«ИСПОЛЬЗОВАНИЕ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ВОЗМОЖНОСТИ И РИСКИ»

Норов Мирфайз Абдулазизович
магистрант ТГЮУ, специальность 70420113.

https://doi.org/10.5281/zenodo.20075884

В условиях стремительной цифровизации общественных отношений киберпреступность становится одной из наиболее опасных форм современной преступности. Расширение использования электронных платежных систем, онлайн-банкинга, цифровых платформ и облачных технологий способствует не только развитию экономики, но и формированию новых способов совершения преступлений.

В последние годы в Республике Узбекистан наблюдается существенный рост преступлений, совершаемых с использованием информационных технологий. Согласно данным МВД Республики Узбекистан, в 2024 году доля киберпреступлений составила 44,4% от общего количества зарегистрированных преступлений, а общий ущерб превысил 603 млрд сумов.[1]

Специфика киберпреступлений проявляется в их высокой латентности, трансграничном характере, технической сложности и использовании современных средств анонимизации. В отличие от традиционных преступлений, значительная часть доказательственной информации существует исключительно в цифровой форме: IP-адреса, серверные журналы, электронная переписка, криптовалютные транзакции, метаданные и иные цифровые следы. Это объективно требует внедрения современных технологий в деятельность правоохранительных органов.

Одним из наиболее перспективных направлений является использование искусственного интеллекта при расследовании киберпреступлений. В научной литературе искусственный интеллект рассматривается как совокупность алгоритмов и программных решений, способных выполнять задачи, требующие интеллектуальной деятельности человека, включая анализ данных, выявление закономерностей и прогнозирование.[2]

Применение искусственного интеллекта позволяет существенно повысить эффективность расследования киберпреступлений за счет автоматизации обработки больших массивов информации. Особое значение имеют технологии Big Data, позволяющие анализировать огромные объемы цифровых данных в режиме реального времени. Как отмечают Mayer-Schönberger и Cukier, технологии Big Data позволяют выявлять скрытые взаимосвязи и закономерности, недоступные традиционным методам анализа.[3]

На практике искусственный интеллект активно применяется в деятельности правоохранительных органов развитых государств. Так, при ликвидации ботнета Emotet в 2021 году правоохранительные органы стран Европейского союза и США использовали алгоритмы анализа больших данных для выявления структуры преступной сети и установления управляющих серверов.[4]

[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.

Аналогичные технологии применялись в ходе расследования атаки на Colonial Pipeline в США, где алгоритмы искусственного интеллекта использовались для анализа блокчейн-транзакций и отслеживания криптовалютных переводов.[5]

Особую роль искусственный интеллект играет в сфере цифровой криминалистики.

Международная практика выделяет четыре базовых этапа цифрового расследования: идентификация, сохранение, анализ и документирование цифровых доказательств.[6] При этом алгоритмы машинного обучения способны автоматически выявлять аномалии в сетевом трафике, обнаруживать вредоносное программное обеспечение и анализировать подозрительные паттерны поведения пользователей.

Несмотря на значительные преимущества, использование искусственного интеллекта в расследовании киберпреступлений связано с рядом серьезных правовых и процессуальных проблем. Одной из ключевых является проблема допустимости цифровых доказательств, полученных с использованием алгоритмических систем.

В уголовном процессе доказательства должны соответствовать требованиям законности, допустимости и достоверности. Однако результаты работы искусственного интеллекта часто имеют вероятностный характер, что вызывает сложности при их процессуальной оценке.

Дополнительную проблему представляет так называемый эффект «черного ящика», при котором алгоритм формирует вывод без возможности полного объяснения механизма принятия решения.[7] В условиях уголовного судопроизводства подобная непрозрачность может привести к нарушению права на защиту и принципа состязательности сторон.

Серьезное значение имеют и вопросы юридической ответственности за ошибки алгоритмов. Искусственный интеллект не обладает самостоятельной правосубъектностью, поэтому ответственность за его использование должна возлагаться на разработчиков, операторов и должностных лиц, принимающих решения на основе результатов алгоритмического анализа.[8]

На международном уровне необходимость регулирования искусственного интеллекта подчеркивается в Рекомендации ЮНЕСКО по этике искусственного интеллекта 2021 года, где закрепляются принципы прозрачности, справедливости, подотчетности и обязательного человеческого контроля за автоматизированными системами.[9]

В Республике Узбекистан вопросы кибербезопасности регулируются Законом «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764.[10] Кроме того, государством принимаются меры по развитию технологий искусственного интеллекта и совершенствованию механизмов цифровой безопасности. Вместе с тем действующее законодательство пока не содержит специальных норм, регулирующих использование искусственного интеллекта в уголовном процессе.

В этой связи представляется необходимым совершенствование законодательства Республики Узбекистан в части:

[5] U.S. Department of Justice. Colonial Pipeline ransomware investigation, 2021.
[6] NIST. Digital Forensics Standards and Guidelines // https://www.nist.gov/forensic-science
[7] Pasquale F. The Black Box Society. — Harvard University Press, 2015.
[8] Мохат П.М. Искусственный интеллект: правовой взгляд. — М.: Буки Веди, 2017.
[9] UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021.
[10] Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан (lex.uz).

определения правового статуса результатов алгоритмического анализа;

разработки национальных стандартов цифровой криминалистики;

установления требований к прозрачности алгоритмов;

обеспечения обязательного человеческого контроля за использованием ИИ;

подготовки специалистов, обладающих одновременно юридическими и техническими знаниями.

Таким образом, искусственный интеллект обладает значительным потенциалом для повышения эффективности расследования киберпреступлений, однако его использование должно сопровождаться четким правовым регулированием, соблюдением процессуальных гарантий и защитой прав человека.

Формирование комплексного механизма применения ИИ в уголовном процессе является одним из важнейших направлений развития современной системы противодействия киберпреступности.

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. Pasquale F. The Black Box Society. — Harvard University Press, 2015.
3. Морхат П.М. Искусственный интеллект: правовой взгляд. — М.: Буки Веди, 2017
4. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2021.
5. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. — London, 2013.
6. Europol. Disruption of Emotet botnet, 2021.
7. UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021.
8. U.S. Department of Justice. Colonial Pipeline ransomware investigation, 2021.
9. NIST. Digital Forensics Standards and Guidelines // https://www.nist.gov/forensic-science.
10. https://www.gazeta.uz/ru/2025/11/06/cybersecurity/