

**ЦИФРОВИЗАЦИЯ В КРИМИНАЛИСТИКЕ:
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ**
Digitalization in forensics: problems and prospects

А. А. Лемтюгина, студент
Уральский юридический институт МВД России
(Екатеринбург, ул. Корепина, 66)

Аннотация

Данная статья рассматривает криминалистику в эпоху цифровых технологий и цифровизации в целом. Отдельно рассматриваются такие аспекты, как влияние цифровизации на методы, технологические вызовы и проблемы, а также перспективы развития подобных технологий в ДАННОЙ сфере.

Ключевые слова: цифровизация, криминалистика, методы, борьба с преступностью, цифровые доказательства, цифровая форензика.

Summary

This article examines criminology in the era of digital technologies and digitalization in general. Aspects such as the impact of digitalization on methods, technological challenges and problems, as well as the prospects for the development of such technologies in the field are considered separately.

Keywords: digitalization, criminalistics, methods, crime control, digital evidence, digital forensics.

В современном мире цифровизация охватывает всё больше сфер нашей жизни, включая и криминалистику. Применение новейших технологий значительно ускоряет и упрощает процесс расследования преступлений, однако вместе с перспективами приходят и новые вызовы. Использование искусственного интеллекта, больших данных и автоматизации предоставляют правоохранительным органам беспрецедентные возможности для анализа и предсказания преступной активности.

Однако внедрение этих технологий сопряжено с рядом проблем, среди которых вопросы конфиденциальности, этики и точности данных [1]. Необходимо тщательно взвешивать потенциальные риски и выгоды, а также разрабатывать стратегии для борьбы с возможными негативными последствиями цифровизации в криминалистике. Эти и другие аспекты требуют глубокого анализа и обсуждения в рамках криминалистической науки и практики.

Влияние цифровизации на методы криминалистики

Цифровизация оказывает глубокое влияние на современную криминалистику, революционизируя методы сбора, анализа и хранения доказательств. Это влияние проявляется в нескольких ключевых аспектах.

Первое и наиболее значимое воздействие цифровизации – улучшение точности и оперативности анализа доказательств. С помощью передовых технологий, таких как 3D-моделирование и компьютерное зрение, криминалисты могут создавать более точные реконструкции преступлений и анализировать мелкие детали на месте происшествия с невиданным ранее уровнем детализации. Кроме того, алгоритмы машинного обучения позволяют обрабатывать большие объемы данных значительно быстрее, чем это было возможно ранее, что является неоценимым при расследованиях, где каждая минута на счету [2].

Другое важное направление – это цифровая форензика, которая стала неотъемлемой частью современных расследований [3, 4]. Рассмотрение цифровых устройств, таких как смартфоны, компьютеры и другие устройства связи, требует от криминалистов новых знаний и навыков. Программное обеспечение для восстановления данных может извлечь информацию, которая была удалена или зашифрована. Это расширяет возможности следствия, позволяя добраться до корней преступных сетей и операций через анализ сообщений, вызовов и других форм общения.

Технологические вызовы и проблемы в криминалистике

Цифровизация в криминалистике несомненно открывает новые возможности для раскрытия преступлений и сбора доказательств. Однако это также влечёт за собой ряд серьёзных технологических вызовов и проблем, которые требуют внимания и решения для дальнейшего развития данной области.

Прежде всего, одной из основных проблем является безопасность данных. В условиях всеобщей цифровизации, информация, используемая в криминалистике, подвергается риску несанкционированного доступа, что может привести к утечке чувствительных данных, компрометации доказательной базы или даже к подмене информации. Решением этой проблемы могут стать усилена кибербезопасность и использование шифрования для защиты хранилищ данных и передачи информации.

Следующий значительный вызов — это обработка больших объемов данных. Криминалистика сталкивается с необходимостью анализировать большие массивы данных, что требует значительных вычислительных мощностей и специализированного программного обеспечения. В связи с этим возникают вопросы касательно выбора методов и инструментов для анализа, которые будут эффективными и одновременно с этим не потребуют чрезмерных временных затрат.

Ещё одной сложной задачей в условиях цифровизации является гарантирование правомерности использования технологий. Необходимо разработать юридические рамки, которые будут регулировать применение цифровых инструментов и методов в криминалистике, чтобы избежать нарушения прав человека и гражданина, обеспечивая при этом эффективное и законное проведение расследований.

Резюмируя, можно сказать, что хотя цифровизация в криминалистике открывает перед правоохранительными органами новые возможности, она также ставит перед ними ряд серьёзных технологических и этических задач. Решение этих проблем требует комплексного подхода, включая усовершенствование технологий, создание нормативной базы, обучение персонала и строгий контроль за соблюдением этических принципов.

Цифровая преступность. Роль цифровых технологий в борьбе с преступностью

Использование компьютерной техники и программного обеспечения в криминалистике сопряжено с определенными трудностями. Одна из основных проблем — это необходимость постоянного обновления технологических навыков у правоохранителей, так как преступники используют всё более сложные технологии. Сейчас много стран сталкиваются с дефицитом квалифицированных специалистов в этой области.

Также проблемой является защита данных. С каждым годом увеличивается количество кибератак на информационные ресурсы, что требует от правоохранительных органов повышенного внимания к вопросам информационной безопасности. Злоумышленники не просто получают доступ к чувствительной информации, но и используют её в криминальных целях, что утяжеляет последствия преступлений.

С другой стороны, развитие технологий открывает перед правоохранительными органами новые перспективы. Так, возможности искусственного интеллекта позволяют не только отслеживать киберпреступления в реальном времени, но и прогнозировать вероятные направления их развития. Алгоритмы машинного обучения могут анализировать огромные массивы данных, выявляя закономерности, которые могли бы остаться незамеченными для человеческого глаза.

Интеграция цифровых технологий в правоохранительные практики способна значительно сократить время, необходимое для разгадывания преступлений, а также повысить точность улик, предъявляемых в суд [5, 6]. В то же время, развитие цифровых технологий требует тщательной балансировки между инновациями и защитой прав человека, что ставит перед правоохранительными органами серьезные этические задачи.

Перспективы развития цифровизации в криминалистике

Одним из значительных направлений в цифровизации криминалистики является разработка и внедрение интегрированных баз данных, которые позволяют объединять информацию из различных источников: полицейских докладов, видеонаблюдения, форензических исследований и т.д. Это обеспечивает более быстрый и точный доступ к необходимым данным, улучшает координацию между различными отделениями и способствует более эффективному расследованию.

Применение искусственного интеллекта (ИИ) и машинного обучения открывает перспективные возможности для анализа больших объемов данных [8]. Эти технологии могут автоматически анализировать видеоматериалы с мест преступления, распознавать лица, номерные знаки автомобилей и другие важные детали. Более того, ИИ способен выявлять сложные закономерности и связи между различными случаями, что ранее было невозможно из-за ограничений человеческого анализа.

Другое направление, которое обещает значительные изменения в будущем, – это сфера кибербезопасности. С увеличением количества преступлений, совершаемых в цифровом пространстве, возрастает и необходимость их эффективного противодействия. Расширение компетенций криминалистов в области кибербезопасности и использование специализированных инструментов для отслеживания и анализа кибератак становится приоритетным направлением развития.

Внедрение цифровых технологий также включает разработку портативных технологических устройств, таких как дроны для съемки мест преступления, портативные сканеры для быстрого сбора доказательств и мобильные лаборатории для проведения форензических анализов на месте. Это позволяет значительно ускорить процесс сбора и анализа данных, что является критически важным в условиях, когда каждая минута может быть решающей [7, 8].

Завершая, можно сказать, что перспективы развития цифровизации в криминалистике кажутся не только обширными, но и необходимыми. Внедрение новых технологий будет способствовать повышению эффективности правоохранительных процедур, скорости расследований и, в конечном счете, укреплению законности и порядка. Однако успех этих усилий будет зависеть от активной поддержки на уровне законодательства, обеспечения адекватного финансирования и обучения кадров, способных работать с новыми цифровыми инструментами.

Библиографический список

1. *Крайнова Н. А.* Международная цифровая безопасность: миф или реальность? // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 42-46.

2. *Никуленко А. В.* О некоторых вопросах кибербезопасности в современном мире: взгляд дилетанта // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 37-41.
3. *Бегишев И. Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27-32
4. *Шуваева М. С., Николаева А. В.* Роль форензики в расследовании киберпреступности. Криминалистический аспект // Международный журнал гуманитарных и естественных наук. 2021. № 6-2. URL: <https://cyberleninka.ru/article/n/rol-forenziki-v-rassledovanii>.
5. *Сахабутдинова А. С., Корчагин А. Г.* Цифровая преступность: причины, виды, тенденции преступности, личность преступника, меры противодействия // Аграрное и земельное право. 2023. №8 (224). URL: <https://cyberleninka.ru/article/n/tsifrovaya-prestupnost-prichiny-vidy-tendentsii-prestupnosti-lichnost-prestupnika-mery-protivodeystviya> (дата обращения: 18.05.2025).
6. *Евдокимов К. Н.* Самодетерминация технотронной преступности в Российской Федерации // Российский судья. 2020. № 7. С. 48- 53. DOI 10.18572/1812-3791-2020-7-48-53. EDN VLDNTX.
7. *Воронин Ю. А.* Преступления в сфере обращения цифровой информации и их детерминанты // ВИКТИМОЛОГИЯ. 2020. № 1 (23). С. 74-83.
8. *Право и этика искусственного интеллекта: учебное пособие / Р. И. Дремлюга.* Владивосток: Издательство Дальневосточного федерального университета, 2021. 94 с.