Дата поступления рукописи в редакцию: 23.04.2025 г.
Дата принятия рукописи в печать: 13.05.2025 г.
DOI: 10.24412/2782-3830-2025-4-252-254

ТААШЕВ Джаримас Борисович,
капитан полиции, преподаватель кафедры организации правоохранительной деятельности Северо-Кавказского института (филиал) Краснодарского Университета МВД РФ,
e-mail: d_taashev@mail.ru

ПРОБЛЕМНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. *Статья посвящена анализу проблемных аспектов применения информационных технологий (ИТ) в расследовании преступлений в цифровом пространстве в России. Предложены пути решения, включая совершенствование законодательства, модернизацию технической базы, оптимизацию взаимодействия подразделений и повышение квалификации кадров. Статья подчеркивает необходимость комплексного подхода для адаптации системы расследования к реалиям цифровой эпохи.*

Ключевые слова: *киберпреступность, информационные технологии, расследование преступлений, цифровая криминалистика, искусственный интеллект.*

TAASHEV Jarimas Borisovich,
Police Captain, Lecturer at the Department of Law Enforcement Organization, North Caucasus Institute (branch) Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

PROBLEMATIC ASPECTS OF THE USE OF INFORMATION TECHNOLOGY IN THE INVESTIGATION OF CRIMES IN THE DIGITAL SPACE

Annotation. *The article examines the problematic aspects of applying information technologies (IT) in the investigation of crimes in the digital space in Russia. Solutions are proposed, including improving legislation, upgrading technical infrastructure, optimizing interagency cooperation, and enhancing personnel training. The article emphasizes the need for a comprehensive approach to adapt the investigation system to the realities of the digital era.*

Key words: *cybercrime, information technologies (IT), crime investigation, digital forensics, artificial intelligence (AI).*

Современное общество характеризуется стремительным развитием информационных технологий (ИТ), которые проникают во все сферы человеческой деятельности, включая криминальную. Цифровое пространство стало не только платформой для коммуникации и обмена информацией, но и ареной для совершения преступлений. В России, как и во всем мире, наблюдается устойчивый рост киберпреступности: в 2023 году было зарегистрировано 677 тысяч преступлений, совершенных с использованием ИТ, что почти в четыре раза больше, чем в 2018 году (175 тысяч). Каждое третье преступление в стране сегодня связано с цифровыми технологиями, что подчеркивает актуальность совершенствования методов их расследования.

Основные виды киберпреступлений включают:

– мошенничество с использованием ИТ (79,4 тысячи случаев в первом квартале 2023 года, рост на 31,5% к 2022 году);
– неправомерный доступ к компьютерной информации (4,7 тысячи атак в 2023 году, рост в три раза);
– распространение вредоносного ПО и DDoS-атаки.

Интересно, что значительная доля киберпреступников (около 10%) — это подростки 14–15

лет, что значительно превышает их долю среди всех преступников (менее 1%). Это указывает на необходимость адаптации методов расследования к особенностям цифрового поведения молодежи.

Технологии анализа больших данных активно используются для выявления закономерностей в поведении преступников и прогнозирования преступлений. В России такие системы применяются, например, в рамках программы «Безопасный город», где данные с камер видеонаблюдения, социальных сетей и мобильных операторов агрегируются для построения моделей криминальной активности. Преимущество Big Data заключается в возможности обрабатывать огромные объемы информации, недоступные традиционным методам. Например, анализ трафика в мессенджерах может помочь установить связи между участниками преступной группы, даже если они используют шифрование. Однако для этого требуются мощные вычислительные ресурсы и квалифицированные аналитики, что в регионах часто отсутствует.

Современные инструменты цифровой криминалистики, такие как Cellebrite UFED или Magnet AXIOM, позволяют извлекать данные даже с поврежденных устройств. В деле о хакерской атаке на банк в 2023 году эксперты восстановили логи, указывающие на IP-адреса злоумышленников, что привело к их задержанию в течение двух недель. Однако сложность современных методов шифрования (например, использование VPN или Tor) затрудняет трассировку, требуя от следователей глубоких технических знаний.

ИТ также позволяют правоохранительным органам сотрудничать с частными компаниями. Например, банки предоставляют данные о подозрительных транзакциях, а IT-компании, такие как «Яндекс» или «VK», передают информацию о пользователях в рамках уголовных дел. В 2023 году такое взаимодействие помогло раскрыть 12 тысяч случаев кибермошенничества. Однако этот процесс осложнен необходимостью соблюдения закона о персональных данных (ФЗ-152), что замедляет доступ к информации.

Технические аспекты связаны с недостаточной оснащенностью правоохранительных органов и сложностью цифровых преступлений. Несмотря на внедрение АРМ, многие подразделения используют устаревшее оборудование и программное обеспечение, неспособное обрабатывать большие объемы данных или противостоять современным методам шифрования, применяемым преступниками.

Например, в 2023 году зафиксировано 1729 случаев утечек данных из российских компаний и госорганов, что свидетельствует о высоком уровне защищенности киберпреступников и слабости ИТ-инфраструктуры следственных органов. Отсутствие специализированных лабораторий цифровой криминалистики в регионах вынуждает отправлять материалы на экспертизу в крупные города, что замедляет расследование.

Еще одной проблемой является нехватка квалифицированных специалистов.

Организация взаимодействия между различными подразделениями — еще одно слабое звено. Например, оперативный доступ к базам данных инженеров-электронщиков, необходимый для анализа цифровых следов, часто затруднен из-за бюрократических процедур. Взаимодействие следователей с сотрудниками дежурных частей и оперативниками требует четкой координации, однако на практике это не всегда реализуется эффективно.

Применение ИТ в расследовании поднимает вопросы конфиденциальности и прав граждан. Использование ИИ для анализа данных социальных сетей или систем видеонаблюдения может привести к нарушению права на частную жизнь. В России, где в 2024 году зафиксировано 170 утечек данных за 2,5 месяца, риск компрометации личной информации особенно высок.

Кроме того, существует проблема «цифровой предвзятости». Алгоритмы ИИ, обученные на исторических данных, могут ошибочно указывать на невиновных лиц, что особенно актуально в условиях роста числа киберпреступлений среди подростков.

Для преодоления проблемных аспектов применения ИТ в расследовании преступлений требуется комплексный подход, включающий правовые, технические, организационные и образовательные меры.

Применение информационных технологий в расследовании преступлений в цифровом пространстве — это одновременно вызов и возможность для правоохранительной системы России. Несмотря на значительный прогресс в использовании ИТ, проблемы правового регулирования, технического оснащения, организации работы и этических дилемм остаются острыми. Актуальная статистика подчеркивает рост киберпреступности и необходимость адаптации методов расследования к новым реалиям.

Предложенные меры — от законодательных изменений до повышения квалификации кадров — способны повысить эффективность борьбы с преступлениями в цифровом пространстве. В условиях, когда Россия занимает первое место по уровню киберугроз, эти шаги становятся не просто желательными, а жизненно необходимыми для обеспечения безопасности общества.

Список литературы:

[1] Журков А. А. Этические аспекты использования систем искусственного интеллекта: международно-правовой опыт // Вестник МГЮА.- 2022.- №4.- С.186-194

[2] Карачаев А.Р. Криминологические аспекты противодействия организованной преступности в условиях цифровизации // Пробелы в российском законодательстве. 2022. Т. 15. № 5. С. 185-189.

[3] Кумахов Т.Т., Абазов А.Б., Шафиева Э.Т. Сквозные цифровые технологии как фактор трансформации экономических знаний специалистов // Журнал прикладных исследований. 2023. № 11. С. 110-114.

[4] Овсянников Д.В. Проблемы использования цифровых доказательств в уголовном судопроизводстве // Российский юридический журнал.- 2015.- № 3.- С. 45–52.

[5] Тропина Т.Л. Цифровая криминалистика: современные методы и вызовы. – Владивосток: Издательство ДВФУ.- 2023.

[6] Машекуашева М.Х. Некоторые аспекты использования в преступных целях искусственного интеллекта. Право и управление. 2024. № 8. С. 376-378.

[7] Машекуашева М.Х. О масштабах информационных угроз в современных условиях. Право и управление. 2023. № 11. С. 17-19.

Spisok literatury:

[1] Zhurkov A. A. E`ticheskie aspekty` ispol`zovaniya sistem iskusstvennogo intellekta: mezhdunarodno-pravovoj opy`t // Vestnik MGYuA.- 2022.- №4.- S.186-194

[2] Karachaev A.R. Kriminologicheskie aspekty` protivodejstviya organizovannoj prestupnosti v usloviyax cifrovizacii // Probely` v rossijskom zakonodatel`stve. 2022. T. 15. № 5. S. 185-189.

[3] Kumaxov T.T., Abazov A.B., Shafieva E`.T. Skvozny`e cifrovy`e texnologii kak faktor transformacii e`konomicheskix znanij specialistov // Zhurnal prikladny`x issledovanij. 2023. № 11. S. 110-114.

[4] Ovsyannikov D.V. Problemy` ispol`zovaniya cifrovy`x dokazatel`stv v ugolovnom sudoproizvodstve // Rossijskij yuridicheskij zhurnal.- 2015.- № 3.- S. 45–52.

[5] Tropina T.L. Cifrovaya kriminalistika: sovremenny`e metody` i vy`zovy`. – Vladivostok: Izdatel`stvo DVFU.- 2023.

[6] Mashekuasheva M.X. Nekotory`e aspekty` ispol`zovaniya v prestupny`x celyax iskusstvennogo intellekta. Pravo i upravlenie. 2024. № 8. S. 376-378.

[7] Mashekuasheva M.X. O masshtabax informacionny`x ugroz v sovremenny`x usloviyax. Pravo i upravlenie. 2023. № 11. S. 17-19.

