Дата поступления рукописи в редакцию: 17.04.2026 г. DOI: 10.24412/2782-3830-2026-6-365-367
Дата принятия рукописи в печать: 02.07.2026 г.

МАКАЗИЕВА Зара Даутовна,
старший преподаватель кафедры уголовного права, процесса и национальной безопасности Чеченского государственного университета имени А. А. Кадырова, e-mail: zara6756@mail.ru

ХАДЖИЕВ У.К.,
старший преподаватель кафедры таможенного дела ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова», e-mail: einstein_95@mail.ru

ТЕХНОЛОГИИ МОНИТОРИНГА ЦИФРОВОГО ПРОСТРАНСТВА В ЦЕЛЯХ ПРЕДУПРЕЖДЕНИЯ ПРАВОНАРУШЕНИЙ

Аннотация. *Предупреждение преступлений в цифровой среде базируется на постоянном мониторинге открытых и закрытых сегментов сети. Автоматизированные системы сканирования способны выявлять аномальную активность, характерную для подготовки DDoS-атак или распространения вредоносного ПО. Технологии лингвистического анализа позволяют в реальном времени отслеживать появление экстремистских призывов или предложений о продаже запрещенных веществ, классифицируя их по степени угрозы и передавая информацию оперативным сотрудникам для принятия мер реагирования.*

Ключевые слова: *цифровая сфера, предупреждение, мониторинг, экстремизм, сетевая атака, международное сотрудничество, следователь, угроза.*

MAKAZIEVA Zara Dautovna,
Senior Lecturer at the Department of Criminal Law, Process and National Security Chechen State University named after A. A. Kadyrov

KHADZHIEV U.K.,
Senior Lecturer, Department of Customs Federal State Budgetary Educational Institution of Higher Education "Grozny State Petroleum Technological University named after M.D. Millionshchikov"

DIGITAL SPACE MONITORING TECHNOLOGIES FOR CRIME PREVENTION

Annotation. *Crime prevention in the digital environment is based on constant monitoring of open and closed network segments. Automated scanning systems are capable of detecting abnormal activity typical for preparing DDoS attacks or spreading malware. Linguistic analysis technologies allow real-time monitoring of the appearance of extremist appeals or offers for the sale of prohibited substances, classifying them according to the degree of threat and transmitting information to operational staff to take response measures.*

Key words*: digital sphere, prevention, monitoring, extremism, network attack, international cooperation, investigator, threat.*

Эффективность мониторинга повышается за счет интеграции данных из различных ведомственных систем и открытых источников. Создание «цифровых ловушек» (honeypots) позволяет изучать методы работы хакеров, не подвергая риску реальную инфраструктуру. Таким образом, современные компьютерные технологии позволяют перейти от расследования уже совершенных деяний к стратегии упреждающего воздействия, минимизируя возможный ущерб от киберпреступности и обеспечивая стабильность информационного пространства [15].

Ликвидация технологического дисбаланса между возможностями организованной преступности и техническими ресурсами следственных подразделений требует системного подхода к обновлению материально-технической базы.

В приоритете — создание централизованных аппаратно программных комплексов, обеспечивающих высокоскоростную обработку массивов данных в масштабе всей страны. Наряду с оснащением важно перестроить систему профессиональной подготовки, включив в учебные планы профильных вузов дисциплины, углубляющие знания об архитектуре компьютерных систем и методах криптографического анализа. Формирование корпуса специалистов, совмещающих компетенции в правовой сфере и информационных технологиях, даст возможность эффективно применять современные средства фиксации виртуальных следов. Только комплексное сочетание кадрового потенциала и современного инструментария обеспечит существенный рост результативности борьбы с высокотехнологичной преступностью [9]. Анализ зарубежной практики показывает, что наиболее результативные модели противодействия киберугрозам строятся на плотном взаимодействии государственных структур и частного сектора. Европол и Интерпол показывают нам как эффективно работает создание совместных центров мониторинга. Международные организации, проводя совместный мониторинг в реальном времени, производят обмен информацией о нововведениях вредоносного ПО и сетевых атаках. Такое сотрудничество позволяет быстро реагировать на международные атаки. [15].

Для следователей из разных регионов применение распределённых систем обеспечивает быстрый доступ к результатам экспертиз и оперативным сводкам, что является очень важным при раскрытии сетевых преступлений. Проводя исследование, мы все больше склоняемся к мнению, что современные компьютерные технологии стали неотъемлемой частью системы раскрытия преступлений, коренным образом меняя традиционные криминалистические практики. Цифровая среда порождает специфические виды следов, требующие применения высокотехнологичных методов их фиксации и анализа. Основной вывод - необходимость перехода от разрозненного использования программных средств к созданию единой интеллектуальной инфраструктуры правоохранительных органов, способной в реальном времени противодействовать киберугрозам.

Анализ теоретических и правовых основ выявил, что действующая нормативная база нуждается в оперативной адаптации к вызовам цифровой эпохи. Ключевой проблемой остаётся процессуальное закрепление статуса электронных доказательств, полученных посредством алгоритмов искусственного интеллекта (ИИ) и методов анализа больших данных (Big Data). Для обеспечения допустимости таких доказательств в судебной практике требуется разработка нормативных стандартов технической верификации и экспертной оценки, исключающих возможность манипуляции цифровой информацией на всех стадиях следственного процесса.

Практическая значимость исследования заключается в систематизации методик работы с волатильными данными и восстановлением удалённой информации. Было показано, что автоматизация поиска доказательств в глобальных сетях и применение биометрических систем идентификации позволяют статистически значимо повысить эффективность оперативно-розыскных мероприятий. Вместе с тем, технологическое преимущество правоохранительных органов возможно лишь при условии постоянного обновления программного обеспечения и устранения кадрового дефицита специалистов с глубокими знаниями в области цифровой криминалистики.

В перспективе дальнейшее совершенствование средств раскрытия преступлений будет неразрывно связано с внедрением предиктивной аналитики и специализированных систем противодействия приёмам сокрытия цифровых следов, таким как стеганография и криптографическая анонимизация. Международное сотрудничество и обмен опытом в области интеграции инновационных компьютерных систем рассматриваются в качестве решающих факторов повышения эффективности борьбы с трансграничной преступностью.

Список литературы:

[1] Криминалистика : учебник / под ред. А. Н. Колесниченко. — 3-е изд., перераб. и доп. — М. : Юрайт, 2020. — 541 с.

[2] Цифровая криминалистика : учеб. пособие / В. Ю. Флегонтов. — 3-е изд. — М. : РИТВУС, 2022. — 256 с.

[3] Инновационные подходы в криминалистике: методы цифровой криминалистики в борьбе с запрещенным контентом // Вестник криминалистики. — 2022. — № 4. — С. 5-20. — URL: https://www.kvsz.ru/ru/nauka/article/99319/view (дата обращения: 15.02.2026).

[4] О соотношении традиционной криминалистики и цифровой криминалистики // Бюллетень Белгородского университета кооперации, экономики и права. — 2023. — № 2. — С. 45-52. — URL: https://brj-bguep.ru/reader/article.aspx?id=27156 (дата обращения: 20.01.2026).

[5] Угрюмов А. Ю. Криминалистическая характеристика киберпреступлений в системах

электронных платежей // Вестник экономической безопасности. — 2023. — № 1. — С. 78-89. — URL: http://e-notabene.ru/view_article.php?id_article=78140 (дата обращения: 10.02.2026).

[6] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.03.2026).

[7] Криминалистика: место цифровой криминалистики в науке и перспективы развития // Информационно-правовые проблемы современной виртуальной среды. — 2023. — № 2. — С. 112-120. — URL: https://www.ippsvfu.ru/jour/article/view/223 (дата обращения: 18.02.2026).

[8] Цифровое состояние криминалистической науки: актуальные и перспективные разработки / А. В. Наумов, И. П. Смирнова. — М. : Юристъ, 2024. — 210 с.

[9] Полозов К. А. Цифровая криминалистика: проблемы и перспективы // Юрист. — 2024. — № 3. — С. 34-41. — URL: https://cyberleninka.ru/article/n/tsifrovoe-sostoyanie-kriminalisticheskoy-nauki-aktualnye-i-perspektivnye-razrabotki-i-ih-prakticheskoe-voploschenie (дата обращения: 12.03.2026).

[10] Единая биометрическая система: отчет о внедрении цифровых технологий в правоохрану / Минцифры России. — М. : Изд-во Минцифры, 2024. — 145 с.

[11] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. — 3rd ed. — Waltham : Academic Press, 2011. — 807 p.

[12] Pollitt M. A History of Digital Forensics // Advances in Digital Forensics VI / eds. K. K. R. Choo, S. Shenoi. — Berlin : Springer, 2010. — P. 3-15.

[13] Reedy P. Interpol Review of Digital Forensics // Forensic Science International. — 2015. — Vol. 249. — P. 1-10.

[14] Garfinkel S. L. Digital Forensics Research: The Next 10 Years // Digital Investigation. — 2010. — Vol. 7, suppl. 1. — P. S64-S73.

[15] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021 [Electronic resource]. — URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2021 (accessed: 15.02.2026).

References:

[1] Forensics: textbook/ed. A.N. Kolesnichenko. - 3rd ed., Revised and add. - M.: Yurayt, 2020. - 541 p.

[2] Digital forensics: tutory. manual/V. Yu. Flegontov. - 3rd ed. - M.: RITVUS, 2022. - 256 s.

[3] Innovative Approaches in Forensic Science: Digital Forensic Techniques in Combating Illicit Content//Bulletin of Forensic Science. — 2022. — № 4. - S. 5-20. - URL: https://www.kvsz.ru/ru/nauka/article/99319/view (access date: 15.02.2026).

[4] On the relationship between traditional forensics and digital forensics//Bulletin of the Belgorod University of Cooperation, Economics and Law. — 2023. — № 2. - S. 45-52. - URL: https://brj-bguep.ru/reader/article.aspx?id=27156 (access date: 20.01.2026).

[5] Ugryumov A. Yu. Forensic characteristics of cybercrimes in electronic payment systems//Bulletin of Economic Security. — 2023. — № 1. - S. 78-89. - URL: http://e-notabene.ru/view_article.php?id_article=78140 (access date: 10.02.2026).

[6] Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technology and Information Protection” [Electronic Resource]. - URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (access date: 05.03.2026).

[7] Forensics: the place of digital forensics in science and development prospects//Information and legal problems of the modern virtual environment. — 2023. — № 2. - S. 112-120. - URL: https://www.ippsvfu.ru/jour/article/view/223 (access date: 18.02.2026).

[8] Digital state of forensic science: current and promising developments/A.V. Naumov, I.P. Smirnova. - M.: Lawyer, 2024. - 210 s.

[9] Polozov K. A. Digital forensics: problems and prospects//Lawyer. — 2024. — № 3. - S. 34-41. — URL: https://cyberleninka.ru/article/n/tsifrovoe-sostoyanie-kriminalisticheskoy-nauki-aktualnye-i-perspektivnye-razrabotki-i-ih-praktich-eskoe-voploschenie (дата обращения: 12.03.2026).

[10] Unified biometric system: report on the introduction of digital technologies in law enforcement/Ministry of Digital Industry of Russia. - M.: Publishing House of the Ministry of Digital Industry, 2024. - 145 s.

[11] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. — 3rd ed. — Waltham : Academic Press, 2011. — 807 p.

[12] Pollitt M. A History of Digital Forensics // Advances in Digital Forensics VI / eds. K. K. R. Choo, S. Shenoi. — Berlin : Springer, 2010. — P. 3-15.

[13] Reedy P. Interpol Review of Digital Forensics // Forensic Science International. — 2015. — Vol. 249. — P. 1-10.

[14] Garfinkel S. L. Digital Forensics Research: The Next 10 Years // Digital Investigation. — 2010. — Vol. 7, suppl. 1. — P. S64-S73.

[15] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021 [Electronic resource]. — URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2021 (accessed: 15.02.2026).