ТРИБУНА МОЛОДОГО УЧЕНОГО

по результатам проведенных международных научно-практических семинаров:
28 ноября 2024 года — «Актуальные проблемы теории и практики уголовного права на современном этапе»;
28 марта 2025 года — «Уголовно-процессуальные и криминалистические аспекты расследования киберпреступлений»

УДК 343.98

Д. С. Кириков
курсант 1 курса факультета милиции
Могилевского института МВД Республики Беларусь

*Научный руководитель: **Д. А. Свиридов**,*
начальник кафедры уголовного права,
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

ЦИФРОВЫЕ СЛЕДЫ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Современные технологии стали неотъемлемой частью жизни, а цифровая среда — важным источником информации, включая данные, которые могут иметь доказательственное значение в расследованиях преступлений. Цифровые следы, оставляемые пользователями в Сети, на устройствах и в облачных сервисах, представляют собой ключевой объект криминалистического анализа.

Актуальность темы обусловлена ростом киберпреступности, мошенничества, кибератак и незаконного использования цифровых технологий. Сегодня преступления могут совершаться как в виртуальном пространстве, так и с применением цифровых инструментов в реальном мире, что делает цифровые следы ценным источником информации для правоохранительных органов.

Цель данной работы — рассмотреть основные криминалистические методы работы с цифровыми следами, включая их обнаружение, анализ и использование в расследованиях. Для этого необходимо изучить классификацию цифровых следов, основные методы их выявления, современные инструменты криминалистики, а также проблемы, возникающие в процессе анализа.

Понимание и развитие криминалистических методов работы с цифровыми следами играют важную роль в обеспечении правопорядка, защите прав граждан и эффективном противодействии преступлениям в цифровой среде.

Цифровые следы представляют собой данные, которые остаются в результате применения электронных устройств и сетевых технологий. Они могут использоваться в криминалистических исследованиях для установления фактов,

обстоятельств преступлений и выявления причастных лиц. Для эффективного анализа цифровых следов важно понимать их классификацию и особенности [1].

Цифровые следы можно разделить на физические и логические. Физические следы — это данные, хранящиеся на материальных носителях информации (жестких дисках, флеш-накопителях, серверах и т. д.), включая файлы, системные журналы и кешированные данные. Логические следы связаны с процессами работы систем и программ (например, временные файлы, следы интернет-активности, логи операционной системы, а также зашифрованные или сжатые данные). Физические следы, как правило, поддаются восстановлению даже после удаления файлов, тогда как логические следы могут быть сложнее для анализа, особенно если они зашифрованы или модифицированы злоумышленником.

Еще одна важная классификация цифровых следов связана с их устойчивостью к изменению или исчезновению. Нестабильные следы — это данные, хранящиеся в оперативной памяти, кеше процессора или других временных хранилищах. Эти следы исчезают при выключении устройства, поэтому их сбор требует быстрого реагирования и специальных инструментов для снятия дампа памяти. Постоянные следы, в отличие от нестабильных, сохраняются на устройствах после их выключения, например, файлы на жестком диске, базы данных, сохраненные логи и резервные копии. Нестабильные следы особенно важны при расследовании атак на серверы и анализе вредоносных программ, так как они могут содержать информацию о запущенных процессах, сетевых соединениях и временных файлах.

По степени доступности цифровые следы делятся на открытые и скрытые. Открытые следы — это данные, доступные для анализа без сложных методов восстановления, например, файлы, журналы событий, история посещений сайтов. Скрытые следы — это информация, которую злоумышленник пытается скрыть или удалить. Это могут быть зашифрованные файлы, стеганографические объекты, замаскированные процессы в системе, а также остаточные следы на дисках после удаления файлов [2]. Обнаружение скрытых цифровых следов требует использования специализированных криминалистических инструментов, таких как программное восстановление данных, анализ файловых систем и методов цифровой стеганографии.

Обнаружение и сбор цифровых следов являются одними из ключевых этапов криминалистического анализа, поскольку от качества их фиксации и сохранности зависит достоверность и пригодность информации в ходе расследования. Современные технологии позволяют злоумышленникам тщательно скрывать следы своей деятельности, поэтому криминалистам приходится применять разнообразные методы для их выявления.

Одним из важнейших способов сбора цифровых следов является анализ данных оперативной памяти. Поскольку нестабильные следы исчезают

при выключении устройства, их фиксация должна проводиться немедленно после обнаружения потенциально важного объекта. В оперативной памяти могут храниться следы работы вредоносного программного обеспечения, данные о запущенных процессах, пароли, ключи шифрования и временные файлы. Для снятия дампа памяти применяются специализированные инструменты.

Другим распространенным методом является изъятие и клонирование носителей информации. Это позволяет сохранить исходную структуру файлов и каталогов для дальнейшего анализа без риска повредить оригинальные данные. Процесс клонирования выполняется с помощью аппаратных и программных средств. Важно учитывать, что любые изменения в изъятых данных могут сделать их недействительными в качестве доказательств, поэтому криминалисты строго следуют процедурам, обеспечивающим неизменность информации.

Логический и физический анализы файловых систем позволяют исследовать структуру жестких дисков, флеш-накопителей и других цифровых носителей. Логический анализ включает изучение видимых файлов и директорий, их метаданных, а также проверку целостности файловой системы. Физический анализ позволяет работать с низкоуровневыми данными, восстанавливать удаленные файлы и исследовать неразмеченные участки диска.

Еще одним важным направлением является изучение сетевых логов и интернет-активности. В процессе расследования анализируются журналы посещений веб-сайтов, история переписки в мессенджерах, данные о соединениях с удаленными серверами и активность в социальных сетях. Специалисты по цифровой криминалистике изучают данные маршрутизаторов, файрволов и серверных логов, чтобы отследить передвижение информации в Сети и установить источник подозрительной активности.

Анализ цифровых следов играет важную роль в криминалистике, помогая выявлять преступников, восстанавливать события и собирать доказательства. В работе рассмотрены виды цифровых следов, методы их обнаружения, сбора и анализа. Современные инструменты позволяют эффективно работать с цифровыми доказательствами, однако новые технологии создают вызовы, связанные с шифрованием и сокрытием данных.

Основные проблемы связаны с правовыми аспектами и защитой персональной информации, но развитие искусственного интеллекта и автоматизированных методов анализа способствует совершенствованию криминалистики. В будущем цифровая криминалистика станет еще более важной для обеспечения безопасности и борьбы с преступностью в цифровой среде.

---

1. Худяков В. В., Ананьев А. А. Цифровые следы // Криминол. журн. 2023. № 4. С. 243–246. URL: https://cyberleninka.ru/article/n/tsifrovye-sledy (дата обращения: 16.04.2025). Перейти к источнику Вернуться к статье

2. Нестеров С. А., Смолина Е. М. Понятие цифрового следа и анализ цифрового следа в образовании // Системный анализ в проектировании и управлении. 2023. № 3. С. 309–314. URL: https://cyberleninka.ru/article/n/ponyatie-tsifrovogo-sleda-i-analiz-tsifrovogo-sleda-v-obrazovanii (дата обращения: 16.04.2025). Перейти к источнику Вернуться к статье