ИСПОЛЬЗОВАНИЕ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ВОЗМОЖНОСТИ И РИСКИ

Норов Мирфайз Абдулазизович
магистрант Ташкентского государственного юридического университета.

https://doi.org/10.5281/zenodo.20058653

Аннотация. *В статье рассматриваются современные проблемы и перспективы использования искусственного интеллекта при расследовании киберпреступлений.*

Анализируются особенности применения технологий машинного обучения, Big Data и цифровой криминалистики в деятельности правоохранительных органов. Особое внимание уделяется вопросам допустимости цифровых доказательств, правовым и этическим рискам использования алгоритмических систем, а также необходимости совершенствования законодательства Республики Узбекистан с учетом международных стандартов и зарубежного опыта. Автором обосновывается необходимость формирования комплексного механизма регулирования искусственного интеллекта в уголовном процессе и разработки специализированных методик расследования киберпреступлений.

Ключевые слова: *искусственный интеллект, киберпреступность, цифровые доказательства, цифровая криминалистика, Big Data, уголовный процесс, кибербезопасность, расследование преступлений, машинное обучение.*

Annotation. *The article examines contemporary issues and prospects of using artificial intelligence in the investigation of cybercrimes. It analyzes the specifics of applying machine learning technologies, Big Data, and digital forensics in the activities of law enforcement agencies. Particular attention is paid to the admissibility of digital evidence, the legal and ethical risks associated with the use of algorithmic systems, as well as the need to improve the legislation of the Republic of Uzbekistan in accordance with international standards and foreign experience. The author substantiates the necessity of forming a comprehensive mechanism for regulating artificial intelligence in criminal proceedings and developing specialized methods for investigating cybercrimes.*

Keywords: *artificial intelligence, cybercrime, digital evidence, digital forensics, Big Data, criminal procedure, cybersecurity, criminal investigation, machine learning.*

Annotatsiya. *Maqolada kiberjinoyatlarni tergov qilishda sun'iy intellektdan foydalanishning zamonaviy muammolari va istiqbollari ko'rib chiqiladi. Huquqni muhofaza qiluvchi organlar faoliyatida mashinaviy o'qitish, Big Data va raqamli kriminalistika texnologiyalarini qo'llash xususiyatlari tahlil qilinadi. Raqamli dalillarning maqbulligi, algoritmik tizimlardan foydalanishning huquqiy va etik xavflari, shuningdek, O'zbekiston Respublikasi qonunchiligini xalqaro standartlar va xorijiy tajriba asosida takomillashtirish zaruriyatiga alohida e'tibor qaratiladi. Muallif tomonidan jinoyat protsessida sun'iy intellektni tartibga solishning kompleks mexanizmini shakllantirish hamda kiberjinoyatlarni tergov qilishning maxsus metodikalarini ishlab chiqish zarurligi asoslab beriladi.*

Kalit so'zlar: *sun'iy intellekt, kiberjinoyatchilik, raqamli dalillar, raqamli kriminalistika, Big Data, jinoyat protsessi, kiberxavfsizlik, jinoyatlarni tergov qilish, mashinaviy o'qitish.*

Современный этап развития информационно-коммуникационных технологий характеризуется активной цифровизацией общественных отношений, что оказывает непосредственное влияние на трансформацию преступности.

Наряду с традиционными формами противоправной деятельности все более широкое распространение получают преступления, совершаемые с использованием цифровых технологий, информационных систем и сети Интернет. В этих условиях киберпреступность становится одной из наиболее опасных угроз информационной безопасности государства, общества и личности.

В Республике Узбекистан данная проблема приобретает особую актуальность в связи с ростом количества преступлений, совершаемых с использованием информационных технологий. Согласно данным Министерства внутренних дел Республики Узбекистан, в 2024 году доля киберпреступлений составила 44,4% от общего числа зарегистрированных преступлений, а общий ущерб от подобных деяний превысил 603 млрд сумов.[1] Основная часть преступлений связана с незаконным использованием банковских карт, распространением вредоносных ссылок, фишинговыми схемами, оформлением онлайн-кредитов и использованием технологий дипфейков.

Развитие киберпреступности объективно требует внедрения современных технологических решений в деятельность правоохранительных органов. Одним из наиболее перспективных направлений становится использование искусственного интеллекта при расследовании преступлений. В научной литературе искусственный интеллект определяется как совокупность программных и аппаратных решений, способных выполнять задачи, требующие интеллектуальной деятельности человека, включая анализ данных, прогнозирование, выявление закономерностей и принятие решений.[2]

Особое значение искусственный интеллект приобретает в сфере расследования киберпреступлений, поскольку традиционные методы обработки информации уже не позволяют эффективно анализировать огромные массивы цифровых данных. В современных условиях следственные органы сталкиваются с необходимостью исследования лог-файлов, сетевого трафика, криптовалютных транзакций, электронной переписки, данных мобильных устройств и иных цифровых следов. Использование технологий Big Data и алгоритмов машинного обучения позволяет существенно ускорить данный процесс.

Как отмечают зарубежные исследователи, технологии Big Data дают возможность выявлять скрытые взаимосвязи между событиями, анализировать цифровое поведение пользователей и прогнозировать потенциальные угрозы. [3] На практике подобные технологии активно применяются в США, странах Европейского союза, Китае и Японии.

Показательным примером является международная операция по ликвидации ботнета Emotet в 2021 году, в рамках которой правоохранительные органы Германии, Нидерландов, США и других государств использовали алгоритмы анализа больших данных для выявления структуры преступной сети и установления управляющих серверов.[4] Аналогичные технологии применялись при расследовании атаки на Colonial Pipeline в США, где искусственный интеллект использовался для анализа блокчейн-транзакций и отслеживания перемещения криптовалютных средств.[5]

[1] https://www.gazeta.uz/ru/2025/11/06/cybersecurity/.
[2] Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2021.
[3] Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. — London, 2013.
[4] Europol. Disruption of Emotet botnet, 2021.
[5] U.S. Department of Justice. Colonial Pipeline ransomware investigation, 2021.

Использование искусственного интеллекта позволяет автоматизировать выявление подозрительных паттернов поведения, анализ сетевого трафика и обнаружение вредоносной активности.

В банковской сфере алгоритмы машинного обучения активно применяются для выявления мошеннических операций и предотвращения незаконного доступа к финансовым ресурсам. Как справедливо отмечают Ариу, Джачинто и Роли, методы машинного обучения значительно повышают эффективность обнаружения киберугроз и анализа цифровых доказательств.[6]

Существенное значение приобретает и цифровая криминалистика. Международная практика выделяет четыре основных этапа цифрового расследования: идентификацию цифровых следов, сохранение данных, их анализ и документирование результатов.[7]

Несоблюдение хотя бы одного из данных этапов может привести к признанию доказательств недопустимыми в уголовном процессе. Вместе с тем использование искусственного интеллекта в расследовании киберпреступлений связано с рядом серьезных правовых и процессуальных проблем. Прежде всего возникает вопрос о допустимости доказательств, полученных с использованием алгоритмических систем. В уголовном процессе Республики Узбекистан доказательства должны соответствовать требованиям законности, допустимости и достоверности. Однако результаты, полученные посредством алгоритмов машинного обучения, нередко имеют вероятностный характер, что вызывает сложности при их оценке. Дополнительную проблему представляет так называемый эффект «черного ящика», при котором алгоритм формирует результат без возможности полного объяснения механизма принятия решения.[8] Это особенно опасно в уголовном процессе, поскольку сторона защиты должна иметь возможность проверить происхождение доказательства, методику его получения и достоверность результатов анализа.

В научной литературе справедливо подчеркивается, что искусственный интеллект не должен заменять следователя или эксперта, а должен использоваться исключительно как вспомогательный инструмент.[9] Алгоритмический вывод не может автоматически подтверждать виновность лица и требует обязательной проверки человеком.

Серьезное значение имеют также вопросы юридической ответственности за ошибки алгоритмов. Искусственный интеллект способен функционировать на основе самообучающихся систем, что затрудняет установление причин возникновения ошибки. В этой связи возникает необходимость определения субъектов ответственности за неправомерные решения, принятые с использованием ИИ. Наиболее обоснованным представляется подход, согласно которому ответственность должна возлагаться на разработчиков, операторов и должностных лиц, использующих соответствующие технологии.[10]

Отдельного внимания заслуживают вопросы защиты персональных данных и соблюдения прав человека.

---

[6] Ariu D., Giacinto G., Roli F. Machine learning in computer forensics // ACM Workshop on Security and Artificial Intelligence. 2011.
[7] NIST. Digital Forensics Standards and Guidelines // https://www.nist.gov/forensic-science
[8] Pasquale F. The Black Box Society. — Harvard University Press, 2015. NIST. Digital Forensics Standards and Guidelines // https://www.nist.gov/forensic-science
[9] Исаков А.А. Искусственный интеллект и расследование киберпреступлений // Вестник науки. 2023.
[10] Мохат П.М. Искусственный интеллект: правовой взгляд. — М.: Буки Веди, 2017.

Использование ИИ предполагает обработку значительных объемов информации, включая сведения о частной жизни, геолокации, банковских операциях и цифровой активности пользователей. При отсутствии эффективных механизмов контроля подобные технологии могут привести к чрезмерному вмешательству в личную жизнь граждан.

Международные документы также акцентируют внимание на необходимости соблюдения этических принципов использования искусственного интеллекта. В частности, Рекомендация ЮНЕСКО по этике искусственного интеллекта подчеркивает необходимость обеспечения прозрачности алгоритмов, недопущения дискриминации и обязательного человеческого контроля за автоматизированными системами.[11]

В Республике Узбекистан правовое регулирование искусственного интеллекта находится на стадии формирования. Важным шагом стало принятие Закона Республики Узбекистан «О кибербезопасности», закрепившего основные принципы обеспечения безопасности информационного пространства.[12] Кроме того, в 2024 году была утверждена Стратегия развития технологий искусственного интеллекта до 2030 года, предусматривающая разработку механизмов безопасного внедрения ИИ и защиту персональных данных. [13] Однако действующее законодательство пока не содержит специальных норм, регулирующих применение искусственного интеллекта в уголовном процессе. Отсутствует четкое определение процессуального статуса результатов алгоритмического анализа, не установлены требования к прозрачности алгоритмов и порядку их проверки.

В этой связи представляется необходимым совершенствование законодательства Республики Узбекистан с учетом международного опыта. В частности, целесообразно:

закрепить в законодательстве понятие искусственного интеллекта и цифровых доказательств;

определить процессуальный статус результатов алгоритмического анализа;

установить обязательные требования к прозрачности и проверяемости алгоритмов;

разработать национальные стандарты цифровой криминалистики;

внедрить механизм обязательного человеческого контроля за использованием ИИ;

создать систему подготовки IT-специалистов в сфере расследования киберпреступлений.

Особое значение имеет подготовка специалистов, обладающих одновременно техническими и юридическими знаниями. На практике многим следователям сложно ориентироваться в сложных цифровых технологиях, поэтому более эффективным представляется обучение IT-специалистов основам уголовного процесса, криминалистики и методики расследования преступлений.

Таким образом, искусственный интеллект обладает значительным потенциалом для повышения эффективности расследования киберпреступлений, однако его использование требует четкого правового регулирования и соблюдения процессуальных гарантий. Для Республики Узбекистан наиболее перспективным направлением является формирование комплексной модели регулирования ИИ, сочетающей развитие цифровых технологий, совершенствование законодательства и обеспечение защиты прав человека.

[11] UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021.
[12] Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан (lex.uz).
[13] Постановление Президента Республики Узбекистан № ПП-358 от 14.10.2024 г. «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года».

Список использованных источников:

1. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан (lex.uz).
2. Постановление Президента Республики Узбекистан № ПП-358 от 14.10.2024 г. «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года».
3. Исаков А.А. Искусственный интеллект и расследование киберпреступлений // Вестник науки. 2023.
4. Мохат П.М. Искусственный интеллект: правовой взгляд. — М.: Буки Веди, 2017.
5. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2021
6. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. — London, 2013.
7. Ariu D., Giacinto G., Roli F. Machine learning in computer forensics // ACM Workshop on Security and Artificial Intelligence. 2011.
8. Pasquale F. The Black Box Society. — Harvard University Press, 2015.
9. UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021
10. NIST. Digital Forensics Standards and Guidelines // https://www.nist.gov/forensic-science
11. U.S. Department of Justice. Colonial Pipeline ransomware investigation, 2021
12. Europol. Disruption of Emotet botnet, 2021.
13. https://www.gazeta.uz/ru/2025/11/06/cybersecurity/.