

УДК 340

## Цифровая криминалистика: сущность и значение<sup>1</sup>

Панкова Диана Александровна, магистрант, Владимирский государственный университет, pani@0400mail.ru

Статья посвящена анализу научно-технических предпосылок цифровизации отечественной криминалистики и определению роли цифровых технологий в развитии криминалистической деятельности. Рассматривается использование искусственного интеллекта в процессе расследования преступлений, совершаемых в цифровой среде, а также обсуждаются ограничения уголовно-процессуального подхода при расследовании киберпреступлений.

Ключевые слова: цифровая криминалистика, цифровая экономика, Интернет, преступление, цифровые технологии, криминалистика.

«Цифровая криминалистика» — новый и еще не устоявшийся термин в науке, причем на сегодняшний день он остается спорным. Целями цифровой криминалистики являются обнаружение, извлечение и анализ данных, а также использование цифровых технологий для сбора доказательств. В более широком аспекте рассматривает цифровую криминалистику Е. П. Ищенко, отмечая, что она знаменует «переход от аналогового представления информации к дискретному — цифровому, позволяющему математизировать все процессы, происходящие в реальной действительности, а также отразить специфику традиционных преступлений, когда они совершаются с помощью новейших информационно-телекоммуникационных технологий».

Ключевые области, в которых цифровые технологии нашли применение в криминалистике, включают:

- киберпреступления и цифровую следственную экспертизу;
- использование больших данных;
- компьютерное моделирование преступлений;
- применение искусственного интеллекта в криминалистике;
- расширенную реальность и виртуальную реальность;
- биометрические технологии и идентификацию преступников;
- кибербезопасность и защиту данных в криминалистике.

На сегодняшний день цифровые технологии пронизывают все значимые сферы деятельности общества и государства; они стали неотъемлемой частью жизнедеятельности каждого человека. Социальные сети играют важную роль в современном обществе, предоставляя платформы для общения, обмена информацией и ведения бизнеса. Однако их популярность привлекает и злоумышленников, использующих данные ресурсы для мошенничества, распространения дезинформации, кибербуллинга и иных противоправных действий.

Ежегодно связь всех аспектов общества с IT-сферой усиливается, а объемы утечек данных увеличиваются. Уже знакомые многим кражи личных данных клиентов приводят к значительным финансовым потерям компаний, а в отдельных случаях — к их банкротству. Помимо персональных данных, существенную часть утечек составляет коммерческая тайна. Во втором полугодии 2024 г. наиболее привлекательными целями для атак на данные являлись госучреждения (13 %), промышленность (10 %), IT-компании (10 %), финансовые организации (8 %) и медицинские учреждения (7 %). При этом 71 % успешных атак был реализован с использованием вредоносного программного обеспечения: 38 % — шифровальщики, 28 % — шпионское ПО или инфостилеры (по отчету Positive

Technologies).

Сотрудники оперативных подразделений сталкиваются с исследованием цифровых следов уже на этапе доследственной проверки материалов. Наибольшее распространение имеет форензика мобильных устройств, где применяются специализированные инструменты и программное обеспечение для извлечения и анализа данных из телефонов правонарушителей, включая восстановление удаленной информации и контактов. С помощью искусственного интеллекта и использования ботов оперативные сотрудники подсистем МВД России выявляют сведения, способствующие установлению личности преступников и их изобличению при минимуме исходных данных. Применение современных криминалистических программных комплексов, таких как «Мобильный криминалист», UFED, Belkasoft Evidence Center, позволяет получать данные из установленных приложений, программ обмена сообщениями, электронной почты, а также извлекать информацию о геолокации, временных маркерах и восстанавливать удаленные файлы.

Использование информационных технологий и компьютерных средств должно быть направлено на сбор, накопление и обработку криминалистически значимой информации. В этой связи особое внимание следует уделять криминалистическим учетам, которые в интегрированном виде отражают достижения технологий обработки данных в сфере раскрытия и расследования преступлений и открывают перспективы автоматизации учета [2, с. 55]. Имеется потребность в модернизации аппаратно-программных комплексов дежурных частей органов внутренних дел. Реализация этой задачи возможна путем внедрения системы, соединяющей автоматический определитель номера с электронной картой местности, откуда поступает сообщение.

Цифровая криминалистика играет важную роль в различных областях деятельности, поскольку фокусируется на исследовании цифровых доказательств и методах их поиска, получения и обеспечения. Нельзя считать Интернет или любое иное техническое устройство полностью безопасной средой. Для повышения эффективности раскрытия преступлений в сфере компьютерной информации необходимы постоянное совершенствование знаний и навыков сотрудников в области цифровизации. В этой связи представляется целесообразным включить цифровую криминалистику в качестве обязательной составной части дисциплины «Криминалистика» при подготовке специалистов юридического профиля, а также обеспечить стандартизацию и сертификацию процедур обработки цифровой информации.

<sup>1</sup> Научный руководитель: Удалов Максим Игоревич — старший преподаватель кафедры уголовно-правовых дисциплин, заведующий кабинетом криминалистики экспертно-лабораторного комплекса, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых.

#### **Примечания**

1. Варыгина А. О., Ломова А. Д. Цифровая криминалистика в условиях современных киберугроз // Наука сегодня: актуальные вопросы теории и практики: сборник статей конференции: в 2 ч. Пенза, 2025. Ч. 1.
2. Дмитриева А. Д., Фединцева А. А., Селезнев А. В. Возможности цифровой криминалистики в современном обществе // Тенденции развития науки и образования. 2023. N 95-3.
3. Дяблова Ю. Л. Криминалистика будущего — цифровая криминалистика? // Актуальные проблемы криминалистики и судебной экспертизы: материалы конференции. Иркутск, 2021.

#### **English version**

Digital forensics: essence and significance

Pankova Diana Aleksandrovna, master's student, Vladimir State University

This article analyzes the scientific and technological prerequisites for the digitalization of Russian forensic science and identifies the role of digital technologies in the development of forensic activities. It examines the use of artificial intelligence in the investigation of crimes committed in the digital environment and discusses the limitations of the criminal procedure framework when addressing cybercrime investigations.

Keywords: digital forensics, digital economy, internet, crime, digital technologies, forensic science.