Intelligence. - Paris: UNESCO, 2021.
[62] Jobin A., Ienca M., Vayena E. The global landscape of AI ethics guidelines // Nature Machine Intelligence. - 2019. - Vol. 1.
[63] Pasquale F. The Black Box Society. - Cambridge, MA: Harvard University Press, 2015.

Двойственный характер технологий искусственного интеллекта отмечается и в отечественных диссертационных исследованиях. В частности, в работе П.С. Швыряева, посвящённой киберпреступности как социальной проблеме, прямо указывается, что искусственный интеллект может выступать эффективным инструментом как предотвращения, так и совершения киберпреступлений, [64] что предполагает необходимость учёта при формировании этического регулирования не только защиты прав подозреваемых и потерпевших, но и предотвращения злоупотребления самой технологией - например, при создании фишинговых сообщений, генерации deepfake-контента или автоматизации мошеннических схем.

В качестве направлений минимизации этических и социальных рисков представляется целесообразным выделить следующие. Во-первых, закрепление принципа обязательного человеческого контроля, согласно которому ни одно решение, затрагивающее права человека (возбуждение уголовного дела, признание лица подозреваемым, применение меры процессуального принуждения, оценка доказательства), не может приниматься исключительно на основании вывода искусственного интеллекта. Во-вторых, обеспечение прозрачности и объяснимости используемых систем в объёме, достаточном для процессуального контроля, без необходимости полного раскрытия исходного кода. В-третьих, внедрение независимого аудита алгоритмов, применяемых при расследовании киберпреступлений, включающего проверку обучающих данных, оценку точности, выявление дискриминационных факторов и анализ возможного вреда для прав человека, что соответствует риск-ориентированному подходу, реализованному в законодательстве Европейского союза. [65] В-четвёртых, развитие национальных стандартов цифровой криминалистики, включающих правила фиксации действий алгоритма, требования к сохранению исходных данных и документированию результатов. В-пятых, организация профессиональной подготовки следователей, прокуроров, судей и экспертов в области цифровой криминалистики и этики искусственного интеллекта, поскольку без соответствующих знаний даже технически совершенная система может быть применена ненадлежащим образом. В-шестых, закрепление принципа минимизации данных, согласно которому обработка должна ограничиваться сведениями, относящимися к предмету доказывания, что соответствует подходам Л. Флориди и М. Таддео к этике данных. [66] В-седьмых, обеспечение права стороны защиты на оспаривание алгоритмического вывода - посредством постановки вопросов специалисту, заявления ходатайств о назначении повторной экспертизы и проверки исходных данных.

7. Направления совершенствования уголовно-процессуального законодательства Республики Узбекистан

Проведённый анализ возможностей и рисков применения искусственного интеллекта при расследовании киберпреступлений, а также сопоставление подходов, сформированных в законодательстве Соединённых Штатов Америки, Европейского союза, Китайской Народной Республики и Японии, позволяют сформулировать ряд

[64] Швыряев П.С. Киберпреступность как социальная проблема: стратегии противодействия: дис. ... канд. юрид. наук. - М., 2022. - 186 с.
[65] European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).
[66] Floridi L., Taddeo M. What is Data Ethics? // Philosophical Transactions of the Royal Society A. - 2016. - Vol. 374, No. 2083.

предложений, направленных на совершенствование уголовно-процессуального законодательства и правоприменительной практики Республики Узбекистан.

Первое. Представляется необходимым закрепить в Уголовно-процессуальном кодексе Республики Узбекистан легальное определение электронных (цифровых) доказательств и определить их процессуальный статус, включая порядок их получения, фиксации, хранения, исследования и оценки. Действующее законодательство, признавая существование категории цифровых доказательств в отдельных нормах, не содержит детализированного регулирования данных вопросов, что создаёт риски признания соответствующих доказательств недопустимыми вследствие процессуальных нарушений при их получении или исследовании.

Второе. Целесообразно дополнить Уголовно-процессуальный кодекс Республики Узбекистан отдельной статьёй (либо принять соответствующий подзаконный нормативный акт), регламентирующей особенности расследования киберпреступлений и порядок использования технологий искусственного интеллекта в следственной деятельности. Данная норма должна предусматривать: обязательное участие специалиста по цифровой криминалистике или IT-эксперта при работе с электронными носителями информации и системами искусственного интеллекта; порядок извлечения, копирования и хранения цифровых данных с применением хеш-функций; требования к обеспечению целостности электронных доказательств; обязательное документирование факта и условий применения алгоритмических систем, включая источники данных, версию программного обеспечения и параметры используемой модели - по аналогии с подходом, реализованным в статьях 14, 16, 22 и 24 китайских Положений о сборе, извлечении, проверке и оценке электронных данных по уголовным делам.[67]

Третье. Принципиальное значение имеет закрепление прямого запрета на принятие процессуальных решений, затрагивающих права и свободы личности (возбуждение уголовного дела, признание лица подозреваемым, применение меры процессуального принуждения, оценка совокупности доказательств), исключительно на основании результатов автоматизированного анализа, без обязательной проверки следователем, прокурором, экспертом или судом. Закрепление данного правила позволит обеспечить соблюдение принципов законности, объективности и презумпции невиновности в условиях расширяющегося применения алгоритмических систем.

Четвёртое. Представляется обоснованной разработка национальных стандартов цифровой криминалистики, устанавливающих единые требования к работе с цифровыми следами, порядку фиксации действий алгоритмических систем, журналированию операций, использованию хеш-функций (MD5, SHA-256) и документированию результатов анализа. При разработке таких стандартов целесообразно использовать в качестве ориентира подходы, сформированные Национальным институтом стандартов и технологий США (NIST) в области цифровой криминалистики и управления рисками искусственного интеллекта.[68]

Пятое. С учётом риск-ориентированного подхода, реализованного в Акте об искусственном интеллекте Европейского союза, [69] целесообразно ввести

[67] Provisions on Several Issues concerning Collection, Extraction, Review and Judgment of Electronic Data in Criminal Cases (2016), Art. 22, 24.
[68] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). - Gaithersburg: National Institute of Standards and Technology, 2023.
[69] European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).

дифференцированное регулирование систем искусственного интеллекта, применяемых правоохранительными органами, в зависимости от степени их влияния на права и свободы личности. Системы, выполняющие вспомогательные функции (например, автоматическую сортировку файлов или индексацию данных), могут быть отнесены к категории низкого или среднего риска, тогда как алгоритмы, результаты которых могут повлиять на решение о подозрении лица, применении меры пресечения или оценке доказательств, должны регулироваться как высокорисковые системы, подлежащие обязательной сертификации и периодическому аудиту.

Шестое. Необходимо законодательно закрепить право стороны защиты на доступ к информации о методике алгоритмического анализа в пределах, необходимых для оспаривания соответствующих доказательств, без раскрытия сведений, составляющих государственную или иную охраняемую законом тайну. Подобное право может быть реализовано посредством постановки вопросов специалисту, привлечённому стороной защиты, либо посредством назначения дополнительной (повторной) экспертизы.

Седьмое. В целях обеспечения защиты персональных данных при использовании искусственного интеллекта в расследовании киберпреступлений целесообразно закрепить принцип минимизации объёма обрабатываемой информации: алгоритмический анализ должен ограничиваться данными, относящимися к предмету доказывания, а порядок обезличивания и уничтожения нерелевантных сведений должен быть прямо урегулирован законодательством. Дополнительно, по аналогии с подходами, сформированными в практике Верховного суда США по делам Riley v. California и Carpenter v. United States,[70] представляется целесообразным рассмотреть вопрос о введении специального судебного контроля (разрешительного порядка) за объёмом извлекаемой информации при изъятии электронных устройств, содержащих значительные массивы персональных данных, не относящихся непосредственно к расследуемому деянию.

Восьмое. Необходимым условием реализации перечисленных предложений является организация системы обязательной специализированной подготовки и сертификации следователей, прокуроров, судей и экспертов в области цифровой криминалистики и применения искусственного интеллекта. Участие в расследовании сложных киберпреступлений лиц, не обладающих необходимыми компетенциями в данной сфере, объективно снижает эффективность расследования и повышает риск процессуальных нарушений.

Реализация перечисленных предложений в совокупности позволит сформировать целостную модель применения искусственного интеллекта в уголовном процессе Республики Узбекистан, сочетающую повышение эффективности расследования киберпреступлений с обеспечением гарантий прав человека, что соответствует как объективным потребностям правоохранительной практики, так и международным стандартам в данной области.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволяет сформулировать ряд обобщающих выводов.

Во-первых, стремительный рост киберпреступности в Республике Узбекистан, отражённый в официальной статистике Министерства внутренних дел, объективно обусловливает необходимость внедрения интеллектуальных аналитических систем в деятельность правоохранительных органов, поскольку традиционные методы

[70] Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. ___ (2018).

расследования не обеспечивают адекватного реагирования на современные цифровые угрозы, характеризующиеся высокой латентностью, трансграничностью и технической сложностью.

Во-вторых, анализ международной практики - расследования ботнета Emotet, атаки на Colonial Pipeline, дел Silk Road и Bitfinex - подтверждает высокую практическую эффективность технологий Big Data, алгоритмов выявления аномалий и систем блокчейн-аналитики при расследовании киберпреступлений. Вместе с тем эффективность данных технологий напрямую зависит от качества организации работы с цифровыми доказательствами на всех этапах - от выявления до документирования.

В-третьих, искусственный интеллект не может быть признан самостоятельным субъектом уголовно-процессуальной деятельности, поскольку он не обладает правосубъектностью и способностью нести юридическую ответственность. Результаты алгоритмического анализа должны рассматриваться исключительно как вспомогательная аналитическая информация, подлежащая обязательной проверке следователем, экспертом, прокурором и судом.

В-четвёртых, сравнительно-правовой анализ подходов США, Европейского союза, Китайской Народной Республики и Японии демонстрирует наличие апробированных моделей регулирования - риск-ориентированной (ЕС), стандартизирующей (США) и детально-процессуальной (КНР), - адаптация которых с учётом национальных особенностей способна существенно повысить качество правового регулирования применения искусственного интеллекта в Республике Узбекистан.

В-пятых, ключевыми направлениями совершенствования уголовно-процессуального законодательства Республики Узбекистан являются: законодательное определение электронных доказательств и их процессуального статуса; установление специального порядка применения искусственного интеллекта при расследовании киберпреступлений; запрет на принятие процессуально значимых решений исключительно на основании алгоритмического вывода; разработка национальных стандартов цифровой криминалистики; внедрение риск-ориентированного регулирования и независимого аудита алгоритмических систем; обеспечение права стороны защиты на оспаривание результатов искусственного интеллекта; усиление защиты персональных данных и развитие профессиональной подготовки кадров.

Таким образом, искусственный интеллект обладает значительным потенциалом повышения эффективности расследования киберпреступлений, однако его применение должно быть юридически определённым, технически проверяемым и этически обоснованным. Только формирование комплексной нормативной модели, сочетающей внедрение современных технологий с сохранением фундаментальных гарантий прав человека, позволит обеспечить как повышение раскрываемости киберпреступлений, так и сохранение доверия общества к правоохранительной и судебной системе Республики Узбекистан.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Газета.uz. Киберпреступность в Узбекистане: статистика МВД за 2024 год [Электронный ресурс]. URL: https://www.gazeta.uz/ru/2025/11/06/cybersecurity/ (дата обращения: 12.06.2026).
2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - Pearson, 2021.

3. Convention on Cybercrime (Budapest Convention). - Council of Europe, 2001.
4. Wall D. Cybercrime: The Transformation of Crime in the Information Age. - Cambridge University Press, 2007.
5. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года (с изменениями и дополнениями) // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
6. UNODC. Comprehensive Study on Cybercrime. - Vienna: United Nations, 2013.
7. Brenner S. Cybercrime and the Law: Challenges, Issues, and Outcomes. - Northeastern University Press, 2010.
8. Уголовный кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
9. OECD. OECD Principles on Artificial Intelligence. - Paris: OECD Publishing, 2019.
10. Kitchin R. Big Data, new epistemologies and paradigm shifts // Big Data & Society. - 2014. - Vol. 1, No. 1.
11. Bryson J. Artificial Intelligence and Legal Personhood // AI & Society. - 2010. - Vol. 25.
12. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
13. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz.
14. Постановление Президента Республики Узбекистан «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий» от 30.04.2025 г. № ПП-153.
15. Постановление Президента Республики Узбекистан «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» от 14.10.2024 г. № ПП-358.
16. Закон Республики Узбекистан «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта» от 21.01.2026 г. № ЗРУ-1115.
17. UNESCO. Recommendation on the Ethics of Artificial Intelligence. - Paris: UNESCO, 2021.
18. European Union. Artificial Intelligence Act (Regulation (EU) 2024/1689).
19. Mayer-Schonberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. - Boston: Houghton Mifflin Harcourt, 2013.
20. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. - 2009. - Vol. 41, No. 3.
21. Europol. Disruption of Emotet Botnet: Press Release. - The Hague: Europol, 2021.
22. U.S. Department of Justice. Colonial Pipeline Ransomware Investigation: Press Release. - Washington, D.C.: DOJ, 2021.
23. United States v. Ulbricht (Silk Road case), 31 F. Supp. 3d 540 (S.D.N.Y. 2014), aff'd 2 Cir. 2017.

24. Астанов И., Хамидов Б. Электрон ёхуд ракамли далилларга оид умумназарий масалалар: муаммо ва ечим // Жамият ва инновациялар - Общество и инновации - Society and Innovations. - 2021. - Special Issue 7. - С. 259-273.
25. NIST. OSAC Standards Library [Электронный ресурс]. URL: https://www.nist.gov/osac/standards-library (дата обращения: 12.06.2026).
26. Deloitte. Forensic Investigators Gain an Edge with AI [Электронный ресурс]. URL: https://www.deloitte.com/ch/en/services/consulting-financial/perspectives/forensic-investigators-gain-an-edge-with-ai (дата обращения: 12.06.2026).
27. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). - Gaithersburg: National Institute of Standards and Technology, 2023.
28. Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 585 U.S. ___ (2018).
29. Kerr O. Digital Evidence and the New Criminal Procedure // Columbia Law Review. - 2020. - Vol. 105.
30. Wexler R. Privacy as Privilege: The Stored Communications Act and Internet Evidence // Stanford Law Review. - 2020. - Vol. 72.
31. European Commission. AI Act: High-Level Summary [Электронный ресурс]. URL: https://artificialintelligenceact.eu/high-level-summary (дата обращения: 12.06.2026).
32. Criminal Procedure Law of the People's Republic of China, Art. 50 (2018 Revision).
33. Provisions on Several Issues concerning Collection, Extraction, Review and Judgment of Electronic Data in Criminal Cases (2016), Art. 14.
34. Овчинский В.С., Ларина Е.С. Искусственный интеллект. Большие данные. Преступность. - М.: Книжный мир, 2018.
35. Мохат П.М. Искусственный интеллект: правовой взгляд. - М.: Буки Веди, 2017.
36. Постановление Пленума Верховного суда Республики Узбекистан № 24 от 24.08.2018 г. «О некоторых вопросах применения норм уголовно-процессуального закона о допустимости доказательств».
37. Исаков А.А. Искусственный интеллект и расследование киберпреступлений // Вестник науки. - 2023. - № 5.
38. Council of Europe. Convention on Cybercrime: Key Facts [Электронный ресурс]. URL: https://www.coe.int/en/web/cybercrime/key-facts (дата обращения: 12.06.2026).
39. Floridi L., Taddeo M. What is Data Ethics? // Philosophical Transactions of the Royal Society A. - 2016. - Vol. 374, No. 2083.
40. Jobin A., Ienca M., Vayena E. The global landscape of AI ethics guidelines // Nature Machine Intelligence. - 2019. - Vol. 1.
41. Pasquale F. The Black Box Society. - Cambridge, MA: Harvard University Press, 2015.
42. Швыряев П.С. Киберпреступность как социальная проблема: стратегии противодействия: дис. ... канд. юрид. наук. - М., 2022. - 186 с.